

TP-LINK®

双核全千兆企业VPN路由器

TL-ER6520G

用户手册

REV1.3.0

1910040665

声明

Copyright © 2016 普联技术有限公司

版权所有，保留所有权利

未经普联技术有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本手册部分或全部内容，且不得以营利为目的进行任何方式（电子、影印、录制等）的传播。

TP-LINK® 为普联技术有限公司注册商标。本手册提及的所有商标，由各自所有人拥有。本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，所作陈述均不构成任何形式的担保。

目录

第 1 章	前言	1
1.1	目标读者	1
1.2	本书约定	1
第 2 章	产品介绍	2
2.1	产品描述	2
2.2	产品特性	2
2.3	产品外观	4
2.3.1	前面板	4
2.3.2	后面板	5
第 3 章	配置指南	6
3.1	登录 Web 界面	6
3.2	Web 界面简介	8
3.2.1	界面总览	8
3.2.2	页面常见按键及操作	9
第 4 章	基本设置	11
4.1	基本概念	11
4.1.1	区段	11
4.1.2	接口	12
4.2	区段设置	13
4.2.1	default 区段	14
4.2.2	接口设置	16
4.3	VLAN 设置	25
4.3.1	VLAN 简介	25
4.3.2	VLAN 设置	30
4.4	交换机设置	33
4.4.1	端口统计	33

4.4.2	端口监控	34
4.4.3	端口流量限制	35
4.4.4	端口参数	36
4.4.5	端口状态	36
第 5 章	DHCP	37
5.1	DHCP 服务器	37
5.1.1	DHCP 协议介绍	37
5.1.2	DHCP 功能介绍	39
5.1.3	DHCP 功能配置	41
5.1.4	DHCP 功能组网应用	45
第 6 章	快速配置	48
6.1	NAT 网关模式	49
6.1.1	WAN 设置	50
6.1.2	LAN 设置	54
6.1.3	DMZ 设置	55
6.2	路由模式	58
第 7 章	对象管理	62
7.1	地址管理	62
7.1.1	地址组	62
7.1.2	地址	63
7.1.3	视图	64
7.2	时间管理	65
7.2.1	时间管理	65
7.2.2	工作日历	66
7.2.3	工作时间	68
7.3	IP 地址池	69
7.4	服务类型	70
第 8 章	传输控制	71

8.1	NAT 设置	71
8.1.1	NAPT	73
8.1.2	一对一 NAT	77
8.1.3	虚拟服务器	80
8.1.4	端口触发	83
8.1.5	ALG 服务	85
8.1.6	NAT DMZ	86
8.2	带宽控制	88
8.3	连接数限制	90
8.4	流量均衡	94
8.4.1	基本设置	94
8.4.2	策略选路	96
8.4.3	ISP 选路	98
8.4.4	线路备份	100
8.5	路由设置	102
8.5.1	静态路由	103
8.5.2	RIP 服务	107
第 9 章	安全管理	111
9.1	ARP 防护	111
9.1.1	ARP 简介	111
9.1.2	ARP 攻击简介	112
9.1.3	ARP 攻击防护	114
9.2	攻击防护	119
9.3	MAC 过滤	120
9.4	访问策略	121
9.4.1	基本概念	121
9.4.2	区段内策略	123
9.4.3	区段内策略应用	126

9.4.4	区段间策略	130
9.4.5	区段间策略应用	133
9.4.6	URL 过滤	140
9.5	应用控制	142
9.5.1	应用限制	142
9.5.2	例外管理	143
9.5.3	数据库	144
第 10 章	VPN	145
10.1	IKE	145
10.1.1	IKE 安全策略	146
10.1.2	IKE 安全提议	148
10.2	IPsec	149
10.2.1	IPsec 安全策略	150
10.2.2	IPsec 安全提议	152
10.2.3	IPsec 安全联盟	153
10.2.4	NAT 穿透	153
10.3	PPTP	154
10.3.1	PPTP 服务器设置	154
10.3.2	PPTP 服务器隧道信息	155
10.4	L2TP	156
10.4.1	L2TP 服务器设置	156
10.4.2	L2TP 服务器隧道信息	157
第 11 章	认证管理	158
11.1	Web 认证介绍	158
11.1.1	简介	158
11.1.2	Web 认证系统	158
11.1.3	Web 认证过程	159
11.2	Web 认证配置	160

11.2.1	一键上网	162
11.2.2	使用内置的 Web 服务器和认证服务器	166
11.2.3	使用外部链接的 Web 服务器和认证服务器	175
11.3	微信连 Wi-Fi	179
11.4	免认证策略	185
11.5	认证状态	187
第 12 章	系统服务	189
12.1	电子公告	189
12.2	动态 DNS	190
12.3	UPnP 服务	191
12.4	DNS 代理	192
第 13 章	系统工具	194
13.1	管理账号	194
13.1.1	修改管理帐号	194
13.1.2	远程管理	195
13.1.3	系统管理设置	196
13.2	设备管理	197
13.2.1	恢复出厂配置	197
13.2.2	备份与导入配置	197
13.2.3	重启路由器	198
13.2.4	软件升级	198
13.3	流量统计	199
13.3.1	接口流量统计	199
13.3.2	IP 流量统计	199
13.4	诊断工具	200
13.4.1	诊断工具	200
13.4.2	在线检测	201
13.5	时间设置	202

13.5.1	时间设置	202
13.5.2	夏令时设置	203
13.6	系统日志	204
13.7	系统参数	205
第 14 章	典型配置举例	206
14.1	组网需求	206
14.2	组网方案及特点	207
14.3	配置步骤	208
14.3.1	配置 VLAN	209
14.3.2	配置区段和接口	210
14.3.3	配置流量均衡	213
14.3.4	配置对象	215
14.3.5	配置访问策略	218
14.3.6	配置 NAT	220
14.3.7	配置 VPN	222
14.3.8	配置应用限制	225
14.3.9	配置局域网 ARP 攻击防护	227
14.3.10	配置攻击防护	229
14.3.11	配置内网流量监控	230
第 15 章	命令行简介	232
15.1	搭建平台	232
15.2	界面模式	232
15.3	在线帮助	233
15.4	命令介绍	234
15.4.1	VLAN 配置命令	234
15.4.2	区段和接口命令	234
15.4.3	系统管理	235
15.4.4	用户信息管理	236

15.4.5	历史命令管理.....	236
15.4.6	退出 CLI.....	237
附录 A	常见问题.....	238
附录 B	规格参数.....	239

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-ER6520G双核全千兆企业VPN路由器，下面简称为TL-ER6520G。
- 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-ER6520G双核全千兆企业VPN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VPN路由器产品，采用基于双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、Web认证、微信连Wi-Fi、防火墙、上网行为管理、流量控制、电子公告等丰富的功能特性，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位双核网络专用处理器，单核主频500MHz；
- 配备容量为256MB的DDRII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

区段与接口

- 支持自定义区段，灵活划分网络区域，便于根据不同区域的安全需要制定相应的防火墙策略。
- 支持区段内绑定多个逻辑接口，并提供多种逻辑接口类型，适应复杂的网络需求，同时充分利用物理端口资源。

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服务器模式，允许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

- 可推广商家微信公众号。
- 支持认证跳转，可向用户推送自定义的图片广告。
- 支持上网时长设置，灵活控制用户认证周期。

上网行为管理

- 提供了针对各种常见应用的一键封杀功能，只需在配置页面中勾选相应选项，即可禁止员工使用常见的IM软件（QQ/Web QQ/阿里旺旺等）、P2P软件（迅雷/迅雷看看/电驴等）、金融软件（大智慧、分析家、同花顺等）、游戏（QQ游戏、迅雷游戏、开心农场、QQ农场等）、代理（http代理、socks4代理、socks5代理）。该系列路由器支持基于用户组配置封杀策略，可针对不同用户分配不同权限，保证关键用户的正常使用。
- 支持基于网站黑白名单及用户组的过滤策略，可限制员工对各类网站的访问权限，避免访问恶意网站带来的潜在危害。

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

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

2.3 产品外观

2.3.1 前面板

TL-ER6520G 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。

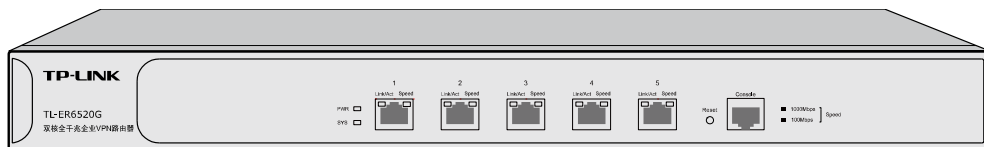


图 2.1 TL-ER6520G 前面板示意图

- 5 个 10/100/1000Mbps 自适应 RJ45 接口

TL-ER6520G 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，详见第 15 章命令行简介。

- Reset 键

复位键。在路由器通电的情况下，使用尖状物按住路由器的 Reset 键，等待 2-5 秒后，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。

■ 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：

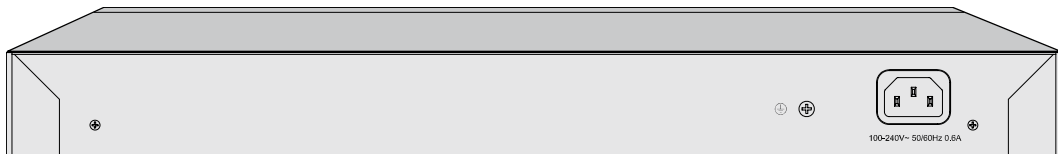


图 2.2 后面板示意图

■ 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0.6A，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。

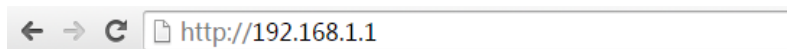
第3章 配置指南

3.1 登录Web界面

第一次登录时，需要确认以下几点：

- 1) 路由器已正常加电启动。
- 2) 管理主机已正确安装有线网卡及该网卡的驱动程序，且已至少安装一种以下浏览器：IE 8.0或以上版本、FireFox最新版本、Chrome最新版本和Safari最新版本。
- 3) 管理主机连接至路由器任一物理端口，且IP地址已设为与路由器default区段同一网段，即192.168.1.X (X为2至254之间的任意整数)，子网掩码为255.255.255.0，默认网关为路由器管理地址192.168.1.1。
- 4) 为保证能更好地体验Web界面显示效果，建议将显示器的分辨率调整到1024×768或以上像素。

打开浏览器（以Chrome浏览器为例），在地址栏输入<http://192.168.1.1>登录路由器的Web管理界面。



路由器登录界面如下图所示。



图 3.1 路由器登录界面

在此界面输入路由器管理账号的用户名和密码（出厂默认值均为admin），以及验证码。路由器成功登录后将看到路由器的系统状态信息，如图 3.2所示。

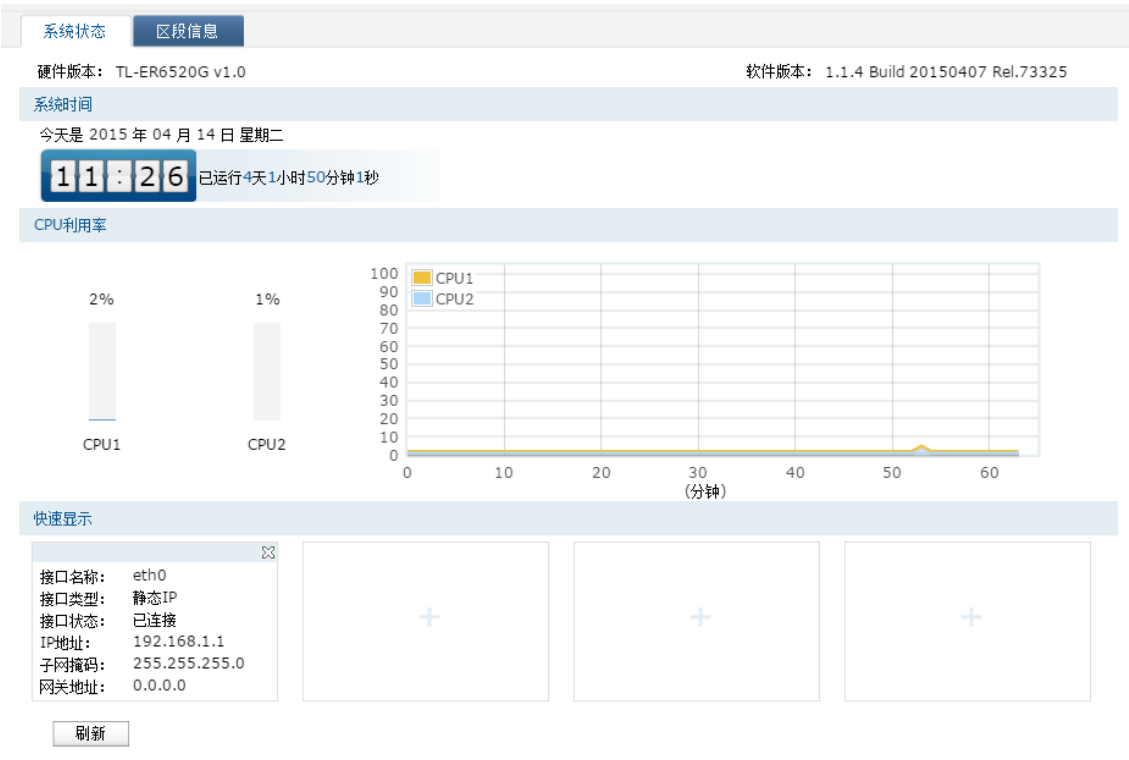


图 3.2 路由器界面首页

在初始界面中，可以在**CPU利用率**区域监测两个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。在**快速显示**区域，点击各区域的< + >按钮选择接口查看接口信息。

浏览到**区段信息**标签页，可以查看路由器上设置的区段和接口信息。在出厂默认情况下，路由器上配置了默认区段default和接口eth0，此时所有物理端口均属于接口eth0。



图 3.3 路由器初始区段

3.2 Web界面简介

3.2.1 界面总览

本路由器典型的Web界面如下图所示。





图 3.4 典型Web界面

在图 3.4典型Web界面区域划分中可以看到，左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，可以通过点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域可分为两部分，条目配置区以及列表管理区。



图 3.5 Web界面区域划分

3.2.2 页面常见按键及操作

按键	含义
	保存最终的配置。
	退出Web页面。



说明：

更改每一个配置后，<新增>和<设置>按键只能使当前配置在设备未重启前生效；若需要在重启设备后配置依旧生效，则需要点击<保存配置>按键。建议在断电重启前<保存配置>，以免丢失配置信息。

条目配置区常见按键：



按键	含义
	添加当前配置条目。
	提交当前的配置。
	修改并保存编辑后的配置信息。
	快速清空当前配置项中已输入的所有信息。
	打开当前功能的帮助页面。

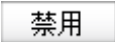

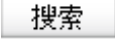


说明：

<修改>按键只有在编辑列表中的条目时才会出现，取代原本的<新增>按键。

列表管理区常见按键：

按键	含义
	选中当前列表中所有条目。
	启用选中的列表条目。

按键	含义
	禁用选中的列表条目。
	删除选中的条目，可批量操作。
	点击后弹出搜索对话框，可以根据输入条件快速搜索条目。

第4章 基本设置

4.1 基本概念

TL-ER6520G提供了灵活的网络安全布局设计，可以创建多个区段并配置策略以调节区段内部及区段之间的信息流。本路由器可为每个区段绑定一个或多个接口，并在每个区段上启用不同的管理和防火墙选项。利用本路由器可以创建网络环境所需的区段，分配每个区段所需的接口数，并且可以根据自己的需要来设计每个接口。

4.1.1 区段

区段是由一个或多个网段组成的集合，需要通过策略对入站和出站信息流进行调整。区段是绑定了一个或多个接口的逻辑实体，是一系列相同或类似功能的接口集合。通过本路由器可以定义多个区段，确切数目可根据网络需要来确定。

在实际网络环境中，通常可以将网络划分为广域网区域、局域网区域和DMZ区域(Demilitarized Zone, 非军事区域)。相对应的，可以在路由器上面定义广域网区段、局域网区段和DMZ区段，如图 4.1所示。

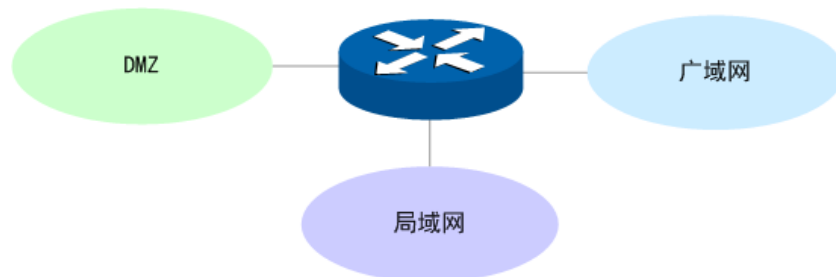


图 4.1 区段概念示意图一

还可以根据实际情况，对区段进行更加细致的定义，如图 4.2所示，在路由器上定义电信区段、联通区段、研发部门区段、财物部门区段、监控服务器区段和邮箱服务器区段。如何定义区段以及设置区段的确切数目，完全取决于用户的需求。

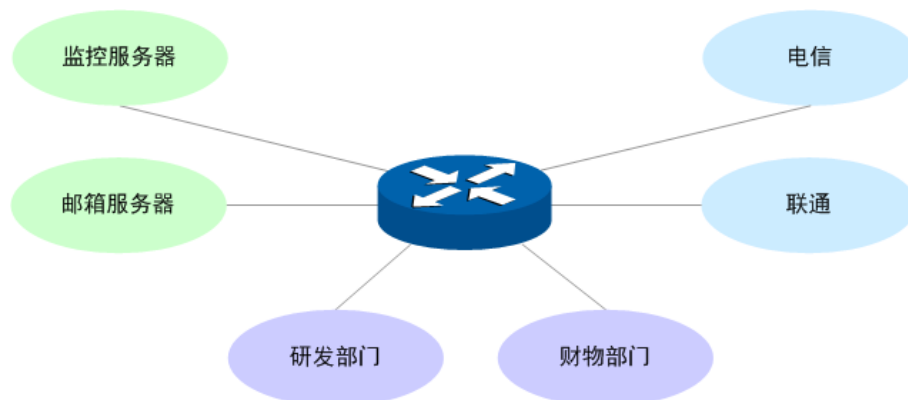


图 4.2 区段概念示意图二

4.1.2 接口

区段的接口可以视为一个入口，TCP/IP信息流可通过它在该区段和其它任何区段之间进行传递。通过定义的策略，可以使两个区段间的信息流朝一个或两个方向流动。通过定义的静态路由规则，可指定信息流从一个区段到另一个区段必须使用的接口。由于可将多个接口绑定到一个区段上，所以制定的静态路由规则对于将信息流引向所选择的接口十分重要。

为进一步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。

1. 物理接口

物理接口与设备上实际存在的组件有关。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。可将物理接口绑定到区段，信息流通过该物理接口进出区段。

TL-ER6520G的物理接口如图 4.3所示，只支持以太网这一种媒体类型。



图 4.3 物理接口概念示意图一

TL-ER6520G的物理接口命名为端口1/2/3/4/5，如图 4.4所示。

统计列表						
参数		端口1	端口2	端口3	端口4	端口5
接收	单播帧	0	0	0	647	0
	广播帧	0	0	0	263	0
	流控帧	0	0	0	0	0
	多播帧	0	0	0	69	0
	所有帧	0	0	0	90403	0
	过小帧	0	0	0	0	0
	正常帧	0	0	0	979	0
	过大帧	0	0	0	0	0
发送	单播帧	0	0	0	775	0
	广播帧	0	0	0	0	0
	流控帧	0	0	0	0	0
	多播帧	0	0	0	0	0
	所有帧	0	0	0	496952	0

刷新 清空所有 帮助

图 4.4 物理接口概念示意图二

2. 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-ER6520G用来划分物理接口的接口有eth、pppoe、pptp和l2tp四种类型。eth是以太网接口，功能上与以太网物理接口相同。eth接口由802.1Q VLAN标记进行区分，pppoe、pptp和l2tp由相关的协议字段进行区分。

信息流必须通过接口才能在区段内或区段间传递。每个区段至少需要定义一个eth接口，而对于跟互联网相连的广域网区段，还可能根据ISP（Internet Service Provider，网络服务提供商）提供的服务不同，需要定义pppoe、pptp或l2tp接口。一个区段可以定义多个eth接口，也可以定义多个pppoe、pptp或l2tp接口。用户可以根据自己的需要来设计每个接口。

4.1.1区段的基本概念介绍里，图 4.1中，在路由器上定义了区段，为了使信息能够传递，需要为每个区段定义接口。图 4.5为广域网区段、局域网区段和DMZ区段各定义了一个eth接口，eth接口名称分别为wan.eth0、lan.eth0和dmz.eth0。假设ISP为广域网区域提供的是PPPoE拨号上网服务，则需要广域网区段里定义一个pppoe接口，图中接口名称为wan.pppoe0。



图 4.5 接口概念示意图

4.2 区段设置

区段是绑定了一个或多个接口的逻辑实体，是一系列相同或类似功能的接口集合。通过本路由器可以定义多个区段，确切数目可根据网络需要来确定。每一个区段都可以根据需求定义多个接口，本路由器接口类型分为eth、pppoe、l2tp、pptp四种。

本节介绍区段设置的相关内容，具体包括以下部分：

- [default区段](#)：通过介绍TL-ER6520G预定义的default区段，介绍区段设置操作。
- [接口设置](#)：介绍TL-ER6520G提供的eth、pppoe、l2tp、pptp四种类型的接口，及其设置。

4.2.1 default区段

TL-ER6520G预定义了一个default区段，所有物理接口都绑定到该区段，该区段有一个eth接口，其IP地址为192.168.1.1，可以通过此IP地址访问路由器Web界面。

进入界面：基本设置 >> 区段设置 >> 区段设置



图 4.6 区段设置界面-default

此界面可以划分成三个区域：左列、区段设置和接口设置。以下简单介绍每一个区域的作用以及可以进行的操作。

左列

显示所有区段名称。点击区段的名称，可以进入相应区段界面进行设置。点击< + >按钮会显示**新增区段**界面，如图 4.7所示。在此界面设置区段名称，点击<确定>按钮，可以创建新区段。



图 4.7 区段设置界面-新增区段

区段名称	输入一个名称来标识一个区段。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。
-------------	---

表 4.1 新增区段界面条目项说明

新增区段完成后，如图 4.8所示。在此界面可以编辑区段和新增接口。



图 4.8 区段设置界面-新增区段完成

区段设置

显示本区段名称和所在的物理接口，在此区域可以修改区段名称，删除所有接口或删除本区段。

区段所在端口	显示该区段关联的物理接口，以及这些物理接口在设备上的位置。图形标记为绿色表示相应物理接口被关联。
修改	输入区段名称，点击此按钮，可以修改该区段名称。
删除所有接口	点击此按钮，删除该区段内所有接口。
删除本区段	点击此按钮，删除该区段。

表 4.2 区段设置界面条目项说明



说明：

如果删除了路由器中的全部接口，导致无法登录路由器Web界面，则可以通过命令行对路由器进行管理配置，详见**第15章命令行简介**；也可以通过Reset键，将路由器恢复成出厂设置，通过IP地址192.168.1.1登录路由器Web界面。

接口设置

显示本区段内所有接口名称，点击接口的名称，可以进入相应接口界面进行设置。点击< + >按钮会显示**新增接口**界面，如图 4.9所示。在此界面选择接口类型，设置接口名称等必要信息，点击<设置>按钮完成。接口设置的详细介绍请参考4.2.2 接口设置。

图 4.9 区段设置界面-新增接口

4.2.2 接口设置

TL-ER6520G提供eth、pppoe、pptp和l2tp四种类型的接口，以下为各接口简单介绍：

- eth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。
- pptp接口：提供PPTP连接方式的接口。虚拟专用拨号网络一般使用PPTP连接方式。
- l2tp接口：提供L2TP连接方式的接口。虚拟专用拨号网络也可以使用L2TP连接方式。



说明：

以上介绍提到的五种接入方式：静态IP、DHCP、PPPoE、PPTP、L2TP，都可以连接到广域网，具体情况请根据ISP（Internet Service Provider，网络服务提供商）提供的服务进行选择。

1. eth接口



说明：

新建eth接口，必须保证有VLAN可供选择，如需设置VLAN，请参考4.3 VLAN设置。

在区段设置界面的接口设置区域，选择接口类型为eth，将出现eth接口的设置界面，图 4.10是 manual连接方式，图 4.11是dhcp连接方式。

新增接口 +

接口类型: eth

接口名称: wan1.eth0

VLAN: VLAN10

连接方式: manual

IP地址: 10.10.10.10

子网掩码: 255.255.255.0

网关地址: 0.0.0.0 (可选)

MTU: 1500 (576-1500)

首选DNS服务器: (可选)

备用DNS服务器: (可选)

MAC地址: 00-14-78-00-02-B6

上行带宽: 1000000 Kbps (100-1000000)

下行带宽: 1000000 Kbps (100-1000000)

开放端口池: 2049 - 65000

参与带宽控制

参与流量均衡

属于管理接口

设置 帮助

图 4.10 eth接口设置-manual连接方式

接口类型	选择接口类型，共有eth、pppoe、pptp、l2tp四种接口类型可供选择。
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。
VLAN	当接口类型选择为eth时，需要在此选择一个该接口指向的VLAN。
连接方式	选择连接方式，有manual和dhcp两种连接方式。 选择manual连接方式，需要进行手动配置；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。
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。
上行带宽	设置接口数据流出的带宽大小, 可设置范围为100-1000000Kbps。
下行带宽	设置接口数据流入的带宽大小, 可设置范围为100-1000000Kbps。
开放端口池	设置作为NAT源端口的端口范围, 范围跨度必须大于或等于100。可设置范围为2049-65000。NAT功能请参考 8.1NAT设置 。
参与带宽控制	选择接口是否参与带宽控制。带宽控制功能介绍请参考 8.2带宽控制 。
参与流量均衡	选择接口是否参与流量均衡。流量均衡功能介绍请参考 8.4流量均衡 。
属于管理接口	选择接口是否属于管理接口。如果选择该接口属于管理接口, 则该接口所在区段为管理区段, 管理区段内的主机可以访问路由器。

表 4.3 eth接口设置界面manual连接方式条目项说明

新增接口 +

接口类型: eth ▼

接口名称: wan1.eth0

VLAN: VLAN10 ▼

连接方式: dhcp ▼

主机名:

MTU: 1500 (576-1500)

MAC地址: 00-14-78-00-02-B6

手动设置DNS服务器

首选DNS服务器:

备用DNS服务器:

上行带宽: 1000000 Kbps (100-1000000)

下行带宽: 1000000 Kbps (100-1000000)

开放端口池: 2049 - 65000

参与带宽控制

参与流量均衡

属于管理接口

设置
帮助

图 4.11 eth接口设置-dhcp连接方式

接口类型	选择接口类型, 共有eth、pppoe、pptp、l2tp四种接口类型可供选择。
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。
VLAN	当接口类型选择为eth时, 需要在此选择一个该接口指向的VLAN。

连接方式	选择连接方式，有manual和dhcp两种连接方式。 选择manual连接方式，需要进行手动配置；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。
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。
MAC地址	设置接口的MAC地址。
手动设置DNS服务器	勾选此项后，可以手动设置接口的DNS地址。
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。
上行带宽	设置接口数据流出的带宽大小，可设置范围为100-1000000Kbps。
下行带宽	设置接口数据流入的带宽大小，可设置范围为100-1000000Kbps。
开放端口池	设置作为NAT源端口的端口范围，范围跨度必须大于或等于100。可设置范围为2049-65000。NAT功能请参考 8.1NAT设置 。
参与带宽控制	选择接口是否参与带宽控制。带宽控制功能介绍请参考 8.2带宽控制 。
参与流量均衡	选择接口是否参与流量均衡。流量均衡功能介绍请参考 8.4流量均衡 。
属于管理接口	选择接口是否属于管理接口。如果选择该接口属于管理接口，则该接口所在区段为管理区段，管理区段内的主机可以访问路由器。

表 4.4 eth接口设置界面dhcp连接方式条目项说明

2. pppoe接口

说明：

新建pppoe接口，必须保证有同一区段里的eth接口可供选择，如需新建eth接口，请参考4.2.2接口设置 1 eth接口。

在区段设置界面的接口设置区域，选择接口类型为pppoe，将出现pppoe接口的设置界面。



wan1.eth0 新增接口 +

接口类型: pppoe

接口名称:

LINK接口: wan1.eth0

用户名:

密码:

启用PPPoE高级设置

检测间隔时间: (0-120秒, 0代表不发送)

检测重试次数: (1-30)

MTU: (576-1492)

服务名: (如非必要, 请勿填写)

首选DNS服务器: (可选)

备用DNS服务器: (可选)

上行带宽: Kbps (100-1000000)

下行带宽: Kbps (100-1000000)

开放端口池: -

手动连接

自动连接

定时连接 连接时段:

参与带宽控制

参与流量均衡

属于管理接口

图 4.12 pppoe接口设置

接口类型	选择接口类型，共有eth、pppoe、pptp、l2tp四种接口类型可供选择。
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。
LINK接口	当接口类型选择为pppoe时，需要在此选择一个本区段下的eth接口作为其链接接口。
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。

启用PPPoE高级设置	勾选此项后，可以手动设置检测间隔时间和重试次数，指定MTU值、服务名及DNS (Domain Name Server, 域名解析服务) 地址。如果不清楚这些参数，请勿勾选此项。
检测间隔时间	设置检测间隔时间，路由器将会按照指定的间隔时间向ISP发送Keep Alive数据包，用于检测链路是否正常。默认值为0，表示不检测链路。
检测重试次数	设置检测重试次数，路由器按照指定的检测间隔时间向ISP发送Keep Alive数据包，如果没有收到ISP回应包的连续重试次数达到设置的值，路由器会断开连接。
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。
备选DNS服务器	设置备用DNS地址，允许留空。
上行带宽	设置接口数据流出的带宽大小，可设置范围为100-1000000Kbps。
下行带宽	设置接口数据流入的带宽大小，可设置范围为100-1000000Kbps。
开放端口池	设置作为NAT源端口的端口范围，范围跨度必须大于或等于100。可设置范围为2049-65000。NAT功能请参考 8.1NAT设置 。
手动连接	用户可在需要上网时手动点击<连接>按钮连入互联网，适合按小时计费的拨号连接上网方式。
自动连接	每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。
定时连接	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 7.2时间管理 。
参与带宽控制	选择接口是否参与带宽控制。带宽控制功能介绍请参考 8.2带宽控制 。
参与流量均衡	选择接口是否参与流量均衡。流量均衡功能介绍请参考 8.4流量均衡 。
属于管理接口	选择接口是否属于管理接口。如果选择该接口属于管理接口，则该接口所在区段为管理区段，管理区段内的主机可以访问路由器。

表 4.5 pppoe接口设置界面条目项说明

3. pptp接口



说明：

新建pptp接口，必须保证在同一区段里已有一个能够正常通信的接口可供选择，接口类型不限。

在区段设置界面的接口设置区域，选择接口类型为pptp，将出现pptp接口的设置界面。

The screenshot shows the configuration page for a PPTP interface. At the top, there's a tab for 'wan1.eth0' and a '+ 新增接口' button. The configuration fields are as follows:

- 接口类型: pptp (dropdown)
- 接口名称: (text input)
- LINK接口: wan1.eth0 (dropdown)
- 用户名: (text input)
- 密码: (text input)
- 服务器地址: (text input) (IP地址或域名)
- MTU: 1460 (text input) (576-1460)
- 上行带宽: 1000000 (text input) Kbps (100-1000000)
- 下行带宽: 1000000 (text input) Kbps (100-1000000)
- 开放端口池: 2049 - 65000 (text input)
- MPPE加密
- 手动连接
- 自动连接
- 定时连接 连接时段: Any (dropdown)
- 参与带宽控制
- 参与流量均衡
- 属于管理接口

At the bottom, there are '设置' (Settings) and '帮助' (Help) buttons.

图 4.13 pptp接口设置

接口类型	选择接口类型，共有eth、pppoe、pptp、l2tp四种接口类型可供选择。
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。
LINK接口	当接口类型选择为pptp时，需要在此选择一个本区段下的其他接口作为其链接接口。pptp接口可以选择其他pptp接口作为其链接接口，但整个链接关系的深度不能超过3层。
用户名	PPTP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	PPTP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。
服务器地址	PPTP拨号的服务器的IP地址或域名，由ISP提供。
MTU	MTU (Maximum Transmission Unit, 最大传输单元)，可以设置数据包的最大长度。取值范围是576-1460之间的整数，默认值为1460。若ISP未提供MTU值，请保持默认值不变。
上行带宽	设置接口数据流出的带宽大小，可设置范围为100-1000000Kbps。

下行带宽	设置接口数据流入的带宽大小，可设置范围为100-1000000Kbps。
开放端口池	设置作为NAT源端口的端口范围，范围跨度必须大于或等于100。可设置范围为2049-65000。NAT功能请参考 8.1NAT设置 。
MPPE加密	勾选此项，可以使用MPPE（Microsoft Point-to-Point Encryption，微软点对点加密术）对PPTP隧道进行加密。
手动连接	用户可在需要上网时手动点击<连接>按钮连入互联网，适合按小时计费的拨号连接上网方式。
自动连接	每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。
定时连接	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，适用于需要限时上网的场合。如需新建时间表，请参考 7.2时间管理 。
参与带宽控制	选择接口是否参与带宽控制。带宽控制功能介绍请参考 8.2带宽控制 。
参与流量均衡	选择接口是否参与流量均衡。流量均衡功能介绍请参考 8.4流量均衡 。
属于管理接口	选择接口是否属于管理接口。如果选择该接口属于管理接口，则该接口所在区段为管理区段，管理区段内的主机可以访问路由器。


表 4.6 pptp接口设置界面条目项说明

4. l2tp接口

说明：

新建l2tp接口，必须保证在同一区段里已有一个能够正常通信的接口可供选择，接口类型不限。

在区段设置界面的接口设置区域，选择接口类型为l2tp，将出现l2tp接口的设置界面。



wan1.eth0 新增接口 +

接口类型: l2tp

接口名称:

LINK接口: wan1.eth0

用户名:

密码:

服务器地址: (IP地址或域名)

MTU: 1460 (576-1460)

上行带宽: 1000000 Kbps (100-1000000)

下行带宽: 1000000 Kbps (100-1000000)

开放端口池: 2049 - 65000

加密方式:

手动连接

自动连接

定时连接 连接时段: Any

参与带宽控制

参与流量均衡

属于管理接口

图 4.14 l2tp接口设置

接口类型	选择接口类型，共有eth、pppoe、pptp、l2tp四种接口类型可供选择。
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。
LINK接口	当接口类型选择为l2tp时，需要在此选择一个本区段下的其他接口作为其链接接口。l2tp接口可以选择其他l2tp接口作为其链接接口，但整个链接关系的深度不能超过3层。
用户名	L2TP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	L2TP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。
服务器地址	L2TP拨号的服务器的IP地址或域名，由ISP提供。
MTU	MTU (Maximum Transmission Unit, 最大传输单元)，可以设置数据包的最大长度。取值范围是576-1460之间的整数，默认值为1460。若ISP未提供MTU值，请保持默认值不变。
上行带宽	设置接口数据流出的带宽大小，可设置范围为100-1000000Kbps。

下行带宽	设置接口数据流入的带宽大小，可设置范围为100-1000000Kbps。
开放端口池	设置作为NAT源端口的端口范围，范围跨度必须大于或等于100。可设置范围为2049-65000。NAT功能请参考8.1 NAT设置。
加密方式	勾选此项，可以在下拉列表之中选择IPsec安全策略，对L2TP隧道进行加密。IPsec功能介绍请参考10.2 IPsec。
手动连接	用户可在需要上网时手动点击<连接>按钮连入互联网，适合按小时计费的拨号连接上网方式。
自动连接	每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。
定时连接	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，适用于需要限时上网的场合。如需新建时间表，请参考7.2时间管理。
参与带宽控制	选择接口是否参与带宽控制。带宽控制功能介绍请参考8.2带宽控制。
参与流量均衡	选择接口是否参与流量均衡。流量均衡功能介绍请参考8.4流量均衡。
属于管理接口	选择接口是否属于管理接口。如果选择该接口属于管理接口，则该接口所在区段为管理区段，管理区段内的主机可以访问路由器。

表 4.7 l2tp接口设置界面条目项说明

配置接口步骤：

- 1) 创建区段。非必须操作，如果在已有区段上创建接口，则不必此项操作。创建界面：基本设置 >> 区段设置 >> 区段设置，在此界面的左列点击<+>按钮，在显示的新增区段界面中输入区段名称，点击<确定>按钮完成。
- 2) 创建VLAN。必须操作。具体操作步骤请参考[配置VLAN步骤](#)。
- 3) 创建eth接口。必须操作。创建界面：基本设置 >> 区段设置 >> 区段设置，进入需要创建接口的区段，在其接口设置区域，点击<+>按钮，在显示的新增接口设置页面，选择接口类型为eth，选择链接的VLAN，输入接口名称等必要信息，点击<设置>按钮完成。
- 4) 创建pppoe、pptp或l2tp接口。非必须操作。创建界面：基本设置 >> 区段设置 >> 区段设置，进入需要创建接口的区段，在其接口设置区域，点击<+>按钮，在显示的新增接口设置页面，选择所需接口类型，选择其链接的接口，输入接口名称等必要信息，点击<设置>按钮完成。

4.3 VLAN设置

4.3.1 VLAN简介

VLAN (Virtual Local Area Network, 虚拟局域网) 是一种将局域网设备从逻辑上划分成一个网段，从而实现虚拟工作组的数据交换技术，这种技术通过在局域网数据帧上定义扩展字段，来对物理网络进行逻辑上的分割，从而限定局域网数据帧的转发范围，缩小广播域。VLAN技术主要应用于交换机和路由器中。

1. 产生背景

局域网的发展是VLAN产生的基础，可以通过了解局域网的有关知识来了解VLAN。

局域网（Local Area Network）是在一个局部的地理范围内（如一个学校、工厂和公司内），将各种计算机、共享设备和数据库等互相联接起来组成的一个封闭式的计算机通信网络。其通常是一个单独的广播域，主要由Hub、网桥或交换机等网络设备连接网络内的所有节点。处于同一个局域网的网络节点之间可以直接通信，而处于不同局域网段的设备之间则必须经过路由器才能通信。下图为使用路由器构建的典型局域网环境。

