

TP-LINK®

工业路由器

用户手册

声明

Copyright © 2020 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.....	3
2.3	产品外观.....	5
2.3.1	前面板.....	5
2.3.2	上面板.....	8
第 3 章	基本设置	10
3.1	登录 Web 页面.....	10
3.2	系统状态.....	11
3.3	接口设置.....	11
3.3.1	接口设置.....	13
3.3.2	网桥设置.....	19
3.4	DHCP 服务.....	20
3.4.1	DHCP 协议介绍.....	20
3.4.2	DHCP 功能介绍.....	23
3.4.3	DHCP 功能配置.....	25
3.4.4	DHCP 功能组网应用.....	28
第 4 章	快速配置	31
4.1	设置接口模式.....	31
4.2	设置 WAN 口.....	32
4.3	设置 LAN 口.....	36
第 5 章	对象管理	38
5.1	地址管理.....	38
5.1.1	地址组.....	38
5.1.2	地址.....	39
5.2	时间管理.....	40
5.3	IP 地址池.....	42

5.4	服务.....	43
第 6 章	AP 管理.....	45
6.1	AP 设置.....	45
6.1.1	AP 设置.....	45
6.1.2	AP 状态.....	49
6.1.3	AP 升级.....	49
6.1.4	智能漫游.....	52
6.2	射频设置.....	53
6.2.1	射频设置.....	54
6.2.2	射频调优.....	57
6.3	无线服务设置.....	59
6.4	客户端状态.....	64
第 7 章	传输控制.....	66
7.1	NAT 设置.....	66
7.1.1	NAPT.....	68
7.1.2	一对一 NAT.....	74
7.1.3	虚拟服务器.....	76
7.1.4	ALG 服务.....	79
7.1.5	NAT-DMZ.....	80
7.2	带宽控制.....	81
7.3	连接数限制.....	84
7.3.1	连接数限制.....	84
7.3.2	连接数监控.....	85
7.4	流量均衡.....	86
7.4.1	基本配置.....	86
7.4.2	ISP 选路.....	88
7.4.3	线路备份.....	90
7.4.4	在线检测.....	92
7.5	路由设置.....	93
7.5.1	策略路由.....	94
7.5.2	静态路由.....	97

7.5.3	系统路由	100
第 8 章	安全管理.....	102
8.1	ARP 防护	102
8.1.1	ARP 简介	102
8.1.2	ARP 攻击简介	103
8.1.3	IP MAC 绑定	105
8.1.4	ARP 扫描	107
8.1.5	ARP 列表	108
8.2	攻击防护	109
8.3	MAC 过滤	110
8.4	访问控制	111
8.4.1	基本概念	111
8.4.2	配置访问规则	112
8.4.3	访问控制应用	114
第 9 章	行为管控.....	119
9.1	应用控制	119
9.1.1	应用控制	119
9.1.2	QQ 黑白名单	120
9.2	网址过滤	121
9.2.1	网站分组	121
9.2.2	网站过滤	123
9.2.3	URL 过滤	124
9.3	网页安全	126
9.4	行为审计	127
9.5	策略库升级	127
第 10 章	VPN.....	128
10.1	IPSec	129
10.1.1	IPSec 安全策略	129
10.1.2	IPSec 安全联盟	133
10.2	L2TP	134
10.2.1	L2TP 服务器设置	134

10.2.2	L2TP 客户端设置.....	135
10.2.3	L2TP 服务器隧道信息.....	137
10.3	PPTP.....	138
10.3.1	PPTP 服务器设置.....	138
10.3.2	PPTP 客户端设置.....	139
10.3.3	PPTP 服务器隧道信息.....	141
10.4	用户管理.....	141
第 11 章	认证管理.....	144
11.1	Web 认证介绍.....	144
11.1.1	简介.....	144
11.1.2	Web 认证系统.....	144
11.1.3	Web 认证过程.....	145
11.2	认证设置.....	146
11.2.1	跳转页面.....	146
11.2.2	组合认证.....	148
11.2.3	远程 Portal.....	157
11.2.4	免认证策略.....	159
11.2.5	认证参数.....	161
11.3	用户管理.....	162
11.3.1	认证用户管理.....	162
11.3.2	用户配置备份.....	163
11.4	认证服务器.....	164
11.4.1	认证服务器.....	164
11.4.2	Radius 服务器.....	165
11.5	认证状态.....	165
第 12 章	系统服务.....	167
12.1	PPPoE 服务器.....	167
12.1.1	全局设置.....	167
12.1.2	账号管理.....	168
12.1.3	例外 IP 管理.....	170
12.1.4	账号信息列表.....	170

12.2	动态 DNS	171
12.2.1	花生壳动态域名	171
12.2.2	科迈动态域名	172
12.2.3	3322 动态域名	172
12.3	DNS 代理	173
12.4	UPnP 服务	174
12.5	文件共享	175
第 13 章	云管理	176
13.1	基本配置	176
13.2	终端上网策略	179
13.2.1	策略点	179
13.2.2	认证点	180
第 14 章	系统工具	181
14.1	管理账号	181
14.1.1	管理帐号	181
14.1.2	远程管理	182
14.1.3	系统管理设置	183
14.2	设备管理	184
14.2.1	恢复出厂配置	184
14.2.2	备份与导入配置	184
14.2.3	重启设备	185
14.2.4	软件升级	186
14.2.5	设备管理	187
14.3	流量统计	187
14.3.1	接口流量统计	187
14.3.2	IP 流量统计	187
14.4	诊断工具	188
14.4.1	诊断工具	188
14.4.2	故障诊断	189
14.5	时间设置	191
14.5.1	时间设置	191

14.6	系统日志.....	193
14.7	系统参数.....	194
14.8	告警器	195
第 15 章	典型配置举例	197
15.1	组网需求.....	197
15.2	组网方案及特点.....	197
15.3	配置步骤.....	199
15.3.1	配置 VLAN	200
15.3.2	配置接口	200
15.3.3	配置流量均衡.....	202
15.3.4	配置对象	204
15.3.5	配置访问策略.....	206
15.3.6	配置 NAT	208
15.3.7	配置 VPN	209
15.3.8	配置应用限制.....	212
15.3.9	配置局域网 ARP 攻击防护.....	214
15.3.10	配置攻击防护	216
15.3.11	配置内网流量统计.....	217
第 16 章	附录 A 常见问题	218
第 17 章	附录 B 规格参数	220

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-ER6225G工业级。
- 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<>尖括号标记文字或图形，表示Web界面的按钮名称，如<确定>或<>。
- 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

TP-LINK 工业路由器专为在恶劣的工业环境下可靠稳定的运行而设计，并提供了一套经济有效的解决方案。

工业路由器支持 IEEE 802.3, IEEE 802.3i, IEEE 802.3u, IEEE 802.3x, IEEE 802.3ab, IEEE 802.3z 协议，支持 10/100/1000Mbps 传输，全双工/半双工，自动翻转 MDI/MDIX，自动侦听。

工业路由器提供 12/24/48 VDC(9.6 - 60 VDC)冗余电源输入，可同时接入三路直流电源，工作温度-40 — 75°C，金属壳防护等级 IP30，在艰苦的工业环境中足够结实耐用。为了在不同的工业环境应用中提供更多的用途，工业路由器可以通过面板的拨码开关开启或禁用端口中断报警功能。

工业路由器可以方便地进行 DIN 导轨安装以及安装在配电箱中，DIN 导轨安装和 IP30 的带 LED 指示灯的金属壳让工业路由器即插即用变得简单可靠。

路由器目前具体包含型号如下：

类型	产品型号	10/100/1000Mbps RJ45 端口	1000Mbps SFP 端口	Combo □
工业路由器	TL-ER6225G 工业级	5	2	2



说明：

- 路由器的 1F 和 2F 端口分别与 RJ45 端口 1 和 2 形成 Combo 口（即复用端口），同一时刻 Combo 口的两个端口只能使用一个，同时接入时，SFP 端口有效。Combo 口为“无”表示该路由器的 SFP 端口为独立的 SFP 端口。
- SFP 端口兼容多模、单模 SFP 光纤模块，可根据实际需求和组网情况选择光纤模块；推荐使用普联技术有限公司 SFP 光纤模块，如 TL-SM311LSA/B-2KM、TL-SM311LSA/B-20KM、TL-SM312LS-20KM 和 TL-SM311LM。

2.2 产品特性

■ 硬件特性

- 提供 5 个 10/100/1000M 自适应 RJ45 端口和 2 个千兆 SFP 端口 (Combo)
- 提供一个 USB 3.0 接口
- 工业级工作温度：-40°C~75°C
- 宽电压输入：9.6V~60VDC
- 多种安装方式：导轨式安装+壁挂安装
- IP30 防护：减少粉尘影响
- 三路电源输入，冗余备份，大大提高产品供电可靠性
- EMS 高防护等级，无惧各种恶劣环境

■ 功能特性

接口

- 提供 5 个千兆物理端口，用户可自由定义端口类型 (WAN/LAN/其他类型)；
- 提供 2 个千兆 SFP 端口 (Combo)，推荐使用 TP-LINK 公司 SFP 光纤模块，如 TL-SM311LSA/B-2KM、TL-SM311LSA/B-20KM、TL-SM312LS-20KM 和 TL-SM311LM。
- 提供多种逻辑接口类型，适应更多复杂的网络适用环境。

VPN

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

Web 认证

- 不需要客户端软件即可实现认证入网，降低网络维护工作量；
- 支持本地认证、Radius 认证和一键上网，满足多种认证需求；
- 可自定义认证跳转页面，实现广告推送。

上网行为管理

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

AP 管理

- AP 设置：对接入的 AP 可实现定时重启和自动固化；对 AP 进行分组管理；
- AP 升级：对接入的指定型号的 AP 进行升级；
- 负载均衡：适用于高密度无线网络环境中，可以准确地在无线网络中平衡 AP 设备的负载，保证该环境中客户端的合理接入，保证每个 AP 的性能和带宽得到最合理的使用。

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，可同时绑定 LAN 口(内网)、WAN 口(外网)主机的 IP 与 MAC 地址信息，有效防止 ARP 欺骗和非法接入；在遭受 ARP 欺骗时，路由器可按照指定频率发送 ARP 更正信息，及时恢复网络正常状态；
- 攻击防护：支持内外网攻击防护功能，可有效防范各种常见的 DoS 攻击、扫描类攻击、可疑包攻击行为，如 TCP Syn Flood、UDP Flood、ICMP Flood、WinNuke 攻击、分片报文攻击、WAN 口 ping、TCP Scan (Stealth FIN/Xmas/Null)、IP 欺骗等。

带宽控制

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

连接数限制

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

设备管理

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

设备维护

- 提供系统日志功能，详尽的日志信息便于快速发现网络异常并及时定位问题原因，实时监测 CPU 利用率等路由器内部关键资源，及时发现潜在的各种危险和攻击；
- 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 检测等多种故障检测工具，并可备份和导入路由器配置文件，方便快速确认网络连通状态。

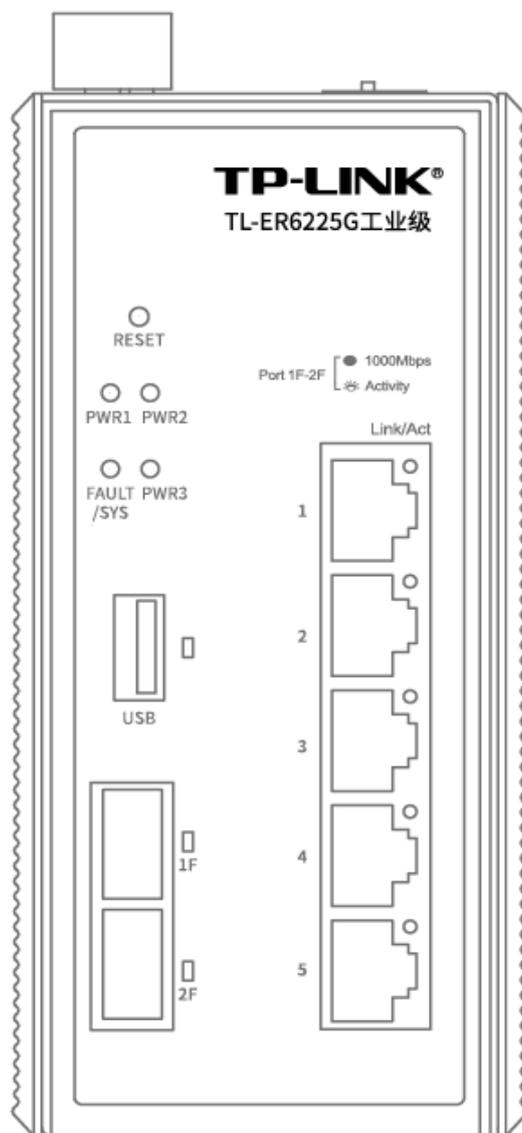
云管理

- 开启云管理后，AP 设置、射频设置、无线设置、认证设置可以在 TP-LINK 商用网络云平台上进行远程集中配置，后续管理维护更加方便。

2.3 产品外观

2.3.1 前面板

TL-ER6225G工业级的前面板由5个10/100/1000Mbps RJ45端口、2个1000Mbps SFP端口、1个USB端口和指示灯组成，如下图所示。



10/100/1000Mbps RJ45 端口

支持 10Mbps、100Mbps 或 1000Mbps 速率自适应功能，支持自动翻转 (Auto-MDI/MDIX) 功能，每个端口对应有一个指示灯，即 Link/Act 指示灯。每个端口都可作为 LAN 口和 WAN 口，无需区分。

1000Mbps SFP 端口

SFP 端口 1F-2F 位于面板左侧，分别与 RJ45 端口 1-2 为 Combo 口，SFP 端口具有单独的指示灯。

USB 口

支持 USB 3.0 协议，用于连接存储设备，具有单独的指示灯。

RESET 按键

用于将路由器恢复出厂设置状态。当路由器正常通电时，长按 RESET 按键持续 5 秒以上。路由器恢复出厂设置后，所有配置参数将会被清除，需要重新进行配置。

指示灯

指示灯，包括 Power、FAULT/SYS、Link/Act 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
PWR1	电源指示灯	常亮	电源由该路输入提供
PWR2		熄灭	该路输入未提供电源
PWR3			
FAULT/SYS	中断报警/系统指示灯	绿色闪烁	系统异常
		红色闪烁	端口中断报警功能开启但端口未正常连接
		其它	系统异常
USB	USB 端口指示灯	常亮	USB 口已正常连接
		熄灭	USB 口未连接设备
Link/Act (1-5)	RJ45 端口状态指示灯	常亮	端口正常连接设备
		闪烁	端口正在传输数据
		熄灭	端口未连接设备
Link/Act (1F-2F)	SFP 端口状态指示灯	绿色常亮	端口正常连接设备且工作在 1000Mbps 速率下
		闪烁	端口正在传输数据
		熄灭	端口未连接设备

表 2.1 指示灯工作状态说明

2.3.2 上面板

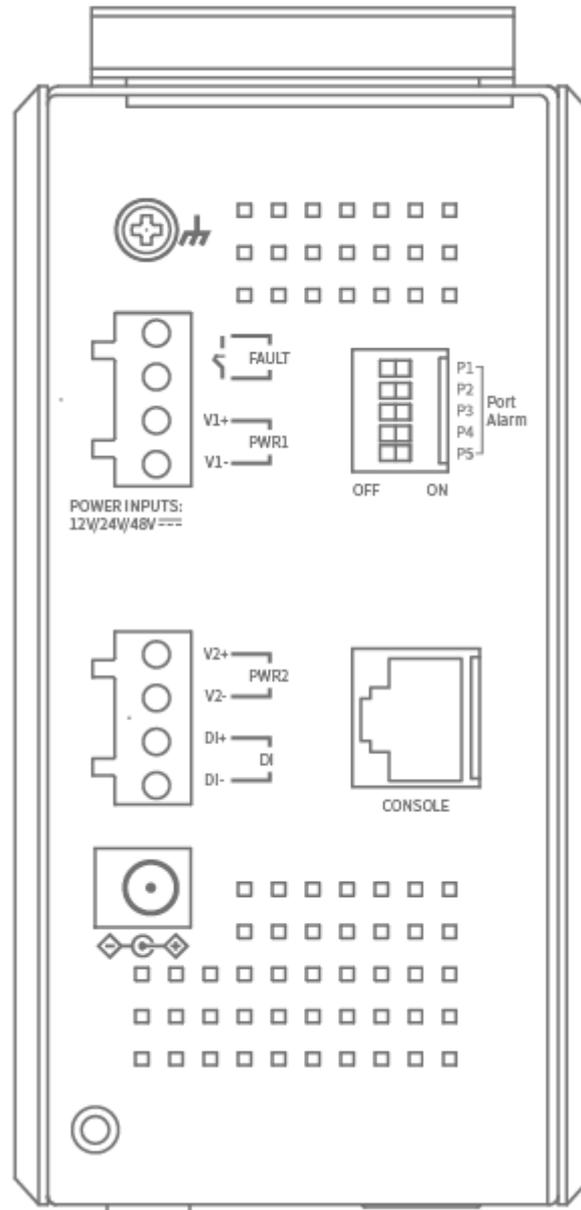


图 2-1 上面板示意图

防雷接地柱

位于面板顶部，请参考《防雷安装手册》进行防雷安装连接，以防雷击。请登录 <https://www.tp-link.com.cn/>，获取最新资料。

报警输出

报警输出端口用于输出继电器报警信号。正常工作时，继电器短路；报警事件触发后，继电器断路。继电器电流负载能力为 1A @24VDC。满足以下三个条件中的任意一个，继电器输出报警信号：

- 1) 正常供电的电源小于 2 路。
- 2) 端口中断故障报警功能开启，且对应端口出现中断故障。
- 3) DI 报警：外部通过数字输入端口输入高电平或低电平报警。

电源接口

路由器提供三路冗余电源输入，即接线端子的两个电源输入 PWR1/PWR2 和 DC-JACK PWR3。如果一个电源失效，剩下的电源仍能正常为路由器供电，保证路由器维持正常的工作状态。

路由器顶板上的两个 4 针接线端子分别有两个触点用于路由器的两个 DC 输入。操作方法如下：

- 1) 将负/正 DC 线插入接线端子的 V-/V+ 端子。
- 2) 为了防止 DC 电线松动，请使用小平刃螺丝刀拧紧接线端子前面的线夹螺丝。
- 3) 将塑料端子块连接器插入位于路由器顶板上的接线端子。

数字输入端口

状态“1”：+13 ~ +30V；状态“0”：-30 ~ +3V

最大输入电流：8mA

拨码开关

拨码开关出厂设置为关闭，拨码开关 P1~P5 分别对应 RJ45 端口 1~5。

拨码开关	设置	描述
PORT ALARM	ON	开启端口中断报警功能
	OFF	关闭端口中断报警功能

Console 端口

Console 端口用于和计算机或其他终端的串口相连以管理或配置路由器。



说明：

- 将 DC 电源连接到路由器输入端前，请确保 DC 电源电压是稳定的。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

第3章 基本设置

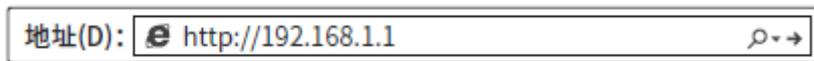
3.1 登录 Web 页面

第一次登录时，请确认以下几点：

- 1) 路由器已正常加电启动，管理端口（TL-ER6225G 工业级出厂默认管理端口为端口 5）已与管理主机相连。
- 2) 管理主机已正确安装有线网卡及该网卡的驱动程序，并已正确安装 IE 8.0 或以上版本的浏览器。
- 3) 管理主机 IP 地址已设为与路由器端口同一网段，即 192.168.1.X（X 为 2 至 254 之间的任意整数），子网掩码为 255.255.255.0。
- 4) 为保证更好地体验 Web 页面显示效果，请将显示器的分辨率调整到 1024×768 或以上像素。

登录路由器 Web 页面方法如下：

- 1) 打开 IE 浏览器，在地址栏输入路由器默认管理地址 <http://192.168.1.1> 登录路由器的 Web 页面。



- 2) 路由器登录页面如下图所示，在此页面输入路由器管理帐号的用户名和密码，出厂默认值均为 admin。



- 3) 成功登录后可以看到当前路由器的系统信息。

3.2 系统状态

路由器成功登录后可以看到路由器的系统状态信息，如下图所示。

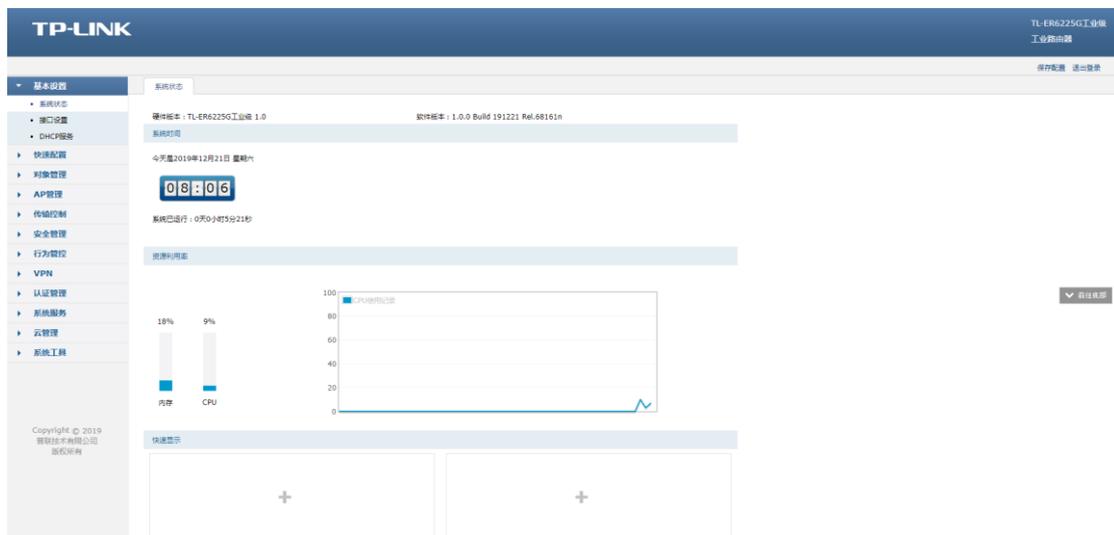


图 3-1 系统状态

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

系统时间：显示路由器当前的系统时间。

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

快速显示：点击各区域的 < + > 按钮可添加并查看接口信息。

保存配置：当路由器进行配置后，退出登录之前请务必保存配置。

退出登录：退出当前登录账号。

3.3 接口设置

为理解本路由器接口的含义，下面分别介绍物理接口和接口的概念。

■ 物理接口

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

TL-ER6225G 工业级的物理接口命名为端口 1/2/3/4/5 和端口 1F/2F，如下图所示。

端口 1/2/3/4/5 可根据需要自行定义 WAN/LAN 口。

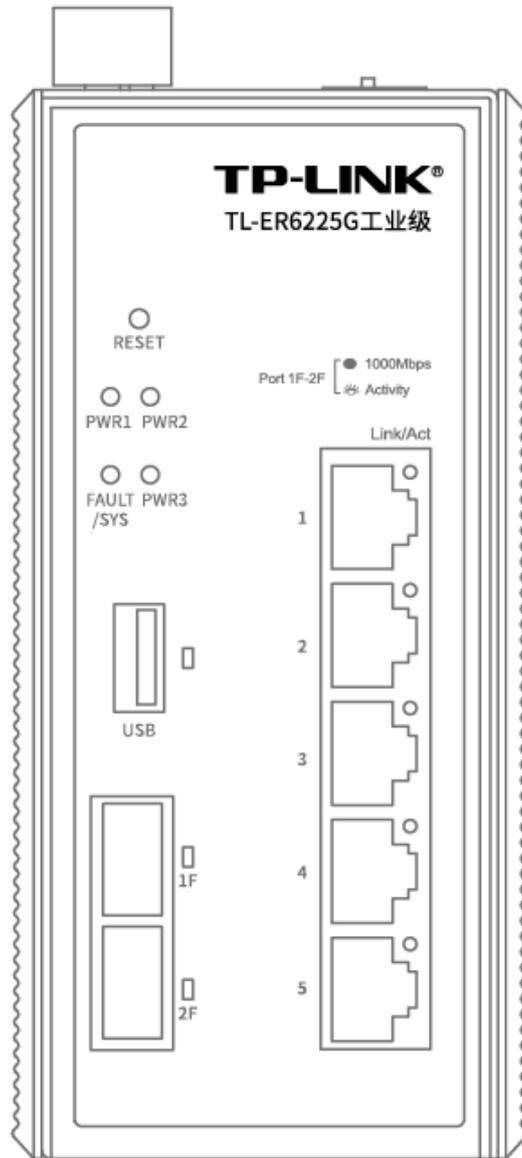


图 3-2 物理接口概念示意图

■ 接口

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

TL-ER6225G 工业级用来划分物理接口的接口有 Ethernet 、PPPoE 两种类型。Ethernet 是以太网接口 , 功能上与以太网物理接口相同。Ethernet 接口由 802.1Q VLAN 标记进行区分 , PPPoE 由相关的协议字段进行区分。

TL-ER6225G 工业级提供 Ethernet 和 PPPoE 两种类型的接口 :

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

- PPPoE 接口：提供 PPPoE 连接方式的接口。xDSL 拨号上网使用 PPPoE 连接方式。



说明：

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

3.3.1 接口设置

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

进入界面：基本设置 >> 接口设置 >> 接口设置



图 3-3 接口设置界面

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

■ Ethernet接口

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

<input type="checkbox"/>	序号	接口类型	接口名称	连接状态	IP地址	子网掩码	网关地址	设置
--	--	--	--	--	--	--	--	--

接口类型: (下拉菜单)

接口名称: (1-12个字符)

关联接口: (下拉菜单)

关联VLAN: UNTAG

连接方式: (下拉菜单)

IP地址:

子网掩码:

网关地址: (可选)

上行带宽: Kbps (100-1000000)

下行带宽: Kbps (100-1000000)

MTU: (576-1500)

首选DNS服务器: (可选)

备用DNS服务器: (可选)

MAC地址:

备注: (可选,50个字符)

管理接口开启:

图 3-4 Ethernet接口设置-静态IP连接方式

接口类型	选择Ethernet接口类型。
接口名称	输入一个名称来标识一个接口。只能输入英文、数字和下划线。
关联接口	在此选择一个物理接口作为其关联接口。
关联VLAN	输入一个该接口所属VLAN的VLAN ID。当勾选“UNTAG”时，从该接口发出的报文不带VLAN TAG；当不勾选“UNTAG”时，从该接口发出的报文带有VLAN TAG。
连接方式	选择连接方式，有静态IP和DHCP两种连接方式。 选择静态IP连接方式，需要进行手动配置IP地址；选择DHCP连接方式，由路由器动态获取IP地址。
IP地址	设置接口的IP地址。
子网掩码	设置接口的子网掩码。
网关地址	设置网关地址，允许留空。

上行带宽	设置接口的上行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
下行带宽	设置接口的下行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
MTU	MTU (Maximum Transmission Unit，最大传输单元)，可以设置数据包的最大长度。取值范围是576-1500之间的整数，默认值为1500。若ISP未提供MTU值，请保持默认值不变。
首选DNS服务器	设置DNS (Domain Name Server，域名解析服务器) 地址，允许留空。
备用DNS服务器	设置备用DNS地址，允许留空。
MAC地址	设置接口的MAC地址。
备注	填写对该接口的备注信息。
管理接口开启	勾选该项使该接口成为管理接口。

表 3.1 Ethernet接口设置界面静态IP连接方式条目项说明

<input type="checkbox"/>	序号	接口类型	接口名称	连接状态	IP地址	子网掩码	网关地址	设置
--	--	--	--	--	--	--	--	--
<div style="border: 1px solid #ccc; padding: 10px;"> <p>接口类型: Ethernet ▼</p> <p>接口名称: eth0 (1-12个字符)</p> <p>关联接口: GE2 ▼</p> <p>关联VLAN: 10 <input type="checkbox"/> UNTAG</p> <p>连接方式: DHCP ▼</p> <p>主机名: (可选)</p> <p>上行带宽: 1000000 Kbps (100-1000000)</p> <p>下行带宽: 1000000 Kbps (100-1000000)</p> <p>MTU: 1500 (576-1500)</p> <p>首选DNS服务器: (可选)</p> <p>备用DNS服务器: (可选)</p> <p>MAC地址: 02-12-AB-B7-2A-06</p> <p>备注: (可选,50个字符)</p> <p>管理接口开启: <input type="checkbox"/></p> <p style="text-align: center;"> <input type="button" value="确定"/> <input type="button" value="取消"/> </p> </div>								

图 3-5 Ethernet接口设置-DHCP连接方式

接口类型	选择Ethernet接口类型。
接口名称	输入一个名称来标识一个接口。只支持英文、数字和下划线。
关联接口	在此选择一个Ethernet接口作为其关联接口。
关联VLAN	输入一个该接口所属VLAN的VLAN ID。当勾选“UNTAG”时，从该接口发出的报文不带VLAN TAG；当勾选“TAG”时，从该接口发出的报文带有VLAN TAG。
连接方式	选择连接方式，有静态IP和DHCP两种连接方式。 选择静态IP连接方式，需要进行手动配置IP地址；选择DHCP连接方式，由路由器动态获取IP地址。
主机名	输入用于标识路由器的名称。
上行带宽	设置接口的上行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
下行带宽	设置接口的下行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
MTU	MTU (Maximum Transmission Unit，最大传输单元)，可以设置数据包的最大长度。取值范围是576-1500之间的整数，默认值为1500。若ISP未提供MTU值，请保持默认值不变。
首选DNS服务器	设置DNS (Domain Name Server，域名解析服务器) 地址。
备用DNS服务器	设置备用DNS地址。
MAC地址	设置接口的MAC地址。
备注	输入对该接口的备注信息。
管理接口开启	勾选该项使该接口成为管理接口。

表 3.2 Ethernet接口设置界面DHCP连接方式条目项说明

■ PPPoE接口



说明：

- 新建 PPPoE 接口，必须保证在同一物理接口下有 Ethernet 接口可供选择，如需新建 Ethernet 接口，请参考 **3.3.1 接口设置 Ethernet 接口**。

PPPoE 接口的设置界面如下图所示。

□	序号	接口类型	接口名称	连接状态	IP地址	子网掩码	网关地址	设置
--	--	--	--	--	--	--	--	--

接口类型:	PPPoE	▼
接口名称:	pppoe1	(1-12个字符)
关联接口:	eth3	▼
用户名:		
密码:		
连接方式:	自动连接	▼
上行带宽:	1000000	Kbps (100-1000000)
下行带宽:	1000000	Kbps (100-1000000)
MTU:	1492	(576-1492)
服务名:		(1-128个字符, 可选)
首选DNS服务器:		(可选)
备用DNS服务器:		(可选)
备注:		(可选, 50个字符)
管理接口开启:	<input type="checkbox"/>	

图 3-6 PPPoE接口设置

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

连接方式	<p>选择上网时连入互联网的方式，共有自动连接、手动连接和定时连接三种方式可供选择。</p> <ul style="list-style-type: none"> 自动连接：每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。 手动连接：需手动拨号连入互联网，适合按小时计费的拨号连接上网方式。 定时连接：在时间下拉列表中选择时间表，设置连接时段，在此时段内路由器如果开启则自动拨号连接，适合用于需要限时上网的场合。如需新建时间表，请参考时间管理
时间	<p>当连接方式选择“定时连接”时，可在下拉列表中选择时间表，设置连接时段，在此时段内路由器如果开启则自动拨号连接，适合用于需要限时上网的场合。如需新建时间表，请参考时间管理。</p>
上行带宽	<p>设置接口的上行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。</p>
下行带宽	<p>设置接口的下行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。</p>
MTU	<p>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。</p>
服务名	<p>输入服务名称，由ISP提供。</p>
首选DNS服务器	<p>设置DNS (Domain Name Server，域名解析服务器) 地址，允许留空。</p>
备用DNS服务器	<p>设置备用DNS地址，允许留空。</p>
备注	<p>输入对该接口的备注信息。</p>
管理接口开启	<p>勾选该项使该接口成为管理接口。</p>

表 3.3 PPPoE接口设置界面条目项说明

配置接口步骤：

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

3.3.2 网桥设置

网桥可以在数据链路层上实现局域网互连，并对网络数据的流通进行管理。在 TL-ER6225G 工业级中，通过创建网桥接口，可以将多个物理接口级联在一起（其中 GE5 将会默认被包含），达到不同接口之间互通的目的。当前系统的网桥接口一般作为“LAN”接口使用。而被桥接的接口配置其它任何业务都将无效。

进入界面：基本设置 >> 接口设置 >> 网桥设置

点击 <  新增 > 按钮，进入网桥设置页面

网桥名称	包含接口	设置
--	--	--
网桥名称： <input type="text" value="LAN"/> 包含接口： <input type="text" value="GE5"/> STP： <input checked="" type="checkbox"/> 启用 <input type="button" value="确定"/> <input type="button" value="取消"/>		

图 3-7 网桥设置

网桥名称	默认为“LAN”，不可更改。
包含接口	选择网桥所需包含的接口。
STP	勾选以启用生成树协议，防止网络环路产生。

表 3.4 网桥设置界面条目项说明

新增的条目会在网桥设置列表里显示出来，如下图所示。

网桥名称	包含接口	设置
LAN	GE1,GE5	

图 3-8 网桥列表

点击条目后的<



说明：

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

3.4 DHCP 服务

当网络存在以下需求时，可以通过DHCP服务器完成网络设备的IP地址配置：

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

3.4.1 DHCP 协议介绍

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

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

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

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

■ DHCP报文格式

DHCP报文的封装格式如下图所示：

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 3-9 DHCP报文格式

OP	报文类型，分为请求类型报文和应答类型报文，1表示此数据包为客户端发出DHCP请求报文，2表示此数据包为服务器相应客户端的DHCP应答报文。
htype	DHCP客户端的网卡类型，常见的类型有ethernet，当htype字段值为1时表示DHCP客户端的网卡为以太网网卡。
hlen	DHCP客户端的网卡地址长度，如果是以太网网卡，则hlen字段值为6字节。
hops	DHCP客户端发出DHCP请求报文时，此字段值设置为0，请求报文在网络中每经过一个DHCP中继，该字段值自动加1，通过此字段可以确定DHCP客户端与服务器之间经过了几个网络。
xid	DHCP客户端发出DHCP请求报文时，在此字段设置一个随机数，网络中不同的DHCP请求过程可通过不同的xid字段值进行区分，DHCP服务器对每个不同的DHCP请求分配不同的地址，DHCP客户端只能接受响应给他的DHCP应答报文，并接受第一个DHCP应答报文分配的IP地址。
secs	DHCP客户端开始DHCP请求时，在DHCP报文的secs字段设置为0，并作为起始时间来统计DHCP请求过程总共花费的时间。目前没有使用，固定为0。
flags	此字段的第一个bit位表示DHCP应答报文的发送方式，1表示广播报文，0表示单播报文，其余bit位目前保留，固定为0。
ciaddr	DHCP客户端的IP地址，DHCP客户端发出请求报文时可根据需要填入原先获得的IP地址。
yiaddr	DHCP服务器分配给客户端的IP地址。

siaddr	为DHCP客户端分配IP地址等信息的服务器IP地址。
giaddr	DHCP中继设备的IP地址。
chaddr	DHCP客户端的硬件地址，以太网网卡的MAC地址。
sname	DHCP服务器名称，可选项。
file	DHCP服务器为客户端指定的启动配置文件名称及路径信息。
options	可选变长选项字段，选项中可以记录DHCP报文类型、有效租期、DNS服务器IP等配置信息。本设备暂不提供options选项识别及通过options选项分配IP地址。

表 3.4 DHCP报文字段含义

■ DHCP地址分配过程

在一个DHCP获取网络参数的过程中，其应用的传输层协议为UDP，客户端向服务器的DHCP服务端口67发出DHCP请求，服务器向客户端的DHCP用户端口68回复响应信息。DHCP客户端和服务端均按照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：

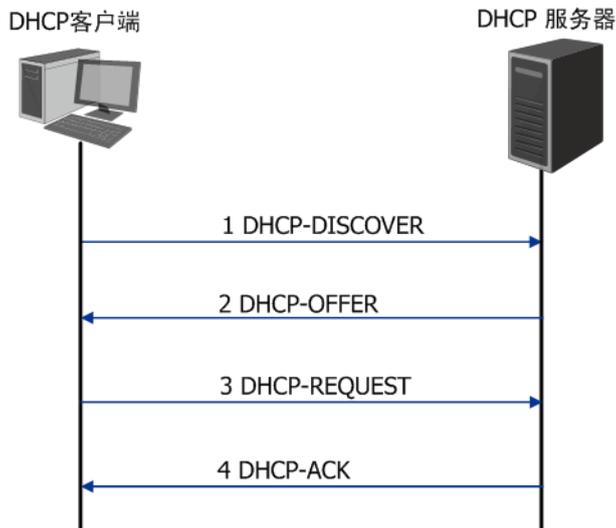


图 3-10 动态获取IP地址的过程

- 1) 发现阶段，客户端以广播方式发送DHCP-DISCOVER报文寻找DHCP服务器。
- 2) 提供阶段，DHCP服务器接收到客户端发送的DHCP-DISCOVER报文后，根据IP地址分配的优先次序从设定的地址段中选出一个IP地址，与其它参数一起通过DHCP-OFFER

报文发送给客户端，发送方式由客户端发送的DHCP-DISCOVER报文中的flag字段决定，具体请见DHCP报文格式的介绍。

- 3) 请求阶段，如果有多台DHCP服务器向该客户端发来DHCP-OFFER报文，客户端只接受第一个收到的DHCP-OFFER报文，然后以广播方式发送DHCP-REQUEST报文，该报文的option字段包含DHCP服务器在DHCP-OFFER报文中分配的IP地址，具体请见DHCP报文格式的介绍。
- 4) 确认阶段，DHCP服务器收到DHCP客户端发来的DHCP-REQUEST报文后，只有DHCP客户端选择的服务器会进行如下操作：如果确认地址分配给该客户端，则返回DHCP-ACK报文；否则将返回DHCP-NAK报文，表明地址不能分配给该客户端。
- 5) 当客户端通过动态获取IP地址时，则DHCP服务器分配给客户端的IP地址具有一定的租期，当租期满后服务器将收回该IP地址。如果DHCP客户端希望继续使用该IP地址，在地址租期到达一半时，可以向服务器发送单播的DHCP-REQUEST报文续约IP地址。

3.4.2 DHCP 功能介绍

本节主要介绍在TL-ER6225G工业级路由器上实现的DHCP服务器功能细节，主要包括五部分内容，**动态地址分配策略**、DHCP服务器功能典型应用环境、DHCP服务器功能实现细节、IP地址重复分配检测和分配IP地址的优先次序。

■ 动态地址分配策略

TL-ER6225G工业级路由器支持两种地址动态分配策略：

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

■ DHCP服务器功能典型应用环境

下图为路由器TL-ER6225G工业级配置为DHCP服务器时的网络拓扑图使用示范，具体的网络环境可根据实际需要调整。

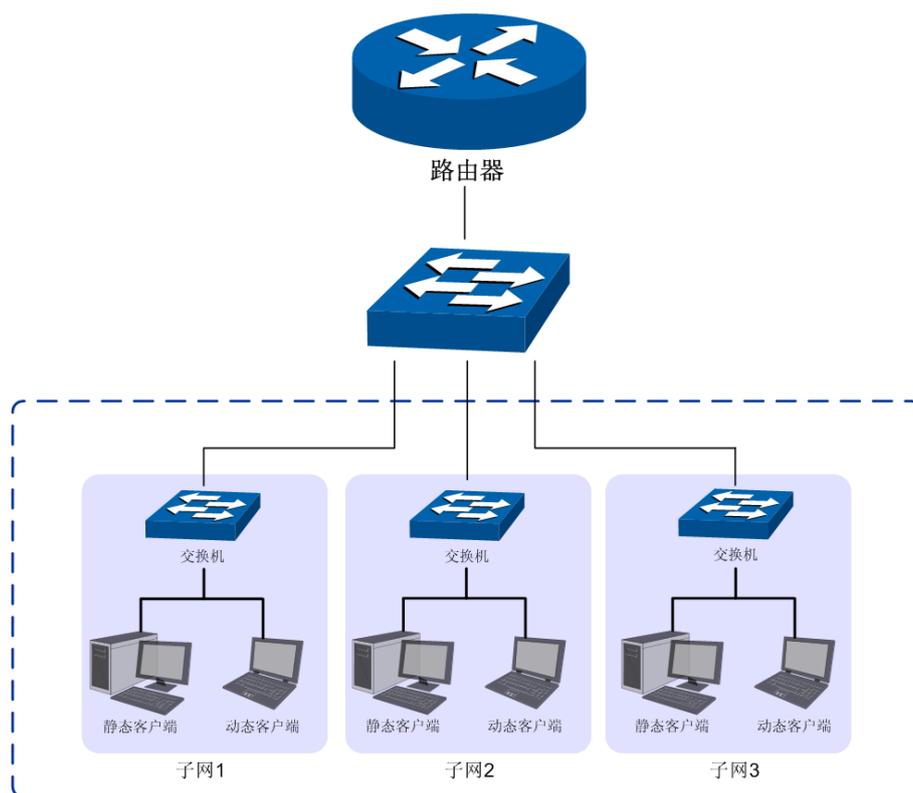


图 3-11 DHCP服务器功能应用环境

如图所示，某IT企业网络按照研发部门的分类分为软件小组、硬件小组和测试小组3个子网，在每个子网中，动态客户端通过“自动获取IP地址”的方式从TL-ER6225G工业级路由器上获得各自所属子网的IP地址，静态客户端手动设置IP地址。

■ DHCP服务器功能实现细节

为了使网络中的设备能够安全顺利的获得IP地址，保证网络的稳定性，TL-ER6225G工业级路由器的DHCP服务器功能可以完成如下任务：

- 1) TL-ER6225G工业级可以为多达64个Ethernet接口类型网络分配地址。



说明：

- 如果 Ethernet 类型接口的 IP 地址是动态获取的，由于其 IP 地址的不确定性，因此暂不提供此类接口的 DHCP 服务器功能。
- 对于 PPPoE 接口，由于其 IP 地址的不确定性，TL-ER6225G 工业级路由器也暂不提供 DHCP 服务器功能。

- 2) 当TL-ER6225G工业级收到DHCP请求报文时，将根据数据包中的VLAN ID信息选择相应接口设定的地址段来分配地址。

- 3) 为Ethernet类型接口网络中的特殊客户端手动绑定静态IP，当此接口收到特殊客户端的DHCP服务请求时，路由器将为客户端分配无限期的固定的IP地址。此类IP地址也会为特殊的客户端保留不会分配给其他客户端。
- 4) IP地址重复分配检测功能，为避免待分配地址已在网络中被使用，而导致分配后造成网络中IP冲突，路由器在分配一个IP地址前，会向所有接口网络发起待分配地址的Ping检测，从而避免IP冲突。

■ IP地址重复分配检测

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

■ 分配IP地址的优先次序

TL-ER6225G工业级路由器为客户端分配IP地址时将遵循以下分配规则秩序：

- 1) DHCP服务器中与客户端MAC地址手动绑定的IP地址。
- 2) DHCP服务器曾经分配给客户端的IP地址。
- 3) 客户端发送的DHCP-DISCOVER报文中指定的IP地址。
- 4) 选择合适的地址段，从中顺序查找可供分配的第一个IP地址。

3.4.3 DHCP 功能配置

DHCP功能配置主要分为配置IP地址段、为特殊客户端绑定青苔地址和查看当前所有的DHCP三部分进行配置。

■ 配置IP地址段

进入界面：基本设置 >> DHCP服务 >> DHCP服务

在DHCP服务界面点击< >按钮，进入DHCP服务设置页面。

□	序号	服务接口	开始地址	结束地址	地址租期	网关地址	首选DNS服务器	状态	设置
--	--	--	--	--	--	--	--	--	--

服务接口:

开始地址:

结束地址:

地址租期: 分钟 (2-2880)

网关地址: (可选)

缺省域名: (可选)

首选DNS服务器: (可选)

备用DNS服务器: (可选)

Option60: (可选)

Option138: (可选)

状态: 启用

图 3-12 DHCP服务配置界面-配置地址段参数

服务接口	选择需要提供 DHCP 服务的 Ethernet 接口。
开始/结束地址	DHCP 服务器自动分配的 IP 的开始/结束地址。
地址租期	输入此地址段中的 IP 地址在每次分配后可供客户端使用的租期。
网关地址	输入此地址段的给客户端分配的默认网关，也可以将接口 IP 地址配置为默认网关。
缺省域名	输入此地址段的给客户端指定的域，与 IP 地址一样共同表示相同子网的计算机的集合，同一接口网络中的计算机通常配置为相同的域名。
首选 DNS 服务器	输入此地址段的给客户端分配的首选 DNS 服务器，也可以将接口 IP 地址配置为 DNS 服务器地址，并由接口为客户端转发域名解析请求。
备用 DNS 服务器	输入此地址段的给客户端分配的备用 DNS 服务器，当首选 DNS 服务器失效时客户端可以向备用 DNS 服务器申请域名解析。
Option60	可选项，请填入厂商信息。具体厂商信息请咨询相关厂商，例如 TP-LINK 的厂商信息为 TP-LINK。
Option138	可选项，请填入 AC (无线控制器) IP 地址。
状态	选择“启用”，则使该绑定条目生效； 未选择“启用”，则使该绑定条目失效。

表 3.5 DHCP服务配置界面对象项说明

配置完成的地址段信息会在 DHCP 服务器列表区域显示出来，如下图所示。

DHCP服务列表									
✔ 启用 ✘ 禁用 + 新增 - 删除 🔍 搜索									
<input type="checkbox"/>	序号	服务接口	开始地址	结束地址	地址租期	网关地址	首选DNS服务器	状态	设置
<input type="checkbox"/>	1	GE5	192.168.1.1	192.168.1.254	120	---	---	已启用 ✘	

图 3-13 DHCP服务配置界面-地址段列表

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

■ 为特殊客户端绑定静态地址

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。

进入界面：基本设置 >> DHCP服务 >> 静态地址分配

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

<input type="checkbox"/>	序号	MAC地址	IP地址	备注	状态	设置
<input type="checkbox"/>	--	--	--	--	--	--

MAC地址: (XX-XX-XX-XX-XX-XX)

IP地址:

备注: (1-32个字符, 可选)

状态: 启用

图 3-14 DHCP服务配置界面-静态地址分配

MAC 地址	输入特殊客户端的 MAC 地址。
IP 地址	输入需要为特殊客户端保留的 IP 地址。该静态 IP 地址需与接口 IP 地址在同一网段。
备注	输入字符串描述该静态地址以便识别。
状态	选择“启用”，则使该绑定条目生效；

	不选择“启用”，则使该绑定条目失效。
--	--------------------

表 3.6 静态地址分配界面条目项说明

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。

<input type="checkbox"/>	序号	MAC地址	IP地址	备注	状态	设置
<input type="checkbox"/>	1	00-19-68-80-10-20	192.168.0.12	---	已启用	

图 3-15 静态地址分配配置界面-静态地址列表

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

■ 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-ER6225G 工业级路由器上获取 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	服务接口	主机名	MAC地址	IP地址	剩余租期
--	--	--	--	--	--

搜索
 全局搜索
 刷新
 自动刷新

图 3-16 DHCP服务器客户端列表

3.4.4 DHCP 功能组网应用

图 3-17为某企业网络的一个分支，网络需求如下：

- 由于部门人数较多，为了避免网络规模过大时容易产生的网络广播问题，研发部门又分为了软件小组、硬件小组和测试小组，3 个小组在接入交换机和中心交换机中通过 VLAN 进行隔离，测试小组使用 IP 地址段 192.168.10.0/24，硬件小组使用 IP 地址段为 192.168.20.0/24，软件小组使用的 IP 地址段为 192.168.30.0/24。
- 路由器 TL-ER6225G 工业级为中心路由器，并在 TL-ER6225G 工业级通过接口策略达到三层互通。
- 在每个小组中，移动客户端通过“自动获取 IP 地址”的方式从路由器上获取正确的子网 IP 地址，静态客户端手动设置 IP 地址。其中每个子网中的移动客户端数目最多为 50 台。

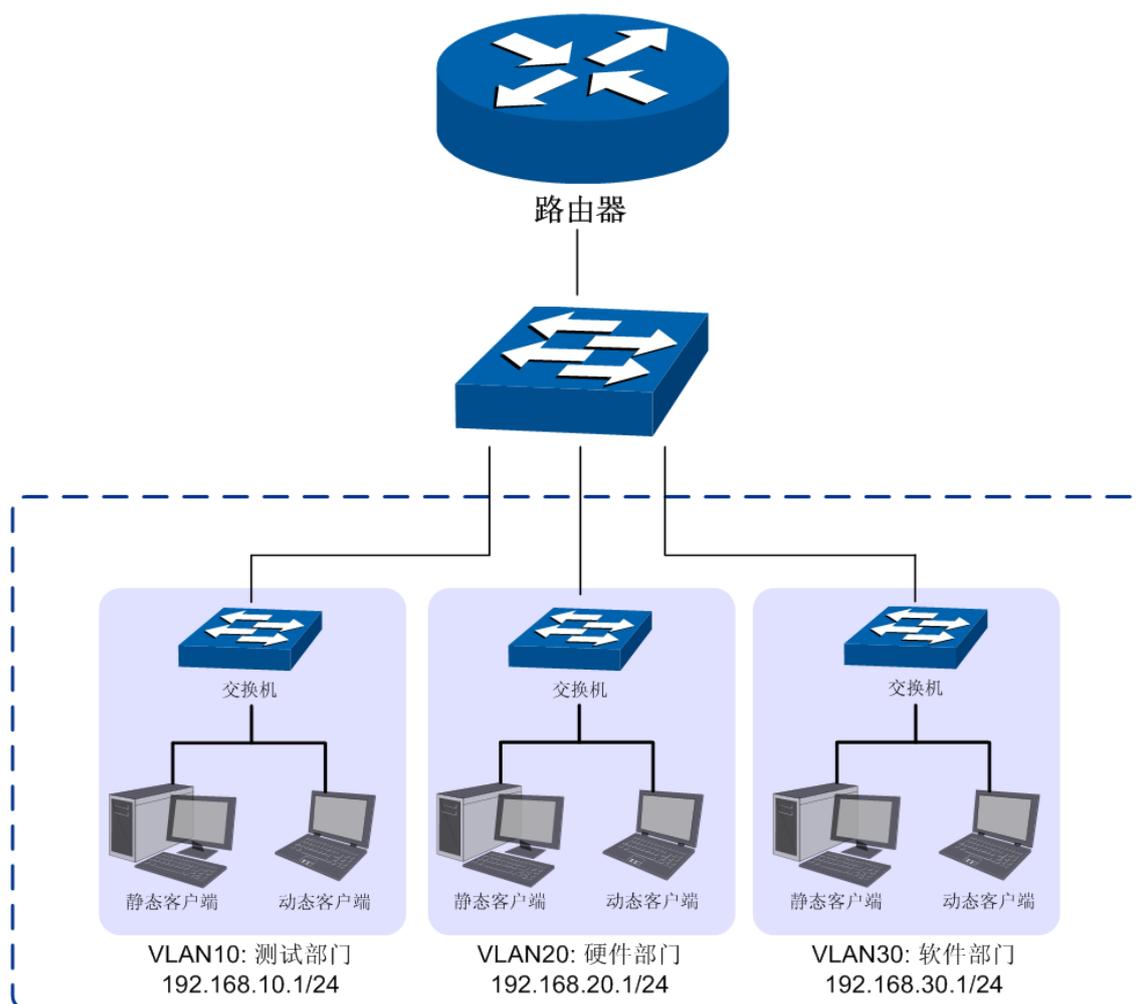


图 3-17 DHCP服务器功能组网举例

配置步骤：

如果要完成上述网络需求，需要按如下顺序配置路由器：

- 1) 创建 Ethernet 接口。必须操作。进入界面：基本设置 >> 接口设置 >> 接口设置，为研发各小组创建 Ethernet 类型接口，设置连接方式为静态 IP。例如为硬件小组创建 Ethernet 接口，命名为“hard_dep”，接口地址设置为 192.168.20.1/24 并与 VLAN20 关联。
- 2) 为动态客户端配置 DHCP 服务器。必须操作。进入界面：基本设置 >> DHCP 服务 >> DHCP 服务，为研发各小组配置 DHCP 服务参数，例如为硬件小组关联的接口“hard_dep”配置 DHCP 服务参数，选择开始/结束地址段为硬件部门 IP 地址段，同时配置网关参数为“hard_dep”的接口地址 192.168.20.1。
- 3) 为静态客户端绑定静态地址。必须操作。进入界面：基本设置 >> DHCP 服务 >> 静态地址分配，为研发各小组静态客户端绑定静态地址，例如在硬件小组关联的接口“hard_dep”下，将静态客户端 MAC 地址和欲分配的静态 IP 地址进行绑定。



说明：

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

第4章 快速配置

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



说明：

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

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



图 4-1 快速配置向导设置界面

4.1 设置接口模式

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



图 4-2 快速配置设置界面-接口模式设置

单击<下一步>，进入NAT模式-NAT-WAN1设置界面。

4.2 设置 WAN 口



说明：

- 快速配置设置的 WAN 接口全部参与带宽控制和流量均衡。

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
 WAN2
 WAN3
 LAN
 LAN

连接方式: 静态IP (手动配置) ▼

IP地址: 0.0.0.0

子网掩码: 255.255.255.0

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: 1000000 Kbps (100-1000000)

下行带宽: 1000000 Kbps (100-1000000)

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

连接方式	选择静态 IP 连接方式，进行手动配置。
IP 地址	设置路由器 WAN 口的 IP 地址。默认为 0.0.0.0。
子网掩码	设置路由器 WAN 口的子网掩码。默认为 255.255.255.0。
网关地址	设置网关地址，允许留空。
首选 DNS 服务器	设置 DNS (Domain Name Server，域名解析服务器) 地址，允许留空。
备用 DNS 服务器	设置备用 DNS 地址，允许留空。
上行带宽	设置当前 WAN 接口数据流出的带宽大小，可设置范围为 100-1000000Kbps。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。可设置范围为 100-1000000Kbps。

表 4.1 WAN口设置界面静态IP连接方式条目项说明

■ 动态IP连接方式

若ISP提供DHCP自动分配地址服务，请选择动态IP自动获取WAN口参数。



如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

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

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

表 4.2 WAN口设置界面动态IP连接方式条目项说明

- PPPoE连接方式

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

The screenshot shows the 'NAT模式-NAT-WAN1设置' (NAT Mode - NAT-WAN1 Settings) interface. At the top, there are icons for WAN1, WAN2, WAN3, and two LAN ports. Below this, the '连接方式' (Connection Type) is set to 'PPPoE (xDSL虚拟拨号)'. There are input fields for '账号' (Account) and '密码' (Password). Below these are radio buttons for '低' (Low), '中' (Medium), and '高' (High) bandwidth. The '上行带宽' (Upload Bandwidth) and '下行带宽' (Download Bandwidth) are both set to '1000000 Kbps (100-1000000)'. At the bottom, there are three buttons: '上一步' (Previous Step), '下一步' (Next Step), and '退出' (Exit).