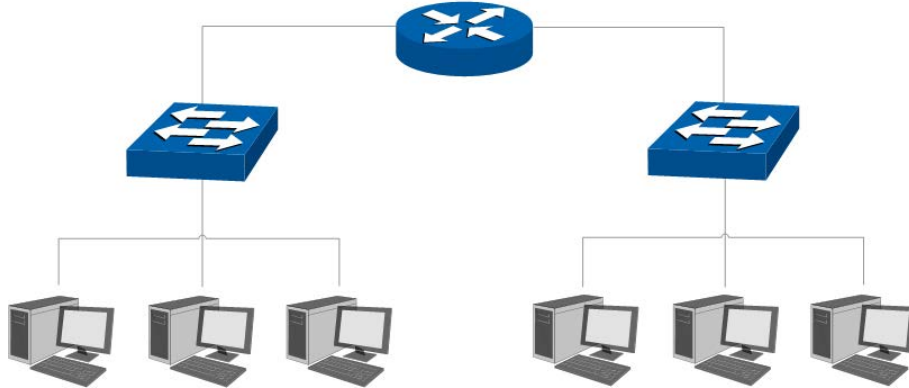


图 4.15 典型局域网拓扑

然而随着网络的不断扩展，接入设备逐渐增多，网络结构也日趋复杂，必须使用更多的路由器才能将不同的用户划分到各自的用户组（广播域）中，在不同的局域网之间提供网络互联。但路由器数量的增多势必会导致网络延时逐渐加长，网络数据传输速度下降。其次，用户是按照物理连接被机械地划分到不同的用户组中，而这种分割方式并没有考虑到用户的工作属性和网络需求。

在这种情况下，VLAN技术应运而生。利用VLAN技术，可以根据用户的工作属性和网络需求，在路由器或者交换机上划分VLAN，将用户划分到不同的工作组中，为不同的工作组执行不同的策略。

同一个VLAN中的用户间通信就和在一个局域网内一样，同一个VLAN中的广播只有VLAN中的成员才能听到，而不会传输到其他VLAN中去，从而控制不必要的广播风暴的产生。同时，若没有路由，不同VLAN之间不能相互通信，从而提高了不同工作组之间的信息安全性。网络管理员可以通过配置VLAN之间的路由来全面管理网络内部不同工作组之间的信息互访。

2. 技术特点

以下是VLAN在实际网络应用中的常用基础拓扑。

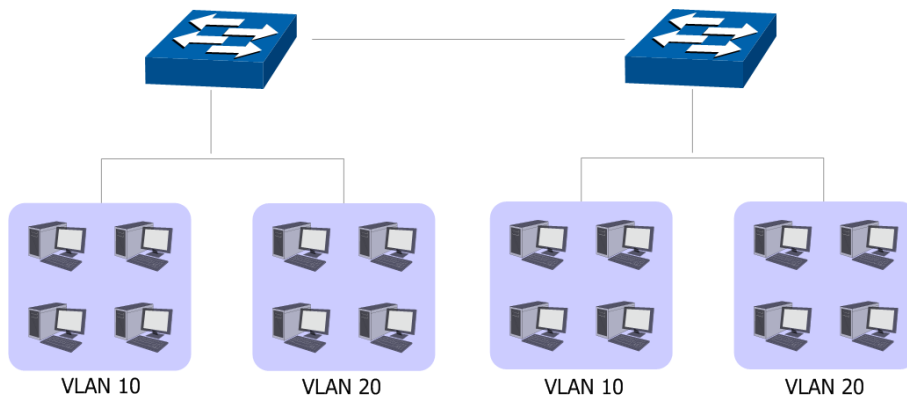


图 4.16 VLAN常用网络拓扑

VLAN的划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个VLAN；一个VLAN包含的用户可以连接在同一台交换机上，也可以跨越交换机。在局域网中使用VLAN功能有如下优点：

- 快速创建虚拟工作组。使用VLAN功能可以快速创建虚拟工作组，只需网络管理者在控制台上进行简单的操作即可，而不必为项目需要将组成员的工作站集合在一起建立一个局域网。
- 增强网络安全。不同VLAN的设备不能互相访问，需要通过路由器或三层交换机等网络层设备对报文进行三层转发，从而确保一个VLAN的数据不会被其他VLAN的设备窃听。
- 提高网络性能。通过VLAN功能可以将广播帧限制在VLAN内，有效控制网络的广播风暴，节省了网络带宽，进而提高网络处理能力。
- 降低网络管理成本。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便为不同区域用户建立工作组。当一个用户从一个位置移动到另一个位置时，使用合适的VLAN划分方法，就不需要重新配置网络属性。

3. 802.1Q VLAN

IEEE于1999年发布了用以规范VLAN实现的IEEE Std 802.1Q标准。藉以此标准，在局域网中的连接设备能够识别对方网络上建立的VLAN并执行相应的通信策略。

IEEE 802.1Q协议标准为各种局域网网络结构定义了VLAN的Tag字段，不同网络结构中，连接设备可以通过共同的数据特征进行VLAN识别。

对于常见的以太网网络模型，其主要的报文封装格式类型有两种，分别为Ethernet II型和802.2/802.3型。对于这两种以太网报文的封装格式，IEEE 802.1Q协议标准在数据帧首部的目的MAC地址（DA）和源MAC地址（SA）后定义了VLAN Tag，用以标识VLAN的相关信息。Tag字段的位置如下图 4.17所示。Tag封装在DA&SA后，它包含四个字段，分别是TPID（Tag

Protocol Identifier, 标签协议标识符)、Priority、CFI (Canonical Format Indicator, 标准格式指示位) 和VLAN ID。

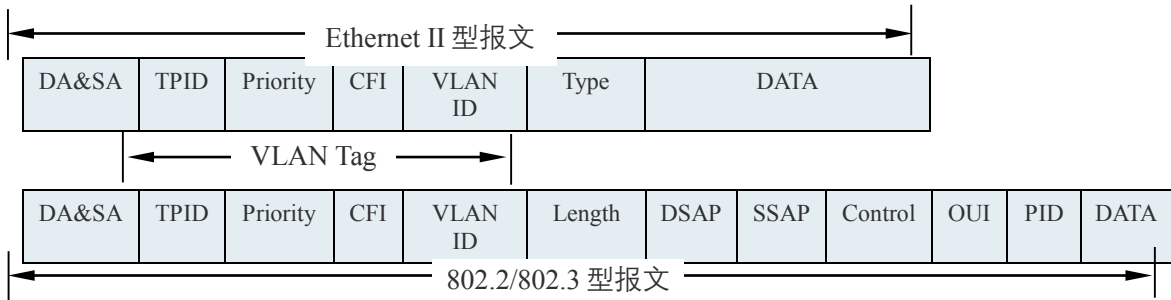


图 4.17 VLAN Tag组成字段

TPID	默认值为0x8100。当TPID字段为0x8100时，表示本数据帧带有Tag。
Priority	数值为0-7，表示数据包的传输优先级。当VLAN ID字段为0时表示此Tag是一个优先级Tag，由IEEE 802.1P协议标准进行规范，详细请查看IEEE 802.1P协议标准。
CFI	数值为0或1。以太网交换机中，CFI总被设置为0。用来表示MAC地址是否以标准格式进行封装。该字段长度为1bit，取值为0表示MAC地址以标准格式进行封装，取1表示以非标准格式封装，缺省取值为0。
VLAN ID	可设置范围为1-4094。用来标识该报文所属VLAN，简称VID。当VLAN ID字段为0时表示此Tag是一个优先级Tag；VLAN ID字段全1为协议预留字段。

表 4.8 Tag字段含义

在802.1Q VLAN基础上，添加其他标识，可以有不同方法实现VLAN，例如在802.1Q VLAN基础上添加MAC识别，从而实现基于MAC的VLAN，此外，还有基于协议的VLAN，基于IP地址的VLAN，基于端口的VLAN等。TL-ER6520G是基于端口实现的VLAN。

4. 端口的链路类型

在创建802.1Q VLAN时，需要根据端口连接的设备设置端口的链路类型。端口的链路类型有下面三种：

- **Access**：端口只能属于1个VLAN，出口规则为UNTAG，即从此端口发送出去的报文不带VLAN Tag，多为连接用户终端设备的端口。如图 4.18所示，设备和普通计算机相连，计算机不能识别带VLAN Tag的报文，所以需要将设备和计算机相连端口的链路类型设置为Access。当Access类型端口加入到其它VLAN时，自动退出原有VLAN。
- **Trunk**：端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，常用于网络设备之间级连。如图 4.18所示，需要将设备1和设备2相连端口的链路类型设置为Trunk。在网络中VLAN经常跨接在不同通信设备上，Trunk类型端口的出口规则为TAG，即从此端口发送出去的报文带有VLAN Tag，能够保证在转发各种VLAN的数据包时不改变其携带的VLAN信息。

- Hybrid: 端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，可以用于网络设备之间连接，也可以用于连接用户设备。如图 4.18所示，与设备2相连的某个网络环境复杂，无法判断网络中的设备是哪种类型或是该网络中有多种类型的设备时，需要将设备2和该网络相连端口的链路类型设置为Hybrid。Hybrid类型端口的出口规则可以根据该端口连接设备的实际情况灵活配置。

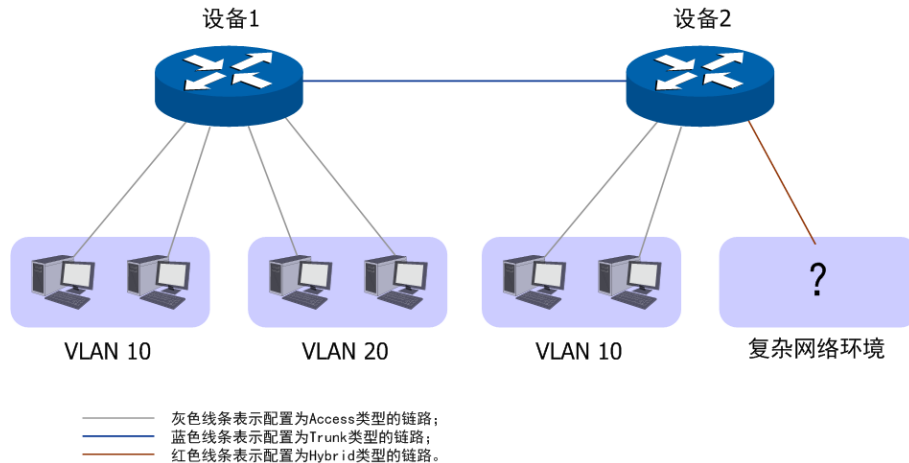


图 4.18 链路类型配置示意图

端口的链路类型本质上是通信设备接收和转发数据帧的处理方式。在实际组网中，根据不同的网络需求，可以为每个端口指定出口规则和入口规则，入口规则表示接收数据帧时的处理方式，出口规则表示转发数据帧时的处理方式。下面详细介绍端口出口规则和入口规则。

Access	接收报文时： 如果报文不带Tag，则接收报文，并为报文添加缺省的VLAN； 如果报文带Tag且VLAN ID = 端口PVID，则接收报文； 如果报文带Tag而VLAN ID ≠ 端口PVID，则丢弃报文。 发送报文时： 去掉Tag后，发送报文。
Trunk	接收报文时： 如果报文不带Tag，则为报文添加缺省VLAN的Tag； 如果报文带Tag且VLAN ID属于端口允许通过的VLAN ID，则接收报文； 如果报文带Tag而VLAN ID不属于端口允许通过的VLAN ID，则丢弃报文。 发送报文时： 保持原有Tag发送报文。
Hybrid	接收报文时： 如果报文不带Tag，则为报文添加缺省VLAN的Tag； 如果报文带Tag且VLAN ID属于端口允许通过的VLAN ID，则接收报文； 如果报文带Tag而VLAN ID不属于端口允许通过的VLAN ID，则丢弃报文。 发送报文时： 当出口规则配置为TAG时，保持原有Tag发送报文。 当出口规则配置为UNTAG时，去Tag后发送报文。

表 4.9 端口出口规则与入口规则

5. PVID

PVID (Port VLAN ID), 通信设备每个物理接口的重要参数, 表示端口默认所属的VLAN。当设备的端口接收到的数据帧不带VLAN Tag时, 设备会根据接收端口的PVID为该报文插入VLAN Tag, 并在端口的缺省VLAN中转发数据帧。PVID主要有下面两个用途:

- 当设备收到不带Tag的数据帧时, 将根据PVID为数据帧插入VLAN Tag并转发。
- PVID指定了端口的缺省VLAN ID, 即默认广播域。当端口接收到UL包或广播包的时候, 设备将这些数据包在该端口的缺省VLAN内广播。

对于不同链路类型的端口, 设置PVID时会会有所不同: 若端口链路类型为Access, 因为该端口只能属于一个VLAN, 所以该端口的PVID不可设置。若端口链路类型为Trunk或Hybrid, 因为该端口可以属于多个VLAN, 所以可以设置, 但所设置的PVID必须是该端口所属VLAN之一。

4.3.2 VLAN设置

设置VLAN时, 需要设置报文中Tag字段的VLAN ID数值, 物理接口的PVID数值和VLAN成员端口的链路类型。

1. 设置VLAN ID

进入界面: 基本设置 >> VLAN设置 >> VLAN设置

在界面的VLAN设置区域, 填入VLAN ID、名称, 勾选对应端口, 点击<新增>按钮手动添加条目。

The screenshot shows the 'VLAN设置' (VLAN Configuration) interface. It includes a form for adding a new VLAN with fields for 'VLAN ID' (set to 10), '名称' (Name, set to VLAN10), '端口设置' (Port Settings) with a table of ports and their link types, and a '备注' (Remarks) field (set to WAN1). Below the form are buttons for '新增' (Add), '清除' (Clear), and '帮助' (Help). At the bottom, there is a 'VLAN列表' (VLAN List) table with columns for selection, serial number, VLAN ID, name, port settings, remarks, and a settings icon.

选择	序号	VLAN ID	名称	端口设置	备注	设置
<input type="checkbox"/>	1	1	vlan1	1(UNTAG),2(TAG),3(UNTAG),4(UNTAG),5(UNTAG)	system vlan	

图 4.19 VLAN设置界面-VLAN设置

VLAN ID	设置Tag字段的VLAN ID数值, 可设置范围为2-4094。
----------------	----------------------------------

名称	输入一个名称来标识该VLAN。
端口设置	此处勾选相应端口。端口链路类型的选择需要到端口设置界面进行，而链路类型不同，TAG标签会有所不同。端口设置请参考 4.3.2 VLAN设置 2 设置PVID和链路类型 。
备注	添加对本条目的说明信息，非必填项。

表 4.10 VLAN设置界面条目说明

新增VLAN的信息会在**VLAN列表**中显示出来。

VLAN列表中的序号1显示的是TL-ER6520G预定义的系统VLAN的信息。系统VLAN名称为vlan1，VLAN ID是1，默认情况下所有的端口都属于此VLAN，所有端口默认链路类型为Access。在图 4.20界面中，可以编辑修改系统VLAN的名称和备注，但是不能删除系统VLAN以及其包含的端口。vlan1被default区段的eth0接口使用。default区段的相关信息，请参考**4.2.1 default区段**。

VLAN设置

VLAN ID: (2-4094)

名称:

端口设置:

<input type="checkbox"/> 端口	链路类型	TAG标签
<input type="checkbox"/> 1	Access	UNTAG
<input type="checkbox"/> 2	Trunk	TAG
<input type="checkbox"/> 3	Hybrid	TAG ▼
<input type="checkbox"/> 4	Access	UNTAG
<input type="checkbox"/> 5	Access	UNTAG

备注: (可选)

VLAN列表

选择	序号	VLAN ID	名称	端口设置	备注	设置
<input type="checkbox"/>	1	1	vlan1	2(TAG),3(UNTAG),4(UNTAG),5(UNTAG)	system vlan	
<input type="checkbox"/>	2	10	VLAN10	1(UNTAG)	WAN1	

图 4.20 VLAN设置界面-VLAN列表



说明:

- 如果新增条目的端口链路类型是Access，则该端口将会被从之前所属的VLAN中去除，添加到新设置的VLAN中。
- 如果在设置VLAN时，导致某个端口不属于任何一个VLAN，则该端口将会被默认添加到系统VLAN中，其PVID为1，TAG标签根据链路类型来决定，Access和Hybrid时为UNTAG，Trunk时为TAG。

2. 设置PVID和链路类型

进入界面：基本设置 >> VLAN设置 >> 端口设置

在此界面可以选择端口链路类型或者设置端口的PVID。

端口设置		
端口	链路类型	PVID
1	access	1
2	trunk	1
3	hybrid	1
4	access	1
5	access	1

设置 帮助

图 4.21 端口设置界面

端口	显示所有物理接口。
链路类型	选择端口链路类型, 可选项有access、trunk和hybrid, 详细介绍请参考4.3.1 VLAN简介 4 端口的链路类型。
PVID	设置端口的PVID, 详细介绍请参考4.3.1 VLAN简介 5 PVID。

表 4.11 端口设置界面条目项说明



说明：

- 每个端口的链路类型和PVID一次只可以修改一项，两者不可以同时修改。
- 系统可能会根据端口的链路类型和所属VLAN的改变而自动修改端口的PVID。
- 如果端口的PVID所关联的VLAN条目被删除，则该端口将可能无法收发报文，需要用户重新为该端口设置一个合法的PVID。

设置完成后可以在关联表界面查看相关信息。

进入界面：基本设置 >> VLAN设置 >> 关联表

关联表		
端口	链路类型	端口所属Vlan
1	Access	1(UNTAG)
2	Trunk	1(TAG)
3	Hybrid	1(UNTAG)
4	Access	1(UNTAG)
5	Access	1(UNTAG)

帮助

图 4.22 关联表界面

配置VLAN步骤：

- 1) 设置端口链路类型。非必须操作，路由器默认全部端口链路类型为Access，如果需求为Access，则不必此项操作。设置界面：基本设置 >> VLAN设置 >> 端口设置，在此界面根据端口连接的设备选择其链路类型，点击<设置>按钮完成。
- 2) 创建VLAN。必须操作。创建界面：基本设置 >> VLAN设置 >> VLAN设置，在此界面设置VLAN ID，输入VLAN名称，勾选VLAN包含的端口，点击<新增>按钮完成。
- 3) 设置端口的PVID。非必须操作。设置界面：基本设置 >> VLAN设置 >> 端口设置，当某个端口有多个VLAN ID时，可以在此选择其默认PVID。
- 4) 查看端口VLAN信息。非必须操作。查看界面：基本设置 >> VLAN设置 >> 关联表，在此界面可以查看每个端口对应的链路类型、PVID和出口规则。

4.4 交换机设置

TL-ER6520G路由器具备一些简单的交换机端口管理功能。在此可以实时查看路由器各端口的数据流通状况，并进行相应的控制和管理。

4.4.1 端口统计

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

进入界面：基本设置 >> 交换机设置 >> 端口统计

统计列表						
参数		端口1	端口2	端口3	端口4	端口5
接收	单播帧	0	6506	0	0	0
	广播帧	0	946	0	0	0
	流控帧	0	0	0	0	0
	多播帧	0	71	0	0	0
	所有帧	0	793342	0	0	0
	过小帧	0	0	0	0	0
	正常帧	0	7523	0	0	0
发送	过大帧	0	0	0	0	0
	单播帧	0	9928	0	0	0
	广播帧	0	1	0	0	0
	流控帧	0	0	0	0	0
	多播帧	0	0	0	0	0
所有帧	0	8048356	0	0	0	

刷新 清空所有 帮助

图 4.23 端口统计界面

单播帧	目的MAC地址为单播MAC地址的正常数据帧数目。
------------	--------------------------

广播帧	目的MAC地址为广播MAC地址的正常数据帧数目。
流控帧	接收/发送的流量控制数据帧数目。
多播帧	目的MAC地址为多播MAC地址的正常数据帧数目。
所有帧	接收/发送所有的数据帧的总字节数（包含校验和错误的帧）。
过小帧	收到的长度小于64字节的数据帧数目（包含校验和错误的帧）。
正常帧	收到的长度在64字节到最大帧长之间的数据帧数目（包含错误帧）。对于不带tag标签的帧，路由器支持的最大帧长为1518字节；对于带tag标签的帧，路由器支持的最大帧长为1522字节。
过大帧	收到的长度大于最大帧长的数据帧数目（包含错误帧）。

表 4.12 端口统计界面项说明

点击<清空所有>按钮可以一次清空所有统计数据。

4.4.2 端口监控

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

进入界面：**基本设置 >> 交换机设置 >> 端口监控**

功能设置		
<input checked="" type="checkbox"/>	启用端口监控	
监控模式：	输出监控	
监控列表		
端口	监控端口	被监控端口
1	<input checked="" type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="checkbox"/>
<input type="button" value="设置"/> <input type="button" value="帮助"/>		

图 4.24 端口监控设置界面

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

表 4.13 端口监控功能设置界面项说明

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

表 4.14 监控列表界面项说明

图 4.24 监控列表的含义是：端口1被选作监控端口，它将对端口2、3、4、5进行输出监控。

应用举例

某企业网络出现异常状况，需要利用端口监控功能捕获网络中的所有数据进行分析。

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

功能设置

启用端口监控

监控模式：输入输出监控

监控列表

端口	监控端口	被监控端口
1	<input type="radio"/>	<input checked="" type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input checked="" type="checkbox"/>
5	<input type="radio"/>	<input checked="" type="checkbox"/>

设置
帮助

4.4.3 端口流量限制

可以在此开启各端口的流量限制功能并进行相应设置。

进入界面：基本设置 >> 交换机设置 >> 端口流量限制

功能设置

端口	入口限制状态	入口限制模式	入口限制速率(Mbps)	出口限制状态	出口限制速率(Mbps)
1	<input checked="" type="checkbox"/> 启用	所有帧	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
2	<input type="checkbox"/> 启用	所有帧	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
3	<input checked="" type="checkbox"/> 启用	所有帧	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
4	<input type="checkbox"/> 启用	所有帧	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
5	<input type="checkbox"/> 启用	所有帧	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>

设置
帮助

图 4.25 端口流量限制设置界面

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

表 4.15 监控列表界面项说明

4.4.4 端口参数

可以在此启用各物理端口及其流量限制，并根据需要设定其协商模式。

进入界面：基本设置 >> 交换机设置 >> 端口参数

功能设置			
端口	端口状态	流量控制	协商模式
1	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	10M 全双工
2	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	自协商
3	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	自协商
4	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	自协商
5	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	自协商
所有端口			
	--	--	--

设置 帮助

图 4.26 端口参数设置界面

端口状态	只有勾选了“启用”该端口才会有数据包的传输，即物理意义上的开启。
流量控制	推荐勾选“启用”以控制调节各端口数据包转发的速率，避免出现拥塞。
协商模式	有10M全/半双工、100M全/半双工、1000M全双工、自协商6种模式可选，择需使用。
所有端口	这一栏可对以上所有端口进行统一设置，比如同时启用或禁用。

表 4.16 端口参数设置界面说明

4.4.5 端口状态

可以在此查看各个端口的基本状态。

进入界面：基本设置 >> 交换机设置 >> 端口状态

状态列表				
端口	端口状态	连接速率(Mbps)	双工模式(Mbps)	流量控制
1	未连接	---	---	---
2	已连接	100	全双工	禁用
3	未连接	---	---	---
4	未连接	---	---	---
5	未连接	---	---	---

刷新 帮助

图 4.27 端口状态界面

第5章 DHCP

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。

5.1 DHCP服务器

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。

5.1.1 DHCP协议介绍

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。

1. DHCP报文格式

DHCP报文的封装格式如下图所示:

op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (312)			

图 5.1 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 5.1 DHCP报文字段含义

2. 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客户端和服务端均按照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：

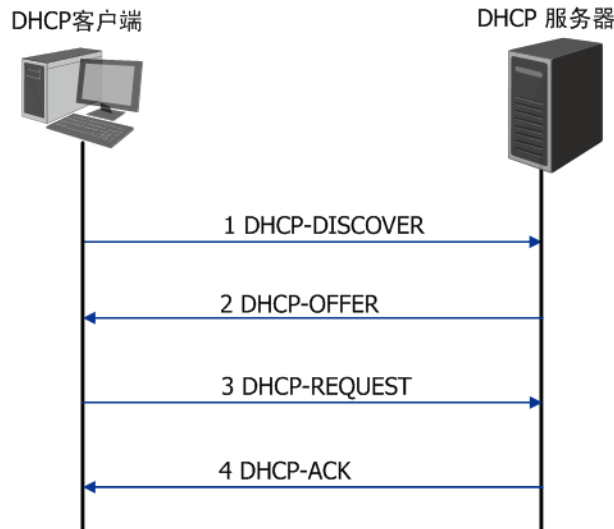


图 5.2 动态获取IP地址的过程

- 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地址池中选出一个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。

5.1.2 DHCP功能介绍

本节主要介绍在TL-ER6520G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。

1. 动态地址分配策略

TL-ER6520G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。

2. DHCP服务器功能典型应用环境

下图为路由器TL-ER6520G配置为DHCP服务器时的网络拓扑图使用示范，具体的网络环境可以根据实际需要调整。

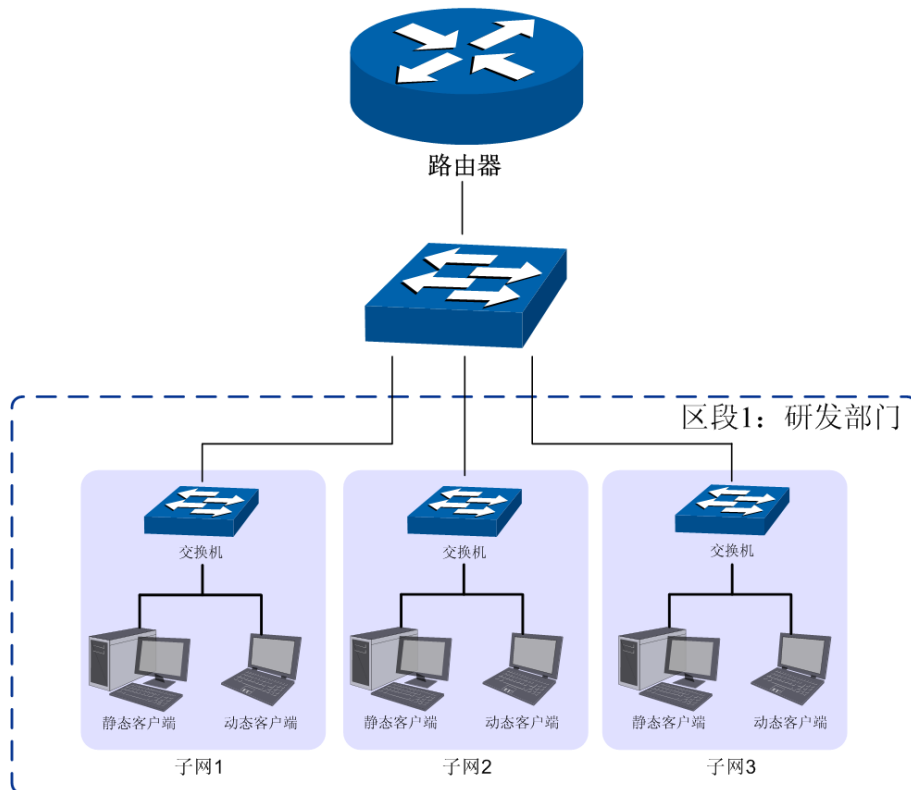


图 5.3 DHCP服务器功能应用环境

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-ER6520G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。

3. 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地获得IP地址，保证网络的稳定性，TL-ER6520G路由器的DHCP服务器功能可以完成如下任务：

- 1) TL-ER6520G可以为多达16个eth接口类型网络分配地址。



说明：

- 如果eth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、pptp、l2tp类型的接口，由于其IP地址的不确定性，TL-ER6520G路由器也暂不提供DHCP服务器功能。

- 2) 当TL-ER6520G收到DHCP请求报文时，将根据数据包中的VLAN ID信息选择相应接口的地址池来分配地址。



说明：

关于TL-ER6520G的VLAN功能相关内容，请参考说明书中的**4.3 VLAN设置**章节。

- 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，会向所有区段中的接口网络发起待分配地址的Ping检测，从而避免IP冲突。

4. IP地址重复分配检测

路由器在分配一个IP地址前，会向所有区段中的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服务器从地址池中选择新的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。

5. 分配IP地址的优先次序

TL-ER6520G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) 选择合适的地址池，从中顺序查找可供分配的第一个IP地址。

5.1.3 DHCP功能配置

DHCP功能配置主要分为配置IP地址池、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。

1. 配置IP地址池

创建可供DHCP分配的地址池

进入界面：基本设置 >> 对象管理 >> IP地址池

在界面的地址池设置区域，创建可供DHCP分配的IP地址池，点击<新增>按钮创建IP地址池。

地址池设置

地址池名称：

地址池范围： -

启用/禁用： 启用 禁用

地址池列表

选择	序号	地址池名称	地址池范围	状态	设置
<input type="checkbox"/>	1	软件部门	192.168.100.51-192.168.100.99	已启用	

图 5.4 IP地址池配置界面-创建地址池

地址池名称	添加对本条目的说明信息。
地址池范围	输入可供分配的地址段起始地址和结束地址。
启用/禁用	选择“启用”，则使该地址池生效； 选择“禁用”，则使该地址池失效。

表 5.2 创建地址池界面条目说明

新增的地址池条目会在下方地址池列表显示出来，如下图中所示。

地址池列表

选择	序号	地址池名称	地址池范围	状态	设置
<input type="checkbox"/>	1	软件部门	192.168.100.51-192.168.100.99	已启用	
<input type="checkbox"/>	2	管理部门	192.168.1.51-192.168.1.99	已启用	

图 5.5 IP地址池配置界面-地址池列表

配置地址池参数

进入界面：基本设置 >> DHCP >> DHCP服务

在地址池创建完成后，需要在DHCP服务界面配置DHCP地址池参数，包括地址的租期、缺省网关以及首选DNS服务器等参数，点击<新增>按钮完成地址池配置。

The screenshot shows the DHCP service configuration interface. The top section, titled '服务设置' (Service Settings), contains the following fields:

- 服务接口 (Service Interface): eth0
- 地址池 (Address Pool): 管理部门 (Management Department)
- 地址租期 (Address Lease Time): 120 分钟 (1-2880)
- 网关地址 (Gateway Address): 192.168.1.1 (Optional)
- 缺省域名 (Default Domain): (Optional)
- 首选DNS服务器 (Preferred DNS Server): 192.168.1.1 (Optional)
- 备用DNS服务器 (Backup DNS Server): 0.0.0.0 (Optional)
- 启用/禁用服务 (Enable/Disable Service): 启用 禁用

Below the settings are buttons for '新增' (Add), '清除' (Clear), and '帮助' (Help). The bottom section, titled 'DHCP服务列表' (DHCP Service List), contains a table with the following data:

选择	序号	服务接口	地址池	租期	网关地址	首选DNS服务器	备用DNS服务器	状态	设置
<input type="checkbox"/>	1	soft_dep	软件部门	120	192.168.100.10	192.168.100.10	0.0.0.0	已启用	

At the bottom of the table are buttons for '全选' (Select All), '启用' (Enable), '禁用' (Disable), '删除' (Delete), and '搜索' (Search).

图 5.6 DHCP服务配置界面-配置地址池参数

服务接口	选择需要提供DHCP服务的接口。
地址池	选择已创建的地址池。请查看 配置IP地址池 部分内容来创建地址池。地址池需要与接口地址在同一网段，否则将无法配置成功。对于特殊地址包括接口的IP地址、主机位为0的网络地址和主机位全为1的网络广播地址，本路由器不会进行分配。
地址租期	输入此地址池中的IP地址在每次分配后可供客户端使用的租期。
网关地址	输入此地址池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	输入此地址池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	输入此地址池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	输入此地址池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。
启用/禁用规则	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 5.3 DHCP服务配置界面条目项说明

配置完成的地址池信息会在下方DHCP服务器列表区域显示出来，如下图所示。

DHCP服务列表									
选择	序号	服务接口	地址池	租期	网关地址	首选DNS服务器	备选DNS服务器	状态	设置
<input type="checkbox"/>	1	eth0	管理部门	120	192.168.1.1	192.168.1.1	0.0.0.0	已启用	
<input type="checkbox"/>	2	soft_dep	软件部门	120	192.168.100.10	192.168.100.10	0.0.0.0	已启用	

图 5.7 DHCP服务配置界面-地址池列表

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

2. 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 >> 静态地址分配

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<新增>按钮手动创建地址池。

静态地址

MAC地址：

IP地址：

服务接口：

备注： (可选)

是否生效： 生效 不生效

地址列表							
选择	序号	MAC地址	IP地址	服务接口	备注	状态	设置
<input type="checkbox"/>	1	00-19-66-80-54-38	192.168.100.1 50	soft_dep	---	已启用	

图 5.8 DHCP服务配置界面-创建地址池

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。
生效接口	选择保留IP地址所属的接口。
备注	输入字符串描述该静态地址以便识别。
是否生效	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 5.4 静态地址分配界面条目说明

**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地址池中的地址；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。

地址列表							
选择	序号	MAC地址	IP地址	服务接口	备注	状态	设置
<input type="checkbox"/>	1	00-19-66-80-54-38	192.168.100.1 50	soft_dep	---	已启用	
<input type="checkbox"/>	2	00-19-66-80-54-36	192.168.1.10	eth0	---	已启用	

图 5.9 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 >> 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。

3. 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-ER6520G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。

客户端列表					
序号	主机名	服务接口	MAC地址	IP地址	剩余租期
1	---	eth0	00-19-66-80-54-36	192.168.1.10	永久
2	---	soft_dep	00-19-66-80-54-38	192.168.100.150	永久

刷新 搜索 帮助

图 5.10 DHCP服务器客户端列表

5.1.4 DHCP功能组网应用

图 5.11为某企业网络的一个分支，网络需求如下：

- 路由器TL-ER6520G为中心路由器，在路由器上将研发部门划分在一个区段内进行管理。
- 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。
- 在TL-ER6520G路由器上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。

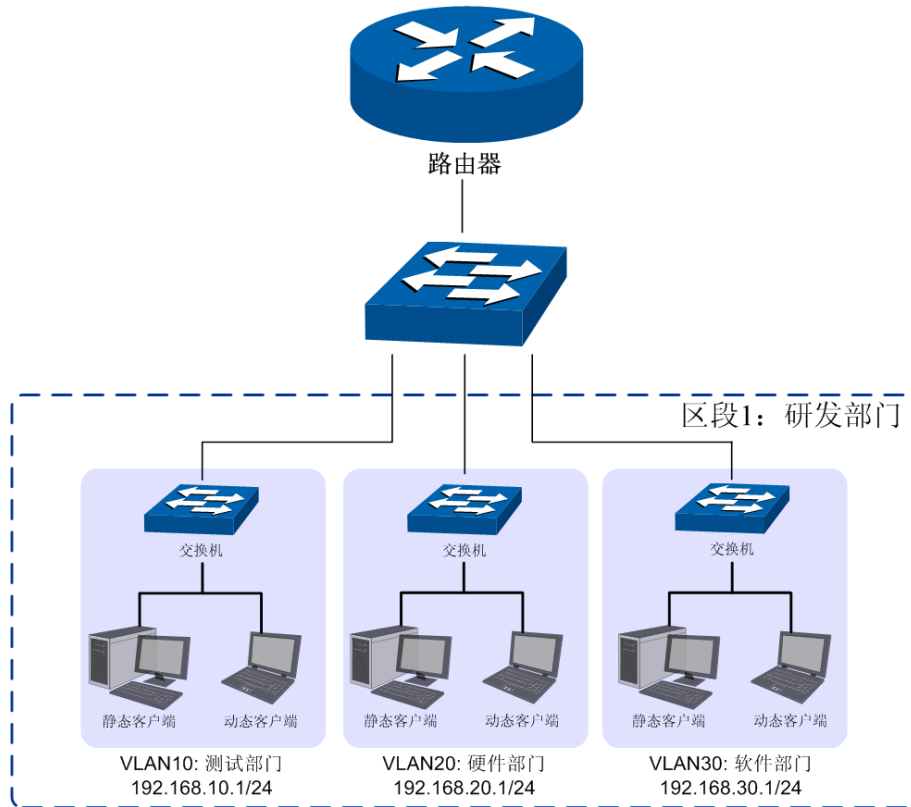


图 5.11 DHCP服务器功能组网举例

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VLAN。必须操作，具体操作步骤请参考VLAN章节[配置VLAN步骤](#)。需要为研发部门各小组配置不同VLAN，如测试部门属于VLAN10，硬件部门属于VLAN20，软件研发部门属于VLAN30。
- 2) 创建区段，同时配置区段下的网络接口。必须操作。创建界面：基本设置 >> 区段设置 >> 区段设置，在此界面的左列点击< + >按钮，在弹出的添加区段对话框中输入新区段的名称，点击<确定>按钮完成。
- 3) 创建eth接口。必须操作。创建界面：基本设置 >> 区段设置 >> 区段设置，为研发各子部门创建eth类型接口，如硬件小组创建eth接口，命名为“hard_dep”，接口地址设置为192.168.20.1/24并与VLAN20关联；为软件小组创建eth类型接口，命名为“soft_dep”，接口地址设置为192.168.30.1/24并与VLAN30关联。
- 4) 创建IP地址池。必须操作。创建界面：基本设置 >> 对象管理 >> IP地址池，为研发各小组创建可供DHCP分配的IP地址池，如硬件小组创建IP地址池，命名为“硬件地址池”，并设置可供分配的地址池为192.168.20.51-192.168.20.100。

- 5) 配置DHCP服务器。必须操作。配置界面：基本设置 >> DHCP >> DHCP服务，如此处为硬件小组关联的接口“hard_dep”配置DHCP服务参数，选择关联的IP地址池为“硬件地址池”，同时配置网关参数为“hard_dep”的接口地址192.168.20.1。



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功能相关内容，请参考说明书中的**4.3 VLAN设置**章节。
- 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6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 6.1所示的快速配置向导，单击<下一步>，可以开始设置。