如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

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

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

表 4.3 WAN口设置界面PPPoE连接方式条目项说明

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

4.3 设置 LAN 口

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

NAT模式-NAT-LAN设置

WAN1WAN2WAN3LANLAN

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)

上一步下一步退出

如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

图 4-6 快速配置设置界面-NAT模式-NAT-LAN设置

IP地址	设置路由器LAN口的IP地址，局域网内部可通过该地址访问路由器。默认为192.168.1.1。
子网掩码	设置路由器LAN口的子网掩码。默认为255.255.255.0。
DHCP服务器	选择开启或关闭DHCP服务。若希望路由器自动为计算机配置TCP/IP参数，请选择“开启”。若选择“关闭”，则起始IP地址、结束IP地址、网关地址、首选DNS服务器、备用DNS服务器各项全部隐藏，不可设。默认为开启。
起始IP地址	设置DHCP服务器自动分配IP地址的起始地址，该地址必须与LAN口IP地址设置在同一网段。默认为192.168.1.100。
结束IP地址	设置DHCP服务器自动分配IP地址的结束地址，该地址必须与LAN口IP地址设置在同一网段。默认为192.168.1.199。

网关地址	设置DHCP分配给客户端的网关地址，推荐设置为LAN口IP地址，允许留空。
首选DNS服务器	设置DNS地址，推荐设为路由器LAN口IP地址，允许留空。
备用DNS服务器	设置备用DNS地址，允许留空。

表 4.4 LAN口设置界面条目项说明

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



图 4-7 快速配置设置界面-完成快速配置向导

第5章 对象管理

5.1 地址管理

5.1.1 地址组

可以在本页面设置自定义地址组，以方便对用户进行组管理。

进入界面：对象管理 >> 地址管理 >> 地址组

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

<input type="checkbox"/>	序号	组名称	地址名称	备注	设置
--	--	--	--	--	--

组名称:	<input type="text" value="g_lan_ip"/>
地址名称:	<input type="text" value="lan-ip"/>
备注:	<input type="text"/> (可选)
<input type="button" value="确定"/>	<input type="button" value="取消"/>

图 5-1 地址管理界面

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

表 5.1 地址管理界面项说明

新增的条目会在**组列表**里显示出来，如下图所示。

<input type="checkbox"/>	序号	组名称	地址名称	备注	设置
--	1	IPGROUP_ANY	---	IPGROUP_ANY	---
<input type="checkbox"/>	2	g_lan_ip	lan-ip	---	 

图 5-2 组列表

如有需要，可点击条目后的<  >按钮进行编辑。条目1为系统默认条目，不可操作。

5.1.2 地址

可以在本页面自定义地址，并加入到已有的组中进行组管理。

进入界面：对象管理 >> 地址管理 >> 地址

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

<input type="checkbox"/>	序号	名称	IP类型	IP段	IP/MASK	备注	设置
<input type="checkbox"/>	--	--	--	--	--	--	--

名称:	<input type="text" value="IP_ANY"/>
IP类型:	<input type="radio"/> IP段 <input checked="" type="radio"/> IP/Mask
	<input type="text" value="0.0.0.0"/> / <input type="text" value="0"/>
备注:	<input type="text" value="IP_ANY"/> (可选)
<input type="button" value="确定"/> <input type="button" value="取消"/>	

图 5-3 用户设置界面

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

表 5.2 用户设置界面项说明

新增的条目会在地址列表里显示出来，如下图所示。

地址列表							
<input type="checkbox"/>	序号	名称	IP类型	IP段	IP/MASK	备注	设置
<input type="checkbox"/>	1	地址	IP段	1.1.1.1-1.1.1.10	---	---	 
<input type="checkbox"/>	2	IP_ANY	IP/Mask	---	0.0.0.0/0	IP_ANY	 

图 5-4 用户设置界面-地址列表

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

5.2 时间管理

可以通过本页面创建时间对象，从而对时间进行管理。

进入界面：对象管理 >> 时间管理 >> 时间管理

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

<input type="checkbox"/>	序号	时间对象名称	工作时间	备注	设置
--	1	Any		Any time	---
--	2	t1		---	---

时间对象名称：

时间设置： 工作日历 手动设置

工作日历：

备注： (可选)

图 5-5 时间管理-工作日历界面

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

表 5.3 时间管理界面项说明

点击“工作日历”，可以设置具体的工作时间，设置界面如下图所示。



图 5-6 工作日历设置

<input type="checkbox"/>	序号	时间对象名称	工作时间	备注	设置
--	1	Any		Any time	---
--	2	t1		---	---

时间对象名称:

时间设置: 工作日历 手动设置

星期: 一 二 三 四 五 六 日

时间段: : - :

备注: (可选)

图 5-7 时间管理-手动设置界面

名称	自定义的时间对象名称。只能输入英文、数字和下划线。
时间设置	选择手动设置。
星期	选择工作日期。

时间段	选择工作时间段
备注	输入对时间对象的具体描述。

表 5.4 时间管理-手动设置界面条目项说明

新增的条目会在时间对象列表里显示出来，如下图所示。

<input type="checkbox"/>	序号	名称	工作日历	备注	设置
--	1	Any		Any time	
<input type="checkbox"/>	2	t1		---	

图 5-8 时间管理界面-时间对象列表

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

5.3 IP 地址池

可以通过本页面设置IP地址池条目，进行地址池的管理。

进入界面：对象管理 >> IP地址池 >> IP地址池

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

--	--	--	--	--	--
地址池名称:	<input type="text" value="address"/>				
起始IP地址:	<input type="text" value="192.168.1.2"/>				
结束IP地址:	<input type="text" value="192.168.1.254"/>				
<input type="button" value="确定"/>		<input type="button" value="取消"/>			

图 5-9 IP地址池设置界面

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

表 5.5 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。

<input type="checkbox"/>	序号	地址池名称	起始IP地址	结束IP地址	设置
<input type="checkbox"/>	1	address	192.168.1.2	192.168.1.254	

图 5-10 IP地址池设置界面-地址池列表

如有需要，可以点击条目后的 < > 按钮进行编辑，点击 < > 按钮可删除该地址池。

5.4 服务

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 >> 服务

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

<input type="checkbox"/>	序号	名称	协议	源端口	目的端口	备注	设置
<input type="checkbox"/>	1	ALL	0-255	源端口 = 0-65535; 目的端口 = 0-65535	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 = 255; Code = 255	icmp		

图 5-11 服务类型设置界面

服务名称	自定义服务的名称。只能输入英文、数字和下划线。
协议类型	在此选择服务所使用的协议。
源端口范围	输入服务所使用的源端口范围，仅TCP或UDP协议需要设置。

目的端口范围	输入服务所使用的目的端口范围，仅TCP或UDP协议需要设置。
Type	输入ICMP协议的类型(type)，填充255时表明所有类型/编码。
Code	输入ICMP协议的编码(code)，填充255时表明所有类型/编码。
协议号	当协议类型选择为“Other”时，在此输入该协议的协议号。
备注	输入对服务类型的具体描述。

表 5.6 服务类型界面项说明

第6章 AP 管理

6.1 AP 设置

6.1.1 AP 设置

可以在此界面进行 AP 设置。

进入界面：AP 管理 >> AP 设置 >> AP 设置

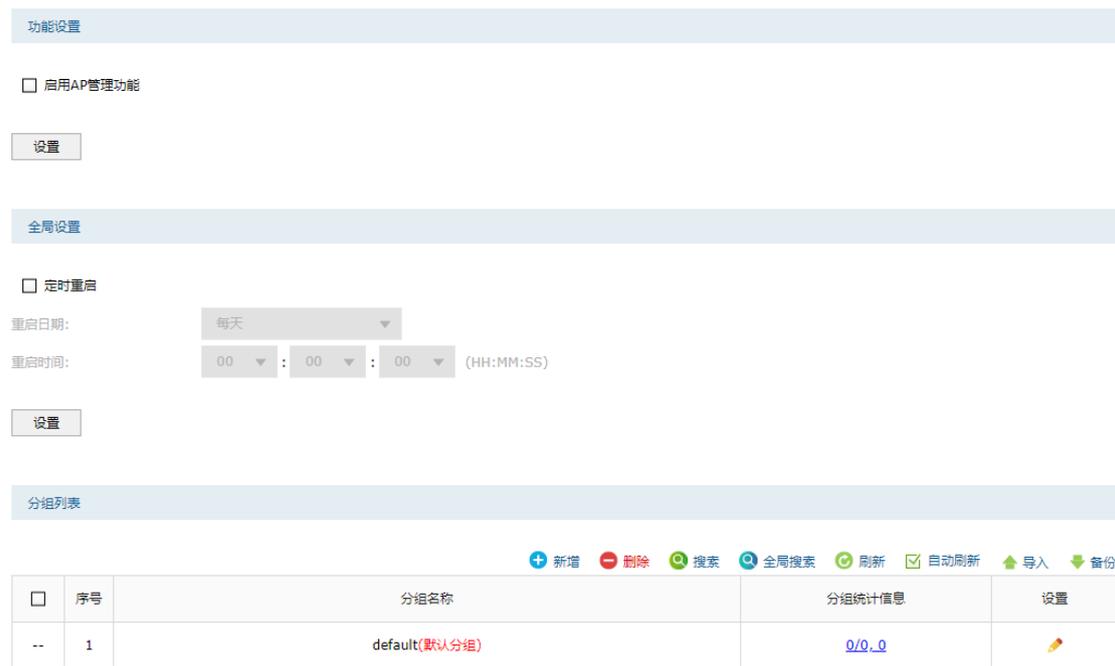


图 6-1 AP 设置界面

功能设置

用于全局启用或禁用 AP 管理功能。

说明：

- 禁用 AP 管理功能将强制所有已关联的 AP 重启。

全局设置

定时重启：若开启该功能，则在设定的时间到达时，所有已接入路由器的 AP 将重启。

分组列表

在此区域，可以对 AP 和模板进行分组管理。序号为 1 的条目是系统预定义的 AP 分组。不允许删除默认分组或非空分组。

分组名称	显示分组名称。默认分组的名称后会加注“(默认分组)”字样。
分组统计信息	形如“X/Y,Z”，X 表示已经成功接入的 AP 数目，Y 表示分组中所有的 AP 数目，Z 表示分组中的模板数量。点击可以进入分组详细列表。
设置	点击 <  > 按钮，可以编辑分组名称。

表 6.1 AP 设置界面条目项说明

新增分组

点击 <  新增 > 创建分组，新增分组界面如下图所示，需要自定义分组名称。输入分组名称后点击 < 确定 > 保存配置。

分组名称: (1-32个字符)

图 6-2 新增分组界面

分组详细列表

点击该分组统计信息内容项显示的内容，可以进入该分组详细列表界面，如下图所示。点击“ 回到分组”，可回到分组列表。

 回到分组
 修改分组
 新增
 删除
 批量编辑
 搜索
 组内搜索
 刷新

<input type="checkbox"/>	序号	名称	型号	硬件版本	软件版本	MAC地址	LED默认状态	状态	设置
<input type="checkbox"/>	--	--	--	--	--	--	--	--	--

图 6-3 分组详细列表界面

分组中的表项分为 AP 条目和 AP 模板两种类型，以下分别进行说明。

AP 条目：用于对 AP 进行参数设置和管理。当一个 AP 接入之后，就会创建与其对应的 AP 条目。AP 条目有固化和未固化的区别。未固化的 AP 条目指 AP 下线或 AC 重启后将消失，并且除“固化”外不能进行任何操作。未固化的 AP 条目名称后会加注“(未固化)”字样。已固化的 AP 条目指除非用户手动删除，否则一直存在。能够进行修改配置、修改分组、修改对应射频口配置和绑定无线服务等操作。

AP 模板：用于设定某种硬件型号的 AP 的参数默认值，一种型号的 AP 只允许创建一个模板。当 AP 接入时，如果存在与其硬件型号匹配的 AP 模板，就会以其中的参数为默认值生

成 AP 条目，且生成的 AP 条目位于模板所在的分组。AP 模板名称后会加注“(模板)”字样。

可以在此管理分组中的 AP 条目和 AP 模板，还可以对已有条目进行操作，下面对部分操作进行说明。

修改分组	将表项移动到其他分组。不能移动未固化的 AP 条目。
固化	固化操作。只能对未固化的 AP 条目执行本操作。

表 6.2 操作说明

点击图分组详细列表中的 <  新增 > 按钮可以添加新条目，新增 AP 条目界面如下图所示，新增 AP 模板界面与其类似，不单独介绍。

<input type="checkbox"/>	序号	名称	型号	硬件版本	软件版本	MAC地址	LED默认状态	状态	设置
--	--	--	--	--	--	--	--	--	--

名称: (1-45个字符)

型号: ▼

硬件版本: ▼

条目类型: ▼

AP保活时间: (20-80秒)

客户端保活时间: (3-1800秒)

客户端闲置时间: (60-86400秒)

AP离线自管理: 开启 关闭

LED默认状态: 开启 关闭

图 6-4 新增 AP 条目界面

名称	<p>设置 AP 名称，方便用户识别和管理。</p> <p>新 AP 接入时产生的 AP 条目的名称格式为“X-NNNN”(X 为型号名或匹配的模板名，N 为数字且四位数字唯一)。为防止冲突，不允许用户自己配置的名称以“-NNNN(N 为数字)”的形式结尾。对于 HDAP 类型的 AP，其内部的两台 AP 会自动在名称末尾添加后缀名以进行区分，且后缀名不可编辑。当修改 HDAP 内部的某一台 AP 名称时，其修改也会同步到另一台 AP 上。</p>
型号	选择 AP 的硬件型号。
硬件版本	选择 AP 的硬件版本号。
条目类型	选择条目类型。

AP 保活时间	<p>设置 AP 的保活时间间隔。</p> <p>AP 与 AC 之间采用保活机制来确认隧道是否正常工作。正常情况下，AP 周期性发送回声请求 (Echo Request) 报文给 AC，AC 收到后发送回声应答 (Echo Response) 报文给 AP。如果 AC 在本端的 6 倍保活时间内没有收到回声请求，或者 AP 在自己的 6 倍保活时间内没有收到 AC 的回声应答，则 AC/AP 会主动断开连接。</p>
客户端保活时间	<p>设置客户端保活时间间隔。</p> <p>客户端保活机制用于检测客户端的异常下线。正常情况下，客户端下线时会向 AC 发送解关联报文，AC 收到之后就会删除客户端信息。如果客户端由于电源故障等原因异常下线就无法通知 AC，客户端的信息就会残留在 AC 的内存中，降低 AC 性能。因此，AP 会主动探测客户端是否存在，如果在保活时间内没有收到客户端的回复，就会通知 AC 删除客户端信息。</p>
客户端闲置时间	<p>AP 与客户端之间连接允许的最大闲置时间。如果 AP 在闲置时间内没有收到来自客户端的数据，那么该客户端将被删除。</p>
AP 离线自管理	<p>启用 AP 离线自管理，则即使该 AP 与 AC 的连接中断，也仍然可以接受新客户端的接入请求，但是该 AP 上配置的所有 Portal 认证条目将会失效。</p>
LED 默认状态	<p>设置 AP 接入时的 LED 指示灯的初始状态。修改该配置项，不会影响 AP 当前的 LED 状态。如果想操作 AP 当前的 LED 状态，请前往“AP 状态”页面进行设置。</p>

表 6.3 新增 AP 条目界面条目项说明

部分机型除了上述设置项还有一些特有的设置项，如下表所示。

MAC 地址 2	<p>只有 HDAP 机型(如 TL-HDAP1800C-PoE)会显示该项。</p> <p>HDAP 内部的右侧 AP 的 MAC 地址，其大小固定为“MAC 地址+2”。</p>
有线 LAN 口 VLAN ID	<p>只有具备额外有线 LAN 口的机型(如 TL-AP300I-PoE)会显示该项。</p> <p>设置 AP 额外有线 LAN 口的 VLAN ID，空表示不设置。</p>
AP 端口汇聚	<p>只有支持此功能的机型会显示该项。(如 TL-HDAP1800C-PoE 在后缀名为“_01”的 AP 中显示)</p> <p>将 AP 的多个物理端口绑定为一个逻辑端口来工作，以提高带宽。</p>

表 6.4 AP 条目界面补充项说明

6.1.2 AP 状态

可在此界面查看接入的 AP 的状态。

进入界面：AP 管理>>AP 设置>>AP 状态

AP状态列表												
选择AP分组: default												
打开LED 关闭LED 重启 搜索 全局搜索 刷新 自动刷新												
<input type="checkbox"/>	序号	AP名称	型号	MAC地址	IP地址	射频列表			在线时长	SSID	LED	链路状况
						射频单元	信道	用户数				
--	--	--	--	--	--	--	--	--	--	--	--	--

图 6-5 AP 状态界面

AP 名称	显示 AP 的名称。
型号	显示 AP 的型号。
MAC 地址	显示 AP 的 MAC 地址
IP 地址	显示 AP 的 IP 地址。
射频列表	显示选中分组下的 AP 的射频信息，包括射频单元名称，所占信道和当前用户数。
在线时长	显示 AP 的在线时长
SSID	显示 AP 的无线网络名称。
LED	显示 AP 的 LED 灯的打开或关闭的状态。
链路状况	显示 AP 的双链路角色，“主用”表示此 AP 正在接受本 AC 的管理，“备用”表示此 AP 与本 AC 建立了连接，但只是作为备份链路，并不接受本 AC 的管理。对于“备用”状态下的 AP，“重启”按钮只能切断连接而不能将 AP 重启。

表 6.5 AP 状态界面条目项说明

6.1.3 AP 升级

可在此界面升级指定型号的 AP 软件版本。

进入界面：AP 管理 >> AP 设置 >> AP 升级

AP 批量升级

显示和配置同一类型号的 AP 的升级信息，点击新增，可定时升级 AP。

AP批量升级

+ 新增
- 删除
🔍 搜索
🔄 刷新
✅ 自动刷新

□	序号	AP型号	硬件版本号	升级软件版本号	升级开始时间	升级进度	升级失败	升级状态	升级方式	设置
--	--	--	--	--	--	--	--	--	--	--

AP型号:

硬件版本号:

当前时间: 2019/12/21 00:43:19

升级开始时间: (YYYY/MM/DD)

: : (HH:MM:SS)

升级软件:

AP 型号	显示 AP 型号的名称。
硬件版本号	显示支持的该型号的硬件版本。
升级软件版本号	显示当前导入的升级软件的版本号，若未导入，则显示为“---”。
升级开始时间	上级文件上传成功后，输入升级开始的时间，点击<确认>按键生效设置。当“升级开关”处于开启状态时，到达设定的时间，此型号的 AP 设备将使用导入的 AP 升级软件进行升级。
升级进度	显示当前升级的进度，X/Y/Z 表示当前检测到有 Z 台该型号的 AP，其中有 Y 台需要升级，X 台已经升级成功。点击可以查看各个 AP 当前的升级状态。
升级失败	显示当前升级失败的 AP 个数，点击可以查看详细日志信息。
升级状态	<p>显示当前 AP 型号的升级状态，点击可以查看该型号下的 AP 的具体升级状态信息。</p> <p>无需升级：当前 AP 型号下没有 AP 需要升级。</p> <p>等待升级：当前 AP 型号下的 AP 在等到升级。</p> <p>正在升级：当前 AP 型号下有 AP 正在升级。</p> <p>升级完成：当前 AP 型号下的所有 AP 都升级完成。</p>
升级方式	显示当前 AP 型号的升级方式，包括在线升级和手动导入升级软件两种方式。

单个 AP 升级

显示和配置在线 AP 的升级信息。

单个AP升级

选择AP分组: default

[搜索](#) [刷新](#) 自动刷新

序号	AP名称	型号	硬件版本	MAC地址	当前软件版本	升级软件版本	状态	软件管理
--	--	--	--	--	--	--	--	--

AP 名称	显示 AP 的名称。
AP 型号	显示 AP 的型号
硬件版本	显示支持的该型号的硬件版本。
MAC 地址	显示 AP 的 MAC 地址
当前软件版本	显示当前导入的升级软件的版本号，若未导入，则显示为“---”。
升级软件版本	显示该 AP 即将升级的软件版本。
状态	<p>显示当前 AP 型号的升级状态。点击可以查看该型号下的 AP 的具体升级状态信息。</p> <p>在线：该 AP 在线但未进行升级</p> <p>等待升级：该 AP 在等待升级</p> <p>检查更新：正在检测该 AP 是否有软件可以更新</p> <p>等待下载软件：检测到有新软件后等待下载软件</p> <p>下载软件：正在下载软件</p> <p>正在升级：该 AP 正在升级</p> <p>正在确认升级结果：正在等待 AP 接入，以确认升级是否成功</p> <p>升级完成：该 AP 升级完成</p> <p>确认升级结果失败：AP 接入版本非升级软件版本</p> <p>传输升级文件失败：在传输升级软件的过程中发生错误</p> <p>确认升级结果超时：AP 在升级后未在规定时间内接入</p> <p>获取软件失败：未获取到最新软件</p> <p>下载软件失败：下载最新软件失败</p> <p>无需升级：该 AP 不需要升级</p> <p>软件不匹配：导入的 AP 软件与当前 AP 的软件版本不兼容</p>

软件管理	可以选择在线升级或手动升级。如果对应的 AP 不支持在线升级功能，则只提供手动升级方式。
------	--

表 6.6 AP 升级设置界面条目项说明



说明：

- “升级进度”以及“升级失败”参数在设备重启后会被清空。
- 对于相同型号的 AP，“批量升级”任务和“单个 AP 升级”任务，不能同时使能。

6.1.4 智能漫游

本界面用于配置智能漫游的参数，以调节不同环境下无线终端的漫游效果。智能漫游的作用在于，对于无线体验较差的终端，AC 主动选取更优的候选 AP，并建议或迫使终端切换到所选择的候选 AP 上，以改善无线上网体验。

进入界面：AP管理 >> AP设置 >> 智能漫游

基本设置

802.11k快速漫游: 启用 禁用

802.11v快速漫游: 启用 禁用

802.11r快速漫游: 启用 禁用

频段漫游参数设置: 2.4G 5G

检测漫游阈值类型: 基于信号强度 基于速率百分比

触发漫游RSSI阈值: dBm (-95~-60)

强制弱信号用户下线: 启用 禁用

高级设置 ↑

漫游阈值检查周期: 秒 (1-10)

漫游差值: dBm (5-15)

终端禁止接入时间: 秒 (0-10)

终端探测上报: 启用 禁用

设置

基本设置

802.11k 快速漫游	启用/禁用 802.11k 快速漫游功能。
802.11v 快速漫游	启用/禁用 802.11v 快速漫游功能。
802.11r 快速漫游	启用/禁用 802.11r 快速漫游功能。

频段漫游参数设置	设置 2.4GHz 频段和 5GHz 频段的漫游参数。
检测漫游阈值类型	配置主动触发用户漫游的检测策略。 基于信号强度：在信号强度低于阈值时触发终端漫游； 基于速率：在终端速率低于阈值时触发终端漫游。 同时启用时，只要满足其中一个条件，就会触发终端漫游。
触发漫游 RSSI 阈值	当终端的信号强度低于所设阈值时，将主动触发终端漫游。触发漫游 RSSI 阈值不能小于强制弱信号用户下线阈值。
强制弱信号用户下线	启用/禁用弱信号用户踢除功能，启用后需设置踢除阈值。路由器将在终端信号强度低于阈值且找到合适的候选邻居 AP 时，踢除终端，以迫使终端连接到体验更好的 AP 上。强制弱信号用户下线阈值不能大于触发漫游 RSSI 阈值。

高级设置

漫游阈值检查周期	检测终端 RSSI 或速率的时间间隔。
漫游差值	触发终端主动漫游的信号强度差值，只有当邻居 AP 的信号强度减去当前连接 AP 的信号强度大于漫游差值时，才建议终端进行主动漫游。
终端禁止接入时间	当触发终端进行主动漫游时，将在非漫游目标的 AP 上设置黑名单，在终端禁止接入时间范围内不让终端接入。
终端探测上报	开启时 AP 会探测周围终端信息并上报给 AC，AC 根据这些信息构建在线终端的 AP 邻居表，对不支持 802.11k 的终端漫游有辅助作用。

6.2 射频设置

可通过本页面查看 AP 射频的主要参数，可通过本地配置或开启云管理功能，然后登录“TP-LINK 商用网络云平台”进行配置。

射频设置

AP 设置、射频设置、无线设置、认证设置可以在 TP-LINK 商用网络云平台上进行远程集中配置，后续管理维护更加方便。如需在 TP-LINK 商用网络云平台上进行远程集中配置相关参数，请不要在本地管理界面配置，点击“去开启云管理”按钮去云管理页面开启云管理功能，然后登录“TP-LINK 商用网络云平台”添加绑定本设备进行配置。

[继续本地配置](#) [去开启云管理](#)

点击去开启云管理，参考进行设置。开启云管理后，AP 设置、射频设置、无线设置、认证设置可以在 TP-LINK 商用网络云平台上进行远程集中配置，后续管理维护更加方便。

点击继续本地配置，进行本地设置页面。

6.2.1 射频设置

进入界面：AP 管理 >> 射频设置 >> 射频设置



□	序号	AP名称	射频单元	射频模式	信道	频段带宽	发射功率	客户限制	状态	设置
□	1	TL-AP300I-DC-0000	1(2.4GHz)	802.11b/g/n	自动	自动	Lv10	100	已启用	

共1条，每页：10条 | 当前：1/1页，1~1条 |

图 6-6 射频列表界面

列表中只显示选中分组下的 AP 的射频信息。点击列表设置栏中的 <> 按键可以编辑对应条目，编辑射频界面如下图所示，设置完毕后点击 <完成> 生效。



AP名称: TL-AP300I-DC-0000 (1-50个字符)

射频单元: 2.4GHz

射频模式: 802.11b/g/n

频段带宽: 自动

信道: 自动

动态信道切换 (DCS): 自动

客户端在线切换: 启用 禁用

检查周期: 8 (3-180分钟, 默认值=8)

信道占用率门限: 50 (1-100, 默认值=50)

容限系数: 20 (1-45, 默认值=20)

发射功率: Lv5

关联最大用户数: 100 (1-100个用户)

天线: 内置天线

分片门限: 2346 (必须是偶数, 256-2346字节)

beacon间隔: 100 (40-1000TU)

Airtime调度: 启用 禁用

RTS门限: 2346 (1-2347字节)

DTIM周期: 1 (1-255)

WMM: 启用 禁用

响应广播探测: 启用 禁用

Short GI: 启用 禁用

弱信号限制: 启用 禁用

弱信号踢除: 启用 禁用

确定 取消 恢复缺省

图 6-7 射频设置界面

AP 名称	显示当前需要设置参数的 AP 名称。不可修改。
射频单元	显示当前需要设置参数的 AP 射频单元。不可修改。
射频模式	设置 AP 射频单元的工作模式。
射频带宽	当射频模式支持 11n 或者 11ac 时，设置频段带宽。
信道	以无线信号作为传输媒体的数据信号传送的通道。若选“自动”，则设备会根据周围的环境自动选择一个合适的信道。
动态信道切换 (DCS)	<p>当信道设置为“自动”时方可配置。可选项有自动、手动和关闭。</p> <p>自动模式会在当前信道环境较差时自动切换到最优信道(默认需 AP 处于无客户端连接状态才会切换)。</p> <p>手动模式点击<重选信道>按钮可立即切换到最优信道(无论是否有客户端连接)。</p> <p>关闭时不会自动切换信道。</p>
客户端在线切换	当动态信道切换 (DCS) 设置为“自动”时方可配置。勾选此项后，AP 在有客户端连接时也会立即执行动态信道切换，这将导致无线客户端断线重连，影响用户使用，请谨慎勾选。
检查周期	当动态信道切换 (DCS) 设置为“自动”时方可配置。检查无线信道环境的周期。若发现当前信道环境较差，则在检查周期到达时会触发信道切换。
信道占用率门限	当动态信道切换 (DCS) 设置为“自动”时方可配置。信道占用率门限值。超过该值即认为当前信道环境较差。
容限系数	当动态信道切换 (DCS) 设置为“自动”时方可配置。信道质量提升的门限值。高于该门限才会真正切换到新信道。
发射功率	设置 AP 射频单元的最大发射功率。
关联最大用户数	设置可以接入该 AP 射频单元的客户端的最大数目。
天线	设置 AP 射频单元的天线模式。

分片门限	<p>当射频模式不含 11n 或者 11ac 时，可设置无线帧数据包的分片门限，此数值必须为偶数。</p> <p>当数据包的长度超过分片门限时，会被自动分成多个数据包。过多的数据包将会导致网络性能降低，所以分片门限不应设置过低。</p>
Beacon 间隔	<p>beacon 帧是设备的广播包，用于发布设备支持的 SSID 无线网络。无线客户端通过收到的 beacon 帧判断该 SSID 是否还存在，如果长时间都没有收到该 SSID 的 beacon 帧，则客户端可以认为该 SSID 已经不存在，客户端就会自动断开与该 SSID 的连接，从而实现无线网络连接同步。</p> <p>beacon 间隔表示设备发送 beacon 广播的实际间隔。单位：TU(Time Unit)，1TU=1024 微秒。</p>
Airtime 调度	启用或禁用 Airtime 调度算法。
RTS 门限	启用 RTS (Request To Send，要求发送) 机制所要求的无线帧的长度门限值。当无线帧长度超过该门限值时，启用 RTS 机制。设置为 2347 表示关闭 RTS 功能。
DTIM 周期	设置信标的 DTIM 周期 (Delivery Traffic Indication Message，数据待传指示信息)。
WMM	<p>当射频模式不含 11n 或者 11ac 时，可设置此项。</p> <p>当射频模式支持 11n 或者 11ac 时，此项不可设置，且强制开启。</p> <p>选择“启用”WMM 后，设备具有无线服务质量功能，可以对音频、视频数据优先处理，保证音频、视频数据的优先传输。</p>
响应广播探测	选择“启用”响应广播探测，AP 会响应客户端的广播探测请求。
Short GI	<p>当射频模式支持 11n 或者 11ac 时，可设置此项。</p> <p>当射频模式不含 11n 或者 11ac 时，此项不可设置，且强制关闭。</p> <p>选择“启用”Short GI (Short Guard Interval，短保护间隔)，可以使设备接收和发送短帧间隔数据包，提高设备的传输速率。</p>
弱信号限制	选择“启用”弱信号限制，在右侧的文本框中输入客户端信号强度门限，可以禁止低于设置门限的客户端接入该无线网络。

弱信号踢除	选择“启用”弱信号踢除，在右侧的文本框中输入客户端信号强度门限，当客户端的信号强度低于设置门限时，踢除此客户端。
-------	--

表 6.7 射频设置界面条目项说明



说明：

- 某些 AP 机型可能不支持动态信道切换 (DCS) 和 Airtime 调度的相关功能；
- 某些 AP 机型可能不支持 5GHz 的 BAND1 信道 (36、40、44、48)，即使可以设置为 BAND1 信道，但实际不生效，生效的信道可在 AP 状态界面查看，进入界面：系统状态 >> AP 状态 >> AP 状态；
- 5GHz 射频单元下，只有在频带带宽设为 20MHz 时，才支持 165 信道；
- HDAP 机型两台 AP 的射频参数可能会联动变化。

6.2.2 射频调优

进入界面：AP 管理 >> 射频设置 >> 射频调优

调优参数设置

信道调优: 启用 禁用

2.4G信道调优

频段带宽: 20MHz

2.4G信道集合: 1,6,11

5G信道调优

频段带宽: 40MHz

5G信道集合: 36,44,149,157

功率调优: 启用 禁用

定时调优: 启用 禁用

设置

立即调优

注意:

- 1、射频调优过程需要大约五分钟时间，且会导致AP无线中断。
- 2、定时调优的时间须与AP定时重启的时间间隔至少10分钟。
- 3、只有信道调优功能开启时，才能开启功率调优功能。

调优参数设置

信道调优	<p>开启/关闭信道调优功能。</p> <p>频段带宽:设置对应频段 (2.4G/5G) 的调优频段带宽。</p> <p>信道集合:设置对应频段 (2.4G/5G) 的调优信道集合。</p>
功率调优	<p>开启/关闭功率调优功能。注意：只有信道调优功能开启时，才能开启功率调优功能。</p> <p>开启功率调优后，需设置覆盖阈值、最大功率、最小功率。</p> <p>覆盖阈值:当开启功率调优时，对于 AP 的布放场景不同，AP 布放距离不同或 AP 布放高度不同，TPC 的覆盖阈值不同，实际使用时需要根据 AP 的实际布放调整 AP 的 TPC，以使 TPC 的结果能达到最优的覆盖效果。阈值越大，TPC 调整的功率值会整体提高。</p> <p>最大/最小功率:设置功率调优时，AP 允许调节的最大/最小功率。配置最大调优功率值和最小调优功率值后，AP 在进行功率调优后，最终生效的功率会在这两个值之间。</p>

定时调优	<p>开启/关闭定时射频调优功能。</p> <p>日期/时间:设置定时射频调优的时间。</p>
------	---

6.3 无线服务设置

可以在此界面设置和查看无线服务，并将无线服务绑定到射频。点击<> 按键可以添加新条目，点击<  > 按键会进入射频绑定列表界面。

进入界面：AP管理 >> 无线服务设置 >> 无线服务设置



图 6-8 无线服务管理界面

■ 新增无线服务条目

点击<  新增 > 按键可以添加新条目，新增无线服务界面如下图所示。



图 6-9 新增无线服务条目界面

状态	设置无线服务条目是否生效。
----	---------------

SSID	<p>SSID (Service Set Identifier · 服务集标识) · 是无线局域网用于身份验证的登录名 · 只有通过身份验证的用户才可以访问本无线网络。为便于标识 · SSID 的名称应该尽量具有唯一性。</p> <p>本产品 SSID 设置支持中文字符 · 当输入的 SSID 包含中文时 · 将出现编码方式选项 · 可选择 UTF-8 或 GBK 编码格式。最长可支持 32 个英文字符 · 16 个 GBK 或者 10 个 UTF-8 中文字符。</p> <p>当 SSID 包含中文字符时 · 选择单一编码格式 · 会由于不同客户端机型和系统上的差异 · 出现某些客户端可能无法正常搜索和显示 SSID 的情况。建议用户在使用中文 SSID 时 · 设置两个使用相同无线网络名称但采用不同编码格式的无线网络。</p>
描述	设置该条目的描述信息 · 以方便管理和查找。
无线网络内部隔离	启用此项 · 使连接到同一个无线网络的客户端实现隔离 · 客户端之间不能互相通信。该功能不能跨 AP 生效 · 即通过不同 AP 接入相同无线网络的客户端之间不能实现隔离。
隐藏无线网络	<p>启用隐藏无线网络 · 局域网中无线终端将搜不到该无线名称。</p> <p>终端需要手动输入无线网络名称进行添加。</p>
安全选项	<p>设置该 SSID 的安全选项。如果不需要对无线网络加密 · 能够让任意主机接入无线网络 · 则可以选择“关闭安全选项”；如果需要对无线网络加密 · 请选择界面中两种安全类型中的一种进行无线安全设置。为保障网络安全 · 推荐启用安全设置。</p> <p>本设备提供的安全类型有：WPA-PSK/WPA2-PSK 和 WPA/WPA2 · 推荐使用 WPA-PSK/WPA2-PSK AES 加密方法。</p> <p>不同的安全类型下 · 安全设置项不同 · 下面将详细介绍。</p>
带宽控制	<p>设置客户端带宽控制功能是否生效。点击“启用”则需要设置带宽控制的模式、最大上行带宽和最大下行带宽。</p> <p>控制模式分为共享模式（所有客户端均分共享带宽控制值）和独占模式（所有客户端独占带宽控制值）。</p>
自动绑定所有 AP	<p>设置无线服务是否自动绑定 AP · 包含之前已经接入的 AP 和之后新接入的 AP（开启此功能后手动绑定功能禁用）。</p> <p>开启此功能需设置自动绑定的射频和 VLAN。</p>

表 6.8 新增无线服务条目界面条目项说明



说明：

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

安全选项中的 WPA-PSK/WPA2-PSK 和 WPA/WPA2 加密方式详细介绍如下：

■ WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK 安全类型是基于共享密钥的 WPA 模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。“WPA-PSK/WPA2-PSK”的设置页面如下，设置完毕后点击<确定>生效。

无线网络管理

✔ 启用
✘ 禁用
+ 新增
 - 删除
 🔍 搜索

<input type="checkbox"/>	序号	SSID	描述	安全选项	状态	射频绑定	设置
<input type="checkbox"/>	--	--	--	--	--	--	--
<div style="border: 1px solid #ccc; padding: 5px;"> <p>状态: <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用</p> <p>SSID: <input type="text"/> (1-32个字符)</p> <p>描述: <input type="text"/> (1-50个字符, 可选)</p> <p>无线网络内部隔离: <input type="radio"/> 启用 <input checked="" type="radio"/> 禁用</p> <p>安全选项: WPA-PSK/WPA2-PSK ▼</p> <p>认证类型: 自动 ▼</p> <p>加密算法: 自动 ▼</p> <p>组密钥更新周期: 86400 (30-604800) 秒, 不更新则为0</p> <p>PSK密码: <input type="text"/> (8-64个字符)</p> <p>带宽控制: <input type="radio"/> 启用 <input checked="" type="radio"/> 禁用</p> <p style="text-align: left;"> <input type="button" value="确定"/> <input type="button" value="取消"/> </p> </div>							
<input type="checkbox"/>	1	AA-BB-CC-DD-EE	11111	---	已启用 ✘	📶	✏️ 🗑️

共1条, 每项: 10 条 | 当前: 1/1页, 1~1条 | 1

图 6-10 WPA-PSK/WPA2-PSK 设置界面

认证类型	选择系统采用的安全模式，即自动、WPA-PSK、WPA2-PSK。默认选项为自动，无线控制器会根据主机请求自动选择 WPA-PSK 或 WPA2-PSK 安全模式。
------	--

加密算法	<p>选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。</p> <p>自动：选择该项后，无线控制器将根据网卡端的加密方式自动选择 TKIP 或 AES 加密方式。</p> <p>TKIP (Temporal Key Integrity Protocol，暂时密钥集成协议)：负责处理无线安全问题的加密部分。</p> <p>AES (Advanced Encryption Standard，高级加密标准)：是美国国家标准与技术研究所用于加密电子数据的规范。该算法汇聚了设计简单、密钥安装快、需要的内存空间少、在所有的平台上运行良好、支持并行处理并且可以抵抗所有已知攻击等优点。</p>
组密钥更新周期	<p>定时更新用于广播和组播的密钥的周期，以秒为单位，最小值为 30，不更新则为 0。</p>
PSK 密码	<p>选择 WPA-PSK/WPA2-PSK 加密时连接无线网络的密码，由 8-63 个 ASCII 码字符或 8-64 个十六进制字符组成。</p>

表 6.9 WPA-PSK/WPA2-PSK 设置界面条目项说明

■ WPA /WPA2

WPA/WPA2 是采用 Radius 服务器进行身份认证并得到密钥的 WPA 或 WPA2 安全模式。由于要架设一台专用的认证服务器，代价比较昂贵且维护也很复杂，所以不推荐普通用户使用此安全类型。“WPA /WPA2” 的设置页面如下，设置完毕后点击<确定>生效。

✔ 启用 ✘ 禁用 ➕ 新增 ➖ 删除 🔍 搜索

□	序号	SSID	描述	安全选项	状态	射频绑定	设置
--	--	--	--	--	--	--	--

状态: 启用 禁用

SSID: (1-32个字符)

描述: (1-50个字符, 可选)

无线网络内部隔离: 启用 禁用

安全选项: ▼

认证类型: ▼

加密算法: ▼

组密钥更新周期: (30-604800) 秒, 不更新则为0

Radius服务器IP:

Radius认证端口: (1024-65535)

Radius计费端口: (0,1024-65535)

Radius密码: (1-64个英文字符)

带宽控制: 启用 禁用

共0条, 每页: 条 | 当前: 0/0页, 0~0条 | ⏪ ⏩

图 6-11 WPA /WPA2 设置界面

认证类型	用于设置无线网络使用加密连接时的认证类型。 WPA/WPA2 加密方式的认证类型包括自动、WPA 和 WPA2 三个选项，自动涵盖 WPA 和 WPA2 两种认证类型，建议认证类型选择自动。
加密算法	用于设置无线网络使用加密连接时的认证类型。 WPA/WPA2 加密方式的认证类型包括自动、WPA 和 WPA2 三个选项，自动涵盖 WPA 和 WPA2 两种认证类型，建议认证类型选择自动。
组密钥更新周期	定时更新用于广播和组播的密钥的周期，以秒为单位，最小值为 30，不更新则为 0。
Radius 服务器 IP	Radius 服务器用来对无线网络内的主机进行身份认证，此项用来设置该服务器的 IP 地址。
Radius 认证端口	设置该 Radius 认证服务采用的端口号。
Radius 计费端口	设置该 Radius 计费服务采用的端口号。
Radius 密码	设置访问 Radius 服务的密码。

表 6.10 WPA /WPA2 设置界面条目项说明

 **说明：**

- 无线网络内的主机若想连接该无线控制器，其无线参数必须与此处设置一致。
- 802.11n 不支持 TKIP 算法，如果在 11n 模式下使用 TKIP 加密会导致 STA 无法正常接入，而在 11b/g/n 模式下使用 TKIP 加密算法，传输速率只能达到 54Mbps。TKIP 是 WPA-PSK/WPA2-PSK 和 WPA/WPA2 加密方式中加密算法的选项。

6.4 客户端状态

可以通过本页面查看连接到 AP 设备上无线网络客户端的相关连接信息。

进入界面：AP管理 >>客户端状态 >> 客户端状态

客户端状态

选择AP分组: default

 断开连接
  搜索
  全局搜索
  刷新
  自动刷新

<input type="checkbox"/>	序号	MAC地址	AP名称	射频单元	SSID	IPv4/IPv6地址	VLAN ID	接入时间	信号强度	断开连接
--	--	--	--	--	--	--	--	--	--	--

图 6-12 客户端状态界面

MAC 地址	显示连接到 AP 的客户端的 MAC 地址。
AP 名称	显示 AP 的名称。
射频单元	显示客户端所连接的射频单元。
SSID	显示接入的 AP 无线网络的名称。
IPv4/IPv6 地址	显示客户端的 IPv4 和 IPv6 地址。
VLAN ID	显示接入用户的 VLAN ID。
接入时间	显示客户端接入的时长。
信号强度	显示信号的强度。
断开连接	点击页面按钮可断开与客户端的连接

表 6.11 客户端状态界面条目项说明

 **说明：**

- 无线主机状态实时速率的显示需要 IP 流量统计的支持，请到运行状态->流量统计->IP 流量统计中打开相关功能。

第7章 传输控制

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

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

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

7.3 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。

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

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

7.1 NAT 设置

本小节主要介绍 NAT 技术、本设备上实现的 NAT 功能特性以及相关功能的配置。

■ NAT 技术简介

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



图 7-1 NAT 地址转换示意图

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

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

■ NAT的分类

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

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

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

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

本设备提供了静态NAT和NAPT两种特性。

■ 本设备的NAT特性

本设备提供了下列 5 种 NAT 相关功能特性：

7.1.1 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。

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

7.1.3 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。

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

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

7.1.1 NAPT

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

■ 配置NAPT

进入界面：传输控制 >> NAT 设置 >> NAPT

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

□	序号	规则名称	出接口	源地址范围	状态	备注	设置
--	--	--	--	--	--	--	--

规则名称:

出接口:

源地址范围: /

状态: 启用

备注:

图 7-2 NAPT 界面-设置 NAPT 规则

规则名称	输入该规则条目的名称。只能输入英文、数字和下划线。
出接口	选择该 NAPT 规则的生效接口，当数据包的源 IP 地址在源地址内，且从该接口转发时，路由器将对数据包进行 NAPT 地址转换。
源地址范围	设置 IP 地址范围，相应的 NAPT 规则条目只对源地址为设定范围内的数据包生效。

状态	勾选“启用”，则使该规则条目生效； 未勾选“启用”，则该规则条目无效。
备注	添加对本条目的说明信息，非必填项。

表 7.1 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。

<input type="checkbox"/>	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 7-3 NAPT界面-映射列表

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

如图 7-3 所示，“eth0”和“isp1”接口连接到广域网，图中 4 条规则分别表示含义：

- 1) 序号为 1 和 2 的规则表示 192.168.0.0/24 和 192.168.1.0/24 两个子网中的计算机通过“eth0”接口访问外部网络时均需要进行 NAPT 地址转换，共用接口的 IP 地址上网；
- 2) 序号为 3 的规则表示计算机 192.168.3.56 通过“eth0”接口上网时需要进行 NAT 地址转换，使用接口的 IP 地址上网；
- 3) 当网络中存在多条外线接口时，如图中“eth0”和“isp1”，访问 Internet 的数据包有可能通过其他接口直接转发到 Internet 中，在这种情况下，需要在路由器上设置多个 NAPT 条目来保证数据包转发到 Internet 时均做 NAPT 地址转换。图中序号为 2 和 4 的规则表示，192.168.1.0/24 子网中的计算机通过“eth0”和“isp1”两条外线访问网络时本设备均会对数据包做 NAPT 地址转换。
- 4) 当局域网中所有主机均需要访问 Internet 时，您需要为所有子网都建立 NAPT 规则，此时可以通过设置全 0 规则快速设置，源地址范围设置为 0.0.0.0/0 即可，如下图所示，图中创建的规则表示所有从“isp1”接口转发的数据均做地址转换。

□	序号	规则名称	出接口	源地址范围	状态	备注	设置
--	--	--	--	--	--	--	--

规则名称:

出接口:

源地址范围: /

状态: 启用

备注:

图 7-4 NAPT界面-全0规则



说明：

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

■ 应用环境

如图 7-5 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-ER6225G 工业级上网。

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，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，因此需要在路由器上创建路由规则。

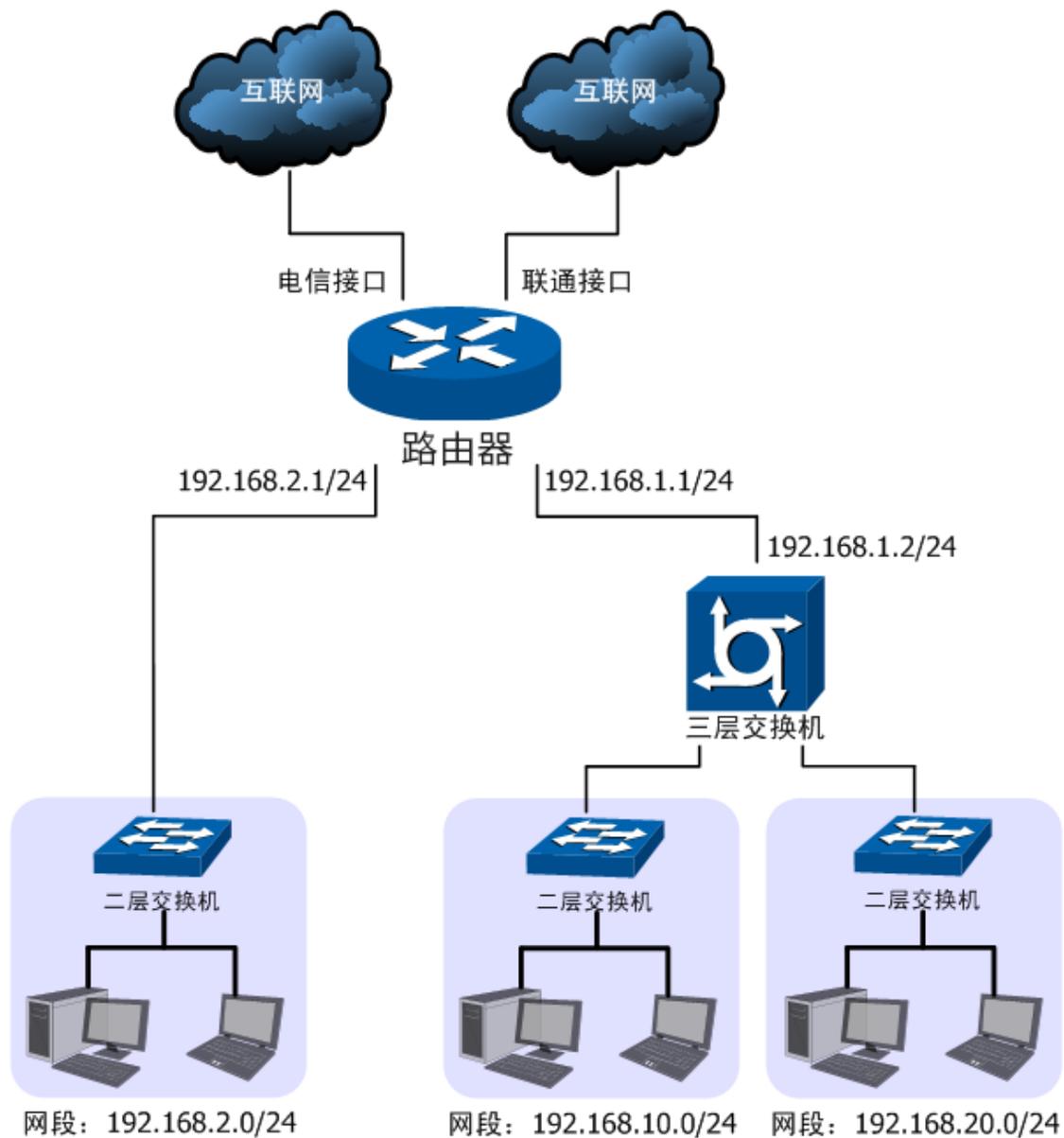


图 7-5 NAPT功能组网应用

配置步骤：

TL-ER6225G 工业级路由器要完成上述网络需求，需要配置 NAPT 功能和路由功能，配置步骤如下：

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

<input type="checkbox"/>	序号	规则名称	出接口	源地址范围	状态	备注	设置
--	--	--	--	--	--	--	--

规则名称:

出接口:

源地址范围: /

状态: 启用

备注:

图 7-6 电信接口 NAT 设置

<input type="checkbox"/>	序号	规则名称	出接口	源地址范围	状态	备注	设置
--	--	--	--	--	--	--	--

规则名称:

出接口:

源地址范围: /

状态: 启用

备注:

图 7-7 联通接口 NAT 设置

- 2) 设置静态路由，必须操作。创建界面：传输控制 >> 路由设置 >> 静态路由。对于网段 192.168.10.0/24，其通过三层交换机连接到路由器的 192.168.1.1/24 接口，因此需要在路由器上建立静态路由条目，使网络 192.168.10.0/24 在路由器上路由可达。静态路由条目配置如图 7-8 所示。

<input type="checkbox"/>	序号	规则名称	目的地址	子网掩码	下一跳	出接口	Metric	可达性	状态	设置
--	--	--	--	--	--	--	--	--	--	--

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

图 7-8 静态路由设置

其中目的地址和子网掩码表示此静态路由条目指向的目标网络，下一跳指通往目标网络的路径上下一个网络节点的 IP 地址，出接口表示从路由器上的哪个接口转发数据包，Metric 表

示该路径的度量值，请保持为 0，以保证该静态路由条目为最优路径。静态路由相关配置方法请参考 7.4.4 在线检测

进入界面：传输控制 >> 流量均衡 >> 在线检测

该页面用于检测接口是否在线。在线检测列表如下图所示。

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

图 7-35 在线检测界面-接口状态列表

如有需要，可以点击条目后的 按钮进行编辑。

序号	接口名	接口状态	设置
1	GE1	不在线	---

接口名:

检测模式: 自动 手动 永远在线

PING检测:

DNS检测:

图 7-36 在线检测界面

接口名	选择需要在线检测的接口。
检测模式	选择自动在线检测、手动在线检测或永远在线,默认为自动在线检测模式。自动模式下，PING 检测选择网关作为目的地址，DNS 检测选择接口 DNS 服务器作为目的地址；手动模式下，您可以自己设置 PING 检测和 DNS 检测的目的地址；永远在线模式下，该接口会被强制设置为永远在线，无需检测。
PING 检测	在手动在线检测模式下，可以输入 PING 检测的目的 IP 地址。输入 0.0.0.0 表示不进行 PING 检测。
DNS 检测	在手动在线检测模式下，可以输入 DNS 服务器的 IP 地址，输入 0.0.0.0 表示不进行 DNS 检测。

表 6-10 在线检测界面项说明

7.1.2 一对一 NAT

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

■ 配置一对一 NAT

进入界面：传输控制 >> NAT 设置 >> 一对一 NAT

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

□	序号	规则名称	出接口	映射前地址	映射后地址	DMZ转发	备注	状态	设置
--	--	--	--	--	--	--	--	--	--

规则名称:

出接口:

映射前地址:

映射后地址:

DMZ转发: 启用

备注:

状态: 启用

图 7-9 一对一 NAT 界面-设置 NAT 规则

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

状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。
----	---

表 7.2 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。

<input type="checkbox"/>	序号	规则名称	出接口	映射前地址	映射后地址	DMZ转发	备注	状态	设置
<input type="checkbox"/>	1	http_server	eth1	192.168.1.10	201.0.0.1	已禁用	---	已启用	

图 7-10 一对一 NAT 界面-映射列表

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

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

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



说明：

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

■ 应用环境

如图 7-11 所示，某企业向电信申请了两个公网 IP “201.1.1.1” 和 “201.1.1.2”，其中地址 “201.1.1.1” 用于为局域网计算机共享上网，而地址 “201.1.1.2” 则用于企业服务器 192.168.100.5 为广域网提供服务。

分析如下：

- 1) 针对服务器 192.168.100.5，需要创建一对一 NAT 规则，保证数据从电信接口转发到广域网时使用固定的 IP 地址进行转换，同时广域网用户可以通过固定的 IP 地址访问服务器。
- 2) 针对需要上网的网段，需要创建 NAT 规则，请参考 7.1.1 NAT 进行配置。

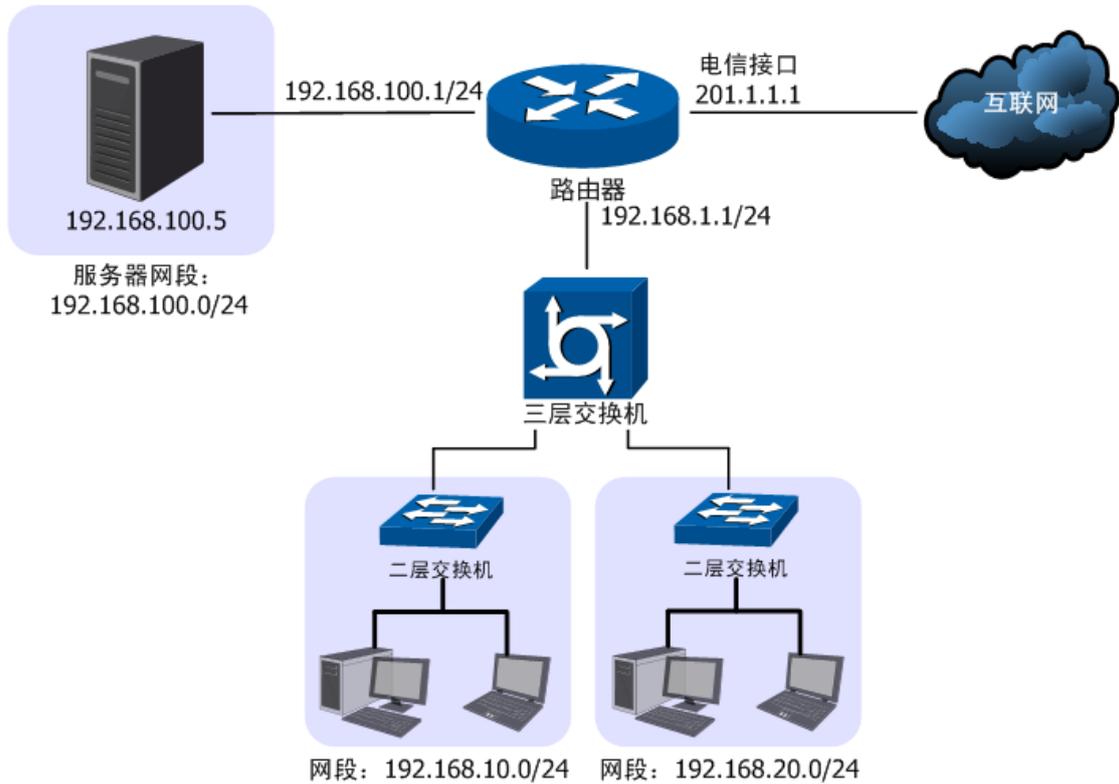


图 7-11 一对一NAT功能组网应用

配置步骤：

TL-ER6225G 工业级路由器要完成上述网络需求，需要为服务器配置一对一 NAT 功能，为其他上网接口配置 NAPT 功能和路由功能，配置步骤如下：

- 1) 设置一对一 NAT 规则。必须操作。创建界面：传输控制 >> NAT 设置 >> 一对一 NAT。配置 192.168.100.5 服务器的数据从电信接口转发时，将做一对一 NAT 映射再转发，映射后地址为 201.1.1.2。
- 2) 设置 NAPT 规则。必须操作。创建界面：传输控制 >> NAT 设置 >> NAPT。配置 192.168.10.0/24 和 192.168.20.0/24 两个网段的数据从电信接口转发时做 NAPT 地址转换。
- 3) 设置静态路由。必须操作。创建界面：传输控制 >> 路由设置 >> 静态路由。对于网段 192.168.10.0/24 和 192.168.20.0/24，其通过三层交换机连接到路由器的 192.168.1.1/24 接口，因此需要在路由器上建立静态路由条目，使网络 192.168.10.0/24 和 192.168.20.0/24 在路由器上路由可达。静态路由条目配置参考 6.5 路由设置

7.1.3 虚拟服务器

在路由器上设置了 NAPT 特性的接口，因防火墙的限制，会拒绝用户向此接口发起的访问请求。当网络中搭建了服务器需要为所有用户开放时，NAPT 特性接口下的用户将无法获得

服务。通过虚拟服务器功能，在设置了 NAPT 特性的接口上开放固定的传输层协议端口，当开放端口收到访问请求时，将把访问请求转发到指定的服务器上，此接口中的用户便能成功访问网络中的服务器，同时不影响网络安全。

■ 配置虚拟服务器

进入界面：传输控制 >> NAT 设置 >> 虚拟服务器

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

□	序号	规则名称	生效接口	外部端口	内部端口	内部服务器IP	服务协议	状态	设置
--	--	--	--	--	--	--	--	--	--
<div style="border: 1px solid #ccc; padding: 5px;"> <p>规则名称: <input type="text" value="web_server"/></p> <p>生效接口: <input type="text" value="isp1"/></p> <p>外部端口: <input type="text" value="12892-12892"/> (1-65535,格式为XX或者XX-XX)</p> <p>内部端口: <input type="text" value="80-80"/> (1-65535,格式为XX或者XX-XX)</p> <p>内部服务器IP: <input type="text" value="192.168.100.5"/></p> <p>服务协议: <input type="text" value="ALL"/></p> <p>状态: <input checked="" type="checkbox"/> 启用</p> <p><input type="button" value="确定"/> <input type="button" value="取消"/></p> </div>									

图 7-12 虚拟服务器界面-设置虚拟服务器

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

表 7.3 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。

<input type="checkbox"/>	序号	规则名称	生效接口	外部端口	内部端口	内部服务器IP	服务协议	状态	设置
<input type="checkbox"/>	1	web_server	isp1	12892-12892	80-80	192.168.100.5	ALL	已启用	

图 7-13 虚拟服务器界面-服务列表

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

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

■ 应用环境

如图 7-14 所示，某企业网络存在普通用户子网和服务器子网，同时向电信运营商申请了一条宽带接入线，子网192.168.1.0/24中的用户通过电信接口访问Internet，而web服务器192.168.100.5则需要通过电信接口给广域网中的用户提供web服务，服务端口为80。

分析如下：

- 1) 普通用户可以通过NAPT功能共享一条宽带接入线上网。
- 2) 服务器通过宽带接入线向广域网发送数据时，为了避免私有网络信息发送到广域网，因此针对服务器子网也需要设置NAPT。
- 3) 为服务器配置虚拟服务器功能，向广域网用户开放一个传输层端口，供广域网用户访问服务器。