图 6.1 快速配置向导设置界面

本向导提供两种路由器系统模式选择：NAT网关模式和路由模式，如图 6.2所示。请根据实际需求选择系统模式，然后单击<下一步>，开始设置。

- **NAT网关模式：**路由器作为网关应用在局域网与广域网之间。该模式下，可以为路由器配置1-4个WAN口，还可以为路由器配置1个硬件DMZ口。
- **路由模式：**路由器连接两个不同区域的网络，这两个区域的主机都必须通过路由规则进行通信。该模式下，可以将路由器划分为1-5个区段，同时为每一个区段配置一个eth接口。

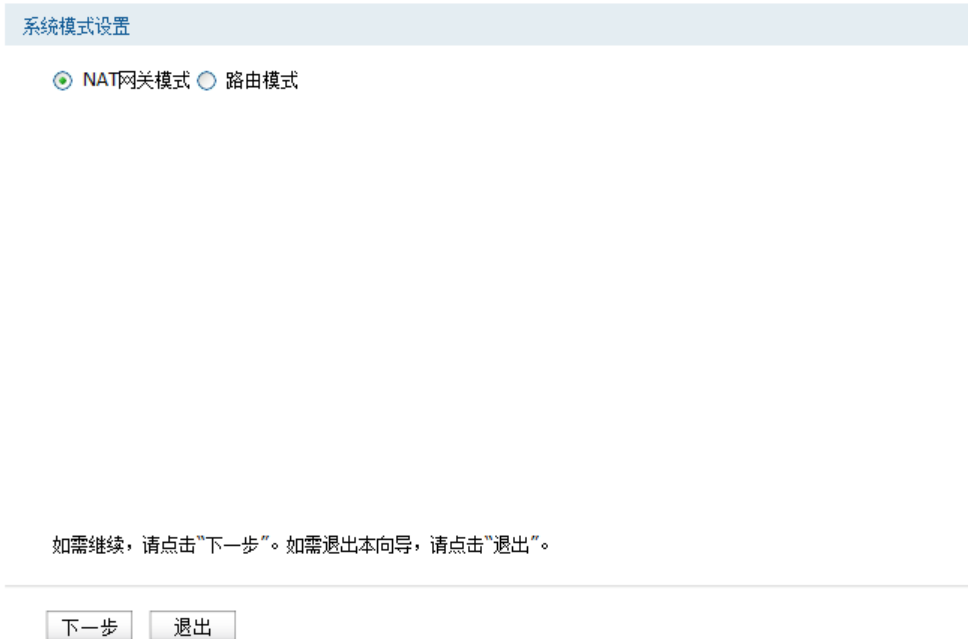


图 6.2 快速配置设置界面-系统模式设置

6.1 NAT网关模式

在系统模式设置界面, 选择NAT网关模式, 如图 6.3所示。单击<下一步>, 可以进入NAT模式-接口模式设置界面。

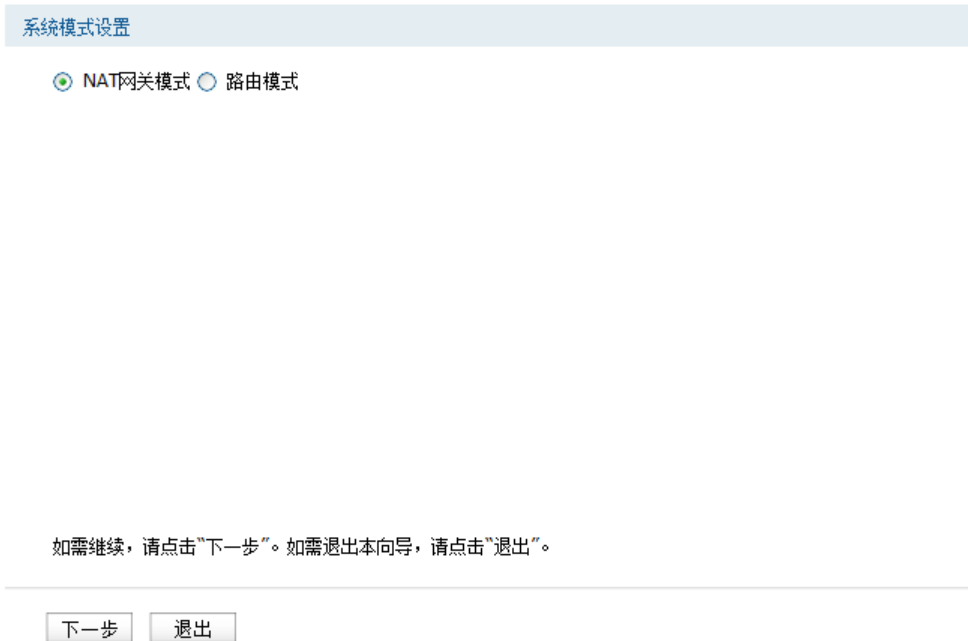


图 6.3 快速配置设置界面-系统模式设置-NAT网关模式

6.1.1 WAN设置



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。

NAT模式-接口模式设置

在NAT模式-接口模式设置界面，如图 6.4所示，可以根据实际需求选择WAN数量，以及勾选是否开启硬件DMZ。单击<下一步>，可以进入NAT模式-NAT-WAN1设置界面。

本路由器支持多种WAN口模式：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。

若开启硬件DMZ，则端口5为DMZ口；不开启，则端口5为LAN口。当WAN数量选择为四WAN口时，硬件DMZ无法开启，此时端口5只能为LAN口。硬件DMZ默认为关闭状态。



如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

图 6.4 快速配置设置界面-NAT模式-接口模式设置

NAT模式-NAT-WAN1设置

在NAT模式-NAT-WAN1设置界面，如图 6.5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。

NAT模式-NAT-WAN1设置

■ WAN1
 ■ LAN
 ■ LAN
 ■ LAN
 ■ DMZ

连接方式：

IP地址：

子网掩码：

网关地址：（可选）

首选DNS服务器：（可选）

备用DNS服务器：（可选）

上行带宽： Kbps

下行带宽： Kbps

如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

图 6.5 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 6.1 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 6.6 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 6.2 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。

NAT模式-NAT-WAN1设置

WAN1
 LAN
 LAN
 LAN
 DMZ

连接方式：

账号：

密码：

上行带宽： Kbps

下行带宽： Kbps

如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

图 6.7 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 6.3 WAN口设置界面PPPoE连接方式条目项说明

如果在图 6.4 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。

6.1.2 LAN设置

NAT模式-NAT-LAN设置

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。

NAT模式-NAT-LAN设置

WAN1
LAN
LAN
LAN
DMZ

IP地址：

子网掩码：

DHCP服务器： 开启 关闭

起始IP地址：

结束IP地址：

网关地址： (可选)

首选DNS服务器： (可选)

备用DNS服务器： (可选)

如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

上一步
下一步
退出

图 6.8 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 6.4 LAN口设置界面条目项说明

设置完成后，如果在图 6.4 NAT模式-接口模式设置界面开启了硬件DMZ，则单击<下一步>，可以进入NAT模式-NAT-DMZ设置界面。如果在图 6.4 NAT模式-接口模式设置界面没有开启硬件DMZ，则进入完成快速配置向导界面。

6.1.3 DMZ设置

1. DMZ简介

DMZ (Demilitarized Zone, 非军事区域) 也称隔离区。如果在图 6.4 NAT模式-接口模式设置界面开启了硬件DMZ，则路由器端口5为DMZ口，允许所有接入此端口的本地主机暴露在广域网中，进行一些特别的网络应用服务，如各种共享服务器、视频会议等。

DMZ物理接口可以工作在两种模式下，广域网模式或局域网模式。

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

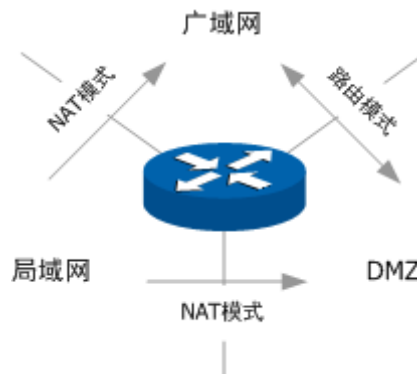


图 6.9 DMZ口工作于广域网模式

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

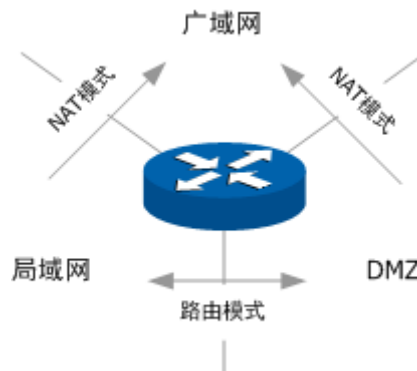


图 6.10 DMZ口工作于局域网模式

2. DMZ设置

NAT模式-NAT-DMZ设置

在NAT模式-NAT-DMZ设置界面，可以选择DMZ接口的工作模式：广域网或局域网。

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

DMZ接口工作于局域网模式，其设置同LAN设置，需要设置路由器DMZ口的IP参数，以及DMZ口DHCP服务。

设置完成后，单击<下一步>，可以进入完成快速配置向导界面。

NAT模式-NAT-DMZ设置

WAN1 LAN LAN LAN DMZ

DMZ模式： 广域网 局域网

IP地址：

子网掩码：

DHCP服务器： 开启 关闭

起始IP地址：

结束IP地址：

网关地址： (可选)

首选DNS服务器： (可选)

备用DNS服务器： (可选)

如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

图 6.11 快速配置设置界面-NAT模式-NAT-DMZ设置

DMZ模式	通过选择接口模式，可以控制DMZ区域与广域网、局域网之间的连接方式。默认为局域网模式。
IP地址	设置DMZ口的IP地址。默认为192.168.2.1。
子网掩码	设置DMZ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。默认为关闭。
起始IP地址	设置DHCP服务器自动分配IP地址的起始地址。
结束IP地址	设置DHCP服务器自动分配IP地址的结束地址。
网关地址	设置DHCP分配给客户端的网关地址，允许留空。

首选DNS服务器	设置DNS地址，允许留空。
备用DNS服务器	设置备用DNS地址，允许留空。

表 6.5 DMZ口设置界面条目项说明

完成快速配置向导

在**完成快速配置向导**界面，如图 6.12所示，可以查看配置的所有参数，如需修改，请单击<上一步>，退回到之前的设置界面修改，如果设置符合需求，请单击<完成>，完成快速配置。路由器完成配置需要几分钟，请耐心等待。快速配置生效之后，需要重新登录路由器。



图 6.12 快速配置设置界面-完成快速配置向导

6.2 路由模式

在**系统模式设置**界面，选择路由模式，如图 6.13所示，单击<下一步>，可以进入**ROUTE模式-接口设置**界面。

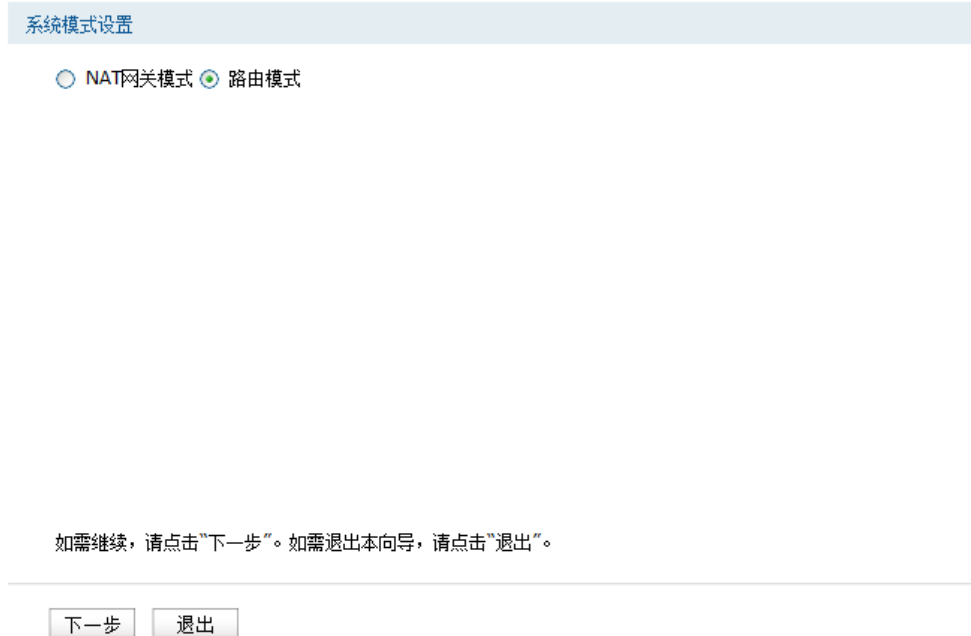


图 6.13 快速配置设置界面-系统模式设置-路由模式

ROUTE模式-接口设置

在**ROUTE模式-接口设置**界面，如图 6.14所示，可以根据实际需求设置接口数目，设置范围为1-5。单击<下一步>，可以进入**ROUTE模式-接口1设置**界面。

设置接口数目为1，路由器只划分一个区段，端口1-5全在同一个区段内，IP地址为接口1设置的地址。设置接口数目为2，路由器划分两个区段，端口1为一个区段，IP地址为接口1设置的地址；端口2-5为另外一个区段，IP地址为接口2设置的地址。设置接口数目为3或4或5，规则类似。



图 6.14 快速配置设置界面-ROUTE模式-接口设置

ROUTE模式-接口1设置

在**ROUTE模式-接口1设置**界面，如图 6.15所示，可以根据实际需求设置接口IP地址和子网掩码。

如果在图 6.14**ROUTE模式-接口设置**界面，设置的接口数目大于1，则接口1设置完成后，单击<下一步>，会进入其他接口设置界面。每个接口设置的IP地址都不能与其他接口地址相同。所有接口设置完成后，单击<下一步>，可以进入**完成快速配置向导**界面。



图 6.15 快速配置设置界面-ROUTE模式-接口1设置

IP地址	设置接口的IP地址，此将作为该区段eth接口的IP地址。默认为0.0.0.0。
子网掩码	设置接口的子网掩码，此将作为该区段eth接口的子网掩码。默认为255.255.255.0。

表 6.6 接口设置界面条目项说明

完成快速配置向导

在完成快速配置向导界面，如图 6.16所示，可以查看配置的所有参数，如需修改，请单击<上一步>，退回到之前的设置界面修改，如果设置符合需求，请单击<完成>，完成快速配置。路由器完成配置需要几分钟，请耐心等待。快速配置生效之后，需要重新登录路由器。

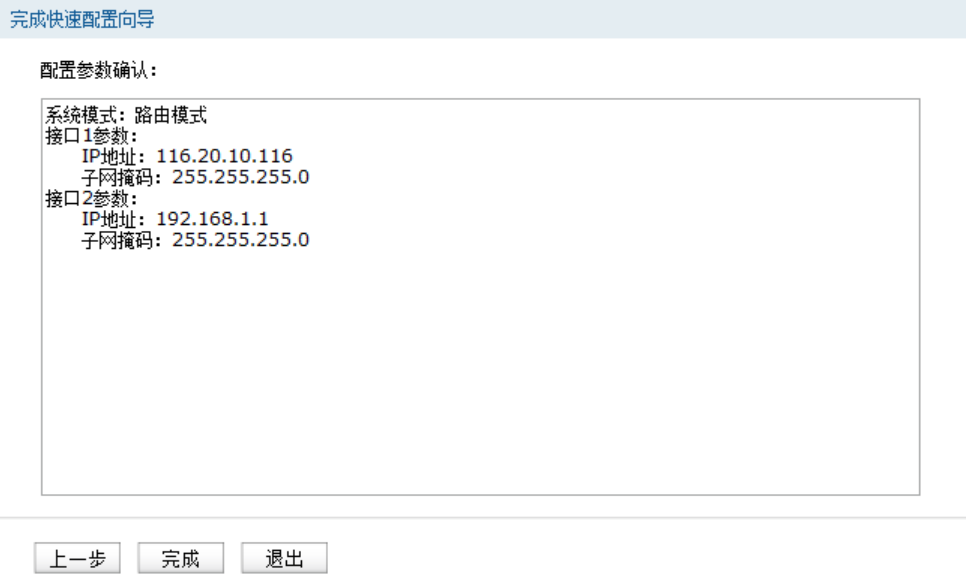


图 6.16 快速配置设置界面-完成快速配置向导

第7章 对象管理



说明：

对象管理中所有功能的条目，点击<新增>添加成功后，将不能修改条目名称。

7.1 地址管理

7.1.1 地址组

可以在本页面设置自定义组，以方便对用户进行组管理。

进入界面：对象管理 >> 地址管理 >> 地址组

组设置

名称：

备注： (可选)

组列表

选择	序号	组名称	备注	设置
<input type="checkbox"/>	1	IPGROUP_ANY	IPGRP_ANY	---
<input type="checkbox"/>	2	g_lan_ip	lan_ip	

图 7.1 组设置界面

组名称	输入一个名称来标识一个组，可以输入1~50个字符。
备注	添加对当前组的说明信息。

表 7.1 组设置界面项说明

新增的条目会在组列表里显示出来，如下图所示。

组列表

选择	序号	组名称	备注	设置
<input type="checkbox"/>	1	IPGROUP_ANY	IPGRP_ANY	---
<input type="checkbox"/>	2	g_lan_ip	lan_ip	

图 7.2 组设置界面-组列表

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，不可操作。

7.1.2 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

地址设置

名称：

IP类型： IP段 IP/Mask

-

备注： (可选)

地址列表

选择	序号	名称	IP类型	IP	备注	设置
<input type="checkbox"/>	1	IP_ANY	IP/MASK	0.0.0.0/0	IP_ANY	---

图 7.3 用户设置界面

名称	输入一个名称来标识地址，可以输入1~50个字符。
IP类型	在此建立源地址范围。主要有以下2种表示方式。 IP段：由起始IP地址到结束IP地址确定IP地址范围。 IP/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 7.2 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。

地址列表

选择	序号	名称	IP类型	IP	备注	设置
<input type="checkbox"/>	1	IP_ANY	IP/MASK	0.0.0.0/0	IP_ANY	---
<input checked="" type="checkbox"/>	2	地址	IP段	1.1.1.1 - 1.1.1.12	---	

图 7.4 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。

7.1.3 视图

可以在此添加地址到特定的组中。

进入界面：对象管理 >> 地址管理 >> 视图



图 7.5 视图界面

组名	在下拉菜单中选择所需设置的组。
可选用户	显示该组可以包含的地址或子组。在 可选用户 列表中，选择一个地址或子组，点击< >> >按钮将其移至 包含用户 列表中后，此地址就包含在所选的组中。
包含用户	显示该组已经包含的地址或子组。在 包含用户 列表中，选择一个地址或子组，点击<<< <<按钮将其移至 可选用户 列表中后，此地址就会从该组中被移除。

表 7.3 视图界面项说明

7.2 时间管理

7.2.1 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

时间对象

名称：

工作日历：

工作时间：

备注：

时间对象列表

选择	序号	名称	工作日历	工作时间	备注	设置
<input type="checkbox"/>	1	Any			---	---
<input type="checkbox"/>	2	t3	time_1	time_2	3	

图 7.6 时间管理界面

名称	自定义的时间对象名称。注意不能与已有的时间对象的名称重复，且名称长度不能超过50个字符。
工作日历	选择一个日历对象。工作日历表示时间对象的年月日。工作日历设置请参考7.2.2工作日历。
工作时间	选择一个工作时间对象。工作时间指明时间对象每日的时间段，由时分来记录。工作时间设置请参考7.2.3工作时间。
备注	输入对时间对象的具体描述。

表 7.4 时间管理界面项说明

新增的条目会在**时间对象列表**里显示出来，如下图所示。

时间对象列表

选择	序号	名称	工作日历	工作时间	备注	设置
<input type="checkbox"/>	1	Any			---	---
<input type="checkbox"/>	2	t3	time_1	time_2	3	

图 7.7 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。

7.2.2 工作日历

可以通过本页面创建工作日历对象，供时间对象使用。

进入界面：[对象管理](#) >> [时间管理](#) >> [工作日历](#)

工作日历

名称：

备注：

日历设置：

2000年							所有日期	日	一	二	三	四	五	六																						
清除							全选		清除		清除		清除		清除		全选																			
1月		2月			3月			4月			5月		6月			7月			8月			9月			10月			11月			12月					
日 一 二 三 四 五 六		日 一 二 三 四 五 六			日 一 二 三 四 五 六			日 一 二 三 四 五 六			日 一 二 三 四 五 六		日 一 二 三 四 五 六			日 一 二 三 四 五 六			日 一 二 三 四 五 六			日 一 二 三 四 五 六			日 一 二 三 四 五 六			日 一 二 三 四 五 六								
2 3 4 5 6 7 8		6 7 8 9 10 11 12			5 6 7 8 9 10 11			2 3 4 5 6 7 8			2 3 4 5 6 7 8		4 5 6 7 8 9 10			2 3 4 5 6 7 8			6 7 8 9 10 11 12			10 11 12 13 14 15 16			14 15 16 17 18 19 20			18 19 20 21 22 23 24			22 23 24 25 26 27 28			26 27 28 29 30		
9 10 11 12 13 14 15		13 14 15 16 17 18 19			12 13 14 15 16 17 18			9 10 11 12 13 14 15			9 10 11 12 13 14 15		11 12 13 14 15 16 17			9 10 11 12 13 14 15			13 14 15 16 17 18 19			17 18 19 20 21 22 23			21 22 23 24 25 26 27			25 26 27 28 29 30			29 30 31					
16 17 18 19 20 21 22		20 21 22 23 24 25 26			19 20 21 22 23 24 25			16 17 18 19 20 21 22			16 17 18 19 20 21 22		18 19 20 21 22 23 24			16 17 18 19 20 21 22			20 21 22 23 24 25 26			24 25 26 27 28 29			28 29 30 31			30 31								
23 24 25 26 27 28 29		27 28 29			26 27 28 29 30 31			23 24 25 26 27 28 29			23 24 25 26 27 28 29		30 31			30 31			27 28 29 30 31			27 28 29 30 31			27 28 29 30 31			27 28 29 30 31								
30 31																																				
2001年1月																																				
日 一 二 三 四 五 六																																				
1 2 3 4 5 6																																				
7 8 9 10 11 12 13																																				
14 15 16 17 18 19 20																																				
21 22 23 24 25 26 27																																				
28 29 30 31																																				

工作日历列表

选择	序号	日历名称	工作日历	备注	设置
该列表为空					

图 7.8 工作日历设置界面

名称	自定义的工作日历名称。不能与已有的工作日历的名称重复，且名称长度不能超过50个字符。
备注	输入对工作日历的具体描述。

表 7.5 工作日历界面项说明

日历设置

日历由两部分组成：

- 年份：在下拉列表中选择工作日历生效的年份。
- 日历：根据所选择的年份，将显示当前年份12个月和次年1月份的日历，可在此选择所需工作日期。默认为选择除周末外的全部日期。

选择工作日期的基本操作有：

- 单击某一日，则这一日将被选中，设置为工作日期；再次单击则取消选中，该日被设置为非工作日期。
- 每个星期日期对应一个<清除>/<全选>按钮，以星期一为例介绍此按钮操作：只要日历中有星期一被选中，按钮显示<清除>，点击按钮，则日历中所有星期一被设置为非工作日期；若日历中没有星期一被选中，按钮显示<全选>，点击按钮，则日历中所有星期一被设置为工作日期。所有日期对应的按钮操作方法类似。

新增的条目会在**工作日历列表**里显示出来，如下图所示。

工作日历列表					
选择	序号	日历名称	工作日历	备注	设置
<input type="checkbox"/>	1	workdate		---	 

图 7.9 工作日历列表

如有需要，可以点击条目后的按钮进行编辑。

7.2.3 工作时间

可以通过本页面创建工作时间对象，以供时间对象模块使用。

进入界面：对象管理 >> 时间管理 >> 工作时间

工作时间

名称：

备注：

时间段：: - :

: - :

工作时间列表

选择	序号	名称	时间段	备注	设置
该列表为空					

图 7.10 工作时间设置界面

名称	自定义的工作时间名称。不能与已有的工作时间的名称重复，且名称长度不能超过50个字符。
备注	输入对工作时间的具体描述。
时间段	<p>时间段指明时间对象在每一日中生效的具体的时间片段。一个工作时间条目最多允许配置8个时间段。</p> <p>时间段由两个部分组成： 开始时间：时间段的起始时间，由时分组成，格式为（00:00）。 结束时间：时间段的截止时间，由时分组成，格式为（00:00）。</p> <p>时间段的每个设置框最多允许输入两位数字，可输入范围为时（0-24），分（0-59），一个设置框中输入完两位数字后，将自动跳转到下一个设置框。输入完成后，点击<+>按钮添加时间段，点击<->可以删除已经添加的时间段。</p>

表 7.6 工作时间界面项说明

新增的条目会在**工作时间列表**里显示出来，如下图所示。

工作时间列表

选择	序号	名称	时间段	备注	设置
<input type="checkbox"/>	1	time_2	00:00-08:00	---	

图 7.11 工作时间设置界面-工作时间列表

如有需要，可以点击条目后的按钮进行编辑。

**说明：**

- 对于每个工作时间条目而言，其多个日时间段之间不能重叠。
- 每个日时间段的开始时间必须早于等于结束时间。

7.3 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**

地址池设置

地址池名称：

地址池范围： -

启用/禁用： 启用 禁用

地址池列表

选择	序号	地址池名称	地址池范围	状态	设置
<input type="checkbox"/>	1	lan_pool	192.168.1.2-192.168.1.254	已启用	

图 7.12 IP地址池设置界面

地址池名称	自定义地址池的名称。
地址池范围	由地址池起始IP和地址池结束IP组成，且地址池起始IP必须不大于地址池结束IP，而且不能与已有的地址池范围重叠。当前一个地址池最多可以包含1024个IP地址。
启用/禁用	选择启用或禁用IP地址池条目。

表 7.7 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。

地址池列表

选择	序号	地址池名称	地址池范围	状态	设置
<input type="checkbox"/>	1	lan_pool	192.168.1.2-192.168.1.254	已启用	

图 7.13 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，点击按钮启用条目，点击按钮禁用条目。

7.4 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](#)

服务类型

服务名称：

协议类型： TCP UDP TCP/UDP ICMP Other

源端口范围： -

目的端口范围： -

备注： (可选)

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

图 7.14 服务类型设置界面

服务名称	自定义服务的名称。
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。
ICMP	输入ICMP协议的类型(type)和编码(code)，填充255时表明所有类型/编码。
备注	输入对服务类型的具体描述。

表 7.8 服务类型界面项说明

第8章 传输控制

当完成网络中的区段划分且为各区段建立了接口后，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：

8.1 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时，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。

8.2 带宽控制：各区段之间发送数据时，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。

8.3 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。

8.4 流量均衡：流量均衡功能采用带宽均衡、选路、线路备份等技术，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。

8.5 路由设置：利用静态路由功能以及动态路由协议RIP，可以保证数据包在网络中以正确的路径进行快速转发。

8.1 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。

1. 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 8.1 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。

2. 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。

3. 本设备的NAT特性

本设备提供了下列六种NAT相关功能特性：

8.1.1 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。

8.1.2 一对一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。

8.1.3 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。

8.1.4 端口触发：当网络中存在某些特殊应用，比如网络游戏MSN Gaming Zone、IP电话和视频会议等，需要设置端口触发功能，保证此类应用能够正常运行。

8.1.5 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。

8.1.6 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。

8.1.1 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。

1. 配置NAPT

进入界面: 传输控制 >> NAT设置 >> NAPT

在界面的NAPT规则区域,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<新增>按钮手动添加条目。

The screenshot shows the NAPT configuration interface. At the top, there is a 'NAPT规则' (NAPT Rule) section with the following fields:

- 规则名称 (Rule Name): nat2
- 源地址范围 (Source IP Range): 192.168.1.0 / 24
- 出接口 (Outgoing Interface): eth0
- 备注 (Remarks): (Optional)
- 启用/禁用规则 (Enable/Disable Rule): 启用 (Enabled) 禁用 (Disabled)

 Below these fields are buttons for '新增' (Add), '清除' (Clear), and '帮助' (Help).

 The middle section is a '映射列表' (Mapping List) table:

选择	序号	规则名称	源地址范围	出接口	状态	备注	设置
<input type="checkbox"/>	1	nat2	192.168.0.0/24	eth0	已启用	---	

 At the bottom of the table are buttons for '全选' (Select All), '启用' (Enable), '禁用' (Disable), '删除' (Delete), and '搜索' (Search).

图 8.2 NAPT界面-设置NAPT规则

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

启用/禁用规则	选择“启用”，则使该规则条目生效； 选择“禁用”，则使该规则条目失效。
----------------	--

表 8.1 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。

NAPT规则

规则名称：

源地址范围： /

出接口：

备注： (可选)

启用/禁用规则： 启用 禁用

映射列表

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

图 8.3 NAPT界面-映射列表

如图所示，“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。

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。

NAPT规则

规则名称：

源地址范围： /

出接口：

备注： (可选)

启用/禁用规则： 启用 禁用

映射列表

选择	序号	规则名称	源地址范围	出接口	状态	备注	设置
该列表为空							

图 8.4 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。

2. 应用环境

如图 8.5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-ER6520G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。

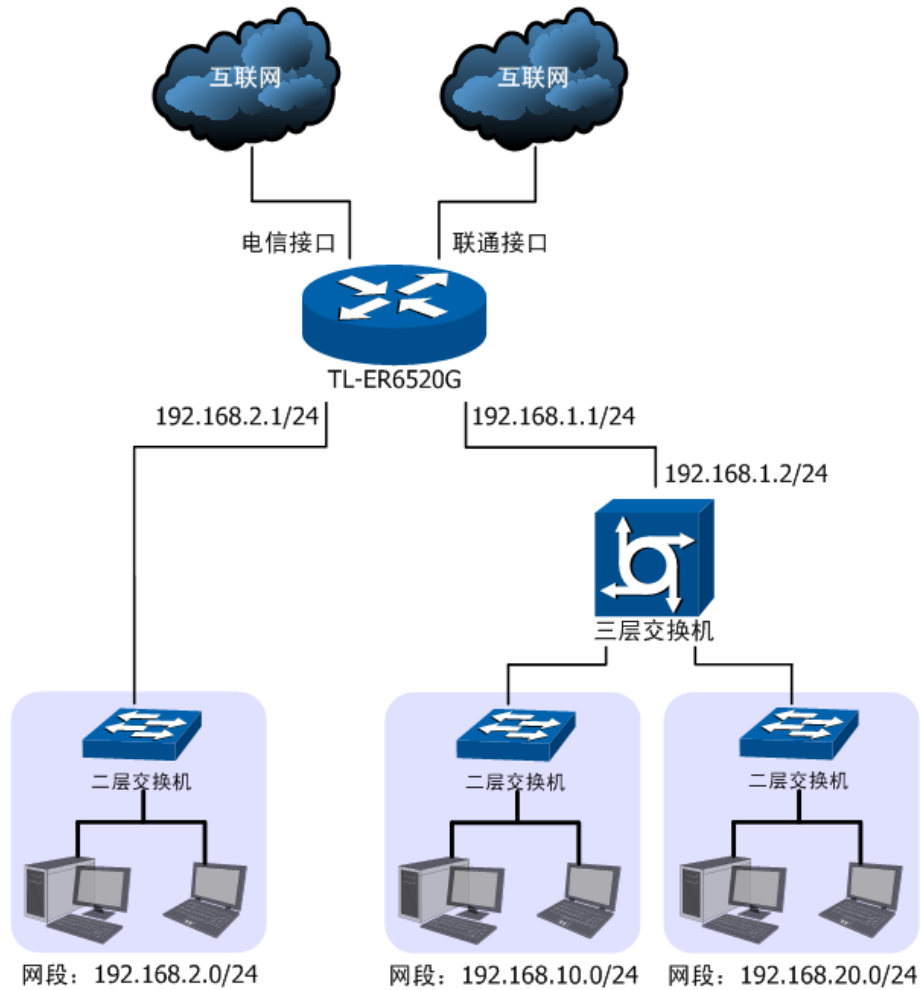


图 8.5 NAPT功能组网应用

配置步骤：

TL-ER6520G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。
- 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 8.6所示。

静态路由规则

名称：

目的地址：

子网掩码：

下一跳：

出接口：

Metric： (0-15)

备注： (可选)

启用/禁用规则： 启用 禁用

图 8.6 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8.5 路由设置。

8.1.2 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。

1. 配置一对一NAT

进入界面：传输控制 >> NAT设置 >> 一对一NAT

在界面的一对一NAT映射区域，填入映射规则地址参数并选择数据包转发接口，点击<新增>按钮手动添加条目。

NAT映射

映射名称：

映射地址： ->

出接口：

DMZ转发： 开启 关闭

备注： (可选)

启用/禁用规则： 启用 禁用

映射列表

选择	序号	名称	映射前地址	映射后地址	出接口	DMZ转发	状态	备注	设置
该列表为空									

图 8.7 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。
映射地址	输入服务器的局域网IP地址和提供NAT地址转换的IP地址。第一个输入框中应填写局域网IP地址，第二个输入框中应填写映射后的IP地址。
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。
DMZ转发	设置是否开启该条NAT映射条目的DMZ转发。开启DMZ转发后，规则生效接口收到目的IP地址为映射后地址的数据包时，将把数据包转发给局域网服务器。如果广域网用户需要自由的访问局域网服务器，需要开启DMZ转发，若不开启，路由器将拒绝用户对服务器的访问。
备注	添加对本条目的说明信息，非必填项。
启用/禁用规则	选择“启用”，则使该规则条目生效； 选择“禁用”，则使该规则条目失效。

表 8.2 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。

NAT映射

映射名称：

映射地址： ->

出接口：

DMZ转发： 开启 关闭

备注： (可选)

启用/禁用规则： 启用 禁用

选择	序号	名称	映射前地址	映射后地址	出接口	DMZ转发	状态	备注	设置
<input type="checkbox"/>	1	http服务器	192.168.1.10	201.0.0.1	isp1	关闭	已启用	---	

图 8.8 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“isp1”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“isp1”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“isp1”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。

2. 应用环境

如图 8.9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8.1.1 NAPT进行配置。

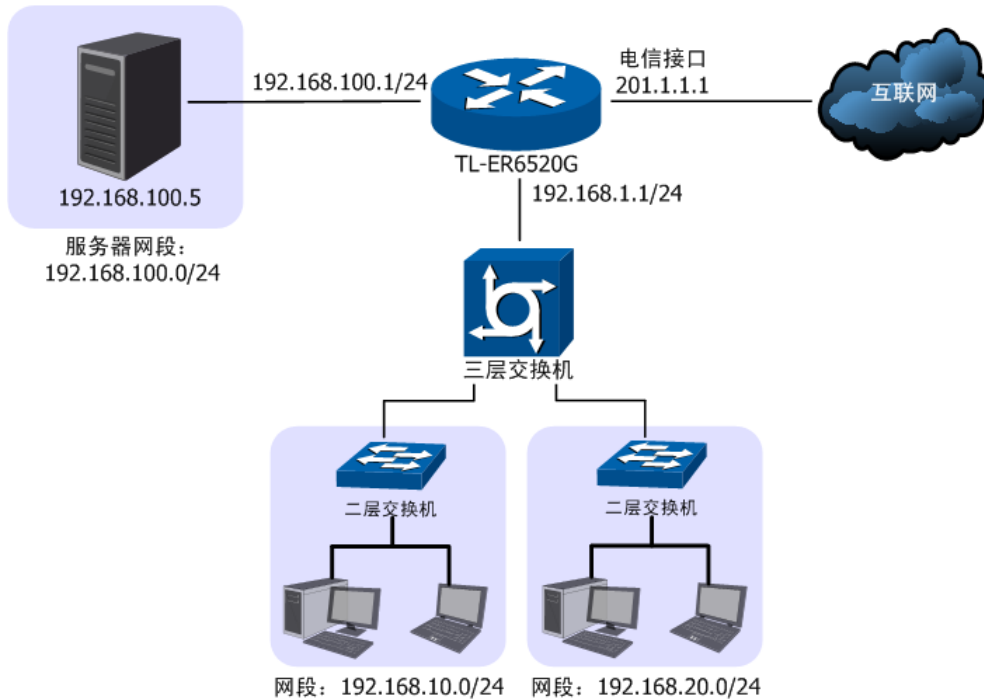


图 8.9 一对一NAT功能组网应用

配置步骤：

TL-ER6520G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, 为其他上网区段配置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8.5 路由设置。

8.1.3 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。

1. 配置虚拟服务器

进入界面：传输控制 >> NAT设置 >> 虚拟服务器

在界面的**虚拟服务**区域，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<新增>按钮手动添加条目。

虚拟服务

接口： isp1

服务名称： web服务器

外部端口： 12892 - 12892

内部端口： 80 - 80

服务协议： TCP/UDP

内部服务器IP： 192.168.100.5

启用/禁用规则： 启用 禁用

新增 清除 帮助

服务列表

选择	序号	服务名称	接口	服务协议	外部端口	内部端口	内部服务器IP	状态	设置
该列表为空									

全选 启用 禁用 删除 搜索

图 8.10 虚拟服务器界面-设置虚拟服务器

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。
服务名称	输入该虚拟服务器的名称，例如可以根据服务器提供的服务特性命名。
外部端口	输入路由器提供给广域网访问时使用的端口，本例中使用12892端口。
内部端口	输入局域网服务器提供服务的端口，如本例中是80端口。

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)。
内部服务器IP	输入服务器的局域网IP地址。
启用/禁用规则	选择“启用”, 则使该规则条目生效; 选择“禁用”, 则使该规则条目失效。

表 8.3 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。

虚拟服务配置界面截图：

接口：isp1

服务名称：

外部端口： -

内部端口： -

服务协议：TCP/UDP

内部服务器IP：

启用/禁用规则： 启用 禁用

新增 清除 帮助

选择	序号	服务名称	接口	服务协议	外部端口	内部端口	内部服务器IP	状态	设置
<input type="checkbox"/>	1	web服务器	isp1	TCP/UDP	12892-12892	80-80	192.168.100.5	已启用	