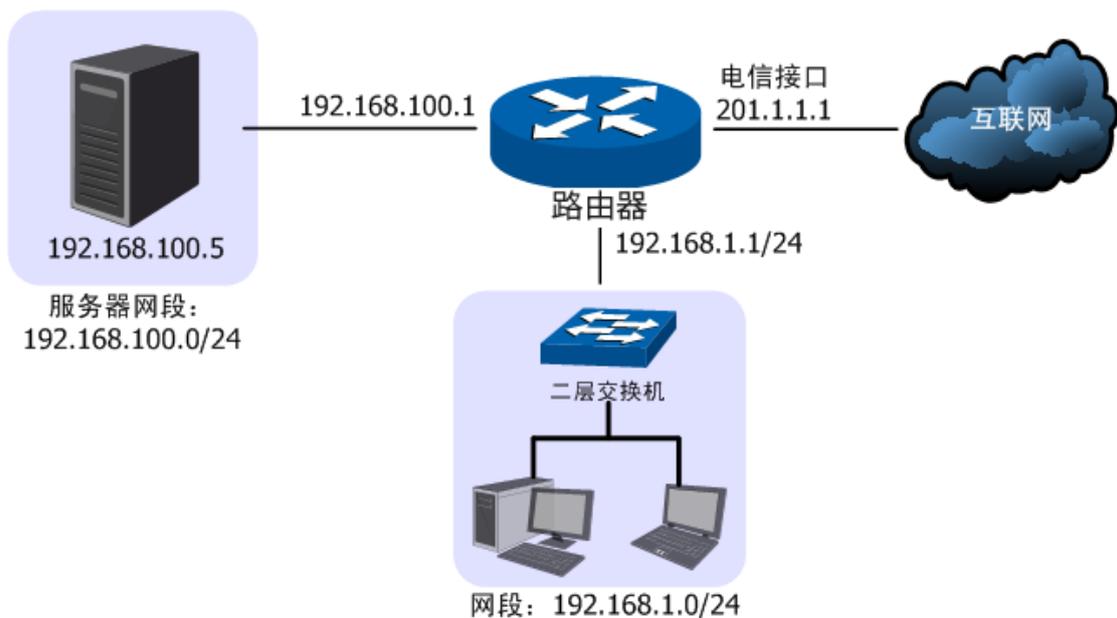


图 7-14 虚拟服务器功能组网应用

配置步骤：

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

- 1) 设置NAPT规则。必须操作。创建界面：传输控制 >> NAT设置 >> NAPT。配置普通用户子网192.168.1.0/24和服务器子网的数据从“电信接口”上网时做NAPT地址转换。
- 2) 设置虚拟服务器功能。必须操作。创建界面：传输控制 >> NAT设置 >> 虚拟服务器。在“电信接口”上为服务器开放一个端口，供广域网用户访问服务器，当开放端口收到来自广域网用户的访问请求时，将把访问请求转发到内网服务器的服务端口上。此处假设开放的外部端口为8080，局域网服务器提供的服务端口为80。
- 3) 访问服务器。可选操作。广域网用户访问网络时，可以通过地址加端口的方式访问服务器。例如本例中的web服务器则可以通过网页浏览器进行访问，地址格式为http://接口地址:开放端口，根据本例中的实际参数则地址为http://201.1.1.1:8080，路由器收到访问请求时将地址转换成<http://192.168.100.5:80>后转发给服务器。



说明：

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

7.1.4 ALG 服务

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

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。
PPTP	用于路由器使用 PPTP 方式进行拨号，或者提供 PPTP 隧道连接服务时，需要启用 PPTP ALG。
SIP	局域网中存在 Internet 多媒体会议、IP 电话等应用是基于 SIP 协议的，需要启用 SIP ALG。

表 7.4 ALG 应用列表

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。

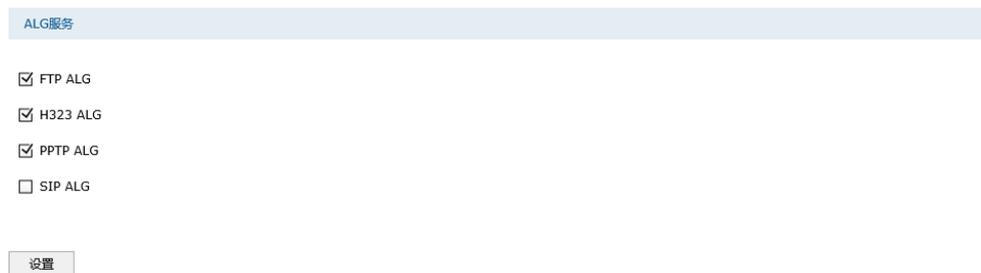


图 7-15 ALG 服务界面-设置 ALG 服务

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

7.1.5 NAT-DMZ

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

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

■ 配置NAT-DMZ

进入界面：传输控制 >> NAT 设置 >> NAT-DMZ

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

□	序号	规则名称	出接口	主机地址	状态	设置
--	--	--	--	--	--	--

规则名称:

出接口:

主机地址:

状态: 启用

图 7-16 NAT DMZ 界面-设置 DMZ 区

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

表 7.5 NAT-DMZ 界面条目项说明

新增的条目会在服务列表中显示出来，如下图所示。

□	序号	规则名称	出接口	主机地址	状态	设置
□	1	bbs	isp1	192.168.200.10	已启用	

图 7-17 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。

7.2 带宽控制

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

■ 配置智能带宽控制

进入界面：传输控制 >> 带宽控制 >> 带宽控制

在界面的功能开关区域，设置带宽控制功能，点击<设置>按钮保存配置。



The screenshot shows a configuration page titled '功能设置' (Function Settings). It contains two checkboxes: '启用带宽控制' (Enable bandwidth control) and '仅当带宽利用率达到 0 %以上时，带宽控制功能才生效' (Bandwidth control function only takes effect when bandwidth utilization reaches 0% or above). Below these is a '设置' (Settings) button.

图 7-18 带宽控制规则界面-功能设置

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

■ 配置带宽控制规则

进入界面：传输控制 >> 带宽控制 >> 带宽控制

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

<input type="checkbox"/>	序号	规则名称	源接口	目的接口	受控地址组	地址类型	最大带宽	带宽模式	生效时间	状态	设置
<input type="checkbox"/>	--	--	--	--	--	--	--	--	--	--	--

规则名称:	<input type="text"/>
源接口:	---
目的接口:	---
受控地址组:	IPGROUP_ANY
地址类型:	<input checked="" type="radio"/> 源地址 <input type="radio"/> 目的地址
最大带宽:	1000 Kbps(100-10000000)
带宽模式:	<input type="radio"/> 共享 <input checked="" type="radio"/> 独立
生效时间:	Any
备注:	<input type="text"/> (可选)
添加到指定位置(第几条):	<input type="text"/> (可选)
状态:	<input checked="" type="checkbox"/> 启用

图 7-19 带宽控制规则界面-设置带宽控制规则

规则名称	输入该规则条目的名称。只能输入英文、数字和下划线。
源接口	选择规则控制的数据源端。

目的接口	选择规则控制的数据目的端。
受控地址组	选择规则控制的地址组，以设置 IP 地址范围，地址组的设置方法地址管理。见此处的受控地址组与下面的受控地址类型共同指定此带宽控制规则的面向对象。例如，设置此规则的生效对象为 IP 地址范围 192.168.10.100-192.168.10.200 的计算机发出的数据包。
地址类型	选择此带宽控制规则生效对象的源或目的计算机的 IP 地址。
最大带宽	选择规则定义的数据流的最大上行带宽，取值范围为 100-100000000Kbps，默认为 1000Kbps。
带宽模式	设置地址组的带宽控制模式：共享模式即受控地址范围内所有 IP 地址带宽总和为当前规则所设置的带宽限制；独立模式即受控地址范围内每一个 IP 地址都将应用当前规则所设置的带宽限制。
生效时间	选择规则生效时间，其他时间规则不生效。Any 为系统默认设置的时间对象，表示所有时间。请在对象管理章节设置时间对象。
备注	添加对当前规则的说明信息。
添加到指定位置	选择将当前规则添加到规则列中的指定位置。若留空，则当前规则将默认添加到已有规则之后。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 7.6 带宽控制规则界面条目项说明

新增的条目会在用户规则列表中显示出来，如下图所示。

<input type="checkbox"/>	序号	规则名称	源接口	目的接口	受控地址组	地址类型	最大带宽	带宽模式	生效时间	状态	设置
<input type="checkbox"/>	1	rule1	eth0	eth1	g_lan_ip	src	1000	共享	Any	已启用	

图 7-20 带宽控制规则界面-规则列表

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

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

配置步骤：

配置带宽控制规则时，需要按照下面步骤进行配置：

- 1) 设置时间对象。必须操作。创建界面：对象管理 >> 时间管理。设置时间对象以便配置带宽控制规则的生效时间。
- 2) 设置地址组。必须操作。创建界面：对象管理 >> 地址管理>> 地址管理。设置地址组以控制需进行带宽控制的 IP 地址范围。
- 3) 设置带宽控制规则。必须操作。创建界面：传输控制 >> 带宽控制 >> 带宽控制。根据受控对象的网络参数设置带宽控制规则。

7.3 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。

7.3.1 连接数限制

■ 配置连接数限制全局特性

进入界面：传输控制 >> 连接数限制 >> 连接数限制

在界面的功能设置区域，全局启用连接数限制功能，点击<设置>按钮保存配置。

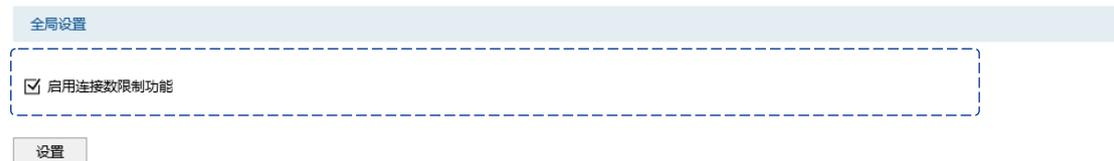


图 7-21 连接数限制界面-功能设置

勾选此项以启用连接数限制功能。不勾选时，所有连接数限制均不生效。

■ 配置连接数限制规则

进入界面：传输控制 >>连接数限制 >> 连接数限制

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

□	序号	规则名称	受控地址组	最大连接数	状态	设置
--	--	--	--	--	--	--

规则名称:

受控地址组:

最大连接数: (数值范围:1-65535)

状态: 启用

图 7-22 连接数限制界面-设置连接数限制规则

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

表 7.7 连接数限制规则界面条目项说明

新增的条目会在规则列表中显示出来，如下图所示。

□	序号	规则名称	受控地址组	最大连接数	状态	设置
<input type="checkbox"/>	1	rule1	g_lan_ip	1000	已启用	

图 7-23 连接数限制界面-规则列表

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

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

7.3.2 连接数监控

进入界面：传输控制 >> 连接数限制 >> 连接数监控

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

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

图 7-24 连接数监控界面-监控现有连接数

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

配置步骤：

配置连接数限制规则时，需要按照下面步骤进行配置：

- 1) 设置受控地址组。必须操作。创建界面：对象管理 >> 地址管理>>地址管理。对于连接数限制功能的受控地址范围，需要先在对象管理中进行设置，在设置连接数限制时将直接选择。
- 2) 启用连接数限制功能并设置规则。必须操作。创建界面：传输控制 >> 连接数限制 >> 连接数限制。根据受控对象的需要设置不同的最大连接数。

7.4 流量均衡

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

7.4.1 基本配置

■ 启用流量均衡

进入界面：传输控制 >> 流量均衡 >> 基本设置

在界面的全局设置区域，选择是否启用流量均衡，点击<设置>按钮保存配置。



图 7-25 基本设置-全局设置界面

勾选此项，则全局开启流量均衡功能。若不勾选，则所有流量均衡功能关闭。

■ 特殊应用程序选路

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

进入界面：传输控制 >> 流量均衡 >> 基本设置

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

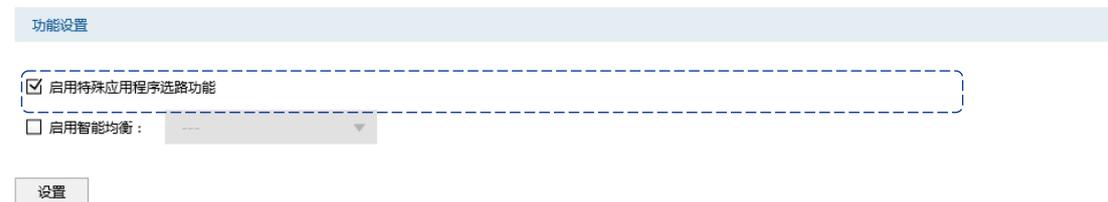


图 7-26 基本设置-特殊应用程序选路功能界面

设置完成后，路由器就会为一些多连接应用程序的数据包选择最优线路。

■ 智能均衡

进入界面：传输控制 >> 流量均衡 >> 基本设置

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

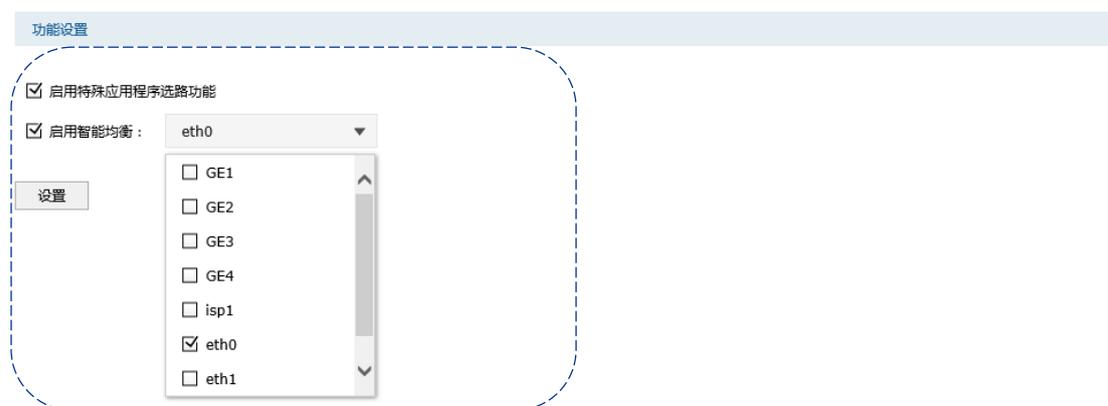


图 7-27 智能均衡设置界面



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。

7.4.2 ISP 选路

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

■ ISP选路设置

进入界面：传输控制 >> 流量均衡 >> ISP 选路

启用 ISP 选路功能

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



图 7-28 ISP 选路界面-启用 ISP 选路功能

导入 ISP 数据库

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



图 7-29 ISP 选路界面-导入 ISP 数据库

用户自定义数据库

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



图 7-30 ISP选路界面-导入用户自定义数据库

ISP 选路设置

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

□	序号	接口	ISP	状态	设置
--	--	--	--	--	--

接口:

ISP:

状态: 启用

图 7-31 ISP 选路界面-ISP 选路设置

接口	选择进行 ISP 选路的接口。
ISP	在下拉列表中选择 ISP。
状态	勾选后启用该 ISP 选路规则

表 7.8 ISP 选路功能设置界面项说明

新增的条目会在选路列表里显示出来，如下图所示。

□	序号	接口	ISP	状态	设置
□	1	eth1	电信	已启用	

图 7-32 ISP 选路界面-选路列表

如有需要，可以点击条目后的< >按钮进行编辑。

说明：

- 智能均衡、策略路由、ISP 选路三个功能可以同时工作，但当三个功能设置有冲突时，路由器执行的优先顺序为：策略路由 > ISP 选路 > 智能均衡。

■ ISP选路典型应用

某网吧使用电信和联通双线接入，带宽分别为 10M，现需要使用 TL-ER6225G 工业级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-ER6225G 工业级路由器：

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

- 2) 在传输控制 >> 流量均衡 >> 基本设置界面，启用特殊应用程序选路功能和智能均衡。
- 3) 在传输控制 >> 流量均衡 >> ISP 选路界面，启用 ISP 选路功能。TL-ER6225G 工业级内嵌了 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

设置

导入ISP数据库

数据库版本: 1.9.0

数据库路径: 浏览

导入

选路列表

+ 新增 - 删除

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

7.4.3 线路备份

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

■ 设置线路备份

进入界面：传输控制 >> 流量均衡 >> 线路备份

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

<input type="checkbox"/>	序号	主接口	备接口	备份模式	生效时间	状态	设置
<input type="checkbox"/>	--	--	--	--	--	--	--

主接口:

备接口:

备份模式: 定时备份 故障备份

生效时间:

状态: 启用

图 7-33 线路备份界面-备份设置

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

表 7.9 线路备份功能设置界面项说明

新增的条目会在线路备份规则列表里显示出来，如下图所示。

<input type="checkbox"/>	序号	主接口	备接口	备份模式	生效时间	状态	设置
<input type="checkbox"/>	1	GE1	GE2	定时备份	Any	已启用	

图 7-34 线路备份界面-主备组列表

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



说明：

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

衡 >> 在线检测界面进行设置。

■ 线路备份举例

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

配置步骤

如果要完成上述网络需求，需要按如下顺序配置 TL-ER6225G 工业级路由器：

- 1) 创建 Ethernet 接口 eth1 和 eth2，并分别连接到线路 1 和线路 2。注意设置接口网络参数时必须勾选参与流量均衡选项。
- 2) 开启在线检测。必须操作。在界面传输控制 >> 流量均衡 >> 在线检测，开启对 eth1 接口和 eth2 接口的在线检测。
- 3) 在传输控制 >> 流量均衡 >> 线路备份界面添加下图所示条目后，当 eth1 接口发生故障时，路由器将自动切换到 eth2 接口。

□	序号	主接口	备接口	备份模式	生效时间	状态	设置
--	--	--	--	--	--	--	--

主接口: eth1

备接口: eth2

备份模式: 定时备份 故障备份

生效时间: Any

状态: 启用

确定 取消

7.4.4 在线检测

进入界面：传输控制 >> 流量均衡 >> 在线检测

该页面用于检测接口是否在线。在线检测列表如下图所示。

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

图 7-35 在线检测界面-接口状态列表

如有需要，可以点击条目后的 按钮进行编辑。

序号	接口名	接口状态	设置
1	GE1	不在线	---
<div style="border: 1px solid #ccc; padding: 5px;"> <p>接口名: <input type="text" value="GE1"/></p> <p>检测模式: <input type="radio"/> 自动 <input checked="" type="radio"/> 手动 <input type="radio"/> 永远在线</p> <p>PING检测: <input type="text" value="0.0.0.0"/></p> <p>DNS检测: <input type="text" value="0.0.0.0"/></p> <p><input type="button" value="确定"/> <input type="button" value="取消"/></p> </div>			

图 7-36 在线检测界面

接口名	选择需要在线检测的接口。
检测模式	选择自动在线检测、手动在线检测或永远在线,默认为自动在线检测模式。自动模式下, PING 检测选择网关作为目的地址, DNS 检测选择接口 DNS 服务器作为目的地址;手动模式下,您可以自己设置 PING 检测和 DNS 检测的目的地址;永远在线模式下,该接口会被强制设置为永远在线,无需检测。
PING 检测	在手动在线检测模式下,可以输入 PING 检测的目的 IP 地址。输入 0.0.0.0 表示不进行 PING 检测。
DNS 检测	在手动在线检测模式下,可以输入 DNS 服务器的 IP 地址,输入 0.0.0.0 表示不进行 DNS 检测。

表 6-10 在线检测界面项说明

7.5 路由设置

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

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

- 1) 目的网络地址：用于标识该条路由条目所指向的目标网络。
- 2) 子网掩码：用于标识目标网络的子网掩码。
- 3) 下一跳地址：用于指定通往目标网络的下一跳路由节点，路由器将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过 ping 工具测试是否可达。
- 4) 下一跳接口：用于标识数据从本地发出的出接口。

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

- 直连路由：通过数据链路层协议发现的，通常指向与路由器直接连接的网络，如 VLAN。
- 静态路由：由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。
- 动态路由：通过相互连接的路由器之间交换彼此的路由信息，然后通过路由选择协议计算出自身的路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。常用的动态路由选择协议有 RIP、OSPF 和 BGP 等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。

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

7.5.1 策略路由

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

■ 策略路由设置

进入界面：传输控制 >> 路由设置 >> 策略路由

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

□	序号	规则名称	服务类型	源地址	目的地址	生效接口	生效时间	强制	备注	状态	设置
--	--	--	--	--	--	--	--	--	--	--	--

规则名称:

服务类型: ▼

源地址: ▼

目的地址: ▼

生效接口: ▼

生效时间: ▼

强制: 接口不在线时仍应用此规则

备注: (可选)

添加到指定位置: (可选)

状态: 启用

图 7-37 策略路由设置界面

规则名称	用户自定义，标识一条选路规则。只能输入英文、数字和下划线。
服务类型	在下拉列表中选择本条规则所针对的服务类型，不属于指定范围内的协议将不会应用选路规则。如果列表中没有您想指定的协议类型，可以在对象管理 >> 服务类型界面设置，详细配置过程请参考 5.4 服务类型小节。
源地址	在下拉列表中选择需要应用选路规则的源地址范围。源地址可以在对象管理 >> 地址管理 >> 地址界面设置。详细配置过程请参考 5.1 地址管理小节。
目的地址	在下拉列表中选择需要应用选路规则的目的地址范围。源地址可以在对象管理 >> 地址管理 >> 地址界面设置。详细配置过程请参考 5.1 地址管理小节。
生效接口	选择指定数据包转发接口。
生效时间	选择规则生效的时间。生效时间可以在对象管理 >> 时间管理界面进行设置。详细配置过程请参考 5.2 时间管理小节。
强制	勾选该条目，接口不在线时仍应用此规则
备注	添加对本条规则的说明信息。
添加到指定位置	输入本条规则在规则列表中的序号以设定该规则的优先级，序号越小表示优先级越高。若留空则系统将按照规则设定的先后顺序对规则进行依次排序。

状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。
----	---

表 7.10 策略路由功能设置界面项说明

新增的条目会在规则列表里显示出来，如下图所示。

<input type="checkbox"/>	序号	规则名称	服务类型	源地址	目的地址	生效接口	生效时间	状态	设置
<input type="checkbox"/>	1	test_1	ALL	IPGROUP_ANY	IPGROUP_ANY	eth1	Any	已启用	

图 7-38 策略路由设置界面-规则列表

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

■ 策略路由典型应用

某企业的网络需求如下：

TL-ER6225G工业级为中心路由器，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-ER6225G 工业级路由器：

- 1) 创建 Ethernet 接口 eth1 和 eth2。注意设置网络参数时必须勾选参与流量均衡选项。
- 2) 在传输控制 >> 路由设置 >> 策略路由界面创建如下两条规则：
- 3) 指定 FTP 数据包由“eth1”接口转发。

<input type="checkbox"/>	序号	规则名称	服务类型	源地址	目的地址	生效接口	生效时间	强制	备注	状态	设置
--	--	--	--	--	--	--	--	--	--	--	--

规则名称:

服务类型:

源地址:

目的地址:

生效接口:

生效时间:

强制: 接口不在线时仍应用此规则

备注: (可选)

添加到指定位置: (可选)

状态: 启用

指定 HTTP 数据包由“eth2”接口转发。

□	序号	规则名称	服务类型	源地址	目的地址	生效接口	生效时间	强制	备注	状态	设置
--	--	--	--	--	--	--	--	--	--	--	--

规则名称:

服务类型:

源地址:

目的地址:

生效接口:

生效时间:

强制: 接口不在线时仍应用此规则

备注: (可选)

添加到指定位置: (可选)

状态: 启用

7.5.2 静态路由

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

■ 配置静态路由

进入界面：传输控制 >> 路由设置 >> 静态路由

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

□	序号	规则名称	目的地址	子网掩码	下一跳	出接口	Metric	可达性	状态	设置
--	--	--	--	--	--	--	--	--	--	--

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, 1-50个字符)

启用/禁用规则: 启用

图 7-39 静态路由界面-设置静态路由

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

表 7.11 静态路由界面条目项说明

新增的静态路由条目会在规则列表中显示出来，如下图所示。

<input type="checkbox"/>	序号	名称	目的地址	子网掩码	下一跳	出接口	Metric	可达性	状态	设置
<input type="checkbox"/>	1	rule1	192.168.3.0	255.255.255.0	192.168.1.2	eth1	0	可达	已启用 	 

图 7-40 静态路由界面-规则列表

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

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

■ 应用环境

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

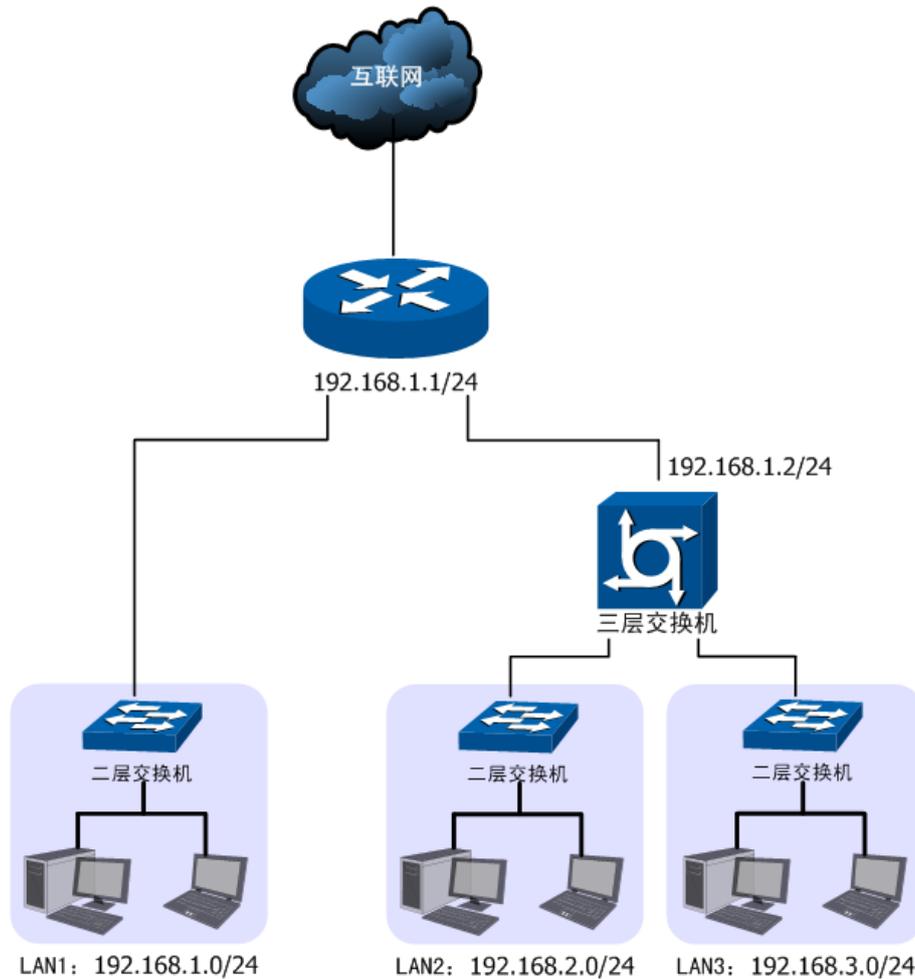


图 7-41 静态路由功能组网应用

配置步骤：

TL-ER6225G 工业级路由器要完成上述网络需求，需要配置静态路由功能，配置步骤如下：

- 1) 创建转发数据包的接口 eth0。创建界面：基本设置 >> 接口设置 >> 接口设置。eth0 具体设置请根据实际需求进行。
- 2) 创建静态路由规则，设置到 LAN2 网段的下一跳地址为三层交换机的级联口 IP 地址 192.168.1.2。创建界面：传输控制 >> 路由设置 >> 静态路由。规则设置如下，点击 <确定>按钮完成。

名称	rule1
目的地址	192.168.2.0
子网掩码	255.255.255.0
下一跳	192.168.1.2

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

表 7.12 创建静态路由-LAN2 网段条目项说明

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

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

表 7.13 创建静态路由-LAN3 网段条目项说明

7.5.3 系统路由

进入界面：传输控制 >> 路由设置 >> 系统路由

系统路由下显示了路由器建立的所有路由规则条目，如下图所示。

条目数量: 6

 刷新

序号	目的地址	子网掩码	下一跳	出接口	Metric
1	192.168.3.0	255.255.255.0	192.168.1.2	eth1	0
2	192.168.2.0	255.255.255.0	192.168.1.100	eth1	1
3	172.28.74.0	255.255.255.0	0.0.0.0	GE2	0
4	192.168.0.0	255.255.255.0	0.0.0.0	eth2	0
5	192.168.1.0	255.255.255.0	0.0.0.0	GE5	0
6	192.168.1.0	255.255.255.0	0.0.0.0	eth1	0