全选 启用 禁用 删除 搜索

图 8.11 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。

2. 应用环境

如图 8.12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。

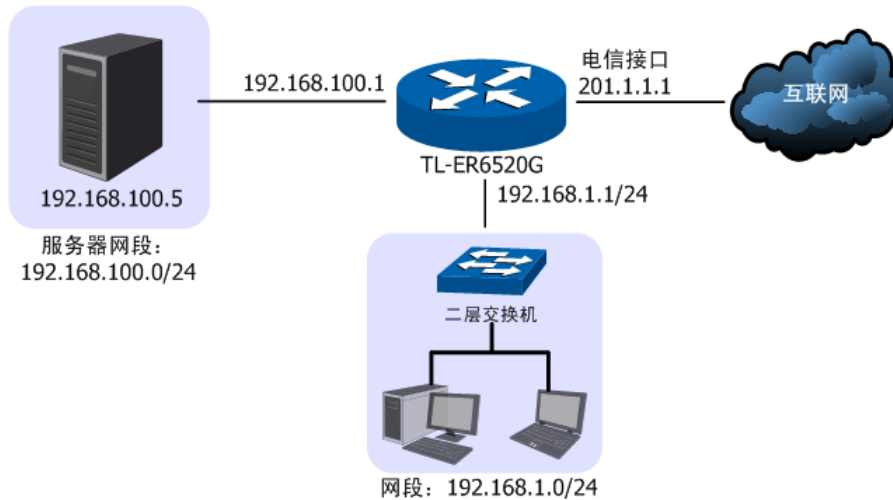


图 8.12 虚拟服务器功能组网应用

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12.2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>

8.1.4 端口触发

当局域网内的客户端访问因特网上的服务器时，对于某些应用，比如网络游戏Sudden Strike、IP电话和视频会议等，客户端向服务器主动发起连接的同时，也需要服务器向客户端发起连接请求。而缺省情况下，路由器上面面向广域网的接口启用了NAPT特性后，会拒绝此接口收到的主动连接请求，此时通信会被中断。

通过设置端口触发功能，在局域网用户向广域网设备发起访问请求时，如果端口为触发端口，则打开数据包转发接口的开放端口，供后续通信使用。当客户端和路由器长时间没有数据交互时，路由器会自动关闭因通信而对外开放的端口，最大限度地保证了局域网的安全。

下表是常见的可能用到端口触发功能的网络应用，当此类应用无法正常运行时请根据下表设置端口触发功能。如果网络应用不在下表统计范围内，请咨询相关应用服务商。

程序名称	开放端口	触发端口
Dialpad	7175	51200-51201, 51210
ICU II	2019	2000-2038, 2050-2051, 2069, 2085, 3010-3030
MSN Gaming Zone	47624	2300-2400, 28800-29000
PC-to-Phone	12053	12120, 12122, 24150-24220
Quick Time 4	554	6970-6999
AOE II Client	47624	2300-2400, 28800-29000
Sudden Strike	47624	2300-2400
Baldurs Gate II	47624	2300-2400

表 8.4 特殊网络应用传输端口列表

1. 配置端口触发

进入界面：传输控制 >> NAT设置 >> 端口触发

在界面的端口触发区域，填入网络应用的开放端口和触发端口，点击<新增>按钮手动添加条目。



图 8.13 端口触发界面-设置端口触发

接口	选择规则生效接口。当路由器收到触发端口的访问请求时，将从此接口转发数据包，以接口IP地址做NAT地址转换，但不转换传输层协议端口，同时打开此接口的相关开放端口。
服务名称	输入服务条目的名称，名称长度需在28个字符以内，中英文均可，一个中文占用2个字符空间。
触发端口	输入触发端口，即应用程序首先发起连接的一个或多个端口。只有该端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。
触发协议	选择在触发端口上使用的数据包传输层协议类型。
开放端口	输入为应用程序提供服务的一个或多个端口。当触发端口上收到连接后，出接口的开放端口打开，应用程序便可以通过这些开放端口发起后续连接。
开放协议	选择在开放端口上使用的数据包传输层协议类型。
启用/禁用规则	选择“启用”，则使该规则条目生效； 选择“禁用”，则使该规则条目失效。

表 8.5 端口触发界面条目项说明

新增的条目会在**触发列表**中显示出来，如下图所示。

端口触发

接口：

服务名称：

触发端口：（支持XX,XX-XX的格式）

触发协议：

开放端口：（支持XX,XX-XX的格式）

开放协议：

启用/禁用规则： 启用 禁用

触发列表

选择	序号	服务名称	接口	触发协议	触发端口	开放协议	开放端口	状态	设置
<input type="checkbox"/>	1	Quick Time 4	isp1	TCP/UDP	554	TCP/UDP	6970-6999	已启用	

图 8.14 端口触发界面-触发列表

如图所示，图中的规则表示当路由器收到TCP或UDP端口为554的访问请求时，通过“isp1”接口转发数据包，使用接口地址对数据包进行地址转换但不转换传输层协议端口，同时打开“isp1”接口的传输层协议端口6970-6999；

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：

- 触发端口与开放端口的取值范围均为1-65535之间的任意整数。开放端口取值可以指定一个连续的范围，如8690-8696。
- 路由器支持16条端口触发规则，每条规则最多支持5组触发端口，且这些触发端口不能重叠。
- 每条规则最多支持5组开放端口，每条规则的开放端口数总和需小于或等于100。
- 请根据实际需要配置端口触发功能，避免黑客利用开放的端口进行网络攻击。

8.1.5 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时就可能会出现问題。

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。
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。
IPsec	当IPsec隧道需要通过本路由器时，需要启用IPsec 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。

表 8.6 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 8.15 ALG服务界面-设置ALG服务

路由器支持五种特殊应用的ALG服务。默认情况下，五种ALG服务均已经启用，建议保持默认值不做改变。

8.1.6 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。

1. 配置NAT DMZ

进入界面：传输控制 >> NAT设置 >> NAT DMZ

在界面的NAT DMZ服务区域，填写DMZ主机的局域网IP地址以及数据包转发接口，点击<新增>按钮手动添加条目。

The screenshot shows the NAT DMZ configuration interface. At the top, there is a form for adding a new service. The fields are: 服务名称 (Service Name) with the value 'bbs', 主机地址 (Host Address) with the value '192.168.200.10', and 接口 (Interface) with a dropdown menu showing 'isp1'. Below these fields are radio buttons for 启用/禁用规则 (Enable/Disable Rule), with '启用' (Enable) selected. At the bottom of the form are three buttons: 新增 (Add), 清除 (Clear), and 帮助 (Help).

Below the form is a table titled 服务列表 (Service List). The table has columns: 选择 (Select), 序号 (Serial Number), 服务名称 (Service Name), 主机地址 (Host Address), 接口 (Interface), 状态 (Status), and 设置 (Settings). The table is currently empty, with the text '该列表为空' (This list is empty) centered below the header. Below the table are five buttons: 全选 (Select All), 启用 (Enable), 禁用 (Disable), 删除 (Delete), and 搜索 (Search).

图 8.16 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。
内部服务器IP	输入DMZ主机的局域网IP地址。
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。
启用/禁用规则	选择“启用”，则使该规则条目生效； 选择“禁用”，则使该规则条目失效。

表 8.7 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。

The screenshot shows the NAT DMZ configuration interface. The form at the top is identical to the previous screenshot, but the 服务列表 (Service List) table now contains one entry. The entry has a checkbox in the 选择 (Select) column, the number '1' in the 序号 (Serial Number) column, 'bbs' in the 服务名称 (Service Name) column, '192.168.200.10' in the 主机地址 (Host Address) column, 'isp1' in the 接口 (Interface) column, and '已启用' (Enabled) in the 状态 (Status) column. In the 设置 (Settings) column, there are two icons: a pencil (edit) and a red circle with a slash (delete). Below the table are the same five buttons: 全选 (Select All), 启用 (Enable), 禁用 (Disable), 删除 (Delete), and 搜索 (Search).

图 8.17 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。

8.2 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。

1. 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

在界面的功能设置区域，设置智能带宽控制功能，点击<设置>按钮保存配置。

功能设置

仅当带宽利用率达到 80 % 以上时，带宽控制功能生效

设置

带宽控制规则

规则名称： rule1

数据流向： RD -> default

受控地址类型： 源地址 目的地址

受控地址范围： 192.168.10.100 - 192.168.10.200

带宽模式： 独立 共享

最大限制带宽： 1000 Kbps (0或100-1000000, 0表示不限制)

规则生效时间： Any

启用/禁用规则： 启用 禁用

新增 清除 帮助

规则列表

选择	序号	规则名称	数据流向	受控地址类型	受控地址范围	模式	最大限制带宽	生效时间	状态	设置
该列表为空										

全选 启用 禁用 删除 搜索

图 8.18 带宽控制规则界面-功能设置

勾选此项启用智能带宽控制，仅当带宽利用率达到指定百分比时，所有带宽控制规则生效。若不勾选，则所有带宽控制规则实时生效。

2. 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

在界面的带宽控制规则区域，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<新增>按钮手动添加条目。



图 8.19 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。
数据流向	设置此带宽控制规则生效的数据流向。第一个框选择发送数据的源区段，假设为区段1；第二个框表示数据转发的目标区段，假设为区段2。则此带宽控制规则对从区段1发往区段2的数据包生效。
受控地址类型	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。
受控地址范围	设置IP地址范围，此处的IP地址范围与上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。
带宽模式	独立模式即受控地址范围内每一个IP地址都将应用当前规则所设置的带宽限制；共享模式即受控地址范围内所有IP地址带宽总和为当前规则所设置的带宽限制。
最大限制带宽	设置受控计算机所能使用的最大限制带宽。
规则生效时间	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。
启用/禁用规则	选择“启用”，则使该规则条目生效； 选择“禁用”，则使该规则条目失效。

表 8.8 带宽控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。

功能设置

仅当带宽利用率达到 % 以上时，带宽控制功能生效

带宽控制规则

规则名称：

数据流向： ->

受控地址类型： 源地址 目的地址

受控地址范围： -

带宽模式： 独立 共享

最大限制带宽： Kbps (0或100-1000000, 0表示不限制)

规则生效时间：

启用/禁用规则： 启用 禁用

规则列表

选择	序号	规则名称	数据流向	受控地址类型	受控地址范围	模式	最大限制带宽	生效时间	状态	设置
<input type="checkbox"/>	1	rule1	RD -> default	源地址	192.168.10.100-192.168.10.200	共享	1000	Any	已启用	

图 8.20 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：RD区段中IP地址为192.168.10.100到192.168.10.200的计算机发往default区段的通信数据将共享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) 设置区段的带宽控制属性。必须操作。创建界面：基本设置 >> 区段设置。根据受控对象的所属接口，在各接口界面中设置是否参与带宽控制。对于每一条带宽控制规则，源区段和目的区段相应的接口均需要参与带宽控制。
- 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 >> 带宽控制规则。根据受控对象的网络参数设置带宽控制规则。

8.3 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。

1. 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。

The screenshot shows the configuration interface for connection number limits. It is divided into two main sections: '功能设置' (Function Settings) and '连接数限制规则' (Connection Number Limit Rules).

功能设置 (Function Settings):

- A checkbox labeled '启用连接数限制' (Enable Connection Number Limit) is checked.
- A '设置' (Settings) button is located below the checkbox.

连接数限制规则 (Connection Number Limit Rules):

- '名称' (Name): An empty text input field.
- '受控地址范围' (Controlled Address Range): A dropdown menu currently set to 'IPGROUP_ANY'.
- '最大连接数' (Maximum Connections): A text input field with '(30-1000)' next to it.
- '启用/禁用规则' (Enable/Disable Rule): Radio buttons for '启用' (Enable) and '禁用' (Disable), with '启用' selected.
- Buttons: '新增' (Add), '清除' (Clear), and '帮助' (Help).

规则列表 (Rule List):

选择	序号	名称	组	最大连接数	状态	设置
该列表为空						

Buttons below the table: '全选' (Select All), '启用' (Enable), '禁用' (Disable), '删除' (Delete), and '搜索' (Search).

图 8.21 连接数限制界面-功能设置

勾选此项以启用连接数控制。不勾选时，所有连接数限制均不生效。

2. 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

在界面的**连接数限制规则**区域，选择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，点击<新增>按钮手动添加条目。



图 8.22 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。
受控地址范围	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。请在对象管理章节设置地址组。
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。
启用/禁用规则	选择“启用”，则使该规则条目生效； 选择“禁用”，则使该规则条目失效。

表 8.9 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。

功能设置

启用连接数限制

连接数限制规则

名称：

受控地址范围：

最大连接数： (30-1000)

启用/禁用规则： 启用 禁用

规则列表

选择	序号	名称	组	最大连接数	状态	设置
<input type="checkbox"/>	1	rule1	RD	1000	已启用	

图 8.23 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“RD”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。

3. 监控连接数

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，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**，点击<新增>按钮手动添加条目。

监控列表

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 8.24 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。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 >> 连接数限制规则。根据受控对象的需要设置不同的最大连接数。

8.4 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，策略选路等，同时支持线路备份功能。要使**流量均衡**中功能生效，首先必须开启**在线检测**。本章节将详细介绍流量均衡的功能实现和配置方法。

8.4.1 基本设置

1. 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。

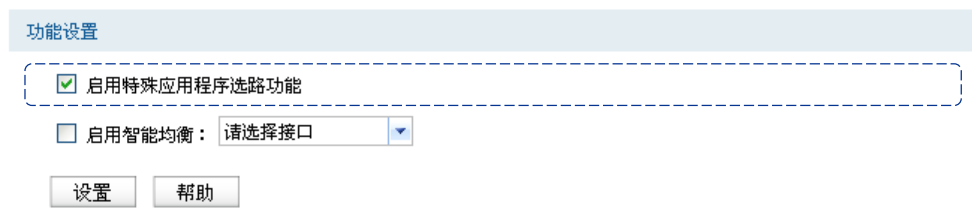


图 8.25 基本设置-特殊应用程序选路功能界面

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。

2. 智能均衡

若要使“智能均衡”生效，必须先在**基本设置 >> 区段设置**界面设置接口带宽。

进入界面：基本设置 >> 区段设置

在界面的**接口设置**区域选择将要参与智能均衡的接口，并设置接口上行带宽和下行带宽，且勾选参与流量均衡选项。

· 接口设置

eth2 eth1 eth0 +

接口类型：

接口状态：已连接

接口地址：

网关地址：

VLAN：

连接方式：

IP地址：

子网掩码：

网关地址： (可选)

MTU： (576-1500)

首选DNS服务器： (可选)

备用DNS服务器： (可选)

MAC地址：

上行带宽： Kbps (100-1000000)

下行带宽： Kbps (100-1000000)

开放端口池： -

参与带宽控制

参与流量均衡

属于管理接口

图 8.26 智能均衡 - 接口设置

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。

功能设置

启用特殊应用程序选路功能

启用智能均衡：

eth2

eth1

图 8.27 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。

8.4.2 策略选路

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。

1. 策略选路设置

进入界面：[传输控制](#) >> [流量均衡](#) >> [策略选路](#)

在界面的**选路规则设置**区域填入策略名称，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<新增>按钮手动添加条目。

图 8.28 策略选路设置界面




策略名称	用户自定义，标识一条选路规则。
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7.4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7.1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7.1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7.2时间管理小节。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条策略选路规则。

表 8.10 策略选路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。

规则列表										
选择	序号	策略名称	协议	源地址	目的地址	生效接口	生效时间	备注	状态	设置
<input type="checkbox"/>	1	test_1	ALL	IP_ANY	IP_ANY	eth2	Any	---	已启用	 

图 8.29 策略选路设置界面-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。

2. 策略选路典型应用

某企业的网络需求如下：

TL-ER6520G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-ER6520G路由器：

- 1) 创建VLAN。必须操作，具体操作步骤请参考VLAN章节[配置VLAN步骤](#)。配置不同VLAN，如VLAN10，VLAN20。
- 2) 创建区段，同时配置区段下的网络接口。必须操作。创建界面：基本设置 >> 区段设置 >> 区段设置，在此界面的左列点击< + >按钮，在弹出的添加区段对话框中输入新区段的名称，点击<确定>按钮完成。
- 3) 创建eth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。
- 4) 在传输控制 >> 流量均衡 >> 策略选路界面创建如下两条规则：
- 5) 指定FTP数据包由“eth1”接口转发。

选路规则设置	
策略名称：	<input type="text" value="test_1"/>
服务类型：	<input type="text" value="FTP"/>
源地址：	<input type="text" value="IP_ANY"/>
目的地址：	<input type="text" value="IP_ANY"/>
生效接口：	<input type="text" value="eth1"/>
生效时间：	<input type="text" value="Any"/>
备注：	<input type="text"/> (可选)
启用/禁用规则：	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
<input type="button" value="新增"/> <input type="button" value="清除"/> <input type="button" value="帮助"/>	

指定 HTTP 数据包由“eth2”接口转发。

8.4.3 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。

1. 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 8.30 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 8.31 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<新增>手动添加ISP选路条目。

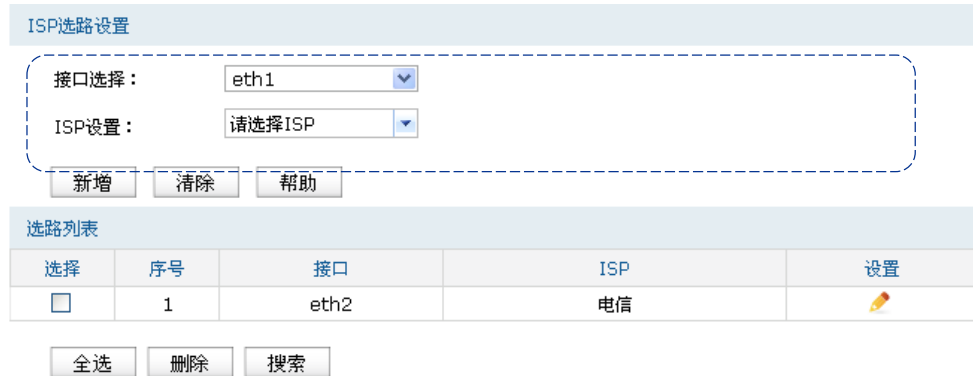


图 8.32 ISP选路界面-ISP选路设置

接口选择	选择进行ISP选路的接口。
ISP设置	在下拉列表中选择ISP。

表 8.11 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。

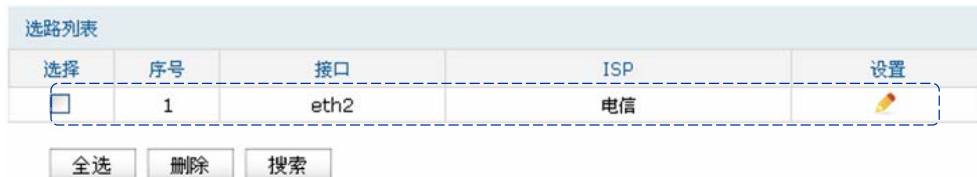


图 8.33 ISP选路界面-选路列表

如有需要，可以点击条目后的<✎>按钮进行编辑。



说明：

智能均衡、策略选路、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：策略选路 > ISP选路 > 智能均衡。

2. 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-ER6520G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-ER6520G路由器：

- 1) 创建VLAN。必须操作，具体操作步骤请参考VLAN章节[配置VLAN步骤](#)。配置不同VLAN，如VLAN10，VLAN20。

- 2) 创建区段，同时配置区段下的网络接口。必须操作。创建界面：基本设置 >> 区段设置 >> 区段设置，在此界面的左列点击< + >按钮，在弹出的添加区段对话框中输入新区段的名称，点击<确定>按钮完成。
- 3) 创建eth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。
- 4) 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。
- 5) 在传输控制 >> 流量均衡 >> 基本设置界面，启用ISP选路功能。TL-ER6520G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。

选路功能设置

启用ISP地址段选路功能

导入ISP数据库

数据库版本: 1.6

数据库路径: 未选择文件

ISP选路设置

接口选择:

ISP设置:

选路列表

选择	序号	接口	ISP	设置
<input type="checkbox"/>	1	eth1	电信	
<input type="checkbox"/>	2	eth2	联通	

8.4.4 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。

1. 设置线路备份

进入界面：传输控制 >> 流量均衡 >> 线路备份

在界面的**备份设置**区域，设置主备接口并选择备份模式，点击<新增>按钮手动添加条目。



图 8.34 线路备份界面-备份设置

主接口选择	选择主接口。接口设置请参考4.2.2接口设置。
备接口选择	选择备接口。接口设置请参考4.2.2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，下方可进行故障备份设置。
备份生效时间	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7.2时间管理。
故障备份	当备份模式为故障备份时，需要在此选择故障备份条件，在主接口正常工作时备份接口不工作，只有当符合故障备份条件时才会启动备份接口。
启用/禁用规则	选择启用或禁用本条线路备份规则。

表 8.12 线路备份功能设置界面项说明

新增的条目会在主备组列表里显示出来，如下图所示。



图 8.35 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。具体可以在系统工具 >> 诊断工具 >> 在线检测界面进行设置。
- 每个主备组中，主/备接口必须处于同一区段。

2. 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-ER6520G路由器：

- 1) 创建VLAN。必须操作，具体操作步骤请参考VLAN章节[配置VLAN步骤](#)。配置不同VLAN，如VLAN10，VLAN20。
- 2) 创建区段，同时配置区段下的网络接口。必须操作。创建界面：基本设置 >> 区段设置 >> 区段设置，在此界面的左列点击< + >按钮，在弹出的添加区段对话框中输入新区段的名称，点击<确定>按钮完成。
- 3) 创建eth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。
- 4) 开启在线检测。必须操作。创建界面：系统工具 >> 检测工具 >> 在线检测，开启对eth1接口和eth2接口的在线检测。
- 5) 在传输控制 >> 流量均衡 >> 策略选路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。

备份设置

主接口选择：

备接口选择：

备份模式： 定时备份 故障备份

故障备份： 任意主线路故障启用备份线路
 所有主线路故障启用备份线路

启用/禁用规则： 启用 禁用

主备组列表

选择	序号	主接口组	备接口组	备份模式	生效时间	状态	设置
该列表为空							

8.5 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、静态路由和RIP三种路由特性。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，下面将详细介绍**静态路由、RIP服务**。

8.5.1 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。

1. 配置静态路由

进入界面：传输控制 >> 路由设置 >> 静态路由

在界面的**静态路由规则**区域，输入静态路由各项参数，点击<新增>按钮手动添加条目。



图 8.36 静态路由界面-设置静态路由

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

表 8.13 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。

静态路由规则

名称：

目的地址：

子网掩码：

下一跳：

出接口：

Metric： (0-15)

备注： (可选)

启用/禁用规则： 启用 禁用

规则列表

选择	序号	名称	目的地址	子网掩码	下一跳	出接口	Metric	状态	备注	设置
<input type="checkbox"/>	1	rule1	192.168.3.0	255.255.255.0	192.168.1.2	eth0	0	已启用	---	

图 8.37 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。

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。

2. 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。

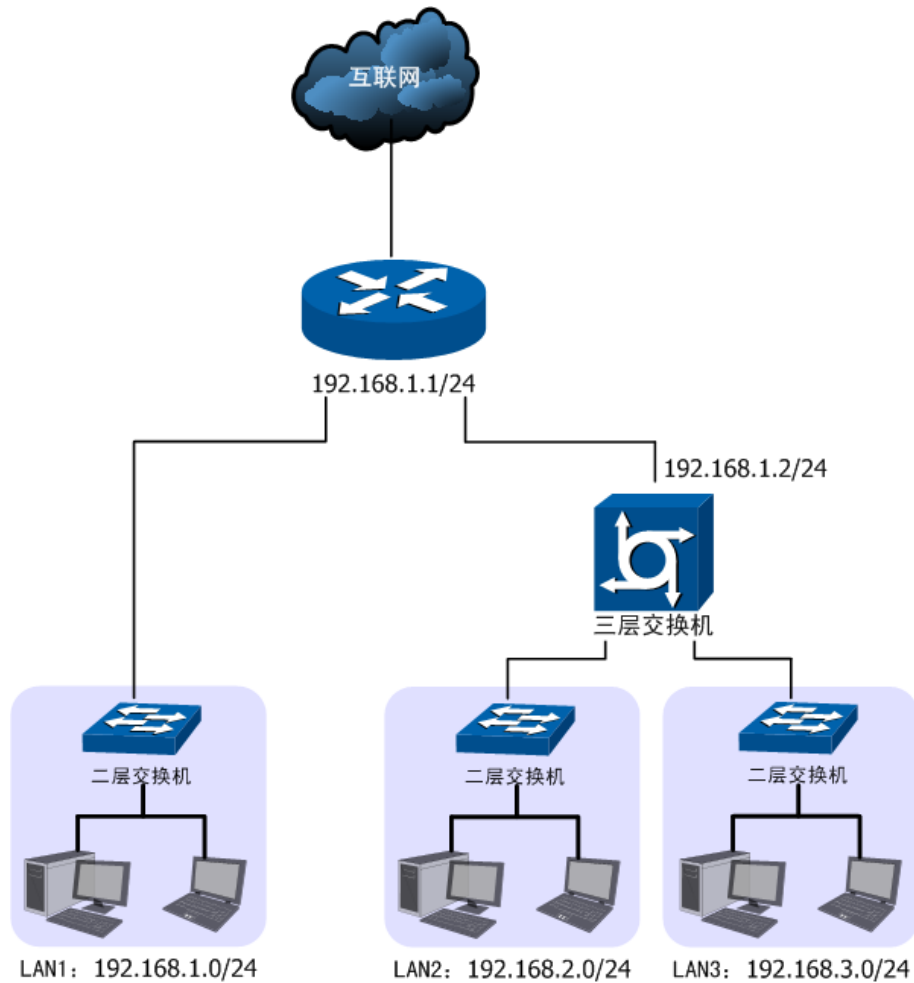


图 8.38 静态路由功能组网应用

配置步骤：

TL-ER6520G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 >> 区段设置 >> 区段设置。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<新增>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<新增>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”

8.5.2 RIP服务

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

RIP协议报文在传输层都以UDP协议进行封装, 源和目的端口都使用520。RIP定义了两种报文类型: 请求报文和响应报文。请求报文用来向邻居发送一个路由请求, 响应报文用来传送路由更新。RIP的度量是基于“跳”数的, 1跳表示与发出报文的路由器直接连接的网络, 16跳表示网络不可达。最优路径即跳数最少的网络链路。如果到相同目标有二个不等速或不同带宽的路由器, 但跳跃计数相同, 则RIP认为两个路由是等距离的, 此时路由器将执行等价路径的负载均衡。

开始时, RIP从每个启用RIP协议的接口广播请求报文。接着, RIP程序进入一个循环状态, 不断地侦听来自其他路由器的RIP请求或响应报文, 而收到请求的邻居路由器则应答包含它们的路由表的响应报文。RIP每隔30秒通过UDP报文以广播形式交换一次路由信息, 并以此更新自己的路由表。如果在180秒内未收到某一路由条目的信息, 则RIP协议就会将该条路由的距离设定成无穷大, 并删除路由表中相关信息。

RIP协议在应用中不断地被完善, 从最初的RIPv1版本基础上逐渐发展出了RIPv2版本的协议。RIPv2相较RIPv1还支持VLSM (Variable Length Subnet Mask, 可变长子网掩码)、简单明文认证、MD5密文认证、CIDR (Classless Inter-Domain Routing, 无类型域间选路) 和多播, 相对于RIPv1应用更加灵活。详细的RIP协议内容请参考RFC 1058。

TL-ER6520G同时支持RIPv1和RIPv2两种版本的协议, 可以根据实际的网络需求设置, 以提高网络性能。

1. 配置RIP服务

进入界面：传输控制 >> 路由设置 >> RIP服务

在界面的RIP服务设置区域，设置RIP协议相关特性，点击<新增>按钮手动添加条目。

RIP服务设置

接口：

接口状态： 启用 禁用

输出版本：

密码认证：

RIP服务条目

选择	序号	接口	接口状态	输出版本	密码认证	设置
该列表为空						

RIP路由表

序号	目的地址	子网掩码	下一跳	出接口	跳数	路由时间
该列表为空						

图 8.39 RIP服务界面-设置RIP服务

接口	选择需要运行RIP协议的接口，例如，局域网规模较大且是三层交换式网络时，可以在连接局域网的接口上运行RIP协议。
接口状态	选择“启用”，则使该接口启用RIP协议； 选择“禁用”，则使该接口禁用RIP协议。
输出版本	选择相应接口的RIP协议版本。其中RIPv2支持多播和广播两种形式。
密码认证	如果应用RIPv2协议版本，可以根据实际网络情况设置密码认证，认证密码不超过15位。由于RIP协议报文没有加密且多数协议分析器都提供RIP报文的封装格式，因此RIP路由器很容易被虚假的RIP报文欺骗。密码认证是防止这类攻击的最佳方法。RIP提供简单认证和MD5两种认证方法，启用密码认证后，接口上收到的所有未经认证的RIP协议报文都会被丢弃。

表 8.14 RIP服务界面条目项说明



说明：

- 当接口连接到了ISP网络，请勿开启RIP协议。
- 只有eth接口才可以设置RIP服务。
- 网络中的路由器需要运行于相同的RIP协议版本，才能有效地进行路由信息交互。

新增的RIP服务接口信息会在**RIP服务条目**中显示出来，如下图所示。

RIP服务设置

接口：

接口状态： 启用 禁用

输出版本：

密码认证：

RIP服务条目

选择	序号	接口	接口状态	输出版本	密码认证	设置
<input type="checkbox"/>	1	dmz_eth1	启用	V2多播	不启用	

RIP路由表

序号	目的地址	子网掩码	下一跳	出接口	跳数	路由时间
1	1.2.2.0	255.255.255.0	1.2.2.1	dmz_eth 1	1	0
2	192.168.1.0	255.255.255.0	1.2.2.2	dmz_eth 1	2	26

图 8.40 RIP服务界面-RIP服务条目

如图所示，序号为1的RIP服务条目表示：启用接口“dmz_eth1”的RIP服务，使用协议版本为v2多播，且不进行密码认证。如有需要，可以点击条目后的按钮进行编辑。

接口运行了RIP服务后，将自动开始路由信息交互，接口直连网络的路由条目也会在**RIP路由表**中显示出来，如下图所示。

RIP服务设置

接口：

接口状态： 启用 禁用

输出版本：

密码认证：

RIP服务条目

选择	序号	接口	接口状态	输出版本	密码认证	设置
<input type="checkbox"/>	1	dmz_eth1	启用	V2多播	不启用	

RIP路由表

序号	目的地址	子网掩码	下一跳	出接口	跳数	路由时间
1	1.2.2.0	255.255.255.0	1.2.2.1	dmz_eth 1	1	0
2	192.168.1.0	255.255.255.0	1.2.2.2	dmz_eth 1	2	26

图 8.41 RIP服务界面-RIP路由表

如图所示，RIP路由表中的两条路由条目分别表示如下含义：

- RIP路由条目1：网络1.2.2.0/24可以通过接口“dmz_eth1”到达，跳数为1即表示该网络是接口“dmz_eth1”直接连接的网络，下一跳地址1.2.2.1则是接口的IP地址；
- RIP路由条目2：网络192.168.1.0/24可以通过接口“dmz_eth1”转发到网络节点1.2.2.2上，跳数为2，即表示从本地接口“dmz_eth1”发往该网络的数据包需要经过1个网络节点来转发。

第9章 安全管理

9.1 ARP防护

9.1.1 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。

1. ARP报文格式

ARP报文的格式如下图所示:

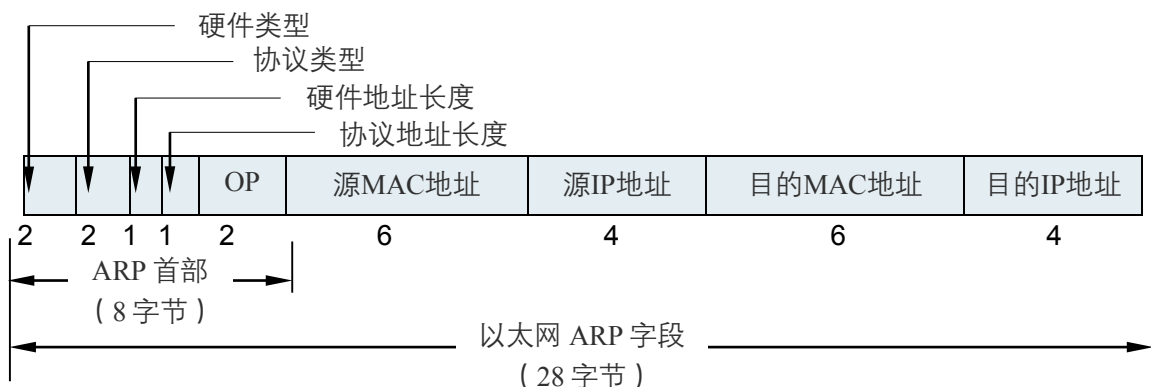


图 9.1 ARP报文格式

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 9.1 ARP报文字段含义

2. 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：

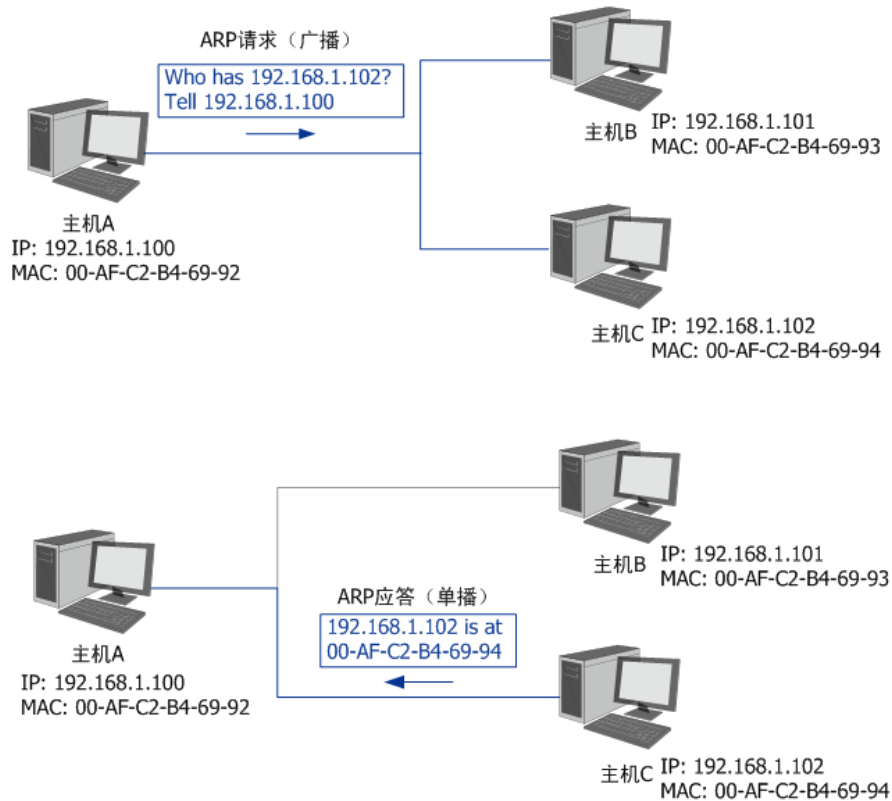


图 9.2 ARP解析过程

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。

9.1.2 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：假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。

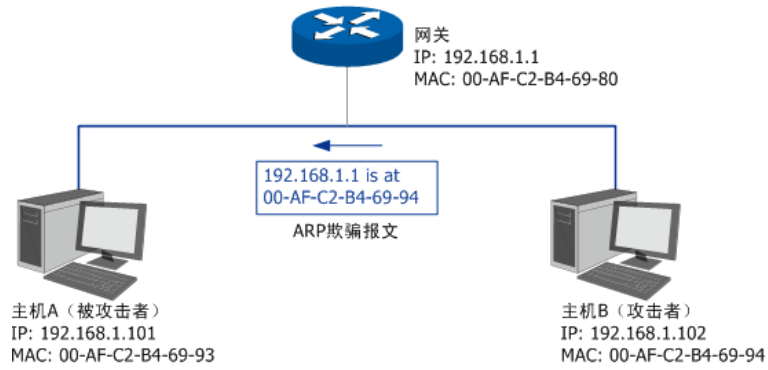


图 9.3 ARP欺骗-欺骗主机

- 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。

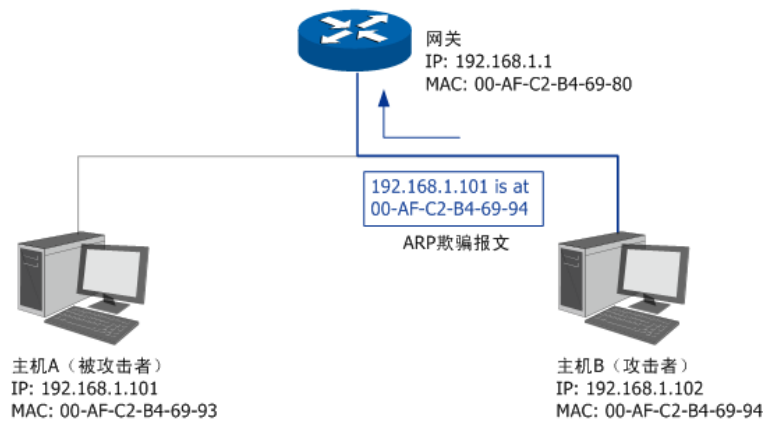


图 9.4 ARP欺骗-欺骗网关

- 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。

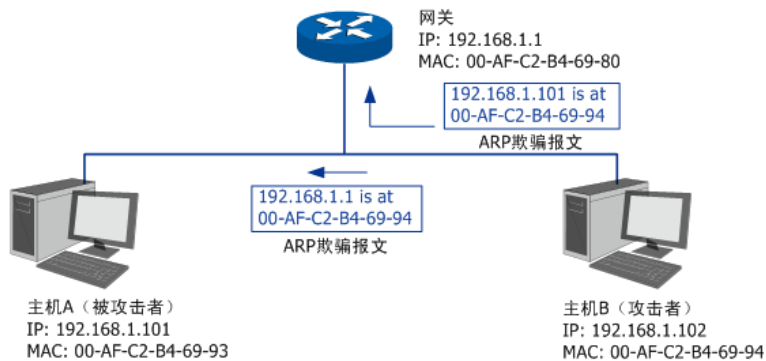


图 9.5 ARP欺骗-双向欺骗

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。

9.1.3 ARP攻击防护

1. 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绑定区域，填入需进行绑定的局域网主机IP、MAC地址信息，点击<新增>按钮手动添加条目。

功能设置

启用ARP防欺骗功能

仅允许IP MAC绑定的数据包通过路由器

生效区段：

允许路由器在发现ARP攻击时发送GARP包

发包间隔： 毫秒

启用ARP日志记录

设置

IP MAC绑定

IP地址：

MAC地址：

出接口：

备注： (可选)

是否生效： 启用 禁用

绑定列表

选择	序号	IP地址	MAC地址	出接口	备注	状态	设置
该列表为空							

图 9.6 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。
启用/禁用规则	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 9.2 IP MAC绑定界面条目说明

新增的条目会在**绑定列表**中显示出来。此时，以图 9.6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。

功能设置

启用ARP防欺骗功能

仅允许IP MAC绑定的数据包通过路由器

生效区段：

允许路由器在发现ARP攻击时发送GARP包

发包间隔： 毫秒

启用ARP日志记录

IP MAC绑定

IP地址：

MAC地址：

出接口：

备注： (可选)

是否生效： 启用 禁用

绑定列表

选择	序号	IP地址	MAC地址	出接口	备注	状态	设置
<input type="checkbox"/>	1	192.168.1.109	40-61-86-FC-75-C4	eth1	test_1	已启用	

图 9.7 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。



图 9.8 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。

如需将扫描结果全部绑定，请点击<全选>按钮，然后单击<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效，这些批量绑定的条目会出现在IP MAC绑定界面的绑定列表中。



图 9.9 ARP绑定列表

批量导入的条目备注一栏默认为import，如有需要，可以点击条目后的<>按钮进行编辑。完成批量绑定后再次扫描，会发现之前的IP MAC条目状态发生了改变。



图 9.10 ARP扫描状态变更

未绑定	表示当前条目未进入绑定列表，可能会被错误的ARP信息更替。
	表示当前条目已进入绑定列表，但还未生效。
	表示当前条目已绑定并生效，可以防御ARP攻击。

表 9.3 ARP绑定图标说明

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。

ARP列表					
选择	序号	IP地址	MAC地址	接口	状态
<input type="checkbox"/>	1	192.168.1.22	00-19-66-80-54-36	eth0	未绑定
<input type="checkbox"/>	2	192.168.1.109	40-61-86-FC-75-C3	eth0	未绑定

图 9.11 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全部绑定，请点击<全选>按钮，然后单击<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效，列表中的条目状态也会随之变更。

ARP列表					
选择	序号	IP地址	MAC地址	接口	状态
<input type="checkbox"/>	1	192.168.1.22	00-19-66-80-54-36	eth0	
<input type="checkbox"/>	2	192.168.1.109	40-61-86-FC-75-C3	eth0	

图 9.12 ARP列表状态变更



未绑定	表示当前条目未进入绑定列表，可能会被错误的ARP信息更替。
	表示当前条目已进入绑定列表，但还未生效。
	表示当前条目已绑定并生效，可以防御ARP攻击。

表 9.4 ARP绑定图标说明

这些批量绑定的条目会出现在**IP MAC绑定**界面的**绑定列表**中。

绑定列表							
选择	序号	IP地址	MAC地址	出接口	备注	状态	设置
<input type="checkbox"/>	1	192.168.1.22	00-19-66-80-54-36	eth0	import	已启用	 
<input type="checkbox"/>	2	192.168.1.109	40-61-86-FC-75-C3	eth0	import	已启用	 

图 9.13 ARP绑定列表

批量导入的条目备注一栏默认为import，如有需要，可以点击条目后的< >按钮进行编辑。

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。

2. 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 9.14 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。推荐勾选。
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。需要在下方选择生效区段。
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。
启用ARP日志记录	路由器会将ARP日志发送到指定的日志服务器中。日志服务器地址即 系统日志 章节中设置的服务器地址。推荐勾选。

表 9.5 ARP功能设置界面项说明

至此，在路由器上的ARP绑定操作就完成了。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。

9.2 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](#)

功能设置

启用防护攻击日志

防Flood类攻击

启用防多连接的TCP SYN Flood攻击 阈值： Pkt/s

启用防多连接的UDP Flood攻击 阈值： Pkt/s

启用防多连接的ICMP Flood攻击 阈值： Pkt/s

启用防固定源的TCP SYN Flood攻击 阈值： Pkt/s

启用防固定源的UDP Flood攻击 阈值： Pkt/s

启用防固定源的ICMP Flood攻击 阈值： Pkt/s

防可疑包攻击

启用防碎片包攻击

启用防TCP Scan(Stealth FIN/Xmas/Null)

启用防Ping of death

启用防Large ping

启用防WinNuke攻击

阻止同时设置FIN和SYN的TCP包

阻止仅设置FIN未设置ACK的TCP包

阻止带选项的IP包

安全限制

严格选路

流标记

空标记

宽松选路

记录路径

时间戳

图 9.15 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 9.6 攻击防护设置界面项说明

9.3 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**

功能设置

启用MAC地址过滤功能

仅允许规则列表的MAC地址访问外网

仅禁止规则列表的MAC地址访问外网

生效区段：

MAC地址过滤规则

名称：

MAC地址：

规则列表

选择	序号	名称	MAC地址	设置
该列表为空				

图 9.16 MAC过滤设置界面

功能设置

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

MAC地址过滤规则

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 9.7 MAC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MAC地址条目进行相应设置。

9.4 访问策略

9.4.1 基本概念

TL-ER6520G能够保障网络安全，具体做法是先检查要求从一个区段到另一区段的通路的所有连接尝试，然后予以允许或拒绝。

本路由器的默认行为是允许所有区段的所有接口直接通信，如图 9.17所示，路由器默认为全局路由模式。如需阻塞区段间的通信，可通过设置访问策略实现。同样，为了防止选定的区段内部信息流通过本路由器，也需要创建访问策略。

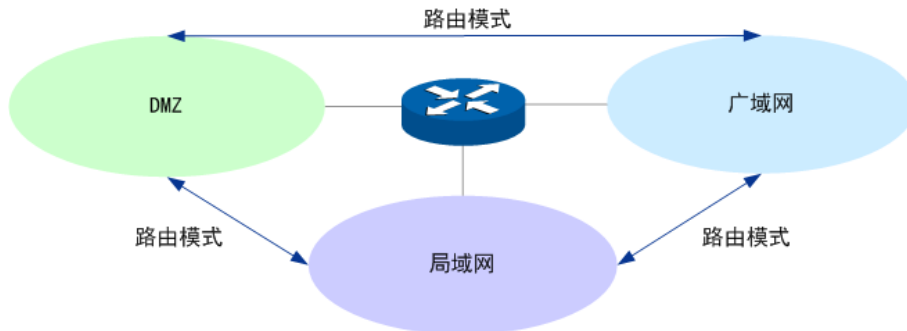


图 9.17 策略概念示意图一

在实际应用中，常常希望局域网内的主机可以共享上网，而广域网内的设备无法主动访问局域网内主机，即局域网与广域网之间的通信模式为NAT模式。这就需要在路由器上创建相应的策略。

如果DMZ区域以路由模式与广域网通信，则DMZ区域与广域网区域一样使用公有地址，不能主动访问局域网。那么，局域网与DMZ区域之间的通信应该为NAT模式，如图 9.18所示。

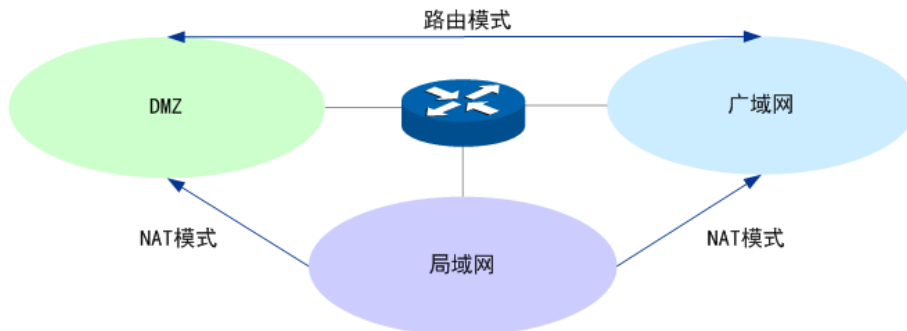


图 9.18 策略概念示意图二

此时，需要在路由器上创建局域网区段到广域网区段和局域网区段到DMZ区段的NAT规则，以及广域网区段到局域网区段和DMZ区段到局域网区段的阻塞策略，如图 9.19所示。

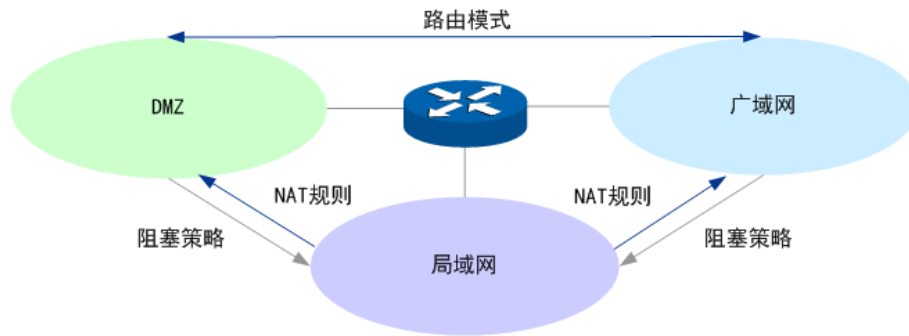


图 9.19 策略概念示意图三

如果DMZ区域以路由模式与局域网之间通信，则DMZ区域与局域网区域一样使用私有地址，广域网不能主动访问DMZ区域。那么，DMZ区域与广域网之间的通信应该为NAT模式，如图 9.20所示。

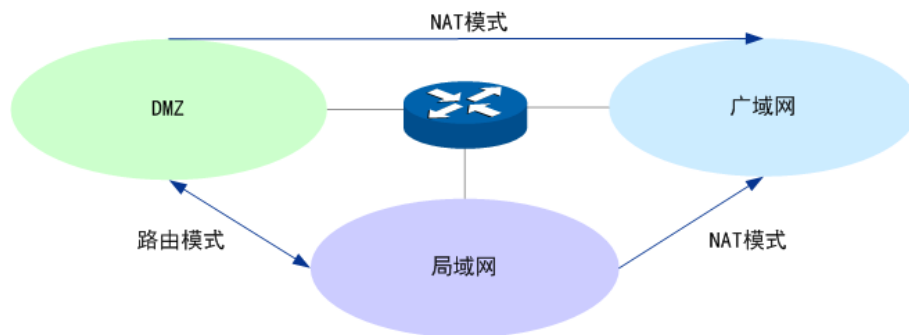


图 9.20 策略概念示意图四

此时，需要在路由器上创建局域网区段到广域网区段和DMZ区段到广域网区段的NAT规则，以及广域网区段到局域网区段和广域网区段到DMZ区段的阻塞策略，如图 9.21所示。

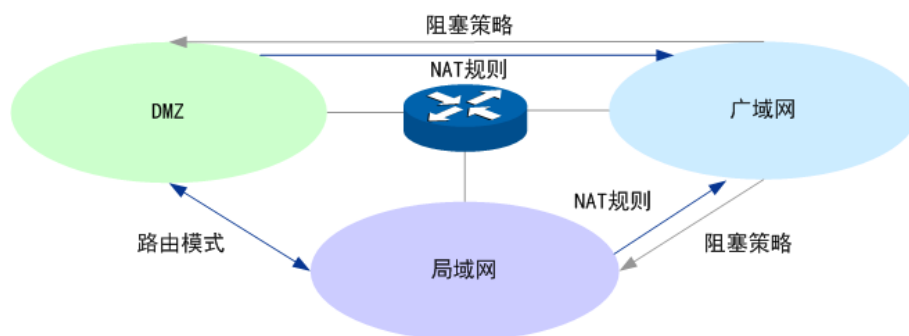


图 9.21 策略概念示意图五

1. 策略生效范围

在创建策略时，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区段中的任何源地址到其它所有区段中的任何目的地址，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、在一个区段中的指定主机与另一区段中的指定主机之间流动。可以参考图 9.22 理解。

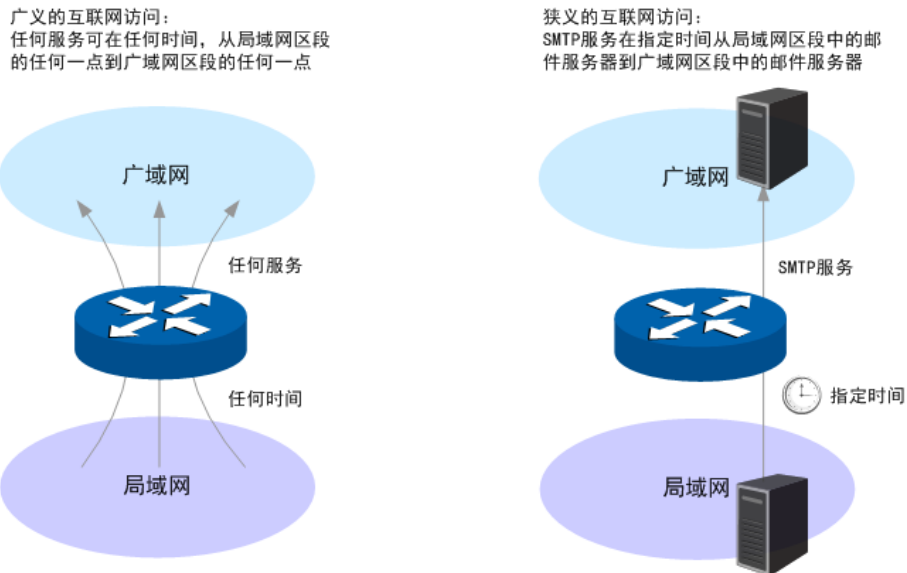


图 9.22 策略生效范围示意图

2. 策略类型

TL-ER6520G的策略分为区段内策略和区段间策略：

- 区段内策略：可以控制从指定区段到任意地址及设备本身的信息流。
- 区段间策略：可以控制从一个指定区段到另一个指定区段的信息流。

两者配置方式基本一致。可以为策略指定优先级，路由器会先处理优先级高的策略。区段内的策略对来自此区段的所有报文生效，因此其优先级高于区段间的策略。

9.4.2 区段内策略

区段内策略提供对指定区段报文的限制。源地址是指定区段内的地址，目的地址可以是任意区段内的任意地址，包括设备本身的地址。区段内策略控制信息流单向流动，主要是控制本区段发送的信息流。

进入界面：安全管理 >> 访问策略 >> 区段内访问规则

在图 9.23界面的访问规则区域，设置规则名称，选择所需的策略类型、服务类型、区段、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<新增>按钮手动添加条目。



图 9.23 区段内访问规则设置界面-访问规则

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7.4服务类型。
区段	在下拉列表中选择本条规则限制的区段。如需新建区段，请参考4.2区段设置。
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。源地址必须是限制区段内的地址。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7.1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地址范围。目的地地址可以是任意区段内的任意地址。路由器预定义“IPGROUP_ANY”地址组表示所有地址。路由器预定义“Me”地址组表示本路由器所有接口的地址。如需新建地址组，请参考7.1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7.2时间管理。
添加到指定位置	勾选该项后，可以将当前设置的访问规则添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

表 9.8 区段内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 9.24中规则效果是：任何时间，区段WAN1内的主机，都不能访问路由器Web界面，此例为**9.4.3 区段内策略应用中应用一**。如需了解区段内访问规则更多应用，可参考**9.4.3 区段内策略应用**。

访问规则

名称:

策略类型: 请选择规则策略

服务类型: ALL

区段: default

源地址范围: IPGROUP_ANY

目的地址范围: IPGROUP_ANY

规则生效时间: Any

添加到指定位置: 第 条

新增 清除 帮助

规则列表

选择	序号	名称	策略类型	服务类型	生效区段	源地址范围	目的地址范围	生效时间	设置
<input type="checkbox"/>	1	WAN1策略1	阻塞	ALL	WAN1	IPGROUP_ANY	Me	Any	

全选 删除 搜索

图 9.24 区段内访问规则设置界面-规则列表

配置区段内访问规则步骤：

- 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**7.4服务类型**。
- 2) 创建区段。非必须操作，如果在已有区段上创建策略，则不必此项操作。创建界面：基本设置 >> 区段设置 >> 区段设置，在此界面的左列点击<+>按钮，在显示的新增区段里设置区段名称，点击<确定>按钮完成。
- 3) 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**7.1地址管理**。
- 4) 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**7.2时间管理**。
- 5) 创建区段内访问规则。必须操作。创建界面：安全管理 >> 访问策略 >> 区段内访问规则，在此界面的访问规则区域，设置规则名称，选择所需的策略类型、服务类型、区段、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<新增>按钮完成。

- 6) 编辑区段内访问规则。非必须操作。编辑界面：安全管理 >> 访问策略 >> 区段内访问规则，在此界面的规则列表区域，可以查看、编辑和删除策略。

9.4.3 区段内策略应用

1. 控制到路由器本身的报文

应用一：

创建策略，使WAN1区段内的主机，不能以任何形式访问路由器。

配置步骤：

- 1) 创建区段WAN1。创建界面：基本设置 >> 区段设置 >> 区段设置。WAN1区段具体设置请根据实际需求进行。
- 2) 创建区段内访问规则。创建界面：安全管理 >> 访问策略 >> 区段内访问规则。规则设置如下，点击<新增>按钮完成。

名称	WAN1策略1
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	Me
规则生效时间	Any

表 9.9 区段内策略应用一设置区段内访问规则

应用二：

与应用一相对应，可以创建策略，使WAN1区段内的主机，只能访问路由器，而不能向其它区段发送报文。

配置步骤：

- 1) 创建区段WAN1。创建界面：基本设置 >> 区段设置 >> 区段设置。WAN1区段具体设置请根据实际需求进行。
- 2) 创建区段内访问规则。创建界面：安全管理 >> 访问策略 >> 区段内访问规则。规则设置如下，点击<新增>按钮完成。

名称	WAN1策略2
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	! Me
规则生效时间	Any

表 9.10 区段内策略应用二设置区段内访问规则

2. 控制某区段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区段，WAN1区段的报文都不能到达该主机。该策略生效效果如下所示：

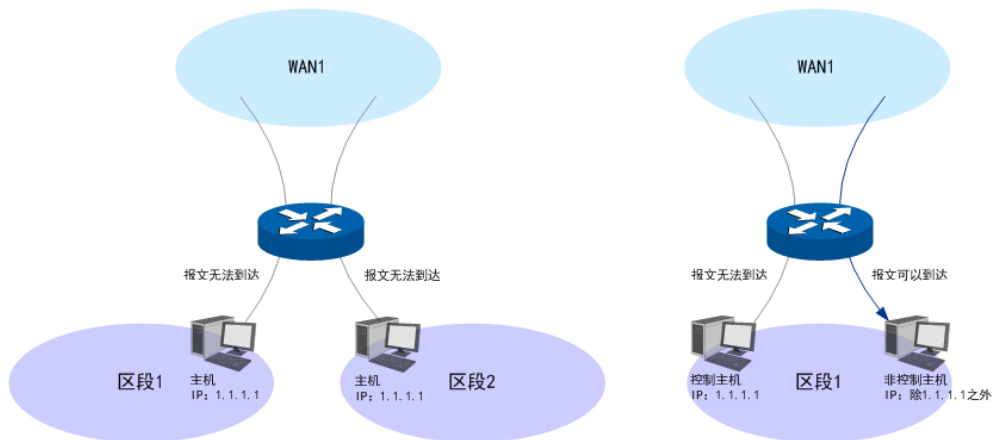


图 9.25 区段内策略应用三

配置步骤：

- 1) 创建区段WAN1。创建界面：基本设置 >> 区段设置 >> 区段设置。WAN1区段具体设置请根据实际需求进行。
- 2) 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**，设置地址组名称为主机，点击<新增>按钮完成。

名称	主机
----	----

表 9.11 区段内策略应用三设置地址组

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

名称	主机IP
IP类型	IP/Mask 1.1.1.1/32

表 9.12 区段内策略应用三设置地址

进入标签页**视图**，组名选择主机，在可选项用户中，选中主机IP，点击<>>>按钮，将主机IP移到包含用户中，点击<设置>按钮完成。

- 3) 创建区段内访问规则。创建界面：安全管理 >> 访问策略 >> 区段内访问规则。规则设置如下，点击<新增>按钮完成。

名称	WAN1策略3
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	主机
规则生效时间	Any

表 9.13 区段内策略应用三设置区段内访问规则

应用四：

现有一个区段LAN，包含了多个网段，其中有LAN1网段IP为10.1.1.0/24，LAN2网段IP为10.1.2.0/24。默认情况LAN区段内的主机都可以互相通信，现在需要阻塞LAN1网段和LAN2网段之间的通信。可以创建策略，阻塞LAN1网段访问LAN2网段。

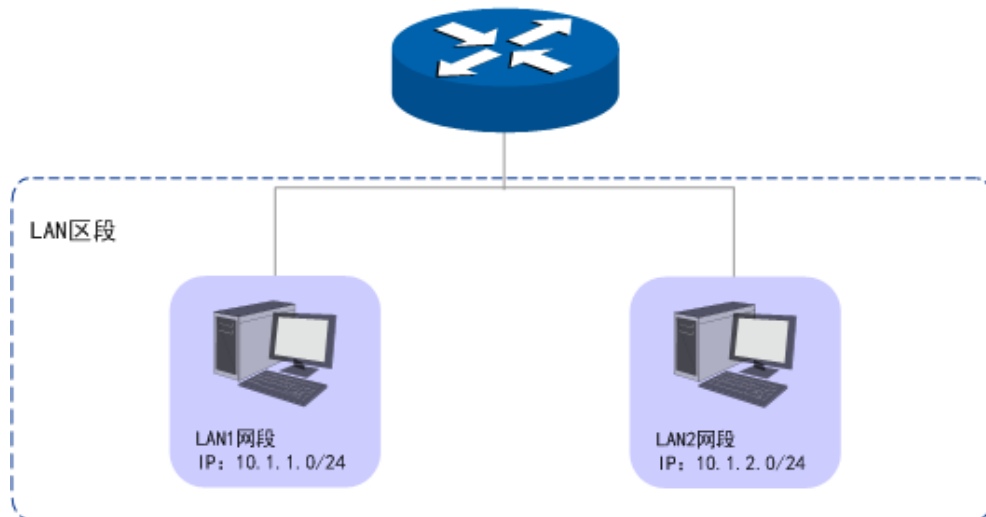


图 9.26 区段内策略应用四

配置步骤：

- 1) 创建区段LAN。创建界面：基本设置 >> 区段设置 >> 区段设置。LAN区段具体设置请根据实际需求进行。
- 2) 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：LAN1网段和LAN2网段。设置地址组名称，点击<新增>按钮完成。

LAN1网段设置如下：

名称	LAN1网段
----	--------

表 9.14 区段内策略应用四设置地址组1

LAN2网段设置如下：

名称	LAN2网段
-----------	--------

表 9.15 区段内策略应用四设置地址组2

进入标签页**地址**，定义两个地址名称：LAN1网段IP和LAN2网段IP。LAN1网段IP，选择IP类型为IP/Mask，输入10.1.1.0/24。LAN2网段IP，选择IP类型为IP/Mask，输入10.1.2.0/24。

LAN1网段IP设置如下：

名称	LAN1网段IP
IP类型	IP/Mask 10.1.1.0/24

表 9.16 区段内策略应用四设置地址1

LAN2网段IP设置如下：

名称	LAN2网段IP
IP类型	IP/Mask 10.1.2.0/24

表 9.17 区段内策略应用四设置地址2

进入标签页**视图**，组名选择LAN1网段，在可选用户中，选中LAN1网段IP，点击<>>>按钮，将LAN1网段IP移到包含用户中，点击<设置>按钮完成。

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

- 3) 创建区段内访问规则。创建界面：安全管理 >> 访问策略 >> 区段内访问规则。规则设置如下，点击<新增>按钮完成。

名称	LAN策略1
策略类型	阻塞
服务类型	ALL
区段	LAN
源地址范围	LAN1网段
目的地址范围	LAN2网段
规则生效时间	Any

表 9.18 区段内策略应用四设置区段内访问规则



说明：

本应用中，按照以上设置完成之后，LAN1网段内的主机，不仅不能访问LAN区段内IP为10.1.2.0/24的主机，也不能访问其他任何区段内IP为10.1.2.0/24的主机。如果还有其他需求，请根据实际应用配置其他策略。

9.4.4 区段间策略

区段间策略可以控制从一个区段传递到另一个区段的信息。源地址和目的地址在不同区段中。区段间策略是有流向的，例如要阻塞区段A和区段B之间的通信，需要配置两条策略，一条策略阻塞区段A发送信息到区段B，另外一条策略阻塞区段B发送信息到区段A。

同时，区段间策略只在控制的两个区段内生效，例如一条策略为：阻塞区段A发送信息到区段B地址组1，假设区段C内也有地址组1，那么，区段A的信息不可以发送到区段B地址组1，但可以发送到区段C地址组1。



说明：

在设置区段间访问规则之前，必须设置区段。区段设置请参考[4.2区段设置](#)。

进入界面：安全管理 >> 访问策略 >> 区段间访问规则

在图 9.27界面的**区段选择**区域，在区段选择下拉列表中勾选要设置的区段，点击<显示>按钮，将出现该区段间访问规则设置项。

图 9.27 区段间访问规则设置界面-区段选择

在图 9.28界面的**访问规则**区域，设置规则名称，选择所需的数据流向、策略类型、服务类型、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<新增>按钮手动添加条目。



图 9.28 区段间访问规则设置界面-访问规则

数据流向	箭头方向代表数据流向和受控地址所在的区段。箭头起始方向表示源地址所在区段，终止方向表示目的地址所在区段。点击转换按钮，可以改变数据流向。
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7.4服务类型。
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。源地址必须是数据流向起始方向区段内的地址。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7.1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地址范围。目的地地址必须是数据流向终止方向区段内的地址。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7.1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7.2时间管理。
添加到指定位置	勾选该项后，可以将当前设置的访问规则添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

表 9.19 区段间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 9.29中规则效果是：任何时间，default区段内的主机，都不能访问dmz区段mail_svr地址组内的地址，此例为**9.4.5 区段间策略应用**中应用二的一条策略。如需了解区段间访问规则更多应用，可参考**9.4.5 区段间策略应用**。

区段选择

区段选择: 请选择区段

显示

default<->wan1 default<->dmz wan1<->dmz

访问规则

数据流向: default -> dmz

名称:

策略类型: 请选择规则策略

服务类型: ALL

源地址范围: IPGROUP_ANY

目的地址范围: IPGROUP_ANY

规则生效时间: Any

添加到指定位置: 第 条

新增 清除 帮助

规则列表

选择	序号	名称	策略类型	服务类型	源区段	目的区段	源地址范围	目的地址范围	生效时间	设置
<input type="checkbox"/>	1	Policy1	阻塞	ALL	default	dmz	IPGROUP_LAN	mail_svr	Any	

全选 删除 搜索

图 9.29 区段间访问规则设置界面-规则列表

配置区段间访问规则步骤：

- 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**7.4服务类型**。
- 2) 创建区段。非必须操作，如果在已有区段上创建策略，则不必此项操作。创建界面：基本设置 >> 区段设置 >> 区段设置，在此界面的左列点击<+>按钮，在显示的新增区段里设置区段名称，点击<确定>按钮完成。
- 3) 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**7.1.1地址组**。
- 4) 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**7.2时间管理**。

- 5) 创建区段间访问规则。必须操作。创建界面：安全管理 >> 访问策略 >> 区段间访问规则，在区段选择下拉列表中勾选所需区段，点击<显示>按钮；再在显示的访问规则区域，设置规则名称，选择所需的数据流向、策略类型、服务类型、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<新增>按钮完成。
- 6) 编辑区段间访问规则。非必须操作。编辑界面：安全管理 >> 访问策略 >> 区段间访问规则，在此界面的规则列表区域，可以查看、编辑和删除策略。

9.4.5 区段间策略应用

1. 应用一

应用需求：

创建策略，使区段WAN1的报文不能到达区段LAN1内IP地址为1.1.1.1的主机。该策略生效效果如下所示：

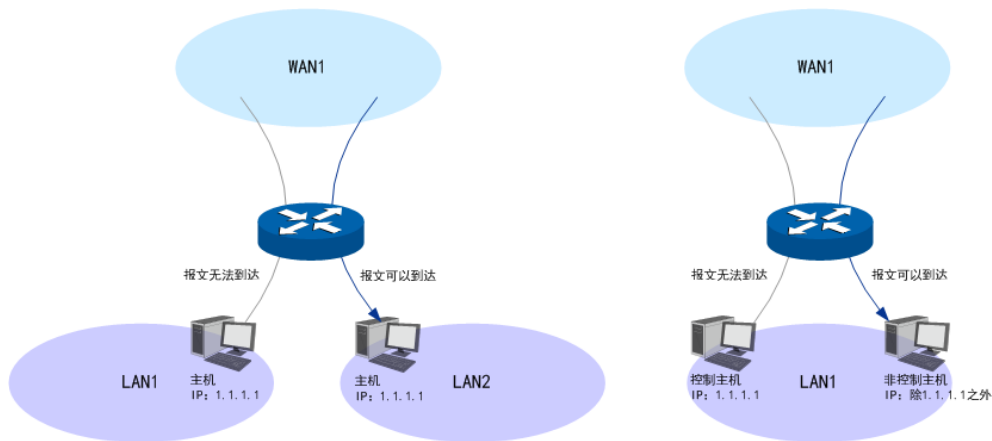


图 9.30 区段间策略应用一

配置步骤：

- 1) 创建区段WAN1和LAN1。创建界面：基本设置 >> 区段设置 >> 区段设置。区段具体设置请根据实际需求进行。
- 2) 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**，设置地址组名称为主机，点击<新增>按钮完成。

名称	主机
----	----

表 9.20 区段间策略应用一设置地址组

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

名称	主机IP
----	------

IP类型	IP/Mask 1.1.1.1/32
-------------	-----------------------

表 9.21 区段间策略应用一设置地址

进入标签页**视图**，组名选择主机，在可选项用户中，选中主机IP，点击<>>按钮，将主机IP移到包含用户中，点击<设置>按钮完成。

- 3) 创建区段间访问规则。创建界面：安全管理 >> 访问策略 >> 区段间访问规则。在区段选择下拉列表中勾选WAN1 <-> LAN1，点击<显示>按钮，然后按照如下所示设置规则，点击<新增>按钮完成。

数据流向	WAN1 -> LAN1
名称	WAN1到LAN1策略1
策略类型	阻塞
服务类型	ALL
源地址范围	IPGROUP_ANY
目的地址范围	主机
规则生效时间	Any

表 9.22 区段间策略应用一设置区段间访问规则

2. 应用二

应用需求：

如图 9.31所示，要将dmz区段中IP地址为1.2.2.5/32的服务器1仅作本地邮件服务器使用。

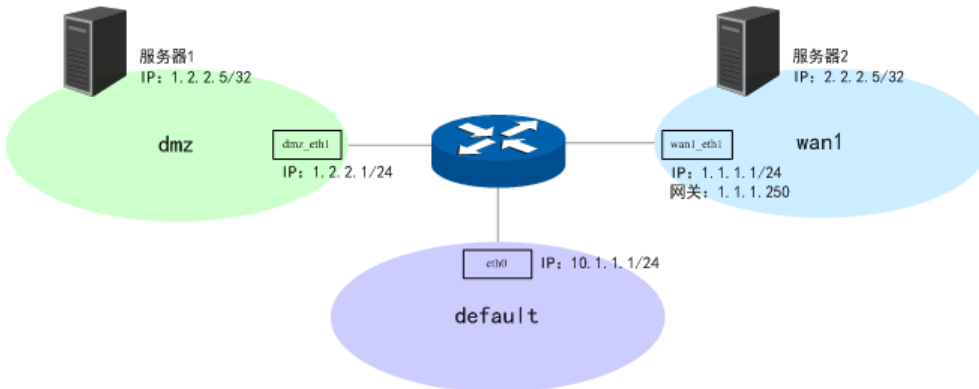


图 9.31 区段间策略应用二

所需策略：

在此应用中，需要创建八个策略以控制电子邮件信息流，前四个策略阻塞本地邮件服务器的所有对外访问和被访问，后四个策略允许本地邮件服务器进行邮件相关通讯。因策略具有优先级，添加中需保证后四个策略的优先级高于前四个策略。

第一个策略：禁止default区段中的用户访问dmz区段的本地邮件服务器。

第二个策略：禁止dmz区段中的本地邮件服务器访问default区段的用户。

第三个策略：禁止wan1区段中的用户访问dmz区段的本地邮件服务器。

第四个策略：禁止dmz区段中的本地邮件服务器访问wan1区段的所有地址。

第五，六个策略：允许default区段中的内部用户发送并检索来自dmz区段中本地邮件服务器的电子邮件。

第七，八个策略：允许dmz区段中的本地邮件服务器发送并检索来自wan1区段中远程邮件服务器的电子邮件。

应用策略所需环境：

在创建策略控制区段间信息流之前，必须先设计应用上述策略的环境。

- 通过快速配置设置区段：

设置wan1区段并将其IP地址指派为1.1.1.1/24，网关设置为1.1.1.250；

设置default区段并将其IP地址指派为10.1.1.1/24；

设置dmz区段并将其IP地址指派为1.2.2.1/24。

- 创建在策略中使用的地址：

设置名称为mail_svr的地址组并将其IP地址指派为1.2.2.5/32；

设置名称为r-mail_svr的地址组并将其IP地址指派为2.2.2.5/32。

- 创建静态路由：

设置到1.2.2.5/32的静态路由，出接口为dmz_eth1。

完成以上设置后，即可创建必需的策略，使受保护的网内外可传输、检索和发送电子邮件。

配置步骤：

- 1) 通过快速配置设置区段。创建界面：快速配置 >> 快速配置。在此界面单击<下一步>，可以开始设置，每一步设置内容如下。在完成快速配置向导界面检查配置参数无误之后，单击<完成>，使配置生效。

系统模式设置	NAT网关模式
NAT模式-接口模式设置	WAN数量：单WAN口 硬件DMZ：开启
NAT模式-NAT-WAN1	连接方式：静态IP IP地址：1.1.1.1 子网掩码：255.255.255.0 网关地址：1.1.1.250 其他项保持默认。

NAT模式-NAT-LAN设置	IP地址: 10.1.1.1 子网掩码: 255.255.255.0 DHCP服务器: 开启 地址池起始地址: 10.1.1.2 地址池结束地址: 10.1.1.254
NAT模式-NAT-DMZ设置	DMZ模式: 广域网 IP地址: 1.2.2.1 子网掩码: 255.255.255.0 DHCP服务器: 关闭

表 9.23 区段间策略应用二设置区段

- 2) 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: mail_svr和r-mail_svr。设置地址组名称, 点击<新增>按钮完成。

mail_svr设置如下:

名称	mail_svr
-----------	----------

表 9.24 区段间策略应用二设置地址组1

r-mail_svr设置如下:

名称	r-mail_svr
-----------	------------

表 9.25 区段间策略应用二设置地址组2

进入标签页**地址**, 定义两个地址名称: mail_svr_ip和r-mail_svr_ip。mail_svr_ip选择IP类型为IP/Mask, 输入1.2.2.5/32。r-mail_svr_ip选择IP类型为IP/Mask, 输入2.2.2.5/32。

mail_svr_ip设置如下:

名称	mail_svr_ip
IP类型	IP/Mask 1.2.2.5/32

表 9.26 区段间策略应用二设置地址1

r-mail_svr_ip设置如下:

名称	r-mail_svr_ip
IP类型	IP/Mask 2.2.2.5/32

表 9.27 区段间策略应用二设置地址2

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

组名选择r-mail_svr, 在可选用户中, 选中r-mail_svr_ip, 点击<>>>按钮, 将r-mail_svr_ip移到包含用户中, 点击<设置>按钮完成。

- 3) 创建静态路由。创建界面：传输控制 >> 路由设置 >> 静态路由。规则设置如下，点击<新增>按钮完成。

名称	DMZ静态路由1
目的地址	1.2.2.5
子网掩码	255.255.255.255
下一跳	1.2.2.1
出接口	dmz_eth1
Metric	0
备注	邮件服务器
启用/禁用规则	启用

表 9.28 区段间策略应用二设置静态路由

- 4) 创建区段间访问规则。创建界面：安全管理 >> 访问策略 >> 区段间访问规则。在区段选择下拉列表中勾选default <-> dmz和wan1 <-> dmz，点击<显示>按钮，然后按照如下所示设置规则，点击<新增>按钮完成。

**说明：**

以下设置中出现的“IPGROUP_LAN”地址组，是快速配置完成后，路由器自动添加的一个地址组，其包含IP地址为default区段的eth0接口IP：10.1.1.1/24。

default <-> dmz区段间访问规则设置如下：

数据流向	default -> dmz
名称	Policy1
策略类型	阻塞
服务类型	ALL
源地址范围	IPGROUP_LAN
目的地址范围	mail_svr
规则生效时间	Any

表 9.29 区段间策略应用二设置区段间访问规则1

数据流向	dmz -> default
名称	Policy2
策略类型	阻塞
服务类型	ALL
源地址范围	mail_svr
目的地址范围	IPGROUP_LAN
规则生效时间	Any

表 9.30 区段间策略应用二设置区段间访问规则2

数据流向	default -> dmz
名称	Policy5
策略类型	允许
服务类型	SMTP
源地址范围	IPGROUP_LAN
目的地址范围	mail_svr
规则生效时间	Any

表 9.31 区段间策略应用二设置区段间访问规则3

数据流向	default -> dmz
名称	Policy6
策略类型	允许
服务类型	POP3
源地址范围	IPGROUP_LAN
目的地址范围	mail_svr
规则生效时间	Any

表 9.32 区段间策略应用二设置区段间访问规则4

wan1 <-> dmz区段间访问规则设置如下：

数据流向	wan1 -> dmz
名称	Policy3
策略类型	阻塞
服务类型	ALL
源地址范围	r-mail_svr
目的地址范围	IPGROUP_ANY
规则生效时间	Any

表 9.33 区段间策略应用二设置区段间访问规则5

数据流向	dmz -> wan1
名称	Policy4
策略类型	阻塞
服务类型	ALL
源地址范围	IPGROUP_ANY
目的地址范围	r-mail_svr
规则生效时间	Any