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

表 7.14 路由规则条目列表

第8章 安全管理

8.1 ARP 防护

8.1.1 ARP 简介

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

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

■ ARP报文格式

ARP报文的格式如下图所示：



图 8-1 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 8.1 ARP 报文字段含义

■ ARP解析过程

在一次 ARP 通信中，源主机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：

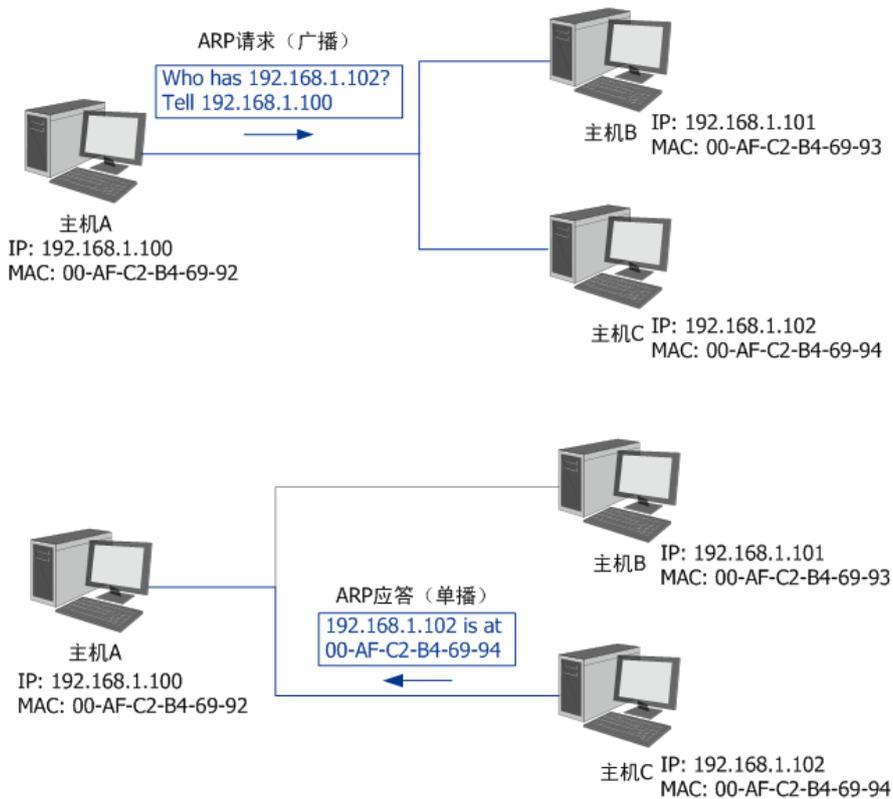


图 8-2 ARP 解析过程

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。

8.1.2 ARP 攻击简介

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

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

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

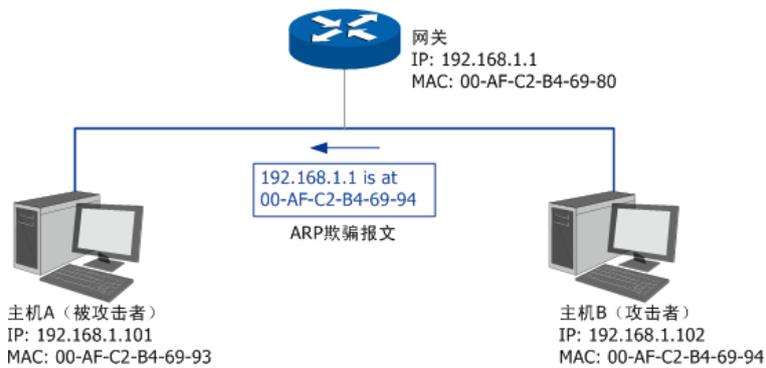


图 8-3 ARP欺骗-欺骗主机

- 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。

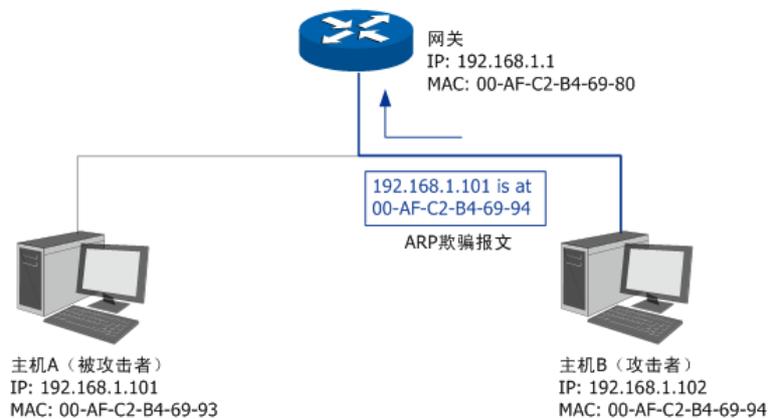


图 8-4 ARP欺骗-欺骗网关

- 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。

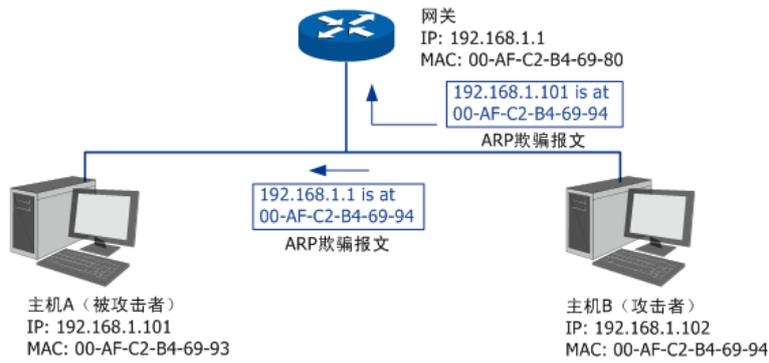


图 8-5 ARP欺骗-双向欺骗

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。

8.1.3 IP MAC 绑定

■ 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。

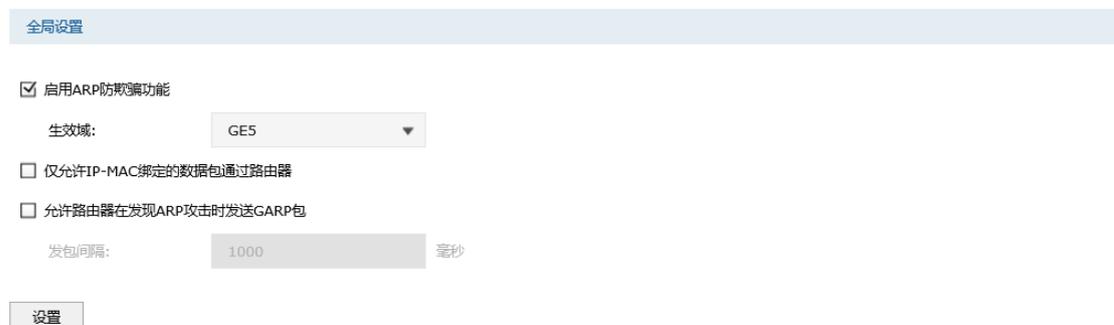


图 8-6 IP-MAC 绑定界面-功能设置

启用 ARP 防欺骗功能	全局功能开关。在开启此项之后，所有的 ARP 防护设置才会生效。开启该功能后，选择生效接口域。
仅允许 IP-MAC 绑定的数据包通过路由器	强制局域网内主机进行 IP-MAC 绑定，没有绑定的主机将无法访问网络。推荐在需要防止非法客户端接入时勾选，勾选条目前请确认已绑定包含管理主机在内的指定主机的 IP-MAC 地址信息。 注意：要开启该功能，需要先开启 ARP 防欺骗功能

允许路由器在发现 ARP 攻击时发送 GARP 包	<p>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。</p> <p>注意：要开启该功能，需要先开启 ARP 防欺骗功能</p>
---------------------------	---

表 8.2 ARP 功能设置界面项说明

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

■ 导入到静态地址分配列表

在 IP-MAC 绑定规则列表中选择条目，并在导入到静态地址分配列表区域点击<导入>，可将条目导入到静态地址分配列表中。

■ 绑定局域网内主机的IP与MAC地址信息

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

导入到静态地址分配列表

导入

IP-MAC绑定规则列表

+ 新增 - 删除

<input type="checkbox"/>	序号	IP地址	MAC地址	生效域	备注	状态	设置
<input type="checkbox"/>	1	192.168.1.55	AA-BB-CC-DD-EE-FF	GE1	---	已启用 -	



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。

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

IP-MAC绑定规则列表

+ 新增 - 删除

<input type="checkbox"/>	序号	IP地址	MAC地址	生效域	备注	状态	设置
--	--	--	--	--	--	--	--

IP地址:

MAC地址: (MAC地址格式:XX-XX-XX-XX-XX-XX)

生效域: ▼

备注: (可选,0-50个字符)

状态: 启用

图 8-7 IP MAC 绑定界面-IP-MAC 绑定

IP 地址	输入一个 IPv4 地址。
MAC 地址	输入与上方 IP 地址正确对应的主机 MAC 地址。
生效域	选择绑定的接口。
备注	添加对本条目的说明信息，非必填项。
状态	选择“启用”，则使该绑定条目生效； 选择“禁用”，则使该绑定条目失效。

表 8.3 IP-MAC 绑定界面条目项说明

新增的条目会在绑定列表中显示出来。此时，以图 8-7中的配置为例，MAC地址为40-61-86-FC-75-C4的主机如果擅自修改了IP地址，便会无法访问网络；反之亦然。

IP-MAC绑定规则列表

+ 新增 - 删除

<input type="checkbox"/>	序号	IP地址	MAC地址	生效域	备注	状态	设置
<input type="checkbox"/>	1	192.168.1.109	40-61-12-34-01-35	eht1	---	已启用	

图 8-8 IP-MAC 绑定界面-绑定列表

8.1.4 ARP 扫描

进入界面：安全管理 >> ARP 防护 >> ARP 扫描

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



图 8-9 ARP 扫描界面

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

如需将扫描结果进行绑定，请选择条目，然后点击导入到 IP-MAC 绑定区域的<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效，这些批量绑定的条目会出现在 IP-MAC 绑定界面的 IP-MAC 绑定规则列表中。

8.1.5 ARP 列表

进入界面：安全管理 >> 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。



图 8-10 ARP 列表界面

列表中未绑定的条目并不是一直存在，除了会被新的 IP-MAC 对应信息更替之外，还会由于长时间未通信或物理连接中断而自动从列表中删除。

如需将列表中的条目绑定，请选择条目，然后点击导入到 IP-MAC 绑定区域的<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效，列表中的条目状态也会随之变更。

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

8.2 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

防Flood类攻击

<input type="checkbox"/> 启用防多连接的TCP SYN Flood攻击	10000	Pkt/s
<input type="checkbox"/> 启用防多连接的UDP Flood攻击	12000	Pkt/s
<input type="checkbox"/> 启用防多连接的ICMP Flood攻击	1500	Pkt/s
<input type="checkbox"/> 启用防固定源的TCP SYN Flood攻击	4000	Pkt/s
<input type="checkbox"/> 启用防固定源的UDP Flood攻击	6000	Pkt/s
<input type="checkbox"/> 启用防固定源的ICMP Flood攻击	600	Pkt/s

防可疑包攻击

- 启用防碎片包攻击
- 启用防TCP Scan(Streach FIN/Xmas/Null)
- 启用防ping of Death
- 启用防Large ICMP
- 启用防WinNuke攻击
- 启用防TearDrop攻击
- 启用防LAND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
- 阻止带选项的包
 - 安全限制 宽松选路
 - 严格选路 记录路径
 - 严格选路 记录路径
 - 流标记 时间戳
 - 空标记

网络扫描防护

- 启用IP地址扫描防护
- 启用端口扫描防护

设置

图 8-11 攻击防护设置界面

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。
网络扫描防护	开启IP地址扫描防护和端口扫描防护，需设置最大扫描速率和黑名单老化时间。当发现某台主机的地址或端口扫描行为的速率超过了最大扫描速率，系统将其判断为攻击者，并将其加入黑名单。加入黑名单的表项在超过黑名单老化时间后自动从黑名单中删除。

表 8.4 攻击防护设置界面条目说明

8.3 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：安全管理 >> MAC 过滤>> MAC 过滤

全局设置

启用MAC地址过滤功能

仅允许规则列表内的MAC地址访问外网

仅禁止规则列表内的MAC地址访问外网

生效接口: GE5

设置

MAC过滤规则列表

+ 新增 - 删除

□	序号	规则名称	MAC地址	设置
--	--	--	--	--

图 8-12 MAC过滤设置界面

全局设置

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

MAC 过滤规则设置

点击 <  新增 > ，配置 MAC 过滤规则。

MAC过滤规则列表

 新增  删除

<input type="checkbox"/>	序号	规则名称	MAC地址	设置
<input type="checkbox"/>	--	--	--	--

规则名称: (1-50字符)

MAC地址:

MAC 地址过滤规则

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

表 8.5 MAC 过滤设置界面项说明

8.4 访问控制

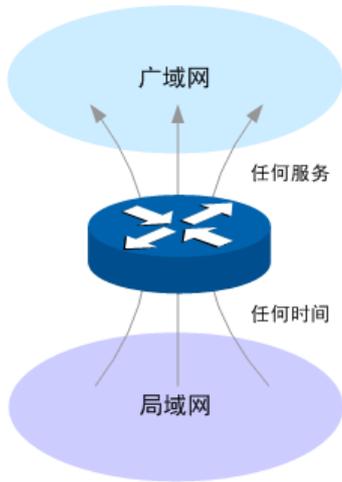
8.4.1 基本概念

在创建访问控制策略时，需要引用路由器对象管理中的以下模块：

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

本路由器提供允许和阻塞两种行为控制信息流，其连同服务类型、源地址、目的地址、时间以及区段，构成了访问策略所必需的几个元素。通过创建策略，定义允许或阻塞在预定时间通过指定源地址到达指定目的地址的信息流的种类，可以控制区段间的信息流。控制范围最大时，可以阻塞所有类型的信息流从一个接口中的任何源地址到其它所有接口中的任何目的地址，而且没有任何预定时间限制。控制范围最小时，可以创建一个策略，只允许一种信息流在预定的时间段内、在一个接口下的指定主机与另一接口下的指定主机之间流动。可以参考图 8-13 理解。

广义的互联网访问：
任何服务可在任何时间，从任何局域网接口到任何广域网接口



狭义的互联网访问：
SMTP服务在指定时间从局域网接口中的邮件服务器到广域网接口中的邮件服务器

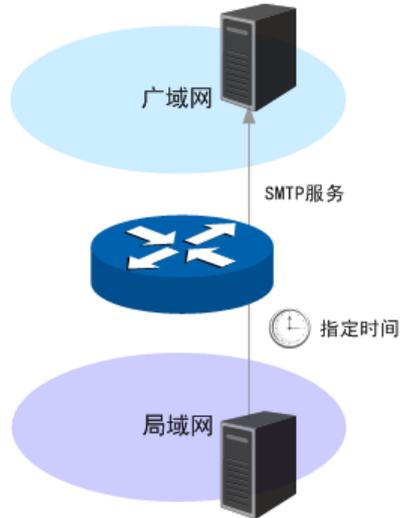


图 8-13 策略生效范围示意图

8.4.2 配置访问规则

进入界面：安全管理 >> 访问控制 >> 访问控制

点击 < 新增，配置访问规则。

□	序号	规则名称	源地址范围	目的地址范围	策略类型	服务类型	生效接口域	生效时间	设置
--	--	--	--	--	--	--	--	--	--

规则名称: (1-50个字符)

策略类型:

服务类型:

生效接口域:

源地址范围:

目的地址范围:

生效时间:

添加到指定位置(第几条): (可选)

图 8-14 访问规则设置界面

规则名称	输入一个名称来标识该访问规则。
策略类型	在下拉列表中选择适用于本条规则的策略类型，可选择阻塞或者允许。 选择“阻塞”，则符合该条规则的所有数据包将无法通过路由器； 选择“允许”，则符合该条规则的数据包能通过路由器。

服务类型	在下拉列表中选择本条规则所针对的服务类型，不属于指定范围内的服务将不会应用该规则。例如策略类型选择为“阻塞”，只选定了FTP一种服务类型时，其他服务类型的数据包仍旧可以通过路由器。如需新建服务类型，请参考5.4服务。
生效接口	在下拉列表中选择本条规则生效的接口。
源地址范围	在下拉列表中选择本条规则限制的源地址范围。源地址必须是所选接口下的地址。路由器预定义“IPGROUP_ANY”地址组表示所有地址。如需新建地址组，请参考5.1地址管理。
目的地址范围	在下拉列表中选择本条规则限制的目的地地址范围。目的地址可以是任意接口下的任意地址。路由器预定义“IPGROUP_ANY”地址组表示所有地址。如需新建地址组，请参考5.1地址管理。
规则生效时间	在下拉列表中选择本条规则生效的时间表。如需新建时间表，请参考5.2时间管理。
添加到指定位置（第几条）	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

表 8.6 访问规则设置界面条目项说明



说明：

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

新增规则信息会在规则列表中显示出来。图 8-15 中规则效果是：任何时间，接口 2 内的主机都不能通过路由器与其他接口进行通信。

规则列表									
<input type="checkbox"/>	序号	名称	源地址范围	目的地址范围	策略类型	服务类型	生效接口	生效时间	设置
<input type="checkbox"/>	1	规则1	IPGROUP_ANY	IPGROUP_ANY	阻塞	ALL	GE2	Any	

图 8-15 区段内访问规则设置界面-规则列表

配置访问规则步骤：

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

- 2) 创建地址组。非必须操作。路由器已预定义部分地址组，如果需要限制的地址组为预定义的，则不必此项操作。具体操作步骤请参考5.1地址管理。
- 3) 创建时间组。非必须操作。路由器已预定义“Any”时间组，表示任何时间，如果需要限制的时间为此，则不必此项操作。具体操作步骤请参考5.2时间管理。
- 4) 创建访问规则。必须操作。创建界面：安全管理 >> 访问控制 >> 访问控制，点击 <  新增 >，设置规则名称，选择所需的策略类型、服务类型、接口、源地址范围、目的地址范围、规则生效时间，然后指定规则的优先级，点击<确定>按钮完成配置。
- 5) 编辑访问规则。非必须操作。编辑界面：安全管理 >> 访问控制 >> 访问控制，在此界面的规则列表区域，可以查看、编辑和删除策略。

8.4.3 访问控制应用

■ 控制到路由器本身的报文

应用一：

创建策略，使GE2中的主机不能以任何形式访问路由器。

配置步骤：

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

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

表 8.7 访问控制应用一创建规则

应用二：

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

配置步骤：

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

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

表 8.8 访问控制应用二创建规则

■ 控制某接口到某个地址组的报文

应用三：

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

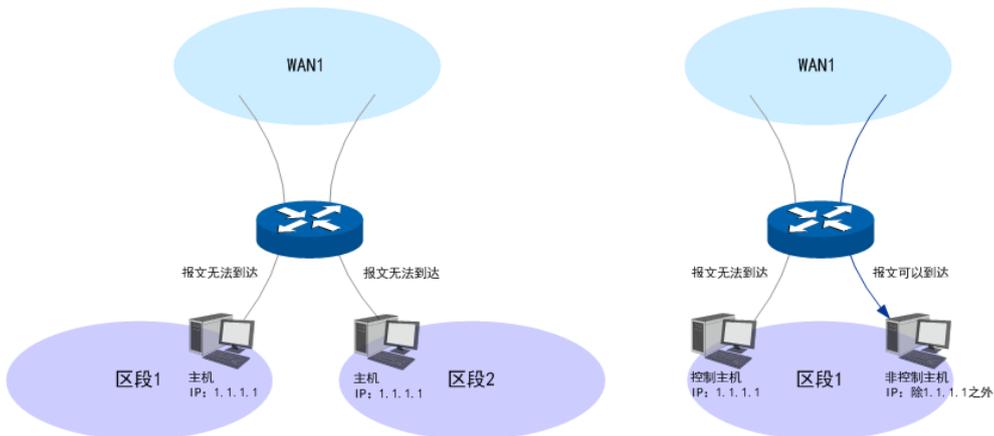


图 8-16 应用三

配置步骤：

- 1) 创建地址组。创建界面：对象管理 >> 地址管理。

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

名称	Host
----	------

表 8.9 访问控制应用三设置地址组

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

名称	HostIP
IP类型	IP/Mask 1.1.1.1/32

表 8.10访问控制应用三设置地址

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

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

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

表 8.11区段内策略应用三设置区段内访问规则

应用四：

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

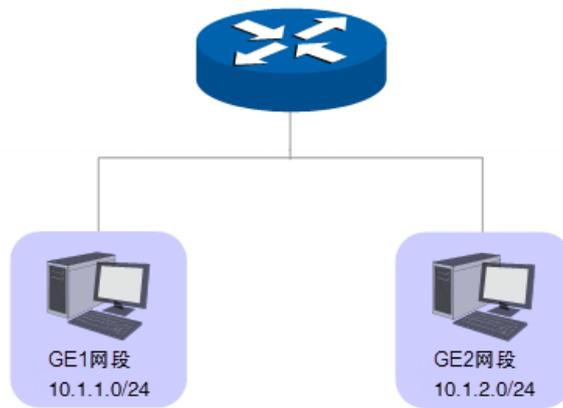


图 8-17 应用四

配置步骤：

1) 创建地址组。创建界面：对象管理 >> 地址管理。

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

GE1网段设置如下：

名称	GE1_Segment
----	-------------

表 8.12访问控制应用四设置地址组1

GE2网段设置如下：

名称	GE2_Segment
----	-------------

表 8.13访问控制应用四设置地址组2

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

GE1网段IP设置如下：

名称	GE1_Segment_IP
IP类型	IP/Mask 10.1.1.0/24

表 8.14访问控制应用四设置地址1

GE2网段IP设置如下：

名称	GE2_Segment_IP
IP类型	IP/Mask 10.1.2.0/24

表 8.15 访问控制应用四设置地址 2

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

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

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

名称	GE1_Policy1
策略类型	阻塞
服务类型	ALL
生效接口	GE1
源地址范围	GE1_Segment
目的地址范围	GE2_Segment
规则生效时间	Any

表 8.16访问控制应用四设置访问规则

第9章 行为管控

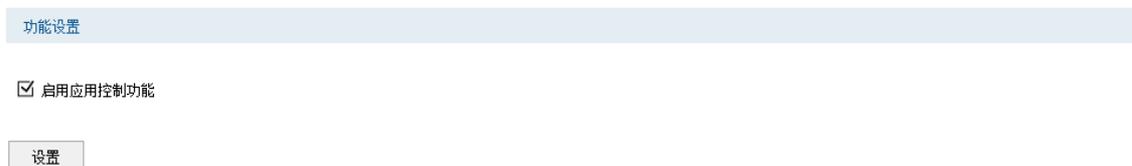
9.1 应用控制

应用控制包括各类软件应用控制功能和 QQ 黑白名单功能。

9.1.1 应用控制

进入界面：行为管控 >> 应用控制 >> 应用控制

启用应用控制规则功能，点击<设置>保存配置。



点击<+ 新增>，设置应用控制规则。点击<确定>保存配置。



图 9-1 应用控制设置界面

应用控制设置

用户组	在下拉菜单中选择所需限制的组。如需新建组，请参考 5.1 地址管理。
-----	------------------------------------

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

表 9.1 应用限制设置界面项说明

9.1.2 QQ 黑白名单

可以在此对指定的 QQ 号码进行相关规则设置。

进入界面：行为管控 >> 应用控制 >> QQ 黑白名单

勾选<启用 QQ 黑白名单>，点击<设置>保存配置。



点击<+ 新增>，设置 QQ 黑白名单规则。点击<确定>保存配置。

<input type="checkbox"/>	序号	用户组	规则类型	生效时间	备注	状态	设置
<input type="checkbox"/>	--	--	--	--	--	--	--

受控地址组:

规则类型: 白名单：允许下列QQ号码登录 黑名单：禁止下列QQ号码登录

QQ号码: 多个QQ号码以换行或者逗号隔开

当使用上述QQ号码时: 记录到系统日志

生效时间:

备注: (可选)

状态: 启用 禁用

添加到指定位置: (可选,指定位置从0开始)

图 9-2 QQ 黑白名单管理界面

QQ 黑白名单规则设置

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

表 9.2 QQ 黑白名单规则设置界面项说明

9.2 网址过滤

9.2.1 网站分组

可以在此对网站进行分组。

进入界面：行为管控 >> 网址过滤 >> 网站分组

网站分组列表					
<input type="checkbox"/>	序号	组名称	组成员	备注	设置
<input type="checkbox"/>	1	视频	*.56.com 更多	---	
<input type="checkbox"/>	2	游戏	*.17173.com 更多	---	
<input type="checkbox"/>	3	财经	*.10jqka.com.cn 更多	---	
<input type="checkbox"/>	4	社交	*.51.com 更多	---	
<input type="checkbox"/>	5	购物	*.360buy.com 更多	---	
<input type="checkbox"/>	6	生活	*.100ye.com 更多	---	
<input type="checkbox"/>	7	音乐	*.1ting.com 更多	---	
<input type="checkbox"/>	8	娱乐	*.67.com 更多	---	
<input type="checkbox"/>	9	论坛	*.daqi.com 更多	---	
<input type="checkbox"/>	10	邮箱	*.eyou.com 更多	---	
<input type="checkbox"/>	11	小说	*.2100book.com 更多	---	
<input type="checkbox"/>	12	体育	*.1soccer.com 更多	---	
<input type="checkbox"/>	13	新闻	*.cankao.com 更多	---	

图 9-3 网站分组列表

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

网站分组列表					
<input type="checkbox"/>	序号	组名称	组成员	备注	设置
--	--	--	--	--	--
<div style="text-align: right;"> 新增 删除 </div> <div style="border: 1px solid #ccc; padding: 10px;"> <p>组名称: <input type="text" value=""/> (1-28个字符)</p> <p>组成员: <input type="text" value=""/></p> <p><input type="button" value="清空"/> 请使用换行或者分号来分隔网址</p> <p>文件路径: <input type="text" value=""/> <input type="button" value="浏览"/> (可选, 文件格式为txt)</p> <p><input type="button" value="导入"/> 您还可以通过导入文件来配置组成员</p> <p>备注: <input type="text" value=""/> (可选)</p> <p><input type="button" value="确定"/> <input type="button" value="取消"/></p> </div>					

图 9-4 网站分组列表界面

网站分组列表设置

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

表 9.3 网站分组界面

9.2.2 网站过滤

在此可对特定的网站进行过滤。

进入界面：行为管控 >> 网址过滤 >> 网站过滤

启用网站过滤功能，点击<设置>保存配置。



图 9-5 网站过滤功能设置界面

点击<+ 新增>，配置网站过滤规则。点击<确定>保存配置。

<input type="checkbox"/>	序号	用户组	策略	网站过滤列表	生效时间	状态	备注	设置
<input type="checkbox"/>	--	--	--	--	--	--	--	--

用户组:

规则类型: 允许访问 禁止访问

选择网站:

访问上述网站时: 记录到系统日志

规则生效时间:

备注: (可选)

添加到指定位置(第几条): (可选)

状态: 启用

图 9-6 网站过滤规则设置界面

用户组	在下拉菜单中选择所需限制的组。如需新建组，请参考 5.1 地址管理。
规则类型	选择规则类型。 允许访问：允许访问下列网站。 禁止访问：禁止访问下列网站。
选择网站	可以选择“所有网站”，使规则对任意网站生效；也可以对已有的网站分组进行勾选。如需新建组，请参考网站分组。
访问上诉网站时	勾选后，访问上述网站的日志将保存到系统中
规则生效时间	指定规则生效时间。如需新建时间对象，请参考 5.2 时间管理。
备注	添加对本条规则的说明信息。
添加到指定位置(第几条)	可以将当前设置的条目添加到规则列表中指定序号的位置。
状态	选择是否启用该条规则。

表 9.4 网站过滤规则设置界面条目项说明

9.2.3 URL 过滤

在此可以配置对 URL 进行过滤的规则。

进入界面：行为管控 >> 网址过滤 >> URL过滤

启用 URL 过滤功能，点击<设置>保存配置。



图 9-7 URL 过滤全局设置界面

点击<+ 新增>，配置 URL 过滤规则。点击<确定>保存配置。

<input type="checkbox"/>	序号	用户组	策略类型	过滤方式	过滤内容列表	生效时间	状态	备注	设置
--	--	--	--	--	--	--	--	--	--

用户组:

策略类型: 允许访问下列的URL 禁止访问下列的URL

过滤方式: 关键字 完整URL

过滤内容列表:
 多个过滤内容以换行或者分号隔开

访问上述网站时: 记录到系统日志

规则生效时间:

状态: 启用

备注: (可选, 1-50个字符)

添加到指定位置(第几条): (可选)

图 9-8 URL 过滤规则列表界面

用户组	在下拉菜单中选择所需限制的组。如需新建组，请参考 5.1 地址管理。
策略类型	选择策略类型。可以选择允许访问下列的 URL 或禁止访问下列的 URL。
过滤方式	选择一种过滤方式。“关键字”过滤即所有包含指定字符的 URL 地址全都进行过滤；“完整 URL”过滤则仅当 URL 地址完全匹配输入的完整 URL 地址时才能进行过滤。 可以同时输入多个关键字或完整 URL 进行批量添加，通过使用空格、逗号或者回车换行来表示不同的关键字或完整 URL。最多可以添加 10 个关键字或完整 URL，每一个关键字或完整 URL 的可输入长度为 1-64 个字符，但输入的总字符数不能超过 300 个（包括相邻两条关键字或 URL 地址之间的分隔符）。
过滤内容列表	输入过滤内容，不同内容条目之间用换行或者分号隔开。
规则生效时间	指定规则生效时间。如需新建时间对象，请参考 5.2 时间管理。

状态	选择是否启用该条规则。
备注	添加对本规则的说明信息。
添加到指定位置 (第几条)	可以将当前设置的条目添加到规则列表中指定序号的位置。

表 9.5 URL 过滤规则列表界面条目项说明

9.3 网页安全

进入界面：行为管控 >> 网页安全 >> 网页安全

启用网页安全功能，点击<设置>保存配置。

功能设置

启用网页安全功能

设置

点击<+ 新增>，配置网页安全规则。点击<确定>保存配置。

□	序号	用户组	文件名后缀	生效时间	备注	状态	设置
--	--	--	--	--	--	--	--

用户组: ---

禁止网页提交: 启用

过滤文件扩展类型: 请使用换行或者分号来隔开文件名后缀

生效时间: Any

备注: (可选)

状态: 启用

确定
取消

图 9-9 网页安全界面

用户组	在下拉菜单中选择所需限制的组。如需新建组，请参考 5.1 地址管理。
禁止网页提交	勾选“启用”，可以禁止所有的 HTTP POST 提交。

过滤文件扩展类型	可以在过滤文件扩展类型编辑框内输入多个扩展名，并以空格、逗号或者回车换行来分隔。
生效时间	指定规则生效时间。如需新建时间对象，请参考 5.2 时间管理。
备注	添加对本规则的说明信息。
状态	选择是否启用该条规则。