表 9.34 区段间策略应用二设置区段间访问规则6

数据流向	dmz -> wan1
------	-------------

名称	Policy7
策略类型	允许
服务类型	SMTP
源地址范围	mail_svr
目的地址范围	r-mail_svr
规则生效时间	Any

表 9.35 区段间策略应用二设置区段间访问规则7

数据流向	wan1 -> dmz
名称	Policy8
策略类型	允许
服务类型	POP3
源地址范围	mail_svr
目的地址范围	r-mail_svr
规则生效时间	Any

表 9.36 区段间策略应用二设置区段间访问规则8

9.4.6 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 >> 访问策略 >> URL过滤

图 9.32 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”, 并根据实际情况选择一种过滤规则。

URL地址过滤规则

名称	输入该规则条目的名称。
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7.1地址管理。
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。
关键字	当过滤方式为“关键字”的时候, 可在此输入指定的关键字字符。
URL地址	当过滤方式为“完整URL”的时候, 可在此输入完整的广域网URL地址。

表 9.37 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。您需要设置完整URL过滤“www.aabbcc.com”，以及关键字过滤“.exe”，如下图，设置完成后点击<新增>按钮保存生效。

功能设置

启用URL地址过滤功能

仅允许访问规则列表中的URL地址

仅禁止访问规则列表中的URL地址

URL地址过滤规则

名称：

组：

过滤方式： 关键字 完整URL

关键字：

规则列表

选择	序号	名称	受控地址	URL地址/关键字	过滤方式	设置
<input type="checkbox"/>	1	1	局域网	www.aabbcc.com	完整URL	
<input type="checkbox"/>	2	2	局域网	.exe	关键字	

9.5 应用控制

9.5.1 应用限制

可以在此启用并设置应用限制功能。

进入界面：安全管理 >> 应用控制 >> 应用限制

图 9.33 应用限制设置界面

功能设置

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

应用限制设置

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7.1地址管理。
限制应用	可以点击“设置列表”在弹出的选择框中对应用进行设置。可以设置的应用包括即时通信、P2P软件、金融软件、游戏、视频软件、网页游戏、基础应用和代理。默认为对除了基础应用和代理的所有应用进行限制。
生效时间	指定规则生效时间。如需新建时间对象，请参考7.2时间管理。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。

表 9.38 应用限制设置界面项说明

规则列表

在规则列表中，可以对已保存的应用限制进行相应设置。

图 9.33 序号1规则的含义：组IPGROUP_ANY进行了应用限制，点击“查看”可在弹出的选择框中看到受限制的应用。应用限制时间为所有时间。该规则已启用。

9.5.2 例外管理

可以在此对例外QQ号码进行相关设置，使其不受应用限制的约束。

进入界面：安全管理 >> 应用控制 >> 例外管理

启用例外QQ号设置

启用例外QQ号码功能

设置

例外QQ号设置

QQ号：

备注： (1-50个字符,可选)

新增 清除 帮助

例外QQ号列表

选择	序号	QQ号	备注	设置
<input type="checkbox"/>	1	1234567	QQ	

全选 删除 搜索

图 9.34 例外管理界面

启用例外QQ号设置

勾选“启用例外QQ号码功能”后，例外QQ号的相关设置才会生效，才可以使设置的例外QQ号码不受应用限制的约束。

例外QQ号设置

QQ号	指定不受应用限制约束的QQ号码，可以同时输入多个QQ号码进行批量添加。
备注	添加对本条规则的说明信息。

表 9.39 例外QQ号设置界面项说明

例外QQ号列表

在例外QQ号列表中，可以查看例外QQ信息，也可以对已保存的例外QQ号码进行相应设置。

9.5.3 数据库

可以在此进行应用特征数据库的升级。

进入界面：安全管理 >> 应用控制 >> 数据库

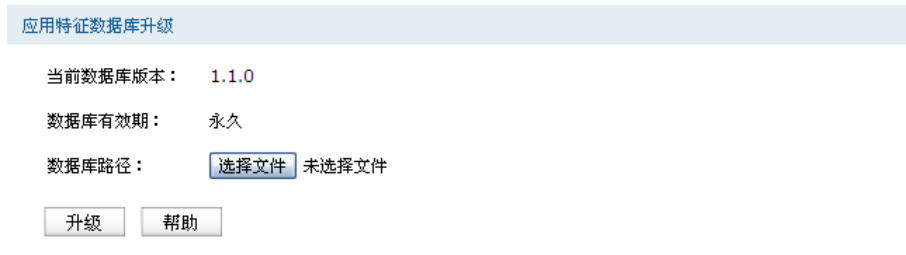


图 9.35 数据库界面

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

第10章 VPN

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

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

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

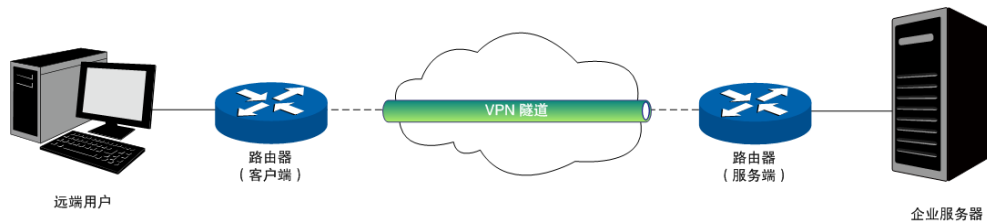


图 10.1 VPN典型拓扑

隧道是通过对数据报的封装实现的, 因为数据报封装和解封的过程都是在路由器上完成, 所以对于用户来说是透明的。TL-ER6520G支持的隧道协议包括三层隧道协议IPsec和二层隧道协议L2TP/PPTP。

10.1 IKE

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

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

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

10.1.1 IKE安全策略

在TL-ER6520G路由器上，可以对IKE协商过程的相关参数进行设置。

进入界面：VPN >> IKE >> IKE安全策略

IKE安全策略设置

安全策略名称：

交换模式： 主模式 野蛮模式

封装模式： 隧道模式 传输模式

协商模式： 初始者模式 响应者模式

模式配置：

本地ID类型： IP地址 NAME

本地ID：

对端ID类型： IP地址 NAME

对端ID：

安全提议一：

安全提议二：

安全提议三：

安全提议四：

预共享密钥：

生存时间： 秒（60-604800）

DPD检测开启： 启用 禁用

DPD检测周期： 秒（1-300）

IKE安全策略列表

选择	序号	名称	交换模式	封装模式	协商模式	安全提议一	安全提议二	安全提议三	安全提议四	设置
<input type="checkbox"/>	1	IKE_1	主模式	隧道模式	初始者	IKE_proposal	----	----	----	

图 10.2 IKE安全策略设置界面

安全策略名称	为IKE安全策略命名。设置好的IKE安全策略可以被应用在IPsec安全策略中。
交换模式	<p>设置IKE第一阶段协商的交换模式，该交换模式必须与对端相同。交换模式有以下两种：</p> <p>主模式（Main mode）：该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。</p> <p>野蛮模式（Aggressive mode）：又称主动模式，该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。</p>
封装模式	<p>设置IKE第一阶段协商的封装模式，该封装模式必须与对端相同。封装模式有以下两种：</p> <p>隧道模式（Tunnel mode）：在该模式下，AH或ESP插在原始IP报文头之前，另外生成一个新的报文头放到AH或ESP之前。从安全性来讲，隧道模式优于传输模式。适用于更普遍的VPN应用。</p> <p>传输模式（Transport mode）：在该模式下，AH或ESP被插入到IP报文头之后但在所有传输层协议之前，或所有其他IPSec协议之前。适用于主机直接访问设备时之间的加密传输。</p>

协商模式	设置IKE协商的模式，该协商模式不必与对端相同。协商模式有以下两种： 初始者模式（Initiator mode）：配置该模式后，IKE才能主动发起协商。 响应者模式（Responder mode）：配置该模式后，IKE不会主动发起协商，需要等待对端发起协商。
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的交换与验证，可以选择“IP地址”或“NAME”，通信双方的设置需保持一致。
本地/对端ID	ID类型选择“IP地址”时，无需进行设置；ID类型选择“NAME”时，可自定义本地/对端的ID。路由器的“本地ID”需与通信对端的“对端ID”保持一致，而“对端ID”则需与通信对端的“本地ID”保持一致。
安全提议	选择用于IKE协商第一阶段的安全提议，如果下拉菜单中没有想选择的条目，请进入10.1.2 IKE安全提议页面创建新条目。主模式下，最多可以选择四条不同的安全提议；野蛮模式下，可以选择一条安全提议。
预共享密钥	设置通信双方互相认证的密钥，双方必须使用同一个预共享密钥。
生存时间	设定ISAKMP SA的生存时间。
DPD检测开启	DPD（Dead Peer Detect，对端存活检测）开启后，IKE一端能够定时主动检测对端的在线状态。
DPD检测周期	当开启DPD检测时可设置检测周期。

表 10.1 IKE安全策略界面项说明

新增的条目会在IKE安全策略列表中显示出来，如下图所示。

IKE安全策略列表										
选择	序号	名称	交换模式	封装模式	协商模式	安全提议一	安全提议二	安全提议三	安全提议四	设置
<input type="checkbox"/>	1	IKE_1	主模式	隧道模式	初始者	IKE_proposal	----	----	----	

图 10.3 IKE策略列表

如有需要，可以点击条目后的按钮进行编辑。

10.1.2 IKE安全提议

进入界面：VPN >> IKE >> IKE安全提议

IKE安全提议设置

安全提议名称：

验证算法：

加密算法：

DH组：

IKE安全提议列表

选择	序号	名称	验证算法	加密算法	DH组	设置
<input type="checkbox"/>	1	IKE_proposal	MD5	3DES	DH1	

图 10.4 IKE安全提议设置界面

安全提议名称	为IKE安全提议命名。设置好的IKE安全提议可以被应用在IKE安全策略中。
验证算法	选择应用于IKE会话的验证算法。路由器支持以下验证算法： MD5 (Message Digest Algorithm, 消息摘要算法): 对一段消息产生128bit的消息摘要，防止消息被篡改。 SHA1 (Secure Hash Algorithm, 安全散列算法): 对一段消息产生160bit的消息摘要，比MD5更难破解。
加密算法	选择应用于IKE会话的加密算法。路由器支持以下加密算法： DES (Data Encryption Standard, 数据加密标准): 使用56bit的密钥对64bit数据进行加密，64bit的最后8位用于奇偶校验。3DES则为三重DES，使用三个56bit的密钥进行加密。 AES (Advanced Encryption Standard, 高级加密标准): AES128/192/256表示使用长度为128/192/256 bit的密钥进行加密。
DH组	Diffie-Hellman算法的组信息，用于产生加密IKE隧道的会话密钥。DH1/2/5分别对应着768/1024/1536 bit的DH组。

表 10.2 IKE安全提议界面项说明

新增的条目会在IKE安全提议列表中显示出来，如下图所示。

IKE安全提议列表

选择	序号	名称	验证算法	加密算法	DH组	设置
<input type="checkbox"/>	1	IKE_proposal	MD5	3DES	DH1	

图 10.5 IKE安全提议列表

如有需要，可以点击条目后的按钮进行编辑。

10.2 IPsec

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

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

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

10.2.1 IPsec安全策略

进入界面：VPN >> IPsec >> IPsec安全策略

启动IPSec功能

启用IPSec功能： 启用 禁用

IPSec安全策略设置

安全策略名称：

启用安全策略： 启用 禁用

本地子网范围： /

对端子网范围： /

选择接口： ▼

对端网关： (IP地址或域名)

协商方式： IKE协商 手动模式

IKE安全策略： ▼

安全提议一： ▼

安全提议二： ▼

安全提议三： ▼

安全提议四： ▼

PFS： ▼

生存时间： 秒 (120-604800)

IPSec安全策略列表

选择	序号	策略名称	本地子网范围	对端子网范围	协商方式	L2TP引用	状态	设置
<input type="checkbox"/>	1	IPsec_1	192.168.1.0/24	0.0.0.0/0	IKE协商	未引用	已启用	

图 10.6 IPsec安全策略设置界面

启用IPsec功能

只有勾选“启用”后，路由器才能应用IPsec。

IPsec安全策略设置

安全策略名称	为IPsec安全策略命名。
启用安全策略	选择启用或禁用当前策略条目。
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。
选择接口	指定本地使用的接口；对端网关设置的“对端网关地址”必须与该接口的IP地址相同。




对端网关	设置对端网关，可以填写对端的IP地址或域名。可配置"0.0.0.0"，表示任意地址。
协商方式	建立IPsec安全隧道可以有两种协商方式。IKE为自动协商，手动模式则需手动设定相关的安全参数。
IKE安全策略	选择“IKE协商”时，可以指定相应的IKE安全策略。如果下拉菜单中没有想选择的条目，请进入 10.1.1 IKE安全策略 页面创建新条目。
安全提议	指定相应的IPsec安全提议。如果下拉菜单中没有想选择的条目，请进入 10.2.2 IPsec安全提议 页面创建新条目。
PFS	PFS(Perfect Forward Secrecy, 完善的前向安全性) 特性使得IKE第二阶段协商生成一个新的密钥材料，该密钥材料与第一阶段协商生成的密钥材料没有任何关联，这样即使IKE第一阶段的密钥被破解，第二阶段的密钥仍然安全。如果没有使用PFS，第二阶段的密钥将根据第一阶段生成的密钥材料来产生，一旦第一阶段的密钥被破解，用于保护通信数据的第二阶段密钥也岌岌可危，这将严重威胁到双方的通信安全。PFS是通过DH算法实现的，通信双方的PFS设置需保持一致。
生存时间	设定IPsec SA的生存时间。
入SPI	选择“手动模式”时，可以设定SPI参数。SPI与隧道对端网关地址、协议类型三个参数共同标识一个IPsec安全联盟，通信对端的“出SPI”值必须与此值相同。
入ESP MD5密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP MD5验证算法的密钥。通信对端的“出 ESP MD5密钥”必须与此值相同。
入ESP 3DES密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP 3DES加密算法的密钥。通信对端的“出 ESP 3DES密钥”必须与此值相同。
出SPI	选择“手动模式”时，可以设定SPI参数。SPI参数唯一标识一个IPsec安全联盟，通信对端的“入SPI”值必须与此值相同。
出ESP MD5密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP MD5验证算法的密钥。通信对端的“入 ESP MD5密钥”必须与此值相同。
出ESP 3DES密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP 3DES加密算法的密钥。通信对端的“入 ESP 3DES密钥”必须与此值相同。

表 10.3 IPsec安全策略界面项说明

新增的条目会在**IPsec安全策略列表**中显示出来，如下图所示。

IPSec安全策略列表								
选择	序号	策略名称	本地子网范围	对端子网范围	协商方式	L2TP引用	状态	设置
<input type="checkbox"/>	1	IPsec_1	192.168.1.0/24	0.0.0.0/0	IKE协商	未引用	已启用	  

图 10.7 IPsec安全策略列表

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：

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](#)。

10.2.2 IPsec安全提议

进入界面：VPN >> IPsec >> IPsec安全提议

IPSec安全提议设置

安全提议名称：

安全协议：

ESP验证算法：

ESP加密算法：

IPSec安全提议列表

选择	序号	名称	安全协议	AH验证算法	ESP验证算法	ESP加密算法	设置
<input type="checkbox"/>	1	IPsec_Proposal	ESP	---	MD5	3DES	
<input type="checkbox"/>	2	IPsec_Proposal1	AH	MD5	---	---	

图 10.8 IPsec安全提议设置界面

安全提议名称	为IPsec安全提议命名。设置好的IPsec安全提议可以被应用在IPsec安全策略中。
安全协议	选择要使用的协议。
AH验证算法	<p>当选择AH安全协议时可设定AH验证算法。路由器支持以下验证算法：</p> <p>MD5 (Message Digest Algorithm, 消息摘要算法): 对一段消息产生128bit的消息摘要，防止消息被篡改。</p> <p>SHA1(Secure Hash Algorithm, 安全散列算法): 对一段消息产生160bit的消息摘要，比MD5更难破解。</p>
ESP验证算法	<p>当选择ESP安全协议时可设定ESP验证算法。路由器支持以下验证算法：</p> <p>MD5 (Message Digest Algorithm, 消息摘要算法): 对一段消息产生128bit的消息摘要，防止消息被篡改。</p> <p>SHA1(Secure Hash Algorithm, 安全散列算法): 对一段消息产生160bit的消息摘要，比MD5更难破解。</p>
ESP加密算法	<p>当选择ESP安全协议时可设定ESP加密算法。路由器支持以下加密算法：</p> <p>DES (Data Encryption Standard, 数据加密标准): 使用56bit的密钥对64bit数据进行加密，64bit的最后8位用于奇偶校验。3DES则为三重DES，使用三个56bit的密钥进行加密。</p> <p>AES(Advanced Encryption Standard, 高级加密标准): AES128/192/256表示使用长度为128/192/256bit的密钥进行加密。</p>

表 10.4 IPsec安全提议界面项说明

新增的条目会在IPsec安全提议列表中显示出来，如下图所示。

IPSec安全提议列表							
选择	序号	名称	安全协议	AH验证算法	ESP验证算法	ESP加密算法	设置
<input type="checkbox"/>	1	IPsec_Proposal	ESP	---	MD5	3DES	
<input type="checkbox"/>	2	IPsec_Proposal1	AH	MD5	---	---	

图 10.9 IPsec安全提议列表

如有需要，可以点击条目后的按钮进行编辑。

10.2.3 IPsec安全联盟

在此将列出路由器上所有已成功建立的IPsec安全联盟相关信息。

进入界面：VPN >> IPsec >> IPsec安全联盟

IPSec安全联盟列表									
序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
1	IPsec_1	3374359 119	in	192.168.10.100<- 172.29.85.199	192.168.1.0/24:0<- 192.168.0.0/24:0,any	ESP	---	MD5	3DES
2	IPsec_1	7811595 72	out	192.168.10.100-> 172.29.85.199	192.168.1.0/24:0-> 192.168.0.0/24:0,any	ESP	---	MD5	3DES

图 10.10 IPsec安全联盟界面

在图 10.10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。

IPSec安全联盟列表									
序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
1	IPsec_2	7811595 72	in	172.29.85.199<- 192.168.10.100	192.168.0.0/24:0<- 192.168.1.0/24:0,any	ESP	---	MD5	3DES
2	IPsec_2	3374359 119	out	172.29.85.199-> 192.168.10.100	192.168.0.0/24:0-> 192.168.1.0/24:0,any	ESP	---	MD5	3DES

10.2.4 NAT穿透

在实际网络应用中，IPsec VPN通信双方的物理连接线路中可能存在着NAT网关，当数据包经过NAT网关时，其IP地址或端口号会改变，这就导致VPN隧道对端收到数据包后验证失败，数据包被直接丢弃。NAT穿透功能可以解决这一问题，实现方法为在原ESP协议的报文外添加新的IP首部和UDP首部。数据包的格式为：新IP/UDP首部|ESP首部|IP首部|数据。由于NAT网关只会改变最外层的IP首部，而且ESP校验不包含IP首部，所以此时IPsec VPN的通信不会受到影响。但是NAT穿透只适用于ESP协议，AH协议的校验包含了IP首部，因此无法与NAT共存。

10.3 PPTP

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

10.3.1 PPTP服务器设置

进入界面: VPN >>PPTP >> PPTP服务器设置

图 10.11 PPTP服务器设置界面

全局管理设置

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

表 10.5 PPTP服务器设置-全局管理设置界面项说明

隧道设置

用户名	设置PPTP认证的用户名。客户端与服务器端的设置需一致。
密码	设置PPTP认证的密码。客户端与服务器端的设置需一致。
本地地址	设置PPTP隧道本端使用的IP地址。
DNS地址	设置DNS服务器的地址。
绑定区段	请选择绑定的区段。当前用户仅对绑定的区段提供PPTP服务。
加密方式	选择是否对隧道进行加密。若启用,则使用MPPE对PPTP隧道加密。




地址池	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。
组网模式	当连入隧道的用户为接入路由器的一个网段时，请选择“站点到站点”模式；当连入隧道的用户是单个计算机时，请选择“PC到站点”模式。
最大会话数	当组网模式选择“PC 到站点”时，可进行隧道容纳最大会话数的设置。
对端子网	PPTP隧道对端局域网所使用的IP地址范围(一般可以填VPN隧道对端设备的LAN口IP地址范围)，由IP和子网掩码组成。
启用/禁用	选择启用或禁用本PPTP隧道。

表 10.6 PPTP服务器设置-隧道设置界面项说明

新增的条目会在**隧道设置列表**中显示出来，如下图所示。

选择	序号	用户名	本地地址	绑定域	加密方式	地址池	组网模式	最大会话数	对端子网范围	状态	设置
<input type="checkbox"/>	1	pptp_1	170.31.20.88	default	已启用	IPool_1	PC到站点	1	---	已启用	 

图 10.12 PPTP隧道设置列表

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。

10.3.2 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 >> PPTP服务器隧道信息

序号	用户名	本地会话ID	对端会话ID	本地IP地址	对端IP地址	对端主机	本地PPP地址	对端PPP地址	状态	断开连接
1	pptp1	183	0	8.8.8.65	8.8.8.198	MikroTik	10.10.10.254	10.10.10.1	已连接	

图 10.13 PPTP隧道信息界面

图 10.13中显示1条目表示目前这条隧道已成功建立，每条隧道会产生会话ID数值对，每个数值对都由两个数字ID组成，客户端和服务器端显示的数值对是对应的。

10.4 L2TP

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

10.4.1 L2TP服务器设置

进入界面: VPN >> L2TP >> L2TP服务器设置

全局管理设置

L2TP链路维护时间间隔: (单位: 秒, 范围: 60-1000)

PPP 链路维护时间间隔: (单位: 秒, 范围: 0-120, 0代表不发送)

隧道设置

用户名:

密码:

本地地址:

DNS地址:

绑定区段:

加密方式: IPsec_1

地址池:

组网模式:

最大会话数: (1-10)

对端子网: /

启用/禁用: 启用 禁用

L2TP服务器设置列表

选择	序号	用户名	本地地址	绑定区段	加密方式	地址池	组网模式	对端子网范围	状态	设置
<input type="checkbox"/>	1	l2tp_1	170.31.20.88	default	已禁用	IPpool_1	PC到站点	---	已启用	<input type="button" value="设置"/>

图 10.14 L2TP服务器设置界面

全局管理设置

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

表 10.7 L2TP服务器设置-全局管理设置界面项说明

隧道设置

用户名	设置L2TP认证的用户名。客户端与服务器端的设置需一致。
密码	设置L2TP认证的密码。客户端与服务器端的设置需一致。
本地地址	设置L2TP隧道本端使用的IP地址。
DNS地址	设置DNS服务器的地址。
绑定区段	请选择绑定的区段。当前用户仅对绑定的区段提供L2TP服务。
加密方式	选择是否对隧道进行加密。若启用, 则使用IPsec对L2TP隧道加密。

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。
组网模式	当连入隧道的用户为接入路由器的一个网段时，请选择“站点到站点”模式；当连入隧道的用户是单个计算机时，请选择“PC到站点”模式。
最大会话数	当组网模式选择“PC到站点”时，可进行隧道容纳最大会话数的设置。
对端子网	L2TP隧道对端局域网所使用的IP地址范围(一般可以填VPN隧道对端设备的LAN口IP地址范围)，由IP和子网掩码组成。
启用/禁用	选择启用或禁用本L2TP隧道。

表 10.8 L2TP服务器设置-隧道设置界面项说明

新增的条目会在**隧道设置列表**中显示出来，如下图所示。

L2TP服务器设置列表										
选择	序号	用户名	本地地址	绑定区段	加密方式	地址池	组网模式	对端子网范围	状态	设置
<input type="checkbox"/>	1	l2tp_1	170.31.20.88	default	已禁用	IPpool_1	PC到站点	---	已启用	

图 10.15 L2TP服务器设置界面

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。

10.4.2 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 >> L2TP服务器隧道信息

隧道信息列表										
序号	用户名	隧道ID	会话ID	本地IP地址	对端IP地址	本地PPP地址	对端PPP地址	对端主机	状态	断开连接
1	test_1	35,35	55,55	172.29.85.228	172.29.85.121	4.4.4.4	12.12.12.12	TP-LINK_SMB_T L-ER6520G	已连接	

图 10.16 L2TP隧道信息界面

图 10.16中显示1条目表示目前这条隧道已成功建立，每条隧道会产生隧道ID数值对和会话ID数值对，每个数值对都由两个数字ID组成，客户端和服务器端显示的数值对是对应的。

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

第11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访问，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，并推送图片广告。

Web 认证和微信连 Wi-Fi 在指定区段内生效。同一区段可以同时启用 Web 认证和微信连 Wi-Fi，此时用户进行何种认证说明如下：

- 1) 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）。
- 2) 若用户直接访问 Web 认证页面（/wportal/webauth），则进行 Web 认证。

11.1 Web 认证介绍

11.1.1 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。

11.1.2 Web 认证系统

Web 认证系统一般网络拓扑如下图所示：

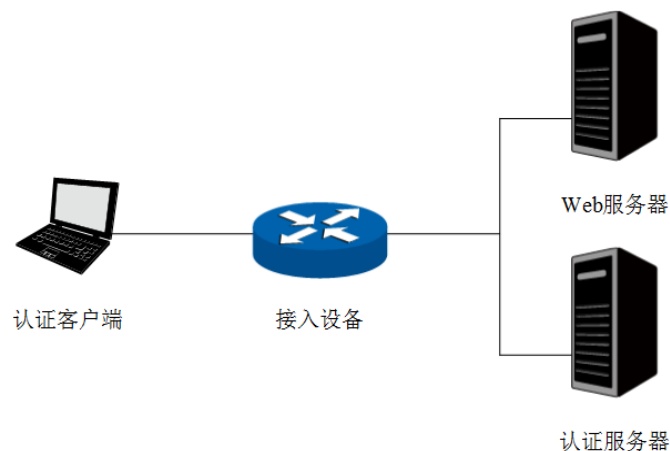


图 11.1 Web 认证系统拓扑图

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。

11.1.3 Web 认证过程

TL-ER6520G Web 认证过程如下图所示：

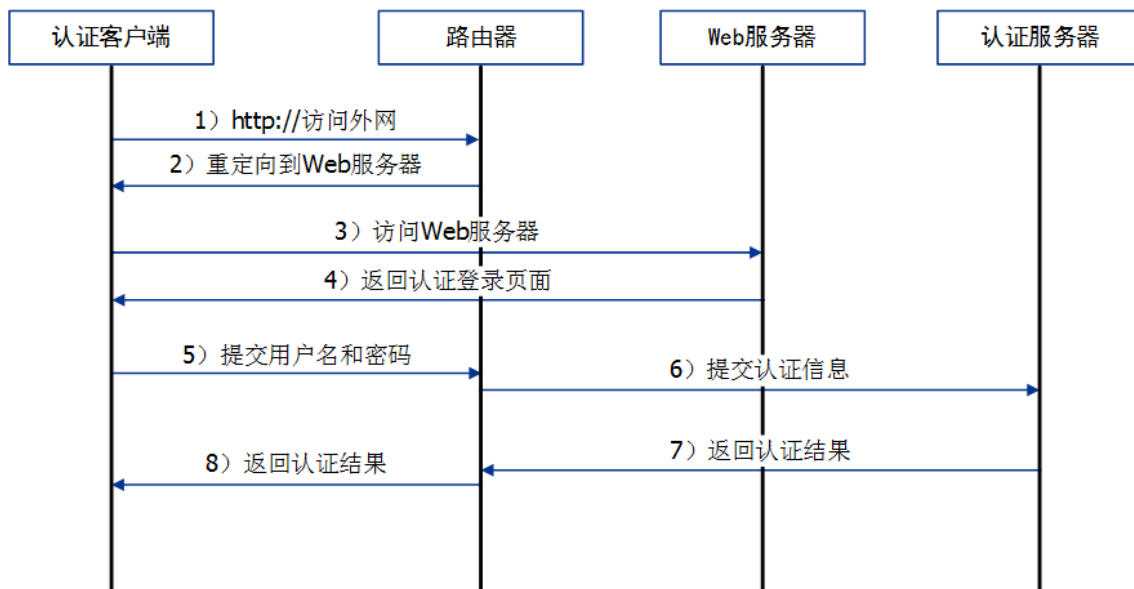


图 11.2 Web 认证过程示意图

- 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。

11.2 Web 认证配置

进入界面：认证管理 >> 认证设置 >> Web 认证

Web认证设置

启用Web认证

生效区段: default

空闲断线时间: 5 分钟 (1-30)

认证页面: 自定义页面

页面标题: (1-50个字符)

背景图片: 选择文件 未选择任何文件 上传

(可选, 图片大小不能超过200KB, 上传图片分辨率建议使用1080*411)

欢迎信息: (1-50个字符)

版权声明: (1-50个字符)

页面预览: 预览认证页面

认证方式: 本地认证

启用到期提醒

页面预览: 预览到期提醒页面

设置 帮助

图 11.3 Web认证界面

在此界面勾选**启用 Web 认证**，选择**生效区段**，可以针对指定区段设置 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-ER6520G 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-ER6520G 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-ER6520G 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-ER6520G 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 11.1 本文档Web认证应用选项搭配说明

11.2.1 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：

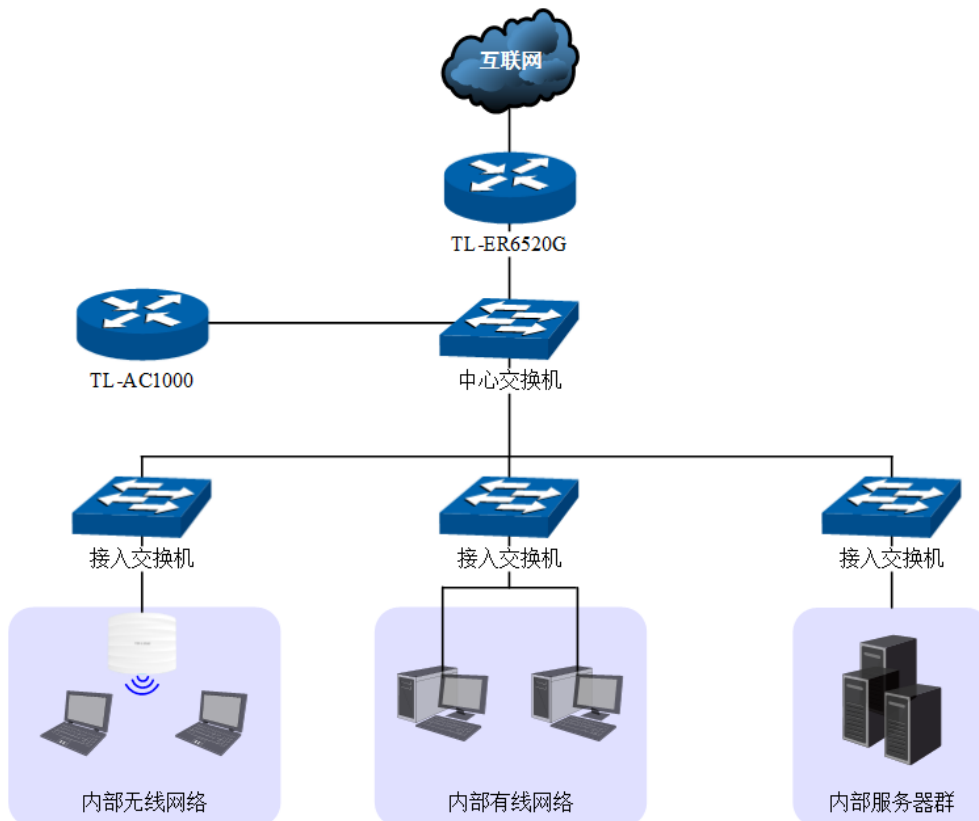


图 11.4 一键上网应用拓扑图

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，可参考如下所示参数设置。

Web认证设置

启用Web认证

生效区段: default

空闲断线时间: 5 分钟 (1-30)

认证页面: 自定义页面

页面标题: XX酒店Web认证 (1-50个字符)

背景图片: 选择文件 未选择任何文件 上传
(可选, 图片大小不能超过200KB, 上传图片分辨率建议使用1080*411)

欢迎信息: 欢迎登录XX酒店Web认证页面 (1-50个字符)

版权声明: Copyright ©2016 (1-50个字符)

页面预览: 预览认证页面

认证方式: 一键上网

免费上网时长: 30 分钟 (1-1440)

设置 帮助

图 11.5 一键上网应用设置界面

启用Web认证	勾选此项，可以启用Web认证功能。
生效区段	选择Web认证功能生效的区段。
空闲断线时间	设置已认证用户空闲断线时间。
认证页面	选择自定义页面。
页面标题	设置Web认证页面的标题。
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, 上传图片分辨率建议使用1080*411。
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。
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。

表 11.2 一键上网应用设置界面项说明

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

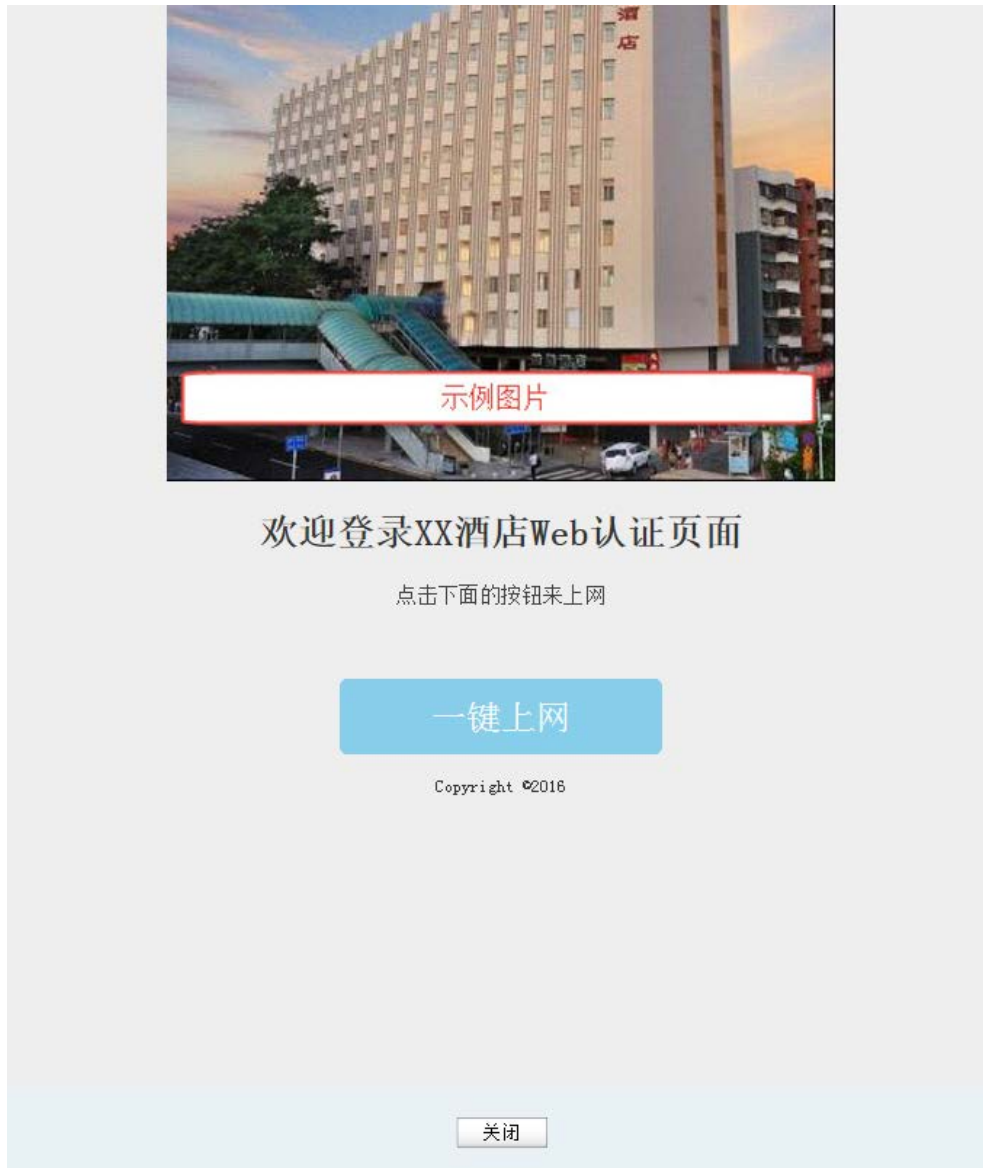


图 11.6 预览一键上网Web认证登录页面

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：xxjudian。
- 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 11.7 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 11.8 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。

11.2.2 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：

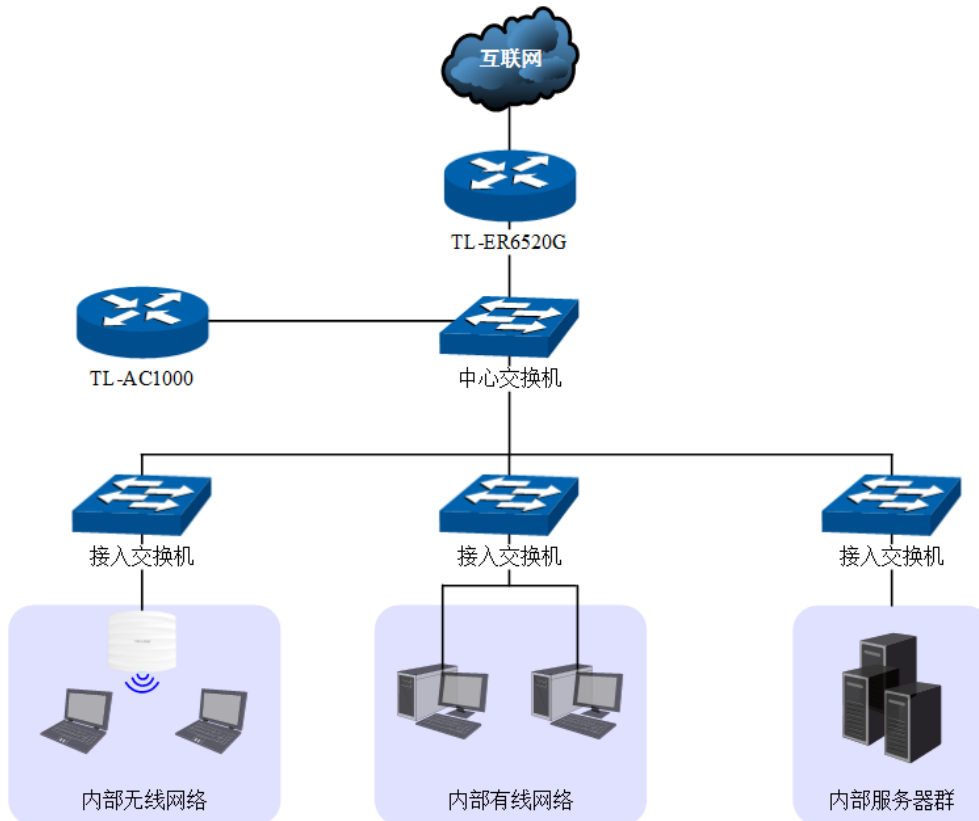


图 11.9 使用内置的Web服务器和认证服务器应用拓扑图

配置方法

1 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**。



图 11.10 用户管理界面

点击<新增>按键，可以新增认证用户。**用户类型**分为正式用户和免费用户。

- 正式用户：给用户连续自然天的上网服务，当账户有效期到期后，该账户无效。

用户设置

用户类型：

用户名： (1-100个英文字符)