表 9.6 网页安全界面条目项说明

9.4 行为审计

可以在此启用对用户的上网行为分析，记录和审计用户上网行为。

进入界面：行为管控 >> 行为审计 >>行为审计

启用上传用户上网行为分析功能，输入行为审计服务器地址，点击<设置>保存配置。

上网行为分析

上传用户上网行为: 启用

行为审计服务器地址:

9.5 策略库升级

可以在此进行应用特征数据库的升级。

进入界面：行为管控 >> 策略库升级 >> 策略库升级

应用特征数据库升级

当前数据库版本: 1.0.0

数据库路径:

图 9-10 数据库界面

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

第10章 VPN

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

VPN 通过隧道技术在两个站点间建立一条虚拟的专用线路，使用端到端的认证和加密保证数据的安全性。隧道技术指数据封装、传输、解封的全过程。VPN 典型拓扑如下图所示。

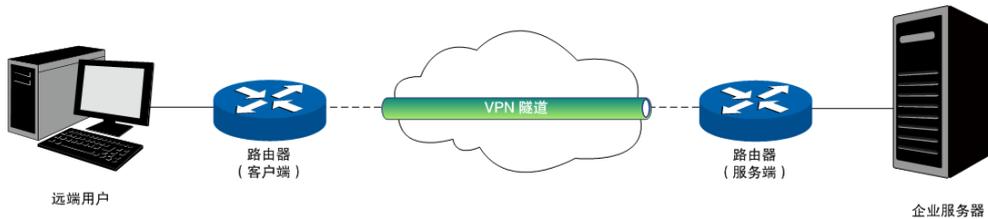


图 10-1 VPN 典型拓扑

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

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

- 二层隧道协议：PPTP、L2TP。

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

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

- 1) PPTP 只能在 IP 网络上使用；L2TP 只要求隧道媒介提供面向数据包的点对点的连接，可在 IP、ATM、帧中继等网络上使用。
- 2) PPTP 只能在两端点间建立单一隧道；L2TP 可在两端点间针对不同的服务质量建立多条隧道。
- 3) PPTP 不支持隧道验证；L2TP 可提供隧道验证，但当 L2TP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，不需要在第 2 层协议上验证隧道。

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

- 三层隧道协议：IPSec。

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

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

10.1 IPSec

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

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

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

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

10.1.1 IPSec 安全策略

进入界面：VPN >> IPSec >> IPSec 安全策略

IPSec安全策略列表

+ 新增 - 删除

□	序号	策略名称	对端网关	本地子网范围	对端子网范围	状态	设置
--	--	--	--	--	--	--	--

点击+ **新增**，进行 IPSec 基本设置。

策略名称: (1-32个字符)

对端网关: (IP地址或域名)

绑定接口: ▼

本地子网范围: /

对端子网范围: /

预共享密钥: (1-128个字符)

状态: 启用

高级设置

图 10-2 IPSec 安全策略基本设置界面

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

表 10.1 IPSec 安全策略基本设置界面项说明

点击+ **高级设置**，进行 IPSec 高级设置。

阶段1设置

安全提议:	md5-3des-dh2	▼
安全提议:	---	▼
安全提议:	---	▼
安全提议:	---	▼
交换模式:	<input checked="" type="radio"/> 主模式	<input type="radio"/> 野蛮模式
协商模式:	<input checked="" type="radio"/> 初始者模式	<input type="radio"/> 响应者模式
本地ID类型:	<input checked="" type="radio"/> IP地址	<input type="radio"/> NAME
本地ID:	<input type="text"/>	(1-28个非空字符)
对端ID类型:	<input checked="" type="radio"/> IP地址	<input type="radio"/> NAME
对端ID:	<input type="text"/>	(1-28个非空字符)
生存时间:	28800	秒(60-604800)
DPD检测开启:	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
DPD检测周期:	10	秒(1-300)

图 10-3 IPsec 安全策略基本设置界面

阶段 1 设置

安全提议	指定相应的 IKE 安全提议，最多可选择四个安全提议。
交换模式	设置 IKE 协商第一阶段的交换模式，该交换模式必须与对端相同。交换模式有以下两种： 主模式：该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。 野蛮模式：该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。

协商模式	<p>设置 IKE 协商的模式，该协商模式可以与对端不同。协商模式有以下两种：</p> <p>初始者模式：配置该模式后，IKE 才能主动发起协商。本地和对端至少有一方必须设置为初始者模式。</p> <p>响应者模式：配置该模式后，IKE 不会主动发起协商，需要等待对端发起协商。本地和对端不能同时为响应者模式。</p>
本地/对端 ID 类型	<p>设置本地和对端的 ID (Identity，身份标识) 类型，用于进行 ID 的交换与认证，可以选择 “IP 地址” 或 “NAME”，通信双方的设置需保持一致。</p>
本地/对端 ID	<p>ID 类型选择 “IP 地址” 时，无需进行设置；ID 类型选择 “NAME” 时，可自定义本地/对端的 ID (任意英文字母和数字的组合)。本地路由器的 “本地 ID” 需与对端路由器的 “对端 ID” 保持一致，而 “对端 ID” 则需与对端路由器的 “本地 ID” 保持一致。</p>
生存时间	<p>设定 IKE SA 的生存时间，单位为秒。</p>
DPD 检测开启	<p>DPD (Dead Peer Detect，对端存活检测) 开启后，IKE 一端能够周期性主动检测对端的链路连接状态。</p>

表 10.2 IPsec 安全策略高级设置界面项说明

阶段2设置

封装模式: 隧道模式 传输模式

安全提议: esp-md5-3des ▼

安全提议: --- ▼

安全提议: --- ▼

安全提议: --- ▼

PFS: none ▼

生存时间: 28800 秒(120-604800)

确定
取消

阶段 2 设置

封装模式	<p>设置隧道中数据报文的封装模式，该封装模式必须与对端相同。封装模式有以下两种：</p> <p>隧道模式：在该模式下，AH 或 ESP 插在原始 IP 报文头之前，另外生成一个新的 IP 报文头放到 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：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的加密传输。</p>
安全提议	指定相应的 IPSec 安全提议，最多可选择四个安全提议。
PFS	选择是否启用 PFS (Perfect Forward Secrecy，完全前向保密)，通信双方的 PFS 设置需保持一致。
生存时间	设定 IPSec SA 的生存时间，单位为秒。

表 10.3 IPSec 安全策略基本设置界面项说明



说明：

- 子网掩码值的相关设置请参考附录 A 常见问题中的问题 4。

10.1.2 IPSec 安全联盟

在此将列出路由器上所有已成功建立的 IPSec 安全联盟相关信息。

进入界面：VPN >> IPSec >> IPSec 安全联盟

IPSec安全联盟列表											
条目数量: 0 刷新											
<input type="checkbox"/>	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 10-4 IPSec 安全联盟界面

在图 10-4 中路由器使用 eth2 接口进行隧道连接，eth2 接口的 IP 地址为 192.168.10.100，对端网关地址为 172.29.85.199。IPSec 隧道的安全提议等相关设置需与对端路由设置相同。

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

条目数量: 0

 刷新

<input type="checkbox"/>	序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
--	1	IPsec_2	781159572	in	172.29.85.199 <- 192.168.10.100	192.168.0.0/24:0 <- 192.168.1.0/24:0,any	ESP	--	MD5	3DES
--	2	IPsec_2	3374359119	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 L2TP

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

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

10.2.1 L2TP 服务器设置

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

进入界面 : VPN >>L2TP >> L2TP 服务器

全局设置

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)

服务器设置

+ 新增 - 删除

<input type="checkbox"/>	序号	服务接口	IPSec加密	状态	设置
--	--	--	--	--	--

图 10-5 L2TP 服务器设置界面

全局设置

L2TP 隧道维护时间间隔	设置 L2TP 隧道维护的时间间隔 , 范围是 60 秒至 1000 秒。设置此时间间隔 , 服务器按照设定间隔发出报文 , 用以确定 L2TP 隧道的连接状态。如无特别要求 , 请保持默认设置。
---------------	--

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

表 10.4 L2TP 服务器设置-全局管理设置界面项说明

点击 <  新增 >，进行隧道设置。

服务器设置
+ 新增 - 删除

<input type="checkbox"/>	序号	服务接口	IPSec加密	状态	设置
--	--	--	--	--	--

服务接口:

IPSec加密:

预共享密钥:

状态: 启用

图 10-6 L2TP 服务器列表

隧道设置

服务接口	绑定接口为服务器端路由器 WAN 端口上出链路口。如有多条上网链路，请根据实际情况，选择其中一条链路承载 L2TP VPN 隧道。此接口的 IP 地址即为 L2TP 服务器的 IP 地址。
IPSec 加密	选择是否使用 IPSec 对 L2TP 隧道加密。可选项有：加密，不加密，可选加密。
预共享密钥	设置 IPSec 加密时通信双方互相认证的密钥，双方必须使用同一个预共享密钥。
状态	选择启用或禁用本 L2TP 隧道。

表 10.5 PPTP 服务器设置-隧道设置界面项说明

10.2.2 L2TP 客户端设置

进入界面：VPN >> L2TP >> L2TP 客户端

全局设置

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)

客户端设置

+ 新增 - 删除

□	序号	隧道名称	用户名	出接口	服务器地址	IPSec加密	对端子网	工作模式	状态	设置
--	--	--	--	--	--	--	--	--	--	--

图 10-7 L2TP服务器设置界面

全局设置

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

表 10.6 L2TP 服务器设置-全局管理设置界面项说明

点击 < + 新增 >，进行隧道设置。

□	序号	隧道名称	用户名	出接口	服务器地址	IPSec加密	对端子网	工作模式	状态	设置
--	--	--	--	--	--	--	--	--	--	--
<div style="display: flex; flex-direction: column;"> <div style="margin-bottom: 5px;">隧道名称: <input style="width: 150px;" type="text"/> (1-12个字符)</div> <div style="margin-bottom: 5px;">用户名: <input style="width: 150px;" type="text"/></div> <div style="margin-bottom: 5px;">密码: <input style="width: 150px;" type="password"/> <div style="display: flex; justify-content: space-between; width: 150px; margin-top: 2px;"> 低 中 高 </div> </div> <div style="margin-bottom: 5px;">出接口: <input style="width: 150px;" type="text"/></div> <div style="margin-bottom: 5px;">服务器地址: <input style="width: 150px;" type="text"/></div> <div style="margin-bottom: 5px;">IPSec加密: <input style="width: 150px;" type="text"/></div> <div style="margin-bottom: 5px;">预共享密钥: <input style="width: 150px;" type="text"/> (1-128个字符)</div> <div style="margin-bottom: 5px;">对端子网: <input style="width: 150px;" type="text"/> / <input style="width: 50px;" type="text"/></div> <div style="margin-bottom: 5px;">上行带宽: <input style="width: 150px;" type="text"/> Kbps (100-1000000)</div> <div style="margin-bottom: 5px;">下行带宽: <input style="width: 150px;" type="text"/> Kbps (100-1000000)</div> <div style="margin-bottom: 5px;">工作模式: <input checked="" type="radio"/> NAT <input type="radio"/> 路由</div> <div style="margin-bottom: 5px;">状态: <input checked="" type="checkbox"/> 启用</div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <input type="button" value="确定"/> <input type="button" value="取消"/> </div> </div>										

图 10-8 L2TP 客户端设置

隧道设置

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

10.2.3 L2TP 服务器隧道信息

在此将列出路由器上所有 L2TP 隧道的相关信息。

进入界面：VPN >> L2TP >> 隧道信息列表

隧道信息列表							
序号	用户名	服务器/客户端	虚拟接口名称	虚拟本地IP	接入服务IP	对端虚拟IP	DNS
--	--	--	--	--	--	--	--

图 10-9 L2TP 隧道信息界面

10.3 PPTP

PPTP (Point-to-Point Tunneling Protocol , 点到点隧道协议) 定义于 IETF 的 RFC2637 中 , 是一种在 PPP (Point to Point Protocol , 点到点) 协议基础上开发的支持按需、多协议 VPN 的二层隧道技术 , 通过跨越基于 TCP/IP 的数据网络创建 VPN , 实现安全的远程访问连接。PPTP的实现基于C/S (Client/Server , 客户端/服务器) 模型 , 在客户端和服务器间建立起 PPTP隧道。客户端使用服务器提供的账户信息拨号连接到服务器上 , 服务器默认在TCP 1723 端口上监听服务 , 从而实现双方的通信。

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

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

10.3.1 PPTP 服务器设置

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

进入界面 : VPN >>PPTP >> PPTP 服务器

全局设置

PPTP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)

服务器列表

+ 新增 - 删除

<input type="checkbox"/>	序号	服务接口	MPPE加密	状态	设置
<input type="checkbox"/>	--	--	--	--	--

图 10-10 PPTP 服务器设置界面

全局设置

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

表 10.7 PPTP 服务器设置-全局管理设置界面项说明

点击 <  新增 >，进行隧道设置。

 新增
  删除

<input type="checkbox"/>	序号	服务接口	MPPE加密	状态	设置
--	--	--	--	--	--

服务接口:

MPPE加密:

状态: 启用

图 10-11 PPTP 服务器列表

隧道设置

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

表 10.8 PPTP 服务器设置-隧道设置界面项说明

10.3.2 PPTP 客户端设置

进入界面：VPN >>PPTP >> PPTP 客户端



图 10-12 PPTP 全局设置

全局设置

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

表 10.9 PPTP 客户端设置-全局管理设置界面项说明

点击 < >，进行隧道设置。



图 10-13 PPTP 客户端列表

隧道设置

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

表 10.10 PPTP 客户端设置-隧道设置界面项说明

10.3.3 PPTP 服务器隧道信息

在此将列出路由器上所有PPTP隧道的相关信息。

进入界面：VPN >> PPTP >> 隧道信息列表

隧道信息列表							
序号	用户名	服务器/客户端	虚拟接口名称	虚拟本地IP	接入服务IP	对端虚拟IP	DNS
--	--	--	--	--	--	--	--

图 10-14 PPTP隧道信息界面

10.4 用户管理

当路由器作为L2TP服务器或PPTP服务器时，需创建用户账号。

进入界面：VPN >>用户管理>>VPN用户管理

VPN用户管理规则列表

+ 新增 - 删除

□	序号	用户名	服务类型	本地地址	地址池	组网模式	对端子网	设置
--	--	--	--	--	--	--	--	--

用户名:

密码:

低 中 高

服务类型:

本地地址:

地址池:

DNS地址:

组网模式:

最大会话数: (1-200)

对端子网: /

图 10-15 PPTP服务器列表

点击 < + 新增 > ，进行账号设置。

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

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

表 10.11 VPN 用户管理界面项说明

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。路由器提供一键上网、Web 认证和短信认证多种认证方式。一键认证可快速登录；Web 认证可以保证网络安全，并推送 Web 广告；短信认证方便移动端用户进行认证。

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：

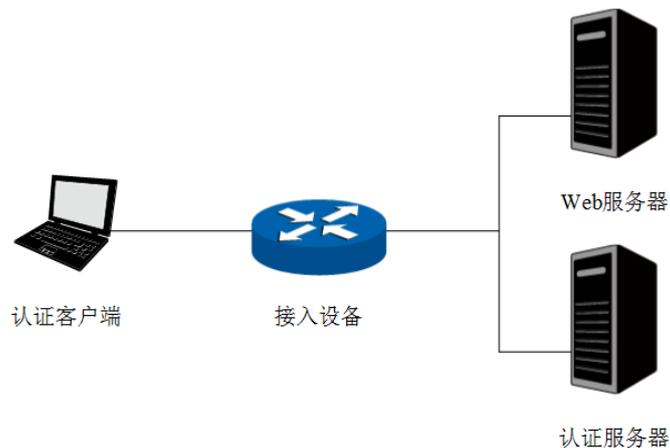


图 11-1 Web 认证系统拓扑图

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-ER6225G 工业级 Web 认证过程如下图所示：

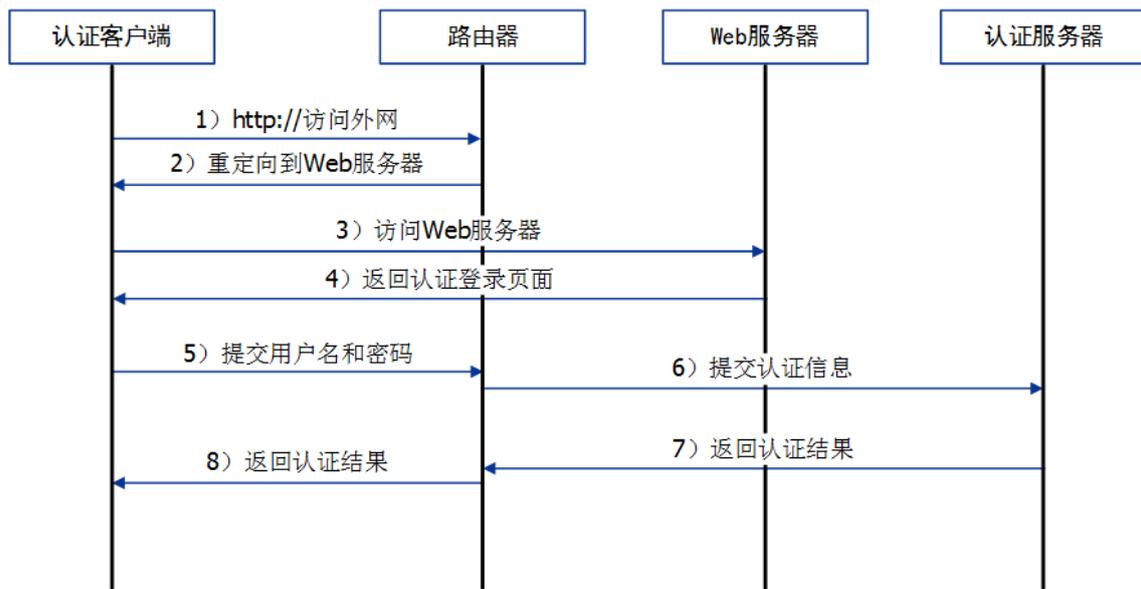


图 11-2 Web 认证过程示意图

- 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 认证设置

TL-ER6225G 工业级的 AP 设置、射频设置、无线设置、认证设置可以在 TP-LINK 商用网络云平台上进行远程集中配置，后续管理维护更加方便。

如需在 TP-LINK 商用网络云平台上进行远程集中配置相关参数，请不要在本地管理界面配置，点击“去开启云管理”按钮去云管理页面开启云管理功能，然后登录“TP-LINK 商用网络云平台”添加绑定本设备进行配置。相关云管理请参考

认证管理

AP设置、射频设置、无线设置、认证设置可以在TP-LINK商用网络云平台上进行远程集中配置，后续管理维护更加方便。
如需在TP-LINK商用网络云平台上进行远程集中配置相关参数，请不要在本地管理界面配置，点击“去开启云管理”按钮去云管理页面开启云管理功能，然后登录“TP-LINK商用网络云平台”添加绑定本设备进行配置。

[继续本地配置](#) [去开启云管理](#)

下面介绍本地管理界面的配置方法。

11.2.1 跳转页面

进入界面：认证管理 >> 认证设置 >> 跳转页面

点击  新增，新增跳转页面模板。设置完成后，请点击确定，保存配置。

<input type="checkbox"/>	序号	模板类型	跳转页面名称	备注	设置
--	--	--	--	--	--

跳转页面名称： (1-50个英文字符、数字、下划线或减号)

模板类型： 本地模板 云模板

备注： (1-50个字符，可选)

* 请选择模板 收起 ^



跳转页面名称	设置跳转页面名称
模板类型	选择本地模板或云模板。 选择云模板，设备将向云端服务器获取页面样式，需联网才能使用
备注	设置跳转页面的备注信息，方便管理和查找。

选中模板后，需要设置认证页和认证成功页的图片文案信息。

设置认证页



认证页

页面标题 ⓘ

欢迎语

版权信息

背景图片

Logo图片

选择接入方式	选择一键上网、账号登录还是手机登录
页面标题	跳转页面的页面标题。
欢迎语	显示跳转页面的欢迎信息。
版权信息	显示跳转页面的版权声明信息。
背景图片	用于页面的背景展示图，图片大小限制在 200KB 以内。
Logo 图片	设置页面的 Logo 图片，图片大小限制在 100KB 以内。

设置认证成功页



认证成功页

页面标题 ⓘ

公告

背景图片

LOGO图片

页面标题	跳转页面的页面标题。
公告	设置页面的提示信息。
背景图片	用于页面的背景展示图，图片大小限制在 200KB 以内。
Logo 图片	设置页面的 Logo 图片，图片大小限制在 100KB 以内。

设置完成后，可查看到当前已有的跳转页面。

<input type="checkbox"/>	序号	模板类型	跳转页面名称	备注	设置
<input type="checkbox"/>	1	本地模板	test1	---	 

11.2.2 组合认证

进入界面：认证管理 >> 认证设置 >> 组合认证

点击  **新增**，新增认证条目。设置完成后，请点击确定，保存配置。

□	序号	跳转页面名称	生效接口	备注	状态	设置
--	--	--	--	--	--	--

跳转页面名称:

生效接口:

认证成功跳转链接:

(1-120个英文字符、数字或英文特殊字符, 可选。
若链接包含IPv6地址, 需用[]包含, 例如: http://[2000::1]/index.html)

认证失败跳转链接:

(1-120个英文字符、数字或英文特殊字符, 可选。
若链接包含IPv6地址, 需用[]包含, 例如: http://[2000::1]/index.html)

备注: (1-50个字符, 可选)

认证方式: 一键上网 Web认证 微信连Wi-Fi 短信认证

状态: 启用 禁用

免费上网时长: 分钟 (1-43200)

注意:
1. 如果配置了认证失败跳转链接, 需在免认证策略增加该链接的放行规则。

跳转页面名称	选择该条目认证方式下的跳转页面模板。 跳转页面设置请参考 11.2.1 跳转页面
生效接口	选择该条目生效对应的接口。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。
认证失败跳转连接	设置认证失败后跳转的 URL 地址。
备注	设置组合认证条目的备注信息, 以方便管理和查找。
认证方式	选择一键上网、web 认证、微信连 Wi-Fi、短信认证等方式



说明：

- 如果配置了认证失败跳转链接, 需在免认证策略增加该链接的放行规则。

如下将详细各认证方式的设置方法

■ 一键上网

一键上网方式使用路由器内置的 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。

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。可使用路由器一键上网功能实现需求。

网络拓扑

酒店网络拓扑如下图所示：

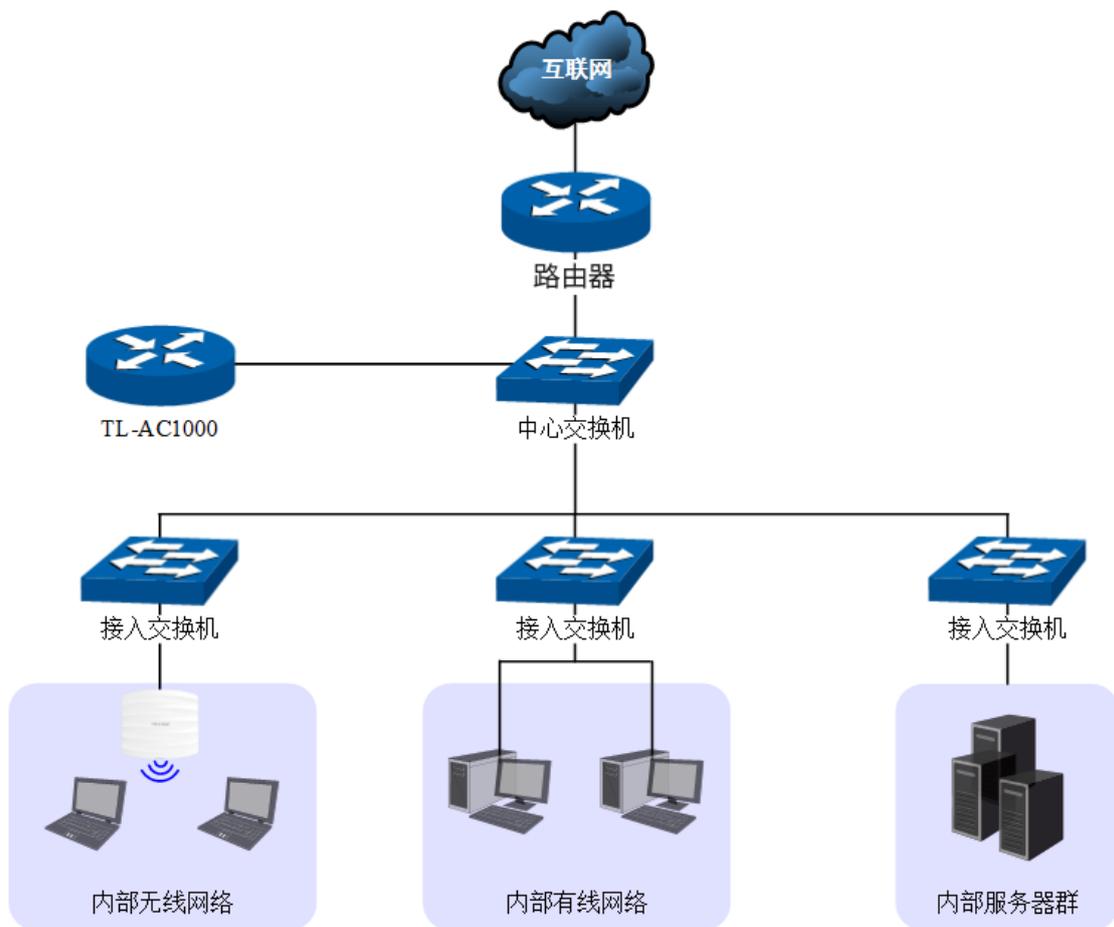


图 11-3 一键上网应用拓扑图

配置方法

1 设置登录的跳转页面模板。

参考 11.2.1 跳转页面。

2 在路由器上设置一键上网的认证规则

认证方式选择一键上网。可参考如下所示参数设置。

认证方式

一键上网 Web认证 微信连Wi-Fi 短信认证

状态: 启用 禁用

免费上网时长: 分钟 (1-43200)

图 11-4 一键上网应用设置界面

认证方式	选择一键上网。
状态	勾选“启用”，开启 Web 认证。
免费上网时长	设置用户免费上网的时长，默认为 60 分钟。

表 11.1 一键上网应用设置界面项说明

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：xxjiudian。
- 不同厂商设备的操作界面可能有所不同，本手册仅以下文所述情况示意。

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



图 11-5 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>按钮释放上网权限。



图 11-6 一键上网用户登录成功页面

3) 免费上网时长到期后，如需继续使用，请打开浏览器，访问任意网址，在弹出的认证页中点击<一键上网>按钮即可再次上网。

■ 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。

配置 Web 服务器

TL-ER6225G 工业级内置有 Web 服务器。

配置认证服务器

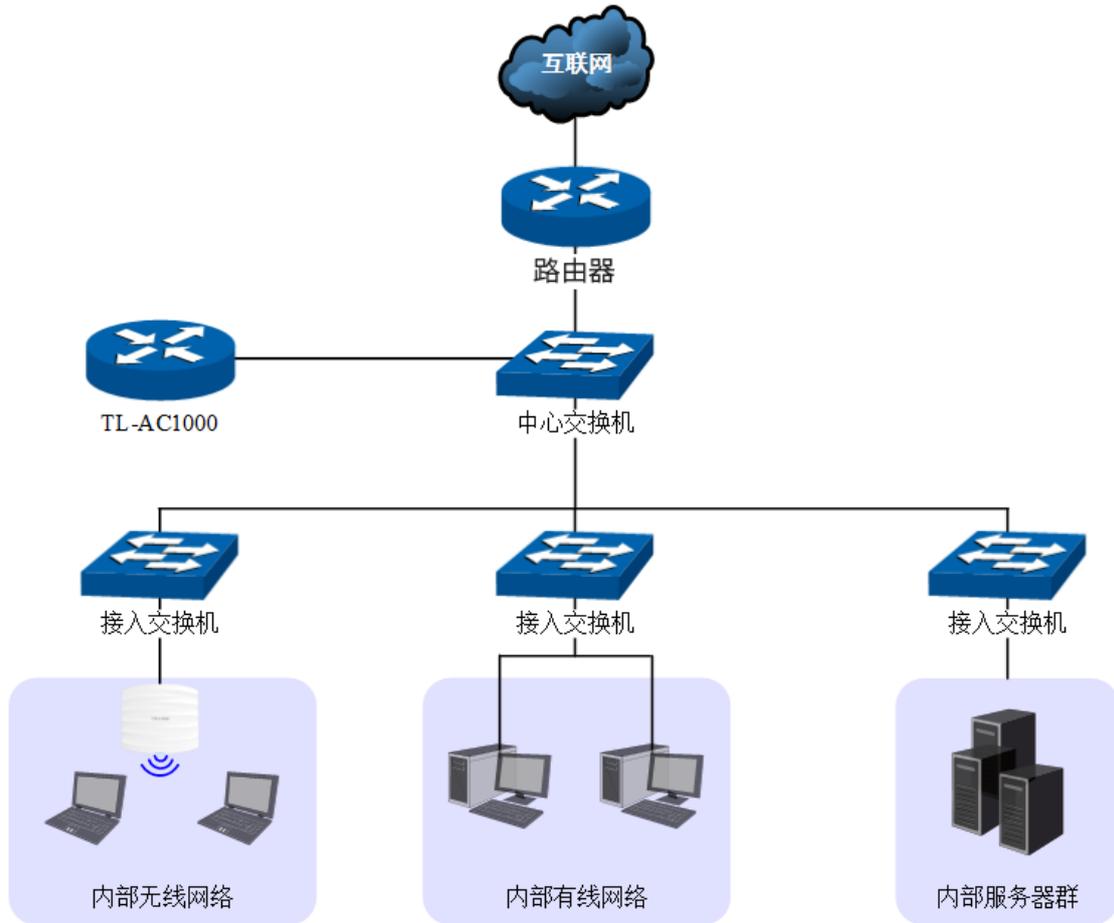
- 本地认证：使用 TL-ER6225G 工业级内置的本地认证服务器，可以通过用户管理功能设置本地认证用户信息。
- radius 认证：使用外部配置的 radius 认证服务器，在 radius 认证服务器上设置认证用户信息。添加外部认证服务器可参考 11.4.2Radius 服务器。