密码： (1-100个英文字符)

账户有效期： (格式：xxxx-xx-xx)

允许认证时间段：

MAC地址绑定方式：

同时登录用户数： (1-2048)

上行带宽： Kbps (0或10-1000000, 0表示不限制)

下行带宽： Kbps (0或10-1000000, 0表示不限制)

姓名： (1-50个字符, 可选)

电话： (1-50个字符, 可选)

备注： (1-50个字符, 可选)

启用/禁用： 启用 禁用

图 11.11 用户管理-用户新增-正式用户界面

用户名	自定义的用户名，不能与已有用户名重复。
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。
账户有效期	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。 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。 静态绑定：手动输入认证客户端MAC地址，绑定对应用户名。
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。
启用/禁用	选择“启用”，则该用户可以通过认证； 选择“禁用”，则该用户不可以通过认证。

表 11.3 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。

用户设置

用户类型: 免费用户 ▼

用户名: mianfei (1-100个英文字符)

密码: ... (1-100个英文字符)

允许认证时间段: 00 : 00 - 24 : 00

免费时长: 30 分钟 (1-1440)

同时登录用户数: 1 (1-2048)

上行带宽: 0 Kbps (0或10-1000000, 0表示不限制)

下行带宽: 0 Kbps (0或10-1000000, 0表示不限制)

备注: (1-50个字符, 可选)

启用/禁用: 启用 禁用

确定
清除
取消
帮助

图 11.12 用户管理-用户新增-免费用户界面

用户名	自定义的用户名，不能与已有用户名重复。
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。
允许认证时间段	允许使用该用户名进行认证的时间段。
免费时长	免费用户上网时间限制。
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。
启用/禁用	选择“启用”，则该用户可以通过认证； 选择“禁用”，则该用户不可以通过认证。

表 11.4 用户管理-用户新增-免费用户界面项说明

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	laifefei	123	禁用	--	00:00-24:00	30	1	0	0	不绑定	00-00-00-00-00-00				
4																

图 11.13 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 11.5 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。

Web认证设置

启用Web认证

生效区段：

空闲断线时间： 分钟（1-30）

认证页面：

页面标题：（1-50个字符）

背景图片： 未选择任何文件

（可选，图片大小不能超过200KB，上传图片分辨率建议使用1080*411）

欢迎信息：（1-50个字符）

版权声明：（1-50个字符）

页面预览：

认证方式：

启用到期提醒

开始提醒时间：账号到期前 天

提醒方式：

提醒页面标题：（1-50个字符）

提醒页面内容：（1-50个字符）

页面预览：

图 11.14 使用内置的Web服务器和认证服务器应用界面

启用Web认证	勾选此项，可以启用Web认证功能。
生效区段	选择Web认证功能生效的区段。
空闲断线时间	设置已认证用户空闲断线时间。
认证页面	选择自定义页面。
页面标题	设置Web认证页面的标题。
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，上传图片分辨率建议使用1080*411。
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。
认证方式	选择本地认证。
启用到期提醒	勾选此项，启用到期提醒功能，为正式用户提供到期提醒服务。
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。
提醒页面标题	设置提醒页面的标题。
提醒页面内容	设置提醒页面的内容。

表 11.6 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<预览认证页面>按键,可以预览自定义的 Web 认证登录页面,如图 11.15 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 11.16 所示。

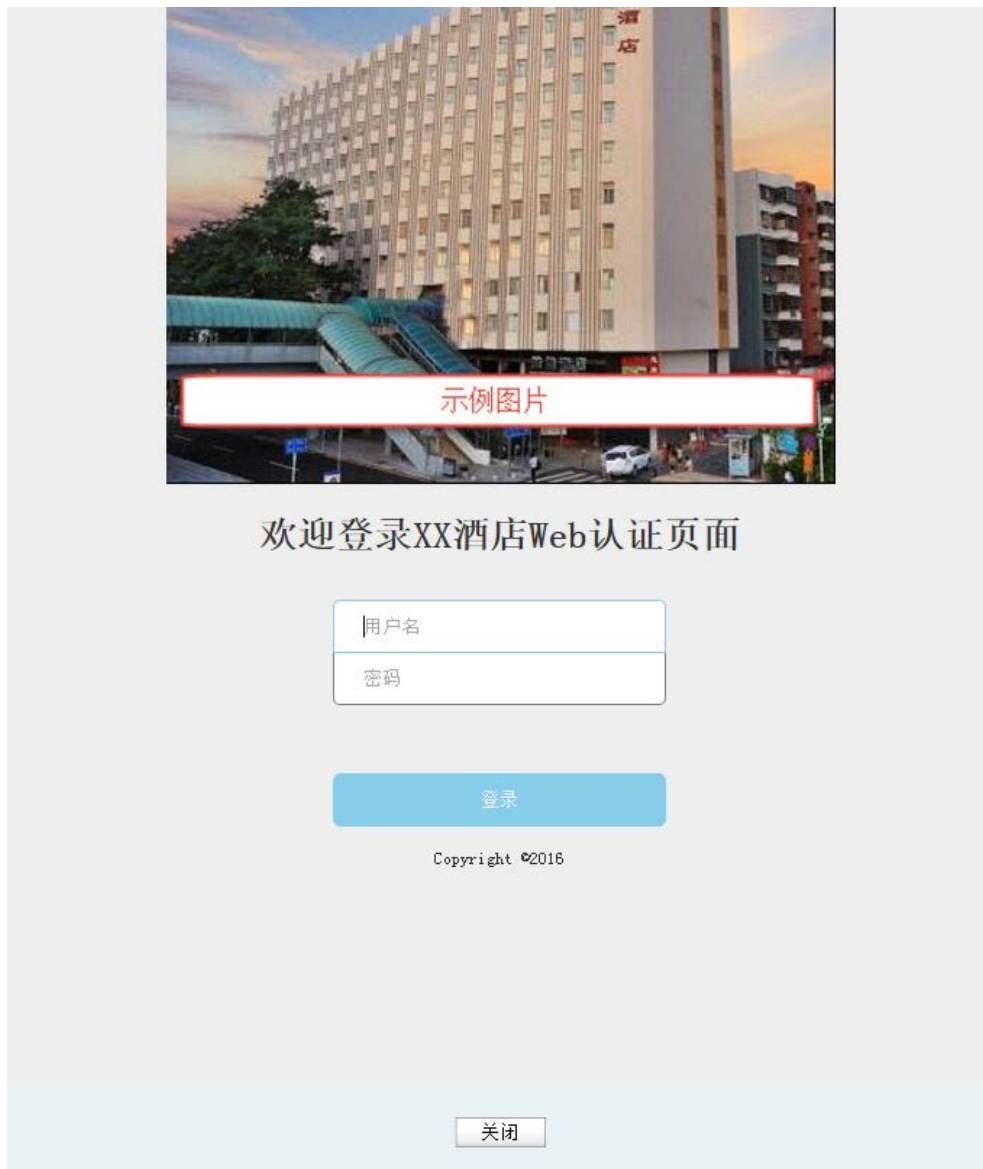


图 11.15 预览Web认证登录页面



图 11.16 预览到期提醒页面

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：xjjudian。
- 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 11.17 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 11.18 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 11.19 免费用户登录成功页面

11.2.3 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：

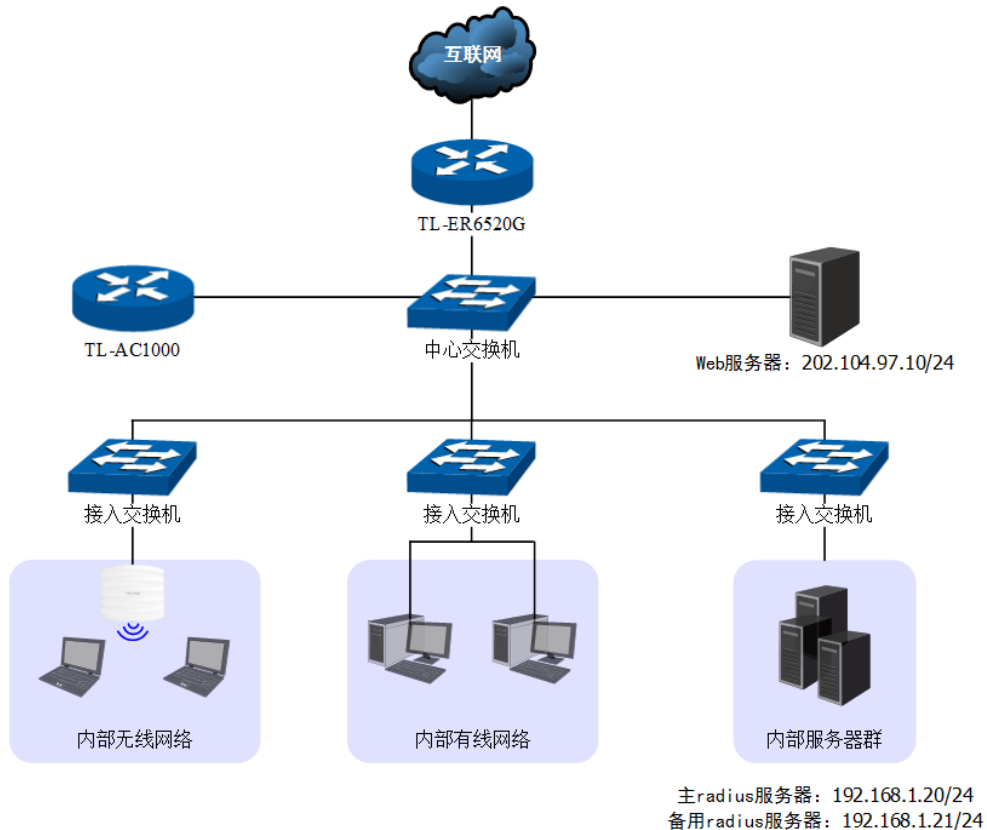


图 11.20 使用外部链接的Web服务器和认证服务器应用拓扑图

准备工作

在设置 Web 认证功能之前，需要做如下准备工作：

1) 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。

2) 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 11.7 网络参数模拟

配置步骤

1 在路由器上设置 Web 认证

- 1) 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。

Web认证设置

启用Web认证

生效区段:

空闲断线时间: 分钟 (1-30)

认证页面:

认证URL: (1-250个英文字符)

认证成功后跳转链接: (1-250个英文字符, 可选)

认证失败后跳转链接: (1-250个英文字符, 可选)

认证方式:

主服务器地址: (1-50个字符, 必选)

备用服务器地址: (1-50个字符, 可选)

认证端口: (1024-65535)

授权共享密钥: (1-120个字符)

失败发送次数: (0-10次)

超时时间: (1-60秒)

认证方式:

图 11.21 使用外部链接的Web服务器和认证服务器应用界面

启用Web认证	勾选此项，可以启用Web认证功能。
生效区段	选择Web认证功能生效的区段。
空闲断线时间	设置已认证用户空闲断线时间。
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、CHAP、MSCHAP和MSCHAPv2。

表 11.8 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 <http://tplogin.cn:8080/wportal/webauth>。
 - 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 11.9 错误码说明表

- 2) 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 **11.4 免认证策略**。

免认证策略设置

策略名称:	<input type="text" value="Web_server"/>	<small>(1-50个字符)</small>
免认证方式:	<input type="text" value="五元组方式"/>	
源IP地址范围:	<input type="text"/>	<small>/ <input type="checkbox"/> (可选)</small>
目的IP地址范围:	<input type="text" value="202.104.97.10"/>	<small>/ <input type="text" value="24"/> (可选)</small>
源MAC地址:	<input type="text"/>	<small>(XX-XX-XX-XX-XX-XX, 可选)</small>
源端口:	<input type="text"/> - <input type="text"/>	<small>(1-65535, 可选)</small>
目的端口:	<input type="text"/> - <input type="text"/>	<small>(1-65535, 可选)</small>
服务协议:	<input type="text" value="TCP"/>	
生效区段:	<input type="text" value="default"/>	
备注:	<input type="text" value="外部Web服务器"/>	<small>(1-50个字符, 可选)</small>
启用/禁用:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	

图 11.22 设置外部Web服务器的免认证策略界面

2 用户上网步骤

- 1) 访问认证页面 <http://202.104.97.10>，在此页面输入酒店分配的用户名和密码，点击<登录>按钮进行认证。
- 2) 若认证成功，网页将自动跳转到 <http://www.jiudian.com>，此时已经可以上网。若认证失败，网页将自动跳转到 <http://www.failed.com/?error=ErrorUserOrPassword> (以错误类型是用户名或密码错误为例示意)，请重新进行认证。
- 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，重新认证后，即可再次上网。

11.3 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：

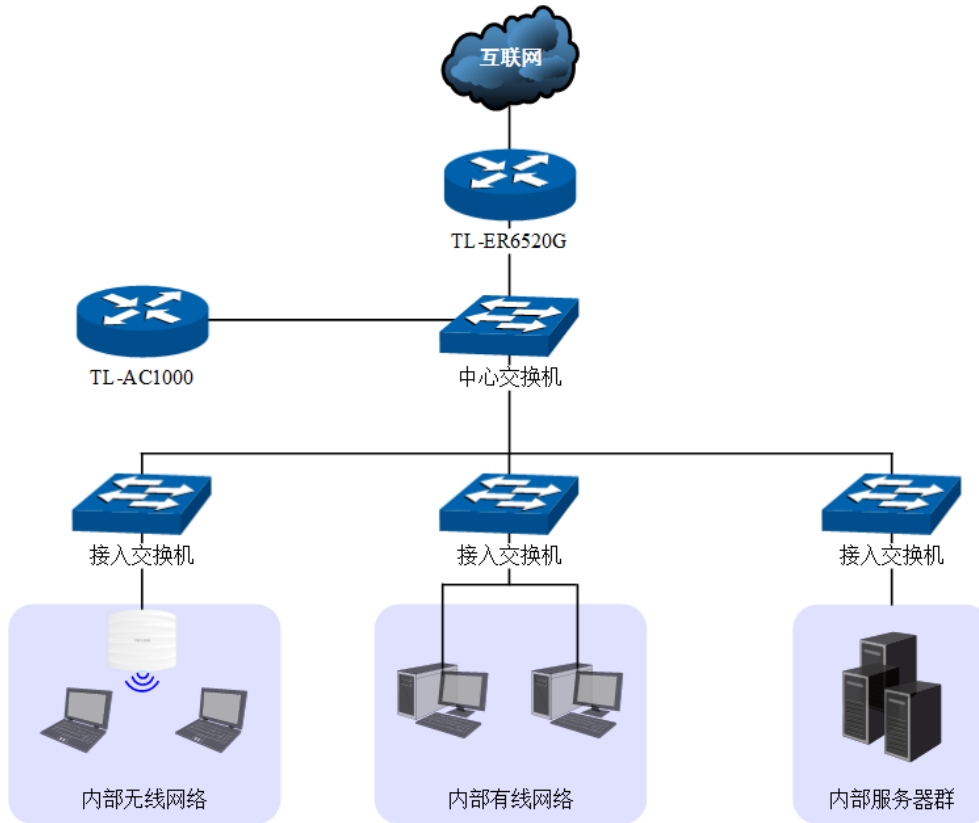


图 11.23 微信连Wi-Fi应用拓扑图

配置方法

1 微信公众号平台后台设置

以订阅号为例，在微信公众号平台后台进行如下设置：

- 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 11.24 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 11.25 新建门店

3) 在微信连 Wi-Fi 功能界面添加设备，如下图所示。

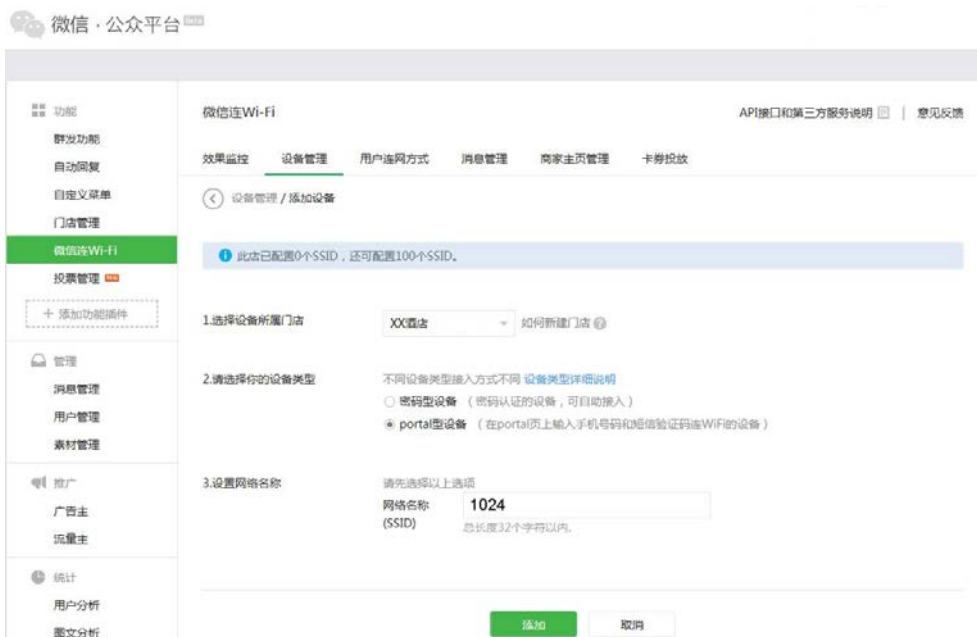


图 11.26 添加设备1

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 11.27 添加设备2

2 在路由器上设置微信连 Wi-Fi 功能

进入页面：认证管理 >> 认证设置 >> 微信连 Wi-Fi，可参考如下参数设置。



图 11.28 微信连Wi-Fi界面

启用微信连Wi-Fi	选择是否启用该微信连 Wi-Fi 条目。
生效区段	选择Web认证功能生效的区段。
免费上网时长	设置用户免费上网的时长。

空闲断线时间	设置已认证用户空闲断线时间。
ShopID	设置微信连 Wi-Fi 门店 ID，可登陆微信公众号官网获取。
AppID	设置微信公众号 ID，可登陆微信公众号官网获取。
SecretKey	设置微信连 Wi-Fi 密钥，可登陆微信公众号官网获取。
Logo 图片	上传认证页面的 Logo 图片。
背景图片	上传认证页面的背景图片。
Logo 信息	设置认证页面的 Logo 信息。
欢迎信息	设置认证页面的欢迎信息。
按钮提示文字	设置认证页面的登录按钮提示文字。
版权声明	设置认证页面的版权信息。

表 11.10 微信连Wi-Fi界面项说明

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。



欢迎使用微信连Wi-Fi

登录

图 11.29 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 11.30 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 11.31 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。

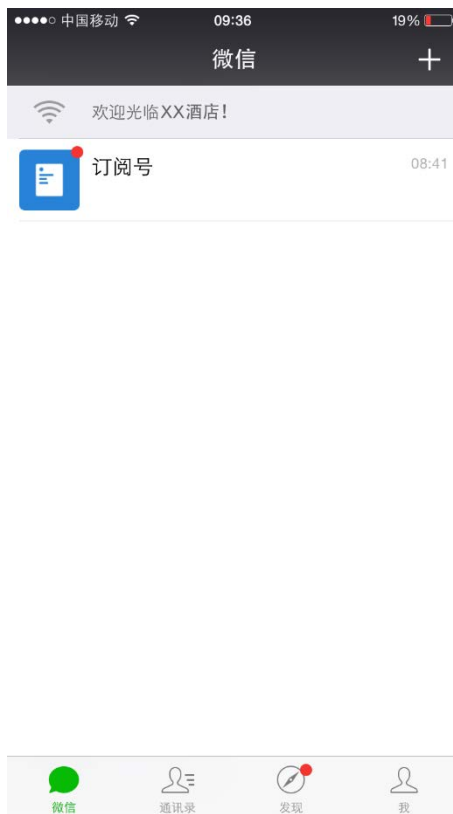


图 11.32 微信页面

11.4 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

免认证策略设置

策略名称: (1-50个字符)

免认证方式: 五元组方式

源IP地址范围: / (可选)

目的IP地址范围: / (可选)

源MAC地址: (XX-XX-XX-XX-XX-XX, 可选)

源端口: - (1-65535, 可选)

目的端口: - (1-65535, 可选)

服务协议: UDP

生效区段: default

备注: (1-50个字符, 可选)

启用/禁用: 启用 禁用

免认证策略列表

选择	序号	策略名称	URL地址	源IP地址范围	目的IP地址范围	源端口	目的端口	服务协议	生效区段	备注	状态	设置
<input type="checkbox"/>	1	dhcp client	---	---	---	68-68	67-67	UDP	---	---	已启用	---
<input type="checkbox"/>	2	dhcp server	---	---	---	67-67	68-68	UDP	---	---	已启用	---
<input type="checkbox"/>	3	dns client	---	---	---	---	53-53	UDP	---	---	已启用	---
<input type="checkbox"/>	4	dns server	---	---	---	53-53	---	UDP	---	---	已启用	---

图 11.33 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。

免认证策略设置

策略名称: (1-50个字符)

免认证方式: 五元组方式

源IP地址范围: / (可选)

目的IP地址范围: / (可选)

源MAC地址: (XX-XX-XX-XX-XX-XX, 可选)

源端口: - (1-65535, 可选)

目的端口: - (1-65535, 可选)

服务协议: UDP

生效区段: default

备注: (1-50个字符, 可选)

启用/禁用: 启用 禁用

图 11.34 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。
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	设置免认证策略的源端口范围。
目的端口	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。
生效区段	选择生效区段，可以针对指定区段设置免认证策略。
备注	设置条目的备注，以方便管理和查找。
启用/禁用	选择“启用”，则使该策略生效； 选择“禁用”，则使该策略失效。

表 11.11 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。

免认证策略设置

策略名称: (1-50个字符)

免认证方式: URL方式

URL地址: (1-128个字符)

源IP地址范围: / (可选)

源MAC地址: (XX-XX-XX-XX-XX-XX, 可选)

生效区段: default

备注: (1-50个字符, 可选)

启用/禁用: 启用 禁用

图 11.35 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。
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。
生效区段	选择生效区段，可以针对指定区段设置免认证策略。
备注	设置条目的备注，以方便管理和查找。
启用/禁用	选择“启用”，则使该策略生效； 选择“禁用”，则使该策略失效。

表 11.12 免认证策略-免认证策略设置-URL方式界面项说明

免认证策略列表

在此区域，可以对已有条目进行操作。序号为1-4的条目是系统预定义的免认证策略，不可操作。序号为1的条目表示：该策略名称为dhcp client，无论是否完成认证，所有从68端口发送到67端口的UDP协议数据包，任何时候都可以通过。该策略已启用。

11.5 认证状态

在此界面可以查看认证成功用户的信息。

进入界面：认证管理 >> 认证状态 >> 认证状态

认证用户列表

选择	序号	认证方式	用户名	接入时间	IP地址	MAC地址	上行速率(Kbps)	下行速率(Kbps)	连接数	操作
<input type="checkbox"/>	1	Web认证-一键上网	N/A	2015-04-09 11:36:36	192.168.1.100	D4:3D:7E:BF:61:5F	0	0	0	

共1条，每页：10条 | 当前：1/1页，1~1条 | [首页](#) [上一页](#) [下一页](#) [尾页](#) 1 [跳转](#)

图 11.36 认证状态界面

认证方式	显示用户登录所使用的认证方式。
用户名	显示用户名。
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。
MAC地址	显示用户的MAC地址。
上行速度	显示用户当前的上传速度。
下行速度	显示用户当前的下载速度。
连接数	显示用户当前所使用的连接数。
操作	点击<  >按键，可断开该用户的连接。

表 11.13 认证状态界面项说明

第12章 系统服务

12.1 电子公告

通过电子公告功能可向局域网内指定用户组发送公告消息。可以在此启用电子公告功能，编辑公告内容并向指定用户发送。

进入界面：系统服务 >> 电子公告

图 12.1 公告设置界面

综合设置

勾选“启用电子公告功能”后，设置的公告才会生效。设置生效区段，路由器仅对生效区段上符合规则的主机发布电子公告。局域网用户在访问外网网页时将会收到公告消息。公告周期可以让路由器每隔指定的时间发布一次公告，周期时长不能小于5分钟。

勾选“启用日志记录”后路由器会记录相关的公告日志。

公告设置

公告名称	输入公告的名称。
标题	输入公告的标题，该项将作为所发布公告的标题。




内容	输入公告的内容。
公告对象	指定被公告的局域网内对象。可以选择“地址组”作为公告对象，也可以不选择，则默认所有IP为公告对象，在条目中显示为Any。如需新建组请参考7.1地址管理。
生效时间	选择公告生效的时间。生效时间设置，请参考7.2时间管理。
发布者	输入公告发布者名称。
备注	添加对本条规则的说明信息。
是否生效	选择当前设置规则是否生效。

表 12.1 公告设置界面项说明

新增的条目会在公告列表里显示出来，如下图所示。

公告列表											
选择	序号	公告名称	标题	内容概要	组	生效时间	发布者	备注	是否生效	设置	
<input type="checkbox"/>	1	公告	公告1	一则公告	IPGROUP_ANY	Any	管理员	---	生效		

图 12.2 公告列表界面

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。

12.2 动态DNS

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

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

路由器作为动态DNS客户端，本身并不提供动态DNS服务。因此，在使用此功能之前，必须进入动态DNS服务提供商的官方主页注册，以获得用户名、密码和域名等信息。TL-ER6520G路由器提供花生壳动态DNS客户端。

进入界面：系统服务 >> 动态DNS >> 花生壳动态域名

功能设置

服务接口：

用户名： [注册用户名](#)

密码：

服务开关： 启用 禁用

域名信息：[查看所有域名](#)

管理列表

选择	序号	接口	用户名	域名	服务类型	连接状态	服务开关	设置
该列表为空								

图 12.3 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。
服务开关	选择启用或禁用花生壳动态域名服务。
域名信息	显示当前登录的DDNS用户所拥有的域名。用户可以申请多个域名，点击“查看所有域名”显示当前用户申请的所有域名，但最多显示16条。

表 12.2 花生壳动态域名登录界面项说明

12.3 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



功能设置

服务接口：

对外生效接口：

启用/禁用服务： 启用 禁用

服务列表


选择	序号	服务名称	协议类型	接口	服务IP地址	外部端口	内部端口	状态
该列表为空								

图 12.4 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 12.3 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-ER6520G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。

12.4 DNS代理

可以通过本页面设置接口的DNS代理功能。



DNS Proxy设置

服务接口：

出接口：

DNS Proxy规则列表

选择	序号	服务接口	出接口
<input type="checkbox"/>	1	eth0	auto

图 12.5 DNS代理设置界面

服务接口	选择在哪些接口上面使用Dns proxy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 12.4 DNS代理设置界面项说明

新增的条目会在**DNS Proxy规则列表**里显示出来，如下图所示。

DNS Proxy规则列表			
选择	序号	服务接口	出接口
<input type="checkbox"/>	1	eth0	auto

图 12.6 DNS代理设置界面

第13章 系统工具

13.1 管理账号

13.1.1 修改管理帐号

在此可以修改登录时使用的用户名和密码。

进入界面：系统工具 >> 管理账号 >> 修改管理帐号

图 13.1 修改管理帐号界面

管理账号

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

表 13.1 修改管理帐号-管理账号界面项说明



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。

会话超时时间

会话超时时间	设置通过Web页面访问路由器的超时时间。登录Web界面后，用户在该设定时间内如无任何操作，路由器将自动断开连接。设置超时时间后，新的超时时间将在下一次登录时生效。
--------	---

表 13.2 修改管理帐号-会话超时时间界面项说明

13.1.2 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

远程管理地址

远程地址范围： /

启用/禁用规则： 启用 禁用

地址列表

选择	序号	远程地址范围	状态	设置
<input type="checkbox"/>	1	182.30.74.100/32	已启用	

图 13.2 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 13.3 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。

地址列表

选择	序号	远程地址范围	状态	设置
<input type="checkbox"/>	1	182.30.74.100/32	已启用	

图 13.3 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：

远程管理地址

远程地址范围： /

启用/禁用规则： 启用 禁用

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：

功能设置

Http服务端口： (80、1024-65535)

Https服务端口： (443、1024-65535)

Telnet服务端口： (23、1024-65535)

Telnet超时时间： 分钟(5-60)

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。

13.1.3 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

功能设置

Http服务端口： (80、1024-65535)

Https服务端口： (443、1024-65535)

Telnet服务端口： (23、1024-65535)

Telnet超时时间： 分钟(5-60)

图 13.4 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。
Telnet服务端口	设置路由器的Telnet服务端口。
Telnet会话超时时间	设置通过Telnet远程访问路由器的超时时间，远程登录路由器后，用户在该设定时间内如无任何指令，路由器将自动断开连接。设置超时时间后，新的超时时间将在下一次登录时生效。

表 13.4 系统管理设置界面项说明

13.2 设备管理

13.2.1 恢复出厂配置

进入界面：系统工具 >> 设备管理 >> 恢复出厂配置

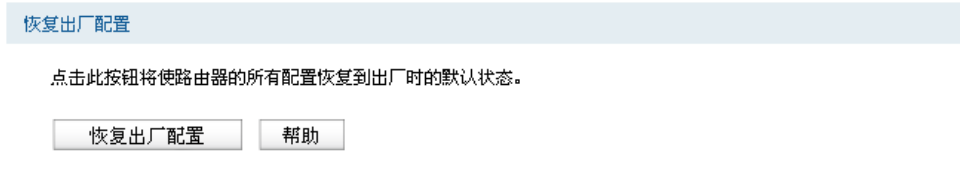


图 13.5 恢复出厂配置界面

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。

13.2.2 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 13.6 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<备份配置信息>按钮，路由器会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

导入配置信息

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



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。

13.2.3 重启路由器

进入界面：系统工具 >> 设备管理 >> 重启路由器



图 13.7 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。

13.2.4 软件升级

进入界面：系统工具 >> 设备管理 >> 软件升级

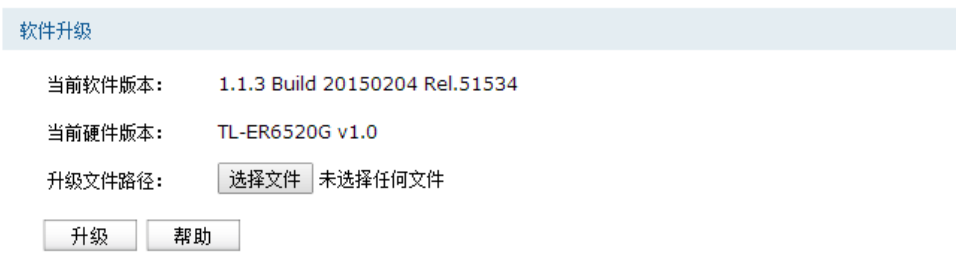


图 13.8 软件升级界面

TP-LINK官方网站 (<http://www.tp-link.com.cn>) 会不定期更新TL-ER6520G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，单击<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。

13.3 流量统计

13.3.1 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**

接口流量统计								
接口	接收速率(Kbps)	发送速率(Kbps)	接收总包数(Pkt)	发送总包数(Pkt)	接收总字节数(Byte)	发送总字节数(Byte)	接收IP分片(Pkt)	接收IP异常包(Pkt)
eth0	0	0	74	84	7899	59096	0	0

刷新 清空统计 帮助

图 13.9 接口流量统计界面

接收/发送速率是以千比特每秒为单位进行统计的，通常所说的1M带宽即1024Kbps。接收/发送总包数统计的是数据包的总个数。接收/发送总字节数统计的则是所有数据包的总字节数。IP分片是指接收到的大小超过WAN口允许接收的最大值，需要分片传输的数据包；IP异常包是指IP封装字段非正常的数据包。

13.3.2 IP流量统计

IP流量统计界面将显示区段与区段之间各个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									
<input checked="" type="checkbox"/> 启用流量统计									
源区段：		default							
目的区段：		wan1							
<input checked="" type="checkbox"/> 启用自动刷新									
保存		帮助							
流量统计列表									
IP地址	当前传输速率 (KB/s)		当前包速率 (Pkt/s)		总包数 (Pkt)		总字节数 (Byte)		连接数
	上行	下行	上行	下行	上行	下行	上行	下行	
192.168.1.109	0	0	0	0	397	0	24122	0	0

当前排序方式为：按IP地址排序 从小到大

刷新 清空

图 13.10 IP流量统计界面

路由器默认勾选“启用流量统计”、“启用自动刷新”选项，启用自动刷新时，路由器每隔10秒刷新一次。选择源区段与目的区段后，相应的流量统计信息将显示在流量统计列表中。

13.4 诊断工具

13.4.1 诊断工具

可在诊断工具界面通过ping命令或tracert命令来诊断当前路由器的网络连接状态。

进入界面：系统工具 >> 诊断工具 >> 诊断工具

PING通信检测

目的IP/域名：

正在检测[192.168.1.199]是否可达，发送的请求包大小为64bytes:

1. 接收到 的应答包：大小：64bytes 时延：1ms 生存时间(TTL): 128.
2. 接收到 的应答包：大小：64bytes 时延：2ms 生存时间(TTL): 128.
3. 接收到 的应答包：大小：64bytes 时延：1ms 生存时间(TTL): 128.
4. 接收到 的应答包：大小：64bytes 时延：1ms 生存时间(TTL): 128.

< 检测完成 >

检测[192.168.1.199]的结果统计:

数据包数目：发送包个数：4， 接收包个数：4， 丢失包个数：0， (0% 丢包率).

时延统计:

最短时延：1ms， 最长时延：2ms， 平均时延：1ms.

路由跟踪检测

目的IP/域名：

正在跟踪[192.168.1.199]，最大跳数为 30 跳:

1. 1ms 1ms 1ms 192.168.1.199

< 跟踪完成 >

图 13.11 诊断工具界面

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。
----------------	---

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。
----------------	--

13.4.2 在线检测

该页面用于检测接口是否在线。

进入界面：[系统工具](#) >> [诊断工具](#) >> [在线检测](#)

检测设置

接口名：

检测开关： 开启 关闭

检测模式： 自动 手动

PING检测：

DNS检测：

接口状态列表

选择	序号	接口名	检测开关	检测模式	PING检测	DNS检测	状态	设置
<input type="checkbox"/>	1	eth0	开启	自动	---	---	接口在线	

图 13.12 在线检测界面

接口名	选择需要在线检测的接口。
检测开关	选择开启或关闭在线检测。开启在线检测时，路由器将综合PING检测和DNS检测的结果判断接口是否在线。
检测模式	选择自动在线检测或者手动在线检测。自动模式下，PING检测选择网关作为目的地址，DNS检测选择接口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。
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 13.5 在线检测界面项说明

新增的条目会在[接口状态列表](#)里显示出来，如下图所示。

接口状态列表

选择	序号	接口名	检测开关	检测模式	PING检测	DNS检测	状态	设置
<input type="checkbox"/>	1	eth0	开启	自动	---	---	接口在线	

图 13.13 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。

13.5 时间设置

13.5.1 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。

进入界面：系统工具 >> 时间设置 >> 时间设置

图 13.14 时间设置界面

当前时间


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

时间设置

<p>通过网络获取系统时间</p>	<p>若路由器可以访问互联网，可选择此项进行网络校时。选择时区后点击<设置>按钮，路由器将在内置NTP（Network Time Protocol，网络校时协议）服务器地址列表中搜索可用地址，并获取时间。若获取失败，请手动设置NTP服务器地址，由于NTP服务器并非固定不变，推荐搜索两个不同的地址，分别填入首选、备用NTP服务器输入框，NTP服务器地址可以为IP地址也可以为域名。设置完毕后点击<设置>按钮，路由器会通过指定的NTP服务器获取网络时间。</p>
--------------------------	--

手工设置系统时间	若路由器暂时不能访问互联网，可以选择对系统时间进行手动设置，或者点击<获取管理主机时间>按钮，系统将自动填入当前管理主机时间信息。设置完毕后点击<设置>生效。
-----------------	---

表 13.6 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。
- 如果夏令时被启用，那么您所设置的时间将会受到夏令时的影响。因此，您需要决定是否需要先关闭夏令时模块再进行时间的设置。

13.5.2 夏令时设置

可以通过本页面对夏令时进行设置。

当前状态

状态：夏令时生效

夏令时设置

启用/禁用： 启用 禁用

模式：手动设置 ▼

手动设置

时间偏移量： 分钟 (0-180)

开始时间： 年 月 日 时 分

结束时间： 年 月 日 时 分

每年生效

设置 帮助

图 13.15 夏令时设置界面

状态	用于显示当前夏令时的运行状态。 夏令时未启用：说明夏令时功能被禁用。如果您要使用夏令时功能，请选择开启此功能。 夏令时未生效：表明当前系统没有按照夏令时来工作。 夏令时生效：表明当前系统按照夏令时来工作。
启用/禁用	选择是否开启夏令时功能。
模式	您可以选择进行设置夏令时的方式。 自动设置：系统将会采用内置夏令时进行设置。 手动设置：您可以选择自己设置夏令时的开始和结束时间。

表 13.7 夏令时设置界面项说明

手动设置

时间偏移量	输入需要把时钟拨快的时间。
开始时间	输入夏令时生效的时间。
结束时间	输入夏令时结束的时间。
每年生效	勾选此选项，表明每一年都按照设置的时间设置夏令时。

表 13.8 夏令时设置界面项说明-手动设置

自动设置

目前内置的国家和地区包括：欧洲，澳大利亚，俄罗斯，新西兰，美国。具体夏令时信息见下表。

欧洲	每年3月份最后一个星期天1点至10月最后一个星期天1点，时间拨快1个小时
澳大利亚	每年10月第一个星期天2点至次年4月第一个星期天3点，时间拨快一个小时
俄罗斯	全年永久夏令时，时间拨快1个小时。
新西兰	每年10月第一个星期天2点至次年3月最后一个星期天3点，时间拨快1个小时
美国	每年3月第二个星期天2点至11月第一个星期天2点，时间拨快1个小时

表 13.9 夏令时设置界面项说明-自动设置

13.6 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

日志列表

序号	时间	日志等级	日志内容
1	2031-01-09 20:45:12	<5> 通知信息	IP地址 192.168.1.109 成功访问本路由器的 web 服务器。

刷新 清空日志

日志设置

启用自动刷新

选择日志等级 <6> 消息报告

发送系统日志

服务器地址： 0.0.0.0

设置 帮助

图 13.16 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仅列出指定等级的日志记录。

各等级描述：

<0> 致命错误	导致系统不可用的错误，红色显示。
<1> 紧急错误	必须对其采取紧急措施的错误，红色显示。
<2> 严重错误	导致系统处于危险状态的错误，红色显示。
<3> 一般错误	一般性的错误提示，橙色显示。
<4> 警告信息	系统仍然正常运行，但可能存在隐患的提示信息，橙色显示。
<5> 通知信息	正常状态下的重要提示信息。
<6> 消息报告	一般性的提示信息。
<7> 调试信息	调试过程产生的信息。

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

13.7 系统参数

您可以通过本页面设置逻辑接口的路由Metric信息。

路由Metric设置

MANUAL接口： (0-15)

DHCP接口： (0-15)

PPPoE接口： (0-15)

PPTP接口： (0-15)

L2TP接口： (0-15)

图 13.17 系统参数设置界面

MANUAL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。
PPTP接口	填写PPTP拨号时的路由Metric信息。
L2TP接口	填写L2TP拨号时的路由Metric信息。

表 13.10 系统参数界面项说明

第14章 典型配置举例

14.1 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；

14.2 组网方案及特点

为满足上述网络需求，使用TL-ER6520G进行组网，网络拓扑如下图所示。

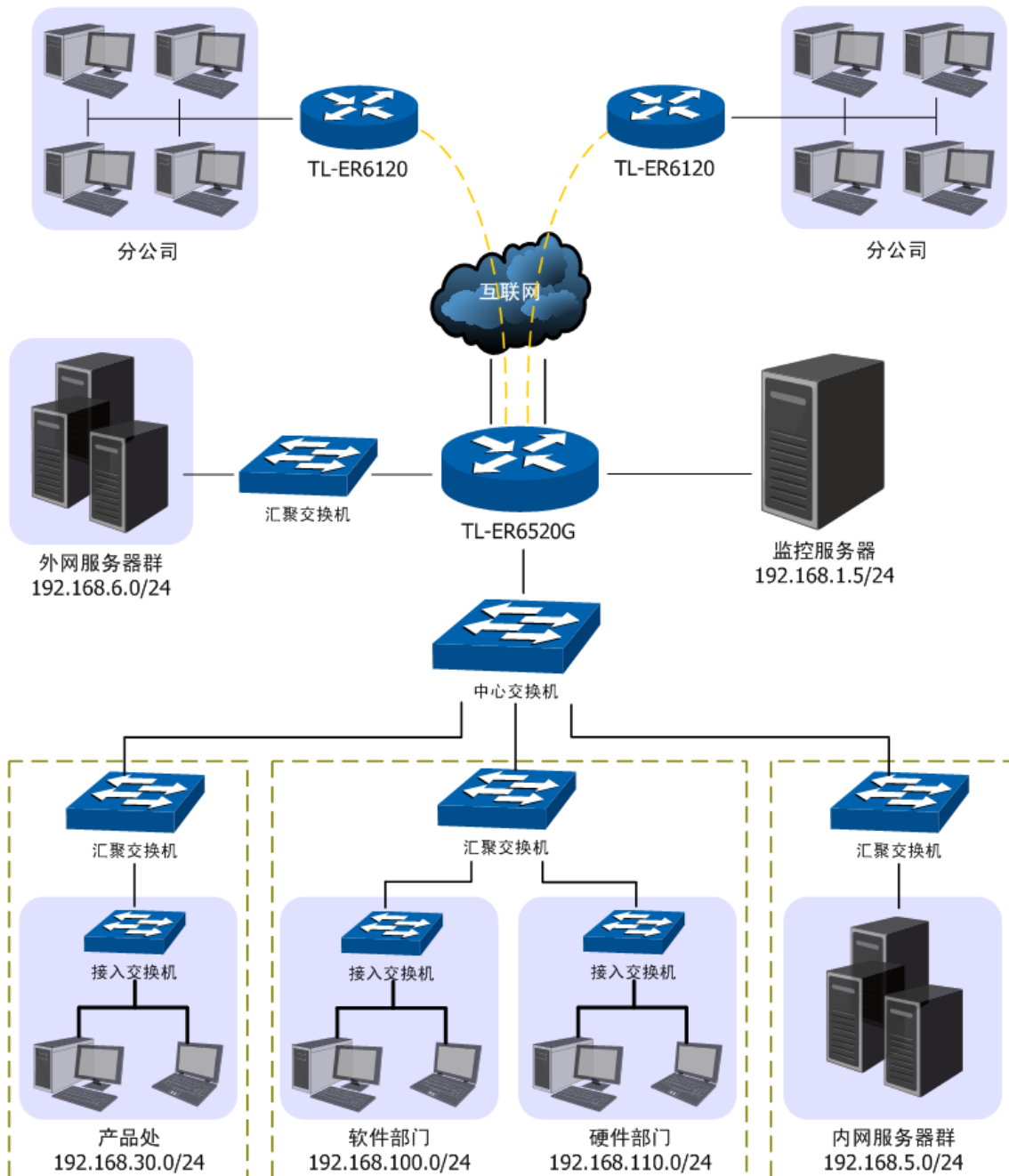


图 14.1 企业整体组网应用

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，可以设置各部门属于不同的网段，在各交换机上通过VLAN相互隔离，在TL-ER6520G上分别属于不同区段下的接口并通过访问策略功能进一步限制各区段之间的网络通信，如以“RD”区段表示研发区段，区段下包含两个接口分别指向软件部门和硬件部门；

- 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；

14.3 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 14.1，在后面的配置步骤中将使用表格中的参数进行举例。

区段	接口名称	描述	物理端口	VLAN	网段
RD	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	product	产品部门	1	30	192.168.30.0/24
SERVER	server	办公服务器群	1	5	192.168.5.0/24
DMZ	dmz	公网服务器群	2	6	192.168.6.0/24
ISP1	isp1	电信	3	10	201.1.1.1/24
ISP2	isp2	联通	4	20	

表 14.1 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1-5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管理接口eth0，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 eth0，也可以是新创建的管理接口。例如，在本例中为了保证整个过程中配置正常，管理计算机可以和监控服务器通过交换机连接到端口5，端口5所属的接口可以保持在出厂默认的管理接口。

根据14.2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。

14.3.1 配置VLAN

由表 14.1可知，本组网需要创建VLAN 5 /6 /10 /20 /30 /100 /110，此处将统一进行介绍。

1. 配置端口链路类型

进入界面：基本设置 >> VLAN设置 >> 端口设置

由表 14.1可知，端口1需要处理多个VLAN的数据，且中心交换机需要通过数据包中的VLAN TAG来转发数据包，因此端口1需要配置为trunk，端口2/3/4只需处理一个VLAN的数据，则可以设置为access，或保持不变。

端口	链路类型	PVID
1	trunk	1
2	access	1
3	access	1
4	access	1
5	access	1

设置 帮助

图 14.2 端口设置界面-设置端口1链路类型

2. 创建VLAN

进入界面：基本设置 >> VLAN设置 >> VLAN设置

根据表 14.1，依次创建VLAN 5 /6 /10 /20 /30 /100 /110，其中VLAN 5 /30 /100 /110，四个VLAN的成员端口均包含端口1，VLAN6的成员端口为端口2，VLAN10的成员端口为端口3，VLAN20的成员端口为端口4，下面以创建VLAN5为例。

VLAN设置

VLAN ID: 5 (2-4094)

名称: 办公服务器群

端口设置:

端口	链路类型	TAG标签
<input checked="" type="checkbox"/> 1	Trunk	TAG
<input type="checkbox"/> 2	Access	UNTAG
<input type="checkbox"/> 3	Access	UNTAG
<input type="checkbox"/> 4	Access	UNTAG
<input type="checkbox"/> 5	Access	UNTAG

备注: (可选)

新增 清除 帮助

图 14.3 VLAN设置界面-创建办公服务器群VLAN

根据表 14.1的VLAN参数，创建所有VLAN后，应该可以在下方的VLAN列表查看已创建的VLAN，如下图所示。

VLAN列表						
选择	序号	VLAN ID	名称	端口设置	备注	设置
<input type="checkbox"/>	1	1	vlan1	5(UNTAG)	system vlan	
<input type="checkbox"/>	2	5	办公服务器群	1(TAG)	---	
<input type="checkbox"/>	3	6	公网服务器群	2(UNTAG)	---	
<input type="checkbox"/>	4	10	电信	3(UNTAG)	---	
<input type="checkbox"/>	5	20	联通	4(UNTAG)	---	
<input type="checkbox"/>	6	30	产品部门	1(TAG)	---	
<input type="checkbox"/>	7	100	研发软件部门	1(TAG)	---	

图 14.4 VLAN设置界面-查看网络中VLAN列表

14.3.2 配置区段和接口

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ISP2六个区段。其中RD区段需要创建两个eth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区段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区段和接口。

1. 创建区段

进入界面：基本设置 >> 区段设置

点击页面左边的区段栏的“+”按钮，在弹出的区段名称页面中输入需要创建的区段名称，点击“确定”按钮后即可完成创建，如图 14.5和图 14.6所示操作，即可创建区段“RD”。



图 14.5 区段设置界面-创建新区段



图 14.6 区段设置界面-设置新区段名称RD

由表 14.1可知，需要创建六个区段，重复上述操作后即可在左边的区段栏查看所有已创建区段，如下图所示。



图 14.7 区段设置界面-查看网络中所有区段

2. 创建eth接口

进入界面：基本设置 >> 区段设置

点击页面左边区段栏的区段名称，即可弹出相应区段的参数信息界面，可以创建接口或修改接口参数。点击接口设置区域的<+>按钮，即可在新增接口页面中创建接口，如下图所示操作，点击<设置>按钮后，即可在区段“RD”中创建“soft_dep”接口。

The screenshot displays the configuration interface for a network zone named 'RD'. On the left, a sidebar lists various zones: default, RD (highlighted), PRODUCT, SERVER, DMZ, ISP1, and ISP2. The main area is titled 'RD' and contains the following fields:

- Zone Name: RD
- Zone Port: (represented by five port icons)
- Buttons: 修改, 删除所有接口, 删除本区段, 帮助
- Interface Settings Section:
 - 新增接口 (+)
 - Interface Type: eth
 - Interface Name: soft_dep
 - VLAN: 研发软件部门
 - Connection Mode: manual
 - IP Address: 192.168.100.1
 - Subnet Mask: 255.255.255.0

图 14.8 区段设置界面-创建软件部门eth接口

根据表 14.1中的参数，重复上述操作为各网段创建eth类型接口，此处将不重复介绍。



说明：

创建连接电信的eth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。

3. 创建其他接口

进入界面：基本设置 >> 区段设置

需要设置一个pppoe类型接口接入联通网络。点击接口设置区域的<+>按钮，如下图所示操作，点击<设置>按钮完成配置。

图 14.9 区段设置界面-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。

14.3.3 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。

1. 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。

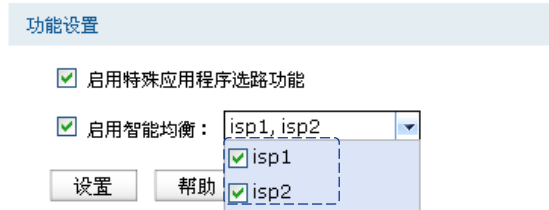


图 14.10 设置智能均衡

2. 配置ISP选路

进入界面：传输控制 >> 流量均衡 >> ISP选路

在界面的**选路功能设置**区域，勾选启用ISP地址段选路功能选项，点击<设置>按钮使ISP选路功能生效。在界面的**ISP选路设置**区域，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<新增>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 14.11 设置ISP选路

3. 配置在线检测

进入界面：系统工具 >> 诊断工具 >> 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 14.12 设置在线检测

14.3.4 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。

1. 创建用户对象

进入界面：对象管理 >> 地址管理 >> 地址组

输入新创建地址组的名称，点击<新增>按钮完成配置。

The image shows the 'Group Settings' interface. It has two input fields:

- 名称: soft_ip
- 备注: (可选)

Buttons: 新增, 清除, 帮助

图 14.13 地址组设置界面-创建地址组

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<新增>按钮完成配置。

图 14.14 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 >> 视图

在本页面中将用户地址段加入地址组中，其他应用涉及的用户对象参数将直接引用地址组。如下图所示，选择可选用户，点击< >> >按钮将用户移入地址组，点击<设置>按钮完成配置。

图 14.15 视图设置界面-设置RD用户组

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

2. 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，选择日期设置工作日历，点击<新增>按钮完成配置。

工作日历

名称：

备注：

日历设置：

2000年	所有日期	日	一	二	三	四	五	六	
		<input type="button" value="清除"/>	<input type="button" value="全选"/>	<input type="button" value="清除"/>	<input type="button" value="清除"/>	<input type="button" value="清除"/>	<input type="button" value="清除"/>	<input type="button" value="清除"/>	<input type="button" value="全选"/>

1月	2月	3月	4月
日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
5月	6月	7月	8月
日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
9月	10月	11月	12月
日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
2001年1月			
日 一 二 三 四 五 六 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31			

工作日历列表

选择	序号	日历名称	工作日历	备注	设置
该列表为空					

图 14.16 工作日历设置界面-创建日常工作日历

进入界面：对象管理 >> 时间管理 >> 工作时间

输入工作时间名称，设置具体时间段，如下图所示操作，点击<新增>按钮完成配置。

图 14.17 工作时间设置界面-设置日常工作时间

进入界面：对象管理 >> 时间管理 >> 时间管理

在本页面中输入时间对象名称，选择包含的工作日历和工作时间，如下图所示，点击<新增>按钮完成配置。

图 14.18 时间对象设置界面-设置工作时间对象

14.3.5 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。

1. 配置区段间访问规则

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

进入界面：安全管理 >> 访问策略 >> 区段间访问规则

在区段选择下拉列表中勾选需要进行通信限制的区段组，点击<显示>按钮弹出相应区段组的配置框，可多选。如本例中我们选择RD区段和其他区段进行限制。

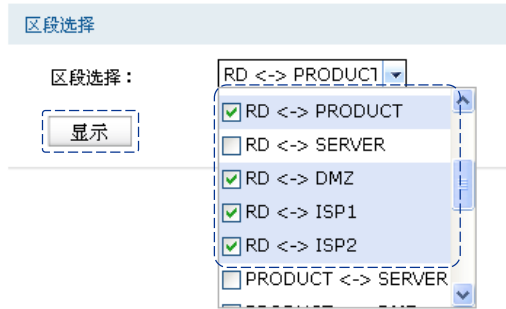


图 14.19 区段间访问规则设置界面-选择区段组

以RD区段和DMZ区段为例，要求RD区段用户在工作时间内不能访问DMZ区段中的服务器。选中RD和DMZ区段的规则设置界面，按图 14.20进行配置，点击<新增>按钮后完成配置。

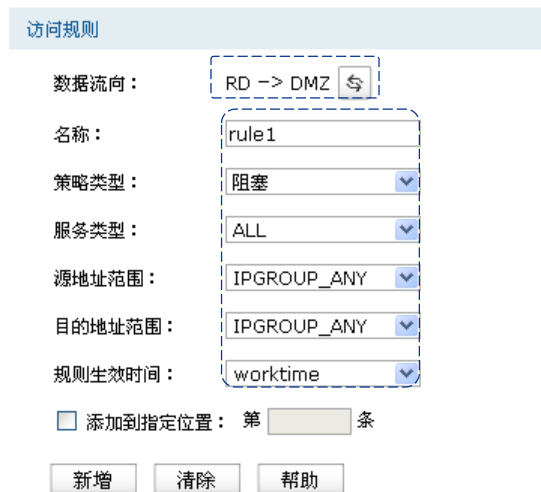


图 14.20 区段间访问规则设置界面-设置RD/DMZ区段间访问规则

此规则表示在“worktime”时间范围内，来源于RD区段发往DMZ区段的任意数据包均将被丢弃不做转发。“worktime”时间对象即14.3.4配置对象介绍的工作时间内的时间对象。

为了信息安全，还需要保证在工作时间内，来源于DMZ区段发往RD区段的任意数据包均将被丢弃不做转发。配置方法如图 14.20所示，只需点击<↔>按钮改变数据流向后再次点击<新增>按钮提交即可。下图为RD区段和DMZ区段之间需要设置的区段间访问规则列表。

规则列表										
选择	序号	名称	策略类型	服务类型	源区段	目的区段	源地址范围	目的地址范围	生效时间	设置
<input type="checkbox"/>	1	rule2	阻塞	ALL	DMZ	RD	IPGROUP_ANY	IPGROUP_ANY	worktime	
<input type="checkbox"/>	2	rule1	阻塞	ALL	RD	DMZ	IPGROUP_ANY	IPGROUP_ANY	worktime	

图 14.21 区段间访问规则设置界面-查看RD/DMZ区段间访问规则列表

任意区段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，可以参考9.4访问策略小节进行介绍。

2. 配置区段内访问规则

由网络的需求分析可知，RD区段中的软件部门和硬件部门不能够直接通信，需要设置区段内访问规则进行限制。

进入界面：安全管理 >> 访问策略 >> 区段内访问规则

RD区段中，需要限制软件部门和硬件部门之间的直接通信，如下图所示内容进行配置，点击<新增>按钮后完成配置。

访问规则

名称： rule1

策略类型： 阻塞

服务类型： ALL

区段： RD

源地址范围： soft_ip

目的地址范围： hard_ip

规则生效时间： Any

添加到指定位置： 第 条

新增 清除 帮助

图 14.22 区段内访问规则设置界面-设置RD区段内访问规则

此规则表示，来源于RD区段中“soft_ip”地址段范围发往目标地址范围是“hard_ip”的数据包，均将被路由器丢弃不做转发。“soft_ip”和“hard_ip”地址对象即14.3.4配置对象介绍的地址对象。

为了信息安全，还需要保证来源于RD区段中“hard_ip”地址段范围发往目标地址范围是“soft_ip”的数据包均将被丢弃不做转发。配置方法同图 14.22所示，只需修改源地址范围和目的地址范围参数后再次点击<新增>按钮提交即可。下图为RD区段需要设置的区段内访问规则列表。

规则列表									
选择	序号	名称	策略类型	服务类型	生效区段	源地址范围	目的地址范围	生效时间	设置
<input type="checkbox"/>	1	rule2	阻塞	ALL	default	hard_ip	soft_ip	Any	
<input type="checkbox"/>	2	rule1	阻塞	ALL	RD	soft_ip	hard_ip	Any	

图 14.23 区段内访问规则设置界面-查看RD区段内访问规则列表

14.3.6 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。

1. 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。



NAPT规则配置界面截图，显示以下配置项：

- 规则名称：napt1
- 源地址范围：192.168.30.0 / 24
- 出接口：isp1
- 备注：（可选）
- 启用/禁用规则： 启用 禁用
- 操作按钮：新增、清除、帮助

图 14.24 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时都做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。

映射列表							
选择	序号	规则名称	源地址范围	出接口	状态	备注	设置
<input type="checkbox"/>	1	napt1	192.168.30.0/24	isp1	已启用	---	
<input type="checkbox"/>	2	napt2	192.168.30.0/24	isp2	已启用	---	

图 14.25 NAPT设置界面-查看产品部门NAPT转发规则

2. 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。



一对一NAT映射配置界面截图，显示以下配置项：

- 映射名称：nat1
- 映射地址：192.168.6.5 -> 211.1.1.5
- 出接口：isp1
- DMZ转发： 开启 关闭
- 备注：（可选）
- 启用/禁用规则： 启用 禁用
- 操作按钮：新增、清除、帮助

图 14.26 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。

14.3.7 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。

1. 设置IKE安全提议

进入界面：VPN >> IKE >> IKE安全提议

在界面的设置区域，输入安全提议名称，选择合适的加密、验证算法及DH组，如下图所示进行操作，点击<新增>按钮后完成配置。

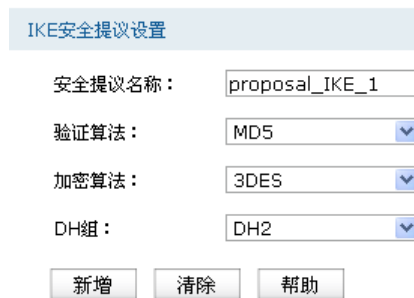


图 14.27 设置IKE安全提议

2. 设置IKE安全策略

进入界面：VPN >> IKE >> IKE安全策略

在界面的设置区域，输入安全策略名称，选择交换模式、封装模式和协商模式，并选择刚才创建的“proposal_IKE_1”IKE安全提议，然后输入预共享密钥，设置生存时间，并开启DPD检测。如图 14.28所示进行操作，点击<新增>按钮后完成配置。

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。

IKE安全策略设置

安全策略名称：

交换模式： 主模式 野蛮模式

封装模式： 隧道模式 传输模式

协商模式： 初始者模式 响应者模式

模式配置：

本地ID类型： IP地址 NAME

本地ID：

对端ID类型： IP地址 NAME

对端ID：

安全提议一：

安全提议二：

安全提议三：

安全提议四：

预共享密钥：

生存时间： 秒 (60-604800)

DPD检测开启： 启用 禁用

DPD检测周期： 秒 (1-300)

图 14.28 设置IKE安全策略

3. 设置IPsec安全提议

进入界面：VPN >> IPsec >> IPsec安全提议

在界面的设置区域，输入安全提议名称，选择合适的安全协议及算法，如下图所示进行操作，点击<新增>按钮后完成配置。

IPsec安全提议设置

安全提议名称：

安全协议：

ESP验证算法：

ESP加密算法：

图 14.29 设置IPsec安全提议

4. 设置IPsec安全策略

进入界面：VPN >> IPsec >> IPsec安全策略

在界面的**启用IPsec功能**区域，点选启用，点击<设置>按钮使IPsec功能生效。在界面的**IPsec安全策略设置**区域，输入安全策略名称，启用安全策略，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。然后选择“IKE协商”，使用刚才创建的“IKE_1”IKE安全策略和“proposal_IPsec_1”IPsec安全提议，PFS选择DH1组，并设置生存时间。如下图所示进行操作，点击<新增>按钮后完成配置。

The screenshot shows the configuration interface for IPsec. It is divided into two main sections:

- 启动IPsec功能 (Start IPsec Function):**
 - 启用IPsec功能: 启用 禁用
 - 设置 (Settings button)
- IPsec安全策略设置 (IPsec Security Policy Settings):**
 - 安全策略名称: IPsec_1
 - 启用安全策略: 启用 禁用
 - 本地子网范围: 192.168.6.0 / 24
 - 对端子网范围: 172.31.10.0 / 24
 - 选择接口: isp1
 - 对端网关: 116.31.85.133 (IP地址或域名)
 - 协商方式: IKE协商 手动模式
 - IKE安全策略: IKE_1
 - 安全提议一: proposal_IPsec_1
 - 安全提议二: ----
 - 安全提议三: ----
 - 安全提议四: ----
 - PFS: DH1
 - 生存时间: 3600 秒 (120-604800)
 - 新增 (Add), 清除 (Clear), 帮助 (Help) buttons

图 14.30 设置IPsec安全策略



说明:

分公司的VPN路由器上也需要做对应的IPsec设置，其中“IPsec安全提议”等设置需与总部保持一致，而“对端网关”则需填写总部路由器VPN接口的IP地址，即图中的isp1接口。

5. 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									
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	1396855 654	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	9123845 68	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

刷新 搜索 帮助

图 14.31 查看IPSec安全联盟

14.3.8 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。

1. 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。

组设置

名称：

备注： (可选)

图 14.32 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<新增>按钮完成配置。

地址设置

名称：

IP类型： IP段 IP/Mask

/

备注： (可选)

图 14.33 地址设置界面-创建产品部职员地址段

进入界面：对象管理 >> 地址管理 >> 视图

在本页面中将产品部职员地址段“group1”加入产品部职员地址组成员列表中，如下图所示，点击<设置>按钮完成配置。



图 14.34 视图设置界面-设置产品部职员用户组

2. 配置应用限制**进入界面：安全管理 >> 应用限制 >> 应用限制**

在界面的**功能设置**区域，勾选启用应用限制功能选项，点击<设置>按钮使应用限制功能生效。在界面的**应用限制设置**区域，选择受控地址组为“PRODUCT”；点击<设置列表>按钮，在显示的界面中勾选需要禁止使用的软件，点击<确定>按钮；最后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<新增>按钮后完成配置。



图 14.35 设置应用限制

14.3.9 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。

1. 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。

功能设置

扫描范围： 192.168.30.1 - 192.168.30.254

开始扫描 帮助

扫描结果

选择	序号	IP地址	MAC地址	状态
<input checked="" type="checkbox"/>	1	192.168.30.21	00-19-66-80-54-36	未绑定

全选 导入 搜索

图 14.36 ARP扫描并绑定

2. 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**区域输入需要绑定的用户的IP地址和MAC地址信息，选择用户接入的接口，点击<新增>按钮即可将条目进行绑定。

IP MAC绑定

IP地址： 192.168.30.51

MAC地址： 00-19-66-3C-A0-21

出接口： product

备注： (可选)

是否生效： 启用 禁用

新增 清除 帮助

图 14.37 手动绑定ARP信息

3. 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**功能设置**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”选项并选择生效区段，本组网中，需要将RD、PRODUCT和SERVER区段的设备进行ARP防护，根据需要勾选“启用ARP日志记录”选项，如下图所示进行操作，点击<设置>按钮完成配置。

功能设置

- 启用ARP防欺骗功能
- 仅允许IP MAC绑定的数据包通过路由器
- 生效区段： RD, PRODUCT, SE
- 允许路由器在发现ARP攻击时发送GARP包
- 发包间隔： 100 毫秒
- 启用ARP日志记录

设置

图 14.38 设置ARP防护功能

14.3.10 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。

功能设置

启用防护攻击日志

防Flood类攻击

启用防多连接的TCP SYN Flood攻击 阈值： Pkt/s

启用防多连接的UDP Flood攻击 阈值： Pkt/s

启用防多连接的ICMP Flood攻击 阈值： Pkt/s

启用防固定源的TCP SYN Flood攻击 阈值： Pkt/s

启用防固定源的UDP Flood攻击 阈值： Pkt/s

启用防固定源的ICMP Flood攻击 阈值： Pkt/s

防可疑包攻击

启用防碎片包攻击

启用防TCP Scan(Stealth FIN/Xmas/Null)

启用防Ping of death

启用防Large ping

启用防WinNuke攻击

阻止同时设置FIN和SYN的TCP包

阻止仅设置FIN未设置ACK的TCP包

阻止带选项的IP包

安全限制 宽松选路
 严格选路 记录路径
 流标记 时间戳
 空标记

图 14.39 设置攻击防护功能

14.3.11 配置内网流量监控

1. 设置端口监控

进入界面：基本设置 >> 交换机设置 >> 端口监控

在界面的功能设置区域，勾选“启用端口监控”选项并设置监控模式为“输入输出监控”；在监控列表区域，将端口5设置为监控端口，端口5连接监控服务器，能够捕获分析网络中的数据，勾选端口1-4为被监控端口，如下图所示进行操作，点击<设置>按钮完成配置。

功能设置

启用端口监控

监控模式：

监控列表

端口	监控端口	被监控端口
1	<input type="radio"/>	<input checked="" type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="checkbox"/>
3	<input type="radio"/>	<input checked="" type="checkbox"/>
4	<input type="radio"/>	<input checked="" type="checkbox"/>
5	<input checked="" type="radio"/>	<input type="checkbox"/>

图 14.40 设置端口监控功能

2. 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	接收速率(Kbps)	发送速率(Kbps)	接收总包数(Pkt)	发送总包数(Pkt)	接收总字节数(Byte)	发送总字节数(Byte)	接收IP分片(Pkt)	接收IP异常包(Pkt)
eth0	0	0	28553	39694	2382639	45601720	0	0
soft_dep	0	0	0	507	0	21294	0	0
hard_dep	0	0	0	1	0	42	0	0
product	0	0	849	2994	73103	1447669	0	0
server	0	0	0	1	0	42	0	0
dmz	0	0	0	507	0	21294	0	0
icm1	0	0.081	171	30803	23290	1126340	0	0

图 14.41 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“启用流量统计”选项并设置需要统计的数据包的源区段和目的区段，并勾选“启用自动刷新”选项，如下图所示配置，点击<设置>按钮即可完成配置。在**统计列表**区域可查看相应的IP流量统计结果，如下图所示。

功能设置

启用流量统计

源区段： default, PRODUC

目的区段： default, RD

启用自动刷新

流量统计列表

IP地址	当前传输速率 (KB/s)		当前包速率 (Pkt/s)		总包数 (Pkt)		总字节数 (Byte)		连接数
	上行	下行	上行	下行	上行	下行	上行	下行	
192.168.1.1	0	0	0	0	0	2	0	96	0
192.168.1.21	0	0	0	0	2	0	96	0	0

图 14.42 查看IP流量统计结果

第15章 命令行简介

CLI (Command Line Interface, 命令行接口) 即命令行, 路由器提供一个用于CLI配置的Console口。可以通过控制台和在局域网内通过Telnet进入命令行界面进行设置。

以下介绍通过控制台访问CLI的方法和一些常用的CLI命令。

15.1 搭建平台

- 1) 使用 Console 线连接路由器和计算机的 Console 口。
- 2) 打开计算机的终端仿真程序 (如 Hyperterminal 程序), 配置如下参数:
 - 波特率: 38400bps
 - 数据位: 8 位
 - 奇偶校验: 无
 - 停止位: 1 位
 - 数据流控制: 无



说明:

若计算机使用Windows XP系统, 可选择开始>所有程序>附件>通讯>超级终端, 打开超级终端, 配置如上所需参数, 也可登录路由器。

- 3) 在主窗口中输入回车键, 可以看到 “TP-LINK>” 的提示符, 如图 15.1 所示, 说明已成功登录路由器。

15.2 界面模式

TL-ER6520G的CLI提供了两个界面模式: 用户模式和特权模式。用户模式下只具有基本的权限, 比如查看系统的信息等。特权模式下则拥有管理路由器的权限, 可以进行各种配置操作等。这样就可以对不同的用户进行适当的权限管理。

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

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

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

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

如下图所示：

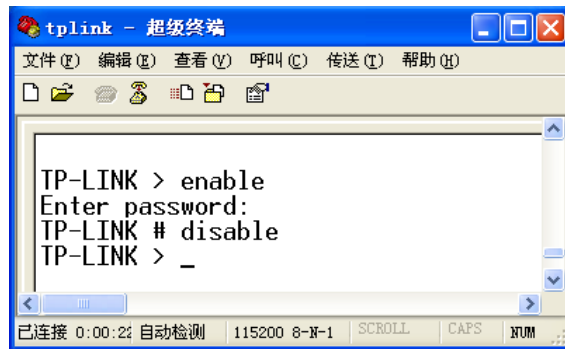


图 15.1 模式切换

15.3 在线帮助

TL-ER6520G提供了命令行在线帮助：

- 1) 在任一模式下，键入“?”获取该视图下所有的命令及其简单描述。例如在用户模式下直接键入问号“?”，可以获得下面提示内容：

disable	Exit the privileged mode
enable	Enter the privileged mode
exit	Exit the CLI (only for telnet)
history	Show command history
port	Configure port
sys	System manager
user	User configuration
vlan	Specify vlan setting zone
zone	Configure zone

- 2) 键入一命令，后接以空格分隔的“?”，如果该命令行位置有关键字，则列出全部关键字及其简单描述。例如在 tp-link > history 命令后键入问号“?”，将会弹出“clear”命令关键字提示。

- 3) 键入一字符串，其后紧接“?”，将列出以该字符串开头的命令。例如在tp-link > dis命令后键入问号“?”，将会弹出完整的命令提示disable。
- 4) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字。例如在tp-link > dis命令后键入问号“?”，将会补全命令为tp-link > disable。
- 5) 命令的输入完成之后，后接以空格分隔的“?”，会显示出一个回车符<cr>，表示此时命令已正确无误，可以执行。

15.4 命令介绍

TL-ER6520G提供了一些CLI命令，通过这些命令可以管理路由器和用户信息。为便于您理解，每条命令后面会注释该条命令的含义。

15.4.1 VLAN配置命令

通过VLAN相关配置命令可以配置VLAN相关功能。

TP-LINK # port config portId: 1-5 1 opType: 0:linktype;1:pvid 0 Linktype: 0:access;1:trunk;2:hybrid 0	设置端口的链路类型或者PVID。
TP-LINK # port show all	显示所有端口的链路类型和PVID。
TP-LINK# port show id 1	显示指定端口的链路类型和PVID。
TP-LINK # port vlan show	显示端口和VLAN之间的关联表。
TP-LINK # vlan config add 3 vlan3 portlist 4	添加vlan条目，指定相关的端口
TP-LINK # vlan config delete id 2	删除指定vlanId的条目
TP-LINK # vlan config show all	显示所有vlan条目
TP-LINK # vlan config show id 5	显示指定VLAN ID的条目

15.4.2 区段和接口命令

可以使用该组命令查看或设置区段和接口。

TP-LINK # zone show all	获取当前所有区段信息列表。
TP-LINK # zone show zone wan1	获取属于指定区段的接口信息列表。
TP-LINK # zone add wan1	添加指定名称的区段。如果无法完成添加操作，则会有相应提示信息返回。
TP-LINK # zone delete zonename wan1	删除指定名称的区段。如果该区段因为某种原因无法被删除，将会有相应的提示信息返回。
TP-LINK # zone delete all	尽可能多地删除所有的区段。如果有某些区段无法删除，则会有相应的提示信息返回。

<pre>TP-LINK # zone inf add wan1.dhcp wan1 eth TP-LINK # zone inf add wan1.pppoe wan1 pppoe TP-LINK # zone inf add pptp1 default pptp</pre>	指定接口名称、所属的区段以及接口的类型，创建一个新的接口。输入创建接口命令后，根据接口类型交互询问相关参数配置，请按照提示输入。
<pre>TP-LINK # zone show infname eth0</pre>	查看指定接口的详细信息，包括：接口的配置信息、运行时间和接口特有参数。
<pre>TP-LINK # zone inf connect wan1_pppoe</pre>	连接指定的接口。
<pre>TP-LINK # zone inf disconnect wan1_pppoe</pre>	断开指定的接口。
<pre>TP-LINK # zone inf delete pptp1</pre>	删除指定的接口。如果该接口因为某种原因无法被删除，将会有相应的提示信息。

15.4.3 系统管理

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

<pre>TP-LINK # sys save config</pre>	保存系统配置。 配置完成后，请使用保存配置命令，当重启设备时可以保证当前所有配置持续生效。
<pre>TP-LINK # sys reboot This command will reboot system, Continue?[Y/N]</pre>	重启系统。Y即YES，表确认；N即NO，表取消。
<pre>TP-LINK # sys restore This command will restore system, Continue?[Y/N]</pre>	恢复出厂配置。Y即YES，表确认；N即NO，表取消。
<pre>TP-LINK # sys export config Server address: [192.168.1.101]192.168.1.100 Username: [admin]ftp Password: [admin]ftp File name: [config.bin] Try to save the configuration file < config.bin > ... Save configuration file < config bin > succeed, file size is 7104 bytes.</pre>	配置文件导出。 举例：现有一台IP地址为192.168.1.100的FTP服务器，服务的用户名/密码是ftp/ftp，如需将当前配置文件以默认文件名config.bin保存到该FTP服务器上，设置如左。
<pre>TP-LINK # sys import config Server address: [192.168.1.101] Username: [admin] Password: [admin] File name: [config.bin] Try to get the configuration file < config.bin > ... Get configuration file < config bin > succeed, file size is 7104 bytes.</pre>	配置文件导入。说明同上。
<pre>TP-LINK > sys show CPU Used Rate: 1%</pre>	查看系统信息。该命令将会显示当前系统的CPU利用率。
<pre>TP-LINK # sys update Server address: [192.168.1.101] Username: [admin] Password: [admin] File name: [update.bin] Try to get the update file < update.bin > ... Get update file < update bin > succeed, file size is 2298608 bytes.</pre>	系统软件升级。

**说明：**

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

15.4.4 用户信息管理

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

TP-LINK > user get Username: admin Password: admin	查询当前参观级用户的用户名及密码。
TP-LINK > user set password Enter old password: Enter new password: Confirm new password:	修改参观级用户的密码。
TP-LINK # user get Username: admin Password: admin	查询当前管理员级用户的用户名及密码。
TP-LINK # user set password Enter old password: Enter new password: Confirm new password:	修改管理员级用户的密码。
TP-LINK # user set username Enter new username: tplink	修改管理员级用户的用户名。

**说明：**

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

15.4.5 历史命令管理

history命令。可以使用该命令查看或清除系统中的历史命令。

TP-LINK > history 1. history 2. sys show 3. history	查看历史命令。
TP-LINK > history clear 1. history 2. sys show 3. history 4. history clear	清除历史命令。

15.4.6 退出CLI

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

TP-LINK > exit

退出系统。

附录 A 常见问题

问题1：无法登录路由器Web管理界面该如何处理？

- 1) 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，Console口登录方法详见**第15章命令行简介**。
- 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、查杀病毒或将其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。Console口登录方法详见**第15章命令行简介**。

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