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。

网络拓扑

酒店网络拓扑如下图所示：



配置方法

- 1 设置登录的跳转页面模板。

参考 11.2.1 跳转页面。

- 2 设置本地认证用户信息。

认证用户设置请参考 11.3.1 认证用户管理

- 3 在路由器上设置 Web 认证的认证规则

认证方式选择 Web 认证。可参考如下所示参数设置。

本地服务器

认证方式

一键上网
 Web认证
 微信连Wi-Fi
 短信认证

状态: 启用 禁用

认证服务器类型:

注意:

1. 如果配置了认证失败跳转链接, 需在免认证策略增加该链接的放行规则。
2. 认证服务器类型为远程服务器时, 若服务器配置了用户上网时间, 则免费上网时长为服务器返回的时间, 否则为本页面配置的免费上网时长。

认证方式	选择本地认证。
------	---------

状态	勾选“启用”，则该条目生效。 不勾选“启用”，则该条目不生效。
认证服务器类型	选择本地认证服务器或远程认证服务器

远程服务器

远程 Radius 服务器的添加方法参考 11.4.2 Radius 服务器

认证服务器组的添加方法参考 11.4.1 认证服务器

认证方式

状态: 启用 禁用

认证服务器类型: 远程服务器

认证服务器组: ---

免费上网时长: 30 分钟 (1-43200)

注意:

1. 如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。
2. 认证服务器类型为远程服务器时，若服务器配置了用户上网时间，则免费上网时长为服务器返回的时间，否则为本页面配置的免费上网时长。

认证方式	选择本地认证。
认证服务器组	选择进行 Web 认证的服务器组。
免费上网时长	认证用户可以免费上网的时长。若 radius 服务器设置了免费上网时长，生效的时间为 radius 服务器设置的时间。

4 用户上网步骤

 **说明：**

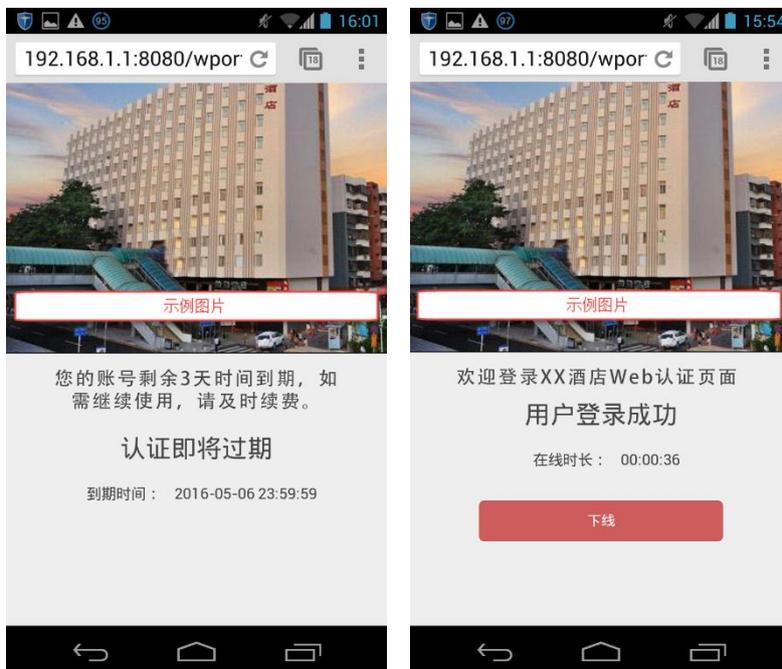
- 以无线客户端为例介绍用户上网步骤，假设酒店 SSID 为：xxjudian。
- 不同厂商设备的操作界面可能有所不同，本手册仅以下文所述情况示意。

- 1) 使用 Wi-Fi 连接 SSID 为“xxjudian”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。



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。

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>按钮释放上网权限。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。



■ 短信认证

认证方式选择短信认证。可参考如下所示参数设置。

认证方式

一键上网	Web认证	微信连Wi-Fi	短信认证
状态:	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用		
免费上网时长:	<input type="text" value="30"/>	分钟 (1-43200)	
验证码有效期:	<input type="text" value="1"/>	分钟 (1-3)	
通道类型:	<input type="text" value="阿里云"/>		
Access Key ID:	<input type="text"/>	(1-50个字符)	
Access Key Secret:	<input type="text"/>	(1-50个字符)	
模板CODE:	<input type="text"/>	(1-50个字符)	
签名名称:	<input type="text"/>	(1-50个字符)	

注意:

- 1、如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。
- 2、若配置了短信认证条目，为了无线PC能够顺利完成认证，需要保证设备可以联网。
- 3、使用短信认证功能前，必须要先在“系统工具->时间设置”中正确地配置本机系统时间。

认证方式	选择本地认证。
状态	勾选“启用”，则该条目生效。 不勾选“启用”，则该条目不生效。
免费上网时长	认证用户可以免费上网的时长。若 radius 服务器设置了免费上网时长，生效的时间为 radius 服务器设置的时间。
验证码有效期	用户在该时间内输入验证码进行验证有效，否则需重新获取验证码。
通道类型	选择阿里云/网易云信/腾讯云/百度云/HTTP 协议作为认证通道

11.2.3 远程 Portal^[a1]

您可以通过本页面设置和查看远程 Portal 认证条目。

进入界面：认证管理 >> 认证设置 >> 免认证策略

点击  新增，新增远程 Portal 条目。设置完成后，请点击确定，保存配置。

□	序号	生效接口	备注	状态	设置
--	--	--	--	--	--

生效接口:

认证成功跳转链接:

(1-120个英文字符、数字或英文特殊字符, 可选。
若链接包含IPv6地址, 需用[]包含, 例如: http://[2000::1]/index.html)

认证失败跳转链接:

(1-120个英文字符、数字或英文特殊字符, 可选。
若链接包含IPv6地址, 需用[]包含, 例如: http://[2000::1]/index.html)

远程Portal地址:

(1-100个英文字符、数字或英文特殊字符。
若链接包含IPv6地址, 需用[]包含, 例如: http://[2000::1]/index.html)

认证服务器类型:

备注: (1-50个字符, 可选)

注意:
 1、如果配置了认证失败跳转链接, 需在免认证策略增加该链接的放行规则。
 2、认证服务器类型为远程服务器时, 若服务器配置了用户上网时间, 则免费上网时长为服务器返回的时间, 否则为本页面配置的免费上网时长。

生效接口	选择该条目生效对应的接口。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。
认证失败跳转连接	设置认证失败后跳转的 URL 地址。
远程 Portal 地址	填写远程 Portal 服务器的地址。
认证服务器类型	选择认证服务器为本地服务器或者远程服务器。
备注	设置组合认证条目的备注信息, 以方便管理和查找。



说明:

- 如果配置了认证失败跳转链接, 需在免认证策略增加该链接的放行规则。
- 认证服务器类型为远程服务器时, 若服务器配置了用户上网时间, 则免费上网时长为服务器返回的时间, 否则为本页面配置的免费上网时长。

11.2.4 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

点击  新增，新增免认证策略条目。路由器支持两种免认证方式：五元组方式和 URL 方式。设置完成后，请点击确定，保存配置。

五元组方式

- 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。

□	序号	策略名称	免认证方式	源IP地址范围	目的IP地址范围	源端口	目的端口	服务协议	状态	设置
--	--	--	--	--	--	--	--	--	--	--

策略名称： (1-50个字符)

免认证方式：

源IP地址范围： / (可选)

源MAC地址： (XX-XX-XX-XX-XX-XX, 可选)

源端口范围： - (1-65535, 可选)

目的IP地址范围： / (可选)

目的端口范围： - (1-65535, 可选)

服务协议：

生效接口域：

备注： (1-50个字符)

状态： 启用

图 11-7 免认证策略-免认证策略设置-五元组方式界面

策略名称	设置免认证策略的名称。只能输入英文、数字和下划线。
免认证方式	选择五元组方式。
源 IP 地址范围	设置免认证策略的源 IP 地址和网络掩码。
源 MAC 地址	设置免认证策略的源 MAC 地址。
源端口范围	设置免认证策略的源端口范围。
目的 IP 地址范围	设置免认证策略的目的 IP 地址和网络掩码。
目的端口范围	设置免认证策略的目的端口范围。

服务协议	设置免认证策略的服务协议。
生效接口域	选择生效接口，可以针对指定接口设置免认证策略。
备注	设置条目的备注，以方便管理和查找。
状态	勾选“启用”，则使该策略生效； 不勾选“启用”，则该策略无效。

表 11.2 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

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

□	序号	策略名称	免认证方式	源IP地址范围	目的IP地址范围	源端口	目的端口	服务协议	状态	设置
--	--	--	--	--	--	--	--	--	--	--

策略名称: (1-50个字符)

免认证方式: URL方式 ▼

URL地址: (1-127个字符)

源IP地址范围: / (可选)

源MAC地址: (XX-XX-XX-XX-XX-XX, 可选)

生效接口域: --- ▼

备注: (1-50个字符)

状态: 启用

图 11-8 免认证策略-免认证策略设置-URL方式界面

策略名称	设置免认证策略的名称。只能输入英文、数字和下划线。
免认证方式	选择 URL 方式。
URL 地址	设置免认证策略的 URL 地址。
源 IP 地址范围	设置免认证策略的源 IP 地址和网络掩码。
源 MAC 地址	设置免认证策略的源 MAC 地址。
生效接口域	选择生效接口，可以针对指定接口设置免认证策略。
备注	设置条目的备注，以方便管理和查找。

状态	<p>勾选“启用”，则使该策略生效；</p> <p>不勾选“启用”，则该策略无效。</p>
----	---

表 11.3 免认证策略-免认证策略设置-URL 方式界面项说明

新增的条目会在免认证策略列表里显示出来，如下图所示。

<input type="checkbox"/>	序号	策略名称	免认证方式	源IP地址范围	目的IP地址范围	源端口	目的端口	服务协议	状态	设置
--	1	dhcp client	五元组方式	---	---	68-68	67-67	UDP	已启用	---
--	2	dhcp server	五元组方式	---	---	67-67	68-68	UDP	已启用	---
--	3	dns client	五元组方式	---	---	---	53-53	UDP	已启用	---
--	4	dns server	五元组方式	---	---	53-53	---	UDP	已启用	---
<input type="checkbox"/>	5	test1	URL方式	---	---	---	---	---	已启用	

图 11-9 免认证策略-免认证策略设置列表

如有需要，可以点击条目后的 按钮进行编辑。

11.2.5 认证参数

本页可以进行认证的全局参数的设置。

进入界面：认证管理 >> 认证设置 >> 认证参数

认证参数

认证老化

认证老化时间: (5-30分钟)

Portal认证端口: (80、1024-65535)

认证模式: 基于SSID 基于接口

认证老化	勾选开启认证老化功能
认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服端口重复。
认证模式	设置 Portal 认证的认证模式 现支持基于 SSID 和基于接口两种模式。

11.3 用户管理

在此页面可以对用户信息进行管理，包含认证用户管理和用户配置备份，前者参照 11.1.2，后者可参考 11.1.3。

11.3.1 认证用户管理

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 >> 用户管理 >> 认证用户管理

点击  新增，新增认证用户。设置完成后，请点击确定，保存配置。

□	序号	用户类型	用户名	有效期/上网时长	MAC地址	备注	状态	设置
--	--	--	--	--	--	--	--	--

用户类型:	<input type="text" value="正式用户"/>	
用户名:	<input type="text"/>	(1-100个字符)
密码:	<input type="text"/>	(1-100个字符)
有效期至:	<input type="text" value="2019/12/31"/>	(格式:YYYY/MM/DD)
允许认证时间段:	<input type="text" value="00:00-24:00"/>	(格式为xx:xx-xx:xx)
MAC地址绑定方式:	<input type="text" value="不绑定"/>	
同时登录用户数:	<input type="text" value="1"/>	(1-1024)
上行带宽:	<input type="text" value="0"/>	Kbps(0或10-1000000,0表示不限制)
下行带宽:	<input type="text" value="0"/>	Kbps(0或10-1000000,0表示不限制)
姓名:	<input type="text"/>	(1-50个字符, 可选)
电话:	<input type="text"/>	(1-50个字符, 可选)
备注:	<input type="text"/>	(1-50个字符, 可选)
状态:	<input checked="" type="checkbox"/> 启用	

图 11-10 认证状态界面

用户类型	用户类型分为正式用户或免费用户。 正式用户：存留在系统中的正式用户，具有一定的有效期，且可以绑定相应的设备 MAC 地址。可以记录更多用户的资料信息。 免费用户：免费用户具有一定的上网时长限制。
用户名	用于认证登录的用户名。
密码	用户登录所使用的密码。
有效期至	正式用户的有效期。
允许认证时间段	允许用户进行认证的时间。

MAC 地址绑定方式	<p>选择是否绑定 MAC 地址，以及绑定的方式。</p> <p>不绑定：不绑定用户的 MAC 地址。</p> <p>静态绑定：手动输入认证客户端 MAC 地址，绑定对应用户名。</p> <p>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。</p>
同时登录用户数	<p>仅当“MAC 地址绑定方式”为“不绑定”时，可设。</p> <p>最多允许同时使用该账号登录的用户数量。</p>
上行带宽	<p>当前用户允许的上行带宽，以 Kbps 为单位，0 表示不限制。当开启此功能时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。</p>
下行带宽	<p>当前用户允许的下行带宽，以 Kbps 为单位，0 表示不限制。当开启此功能时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。</p>
姓名	<p>可选记录当前用户姓名。</p>
电话	<p>可选记录当前用户电话。</p>
备注	<p>可选记录当前用户备注。</p>
状态	<p>是否启用当前用户规则。</p>

表 11.4 认证状态界面项说明

新增条目会在规则列表中显示出来，如下所示：

<input type="checkbox"/>	序号	用户类型	用户名	有效期/上网时长	MAC地址	备注	状态	设置
<input type="checkbox"/>	1	免费用户	test1	---	---	---	已启用	

11.3.2 用户配置备份

您可以通过本页面来备份和下载用户配置信息。

进入界面：认证管理 >> 用户管理 >> 用户配置备份

点击备份，存储当前配置信息；选择配置文件，点击导入，导入用户信息。

备份配置信息

备份

导入配置信息

文件路径: 浏览

导入

11.4 认证服务器

TL-ER6225G 工业级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。

11.4.1 认证服务器

进入界面：认证管理 >> 认证服务器 >> 认证服务器

你可以通过该页面管理认证服务器组，点击  新增，新增认证服务器。设置完成后，请点击确定，保存配置。

<input type="checkbox"/>	序号	组名称	协议类型	备注	设置
--	--	--	--	--	--

组名称: (1-50个英文字符、数字、下划线或减号)

协议类型: RADIUS

主服务器: ▼

备用服务器: ▼ (可选)

恢复时间: (30-1440分钟)

备注: (1-50个字符, 可选)

组名称	自定义的认证服务器组名称，注意不能与已有服务器组名称重复。
协议类型	该组中认证服务器的类型，目前只支持 Radius。
主服务器	选择特定类型的认证服务器为该组的主服务器，主服务器在认证过程中将优先被使用。
备用服务器	备用服务器在主服务器发生故障时启用，备份服务器为可选项。
恢复时间	当主服务器发生故障后，重新尝试使用主服务器的时间间隔。
备注	您可以对认证服务器组进行描述。

11.4.2 Radius 服务器

进入界面：认证管理 >> 认证服务器 >> 认证服务器

你可以通过该页面添加、修改或者删除一个外部 Radius 服务器。·点击  新增，新增 Radius 服务器。设置完成后，请点击确定，保存配置。

□	序号	名称	地址	认证端口	计费端口	认证方式	设置
--	--	--	--	--	--	--	--

服务器名称:	<input type="text"/>	(1-50个英文字符、数字、下划线或减号)
服务器地址:	<input type="text"/>	(IP地址或域名, 1-250个英文字符)
认证端口:	<input type="text" value="1812"/>	(1024-65535)
计费端口:	<input type="text" value="0"/>	(0, 1024-65535)
共享密钥:	<input type="text"/>	(1-120个字符)
重复发送次数:	<input type="text" value="3"/>	(0-10次)
超时时间:	<input type="text" value="3"/>	(1-60秒)
NAS IP地址:	<input type="text"/>	(可选)
认证方式:	<input type="text" value="PAP"/>	

服务器名称	配置 Radius 服务器的名称。
服务器地址	设置服务器的地址，IPv4、IPv6 地址或者 DNS 域名。
认证端口	服务器监听认证报文的端口。
计费端口	服务器监听计费报文的端口，0 表示不启用计费功能。
共享密钥	Radius 服务器配置的共享密钥。
重复发送次数	当客户端发送请求后，如果没有收到回复，重复发送请求的次数。
超时时间	当客户端发送请求后，数据包超时时间。
NAS IP 地址	进行 Radius 认证或计费时，NAS-IP-Address 字段的 IP 地址值（一般填写 AC 与 Radius 服务器交互的实际 IP 地址，也可以为空）。
认证方式	使用的认证方式，有 PAP、CHAP、MSCHAP 和 MSCHAPv2。

11.5 认证状态

进入界面：认证管理 >> 认证状态

可统一查看管理已认证的用户。

<input type="checkbox"/>	序号	认证方式	用户名	认证时间	MAC地址	IP地址	设置
--	--	--	--	--	--	--	--

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

第12章 系统服务

12.1 PPPoE 服务器

PPPOE 即 PPP over Ethernet，是指在以太网中传输 PPP 的技术，通过 PPPoE 可以防范 ARP 欺骗，同时为客户端统一分配 IP 以及 DNS 等参数，有效避免了静动态 IP 方式因地址冲突或者参数设置不当导致无法访问外网的问题，还可以结合 Radius 服务器对客户进行认证、授权以及计费，目前国内 ISP 多采用 PPPoE 作为接入认证方式。

TL-ER6225G 工业级支持 PPPoE 服务器，通过给局域网内用户分配账号来实现对用户网络使用的管理。

12.1.1 全局设置

进入界面：系统服务 >> PPPoE 服务器 >> 全局设置

根据您的网络环境，对 PPPoE 服务器进行正确的配置，以保证高效管理网络。配置完成后，点击设置生效。

全局设置

PPPoE服务器:	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
强制PPPoE拨号:	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
拨号用户互访:	<input checked="" type="radio"/> 允许	<input type="radio"/> 禁止
服务接口:	---	
首选DNS服务器地址:	<input type="text"/>	(X.X.X.X, 可选)
备选DNS服务器地址:	<input type="text"/>	(X.X.X.X, 可选)
系统最大会话数:	<input type="text" value="50"/>	(1-1000)
最大未应答LCP包数:	<input type="text" value="10"/>	(1-60)
空闲断线时间:	<input type="text" value="30"/>	分钟 (0-10080)
认证方式:	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP-V2	

PPPoE 服务器	选择<启用>，开启 PPPoE 服务器功能；选择<禁用>，关闭 PPPoE 服务器功能。
强制 PPPoE 拨号	选择<启用>，开启强制 PPPoE 拨号功能；选择<禁用>，关闭 PPPoE 强制拨号功能。功能开启后，生效接口下仅有拨号用户和例外 IP 的用户能使用网络。设置例外 IP，请到例外 IP 管理页面进行设置。
拨号用户互访	选择<允许>，开启拨号用户互访功能；选择<禁止>，禁止拨号用户互访功能。拨号用户互访功能允许拨号用户之间互相通信。建议选择禁止。

服务接口	该用户接入网络的接口。接口只能设置为带 IP 的静态接口。
首选/备选 DNS 服务器地址	请正确填写，服务商提供的当地 DNS 地址，缺省为空。
系统最大会话数	PPPoE 可同时在在线的最大用户数。建议填写 256。
最大未应答 LCP 包数	作为最大未应答 LCP 包数，缺省为 10。PPPoE 拨号成功之后，服务器会发送 LCP 数据包检测线路是否正常，如果超过设置的最大未应答数据包数，服务器即认为 PPPoE 线路断开连接。
空闲断线时间	如果在填写的时间范围内没有进行上网操作，路由器即认为客户端 PPPoE 断开连接。缺省为 30。请填写 0-10080 (分钟)，即最大为 7 天。0 代表不空闲断线。
认证方式	支持本地认证且提供四种认证方式，请至少选择一种。建议全部勾选。



注意：

- 当未应答的 LCP 包数到达最大未应答 LCP 包数时会断开链接。
- PPPoE 服务器的服务接口不能为被桥接的接口，只能设置为带 IP 的静态接口，否则 PPPoE 服务器功能无效。
- 开启 PPPoE Server 功能，请到 NAT 设置添加 NAPT 规则。
- 账号引用的地址池禁止与服务接口地址同一网段。
- 例外 IP 地址段需与服务接口同一网段，但不能包含服务接口 IP。

12.1.2 账号管理

进入界面：系统服务 >> PPPoE 服务器 >> 账号管理

你可以通过该页面添加和管理用户账号，点击  新增，新增账号。设置完成后，请点击确定，保存配置。

□	序号	账号	地址池	最大会话数	账号到期时间	MAC地址	定时断线时间	备注	状态	设置
--	--	--	--	--	--	--	--	--	--	--

账号: (1-100个字符)

密码: (1-100个字符)

地址池: ▼

最大会话数: (1-1000)

账号到期时间: (格式: YYYY/MM/DD)

带宽模式: 共享 独立

上行带宽: Kbps (0或100-1000000, 0表示不限制)

下行带宽: Kbps (0或100-1000000, 0表示不限制)

备注: (可选, 1-50个字符)

启用/禁用规则: 启用 禁用

账号高级设置: 启用 禁用

MAC绑定方式: ▼

定时断线时间: (0-168小时)

账号	用户拨号所使用的账号，可以自定义
密码	户拨号所使用的密码，可以自定义。
地址池	分配给用户的地址范围。 添加地址池请参考 5.3IP 地址池
最大会话数	该账号同时允许接入的最大用户数。建议填写 1，即该账号只能给一个用户进行拨号。
账号到期时间	该账号到期的时间，建议默认值。
带宽模式	设置账号带宽控制模式：共享表示账号的所有用户共用带宽；独立表示账号的所有用户独占带宽。
上行带宽	当前账号用户允许的上行带宽，以 Kbps 为单位，0 表示不限制。
下行带宽	当前账号用户允许的下行带宽，以 Kbps 为单位，0 表示不限制。
备注	您可以设置规则条备注，以方便您管理和查找。备注最多支持 50 个字符。
启用/禁用规则	您可以选择<启用>，使该规则生效。您也可以选择<禁用>，使该规则失效。
账号高级设置	设置账号的高级属性，如 MAC 绑定、定时断线等

MAC 绑定方式	<p>不绑定：不进行用户和 MAC 的绑定。</p> <p>静态绑定：静态绑定一个 MAC 地址，该账户只能在该 MAC 的主机上登录。</p> <p>动态绑定：当用户第一次登录的时候记录其 MAC，以后用户的登录必须使用该 MAC。</p>
定时断线时间	设置定时断线的时间，当定时断线时间为 0 时，表示不会定时断线。

12.1.3 例外 IP 管理

进入界面：系统服务 >> PPPoE 服务器 >> 例外 IP 管理

例外 IP 为用户不需要通过拨号就可以访问网络的 IP 地址。你可以通过该页面添加和管理例外 IP 地址，点击  新增，新增 IP。设置完成后，请点击确定，保存配置。

<input type="checkbox"/>	序号	起始IP地址	结束IP地址	备注	状态	设置
	--	--	--	--	--	--

起始IP地址: (X.X.X.X)

结束IP地址: (X.X.X.X)

备注: (可选, 1-50个字符)

启用/禁用规则: 启用 禁用

起始 IP 地址	用户拨号所使用的账号，可以自定义
结束 IP 地址	户拨号所使用的密码，可以自定义。
备注	<p>分配给用户的地址范围。</p> <p>添加地址池请参考 5.3IP 地址池</p>
启用/禁用规则	该账号同时允许接入的最大用户数。建议填写 1，即该账号只能给一个用户进行拨号。

12.1.4 账号信息列表

进入界面：系统服务 >> PPPoE 服务器 >> 账号信息列表

可查看当前所有用户账号。

□	序号	账号	状态	IP地址	MAC地址	在线时间	备注	断开连接
--	--	--	--	--	--	--	--	--

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-ER6225G 工业级路由器提供花生壳动态 DNS 客户端、科迈动态 DNS 客户端和 3322 动态 DNS 客户端。

12.2.1 花生壳动态域名

进入界面：系统服务 >> 动态 DNS >> 花生壳动态域名

□	序号	服务接口	用户名	启用/禁用	状态	域名	服务类型	设置
--	--	--	--	--	--	--	--	--

服务接口:

用户名/域名: [注册用户名](#)

密码:

状态: 启用

图 12-1 花生壳动态域名登录界面

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

表 12.1 花生壳动态域名登录界面项说明

12.2.2 科迈动态域名

进入界面：系统服务 >> 动态 DNS >> 科迈动态域名

<input type="checkbox"/>	序号	服务接口	用户名	启用/禁用	状态	域名	服务类型	设置
--	--	--	--	--	--	--	--	--

服务接口:

用户名/域名: [注册用户名](#)

密码:

状态: 启用

图 12-2 科迈动态域名登录界面

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

表 12.2 3322 动态域名登录界面项说明

12.2.3 3322 动态域名

进入界面：系统服务 >> 动态 DNS >> 3322 动态域名

<input type="checkbox"/>	序号	服务接口	用户名	启用/禁用	状态	域名	设置
--	--	--	--	--	--	--	--

服务接口:

用户名: [注册用户名](#)

密码:

域名信息:

状态: 启用

图 12-3 3322 动态域名登录界面

服务接口	选择登录 3322 动态域名服务器的接口。
------	-----------------------

用户名	填入在 3322 网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录 3322 网站进行注册。
密码	填入在 3322 网站注册该用户名时所设置的密码。
域名信息	用户名绑定的域名信息。
状态	勾选“启用”，则该条目生效； 不勾选“启用”，则该条目不生效。

表 12.3 3322动态域名登录界面项说明

12.3 DNS 代理

进入界面：系统服务 >> DNS 代理

可以通过本页面设置接口的DNS代理功能。

<input type="checkbox"/>	序号	规则名称	服务接口	出接口	设置
<input type="checkbox"/>	--	--	--	--	--

规则名称:

服务接口: ▼

出接口: ▼

图 12-4 DNS 代理设置界面

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

表 12.4 DNS 代理设置界面项说明

新增的条目会在 DNS 代理规则列表里显示出来，如下图所示。

<input type="checkbox"/>	序号	规则名称	服务接口	出接口	设置
<input type="checkbox"/>	1	rule1	test	auto	 

图 12-5 DNS 代理设置界面

12.4 UPnP 服务

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

如果应用程序支持UPnP协议 , 而局域网中的主机安装了UPnP组件 , 路由器开启了UPnP服务后 , 局域网中的主机就可以根据软件的需要自动地在路由器上打开相应的端口 , 使得外部主机上的应用程序在需要时能够通过打开的端口访问内部主机上的资源 , 这样原本受限于NAT的功能便可以正常使用。例如 , Windows XP和Windows ME系统上安装的MSN Messenger , 在使用音频和视频通话时就可以利用UPnP协议 , 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

□	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	设置
--	--	--	--	--	--	--	--	--	--

图 12-6 UPnP 服务设置界面

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

表 12.5 UPnP 服务设置界面项说明

启用 UPnP 后 , 所有应用到 UPnP 的连接规则会显示在服务列表中 , TL-ER6225G 工业级可以同时支持 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。

12.5 文件共享

进入界面：系统服务 >> 文件共享

通过本页面您可以设置启用/禁用 USB 存储共享。



注意：

- 使用本功能前，请先将您的 USB 存储设备格式化为 FAT 或 NTFS 格式。
- 可使用 Windows 资源管理器或其他支持 GBK 编码的 FTP 客户端访问您的 USB 存储设备。

功能设置

- 1.使用本功能前，请先将您的USB存储设备格式化为FAT或NTFS格式。
- 2.可使用Windows资源管理器或其他支持GBK编码的FTP客户端访问您的USB存储设备。

FTP服务器状态: 开启 关闭

选择生效接口:

FTP登录方式:

USB设备列表

序号	存储设备	FTP服务器地址
--	--	--

功能设置

配置完成后，点击设置，存储配置信息。

FTP 服务器状态	启用该功能后，内网主机可以通过 FTP 服务器地址访问您插在路由器上的 USB 存储设备。滑块为灰色表示禁用，滑块为蓝色表示启用。
选择生效接口	选择你所需要访问 USB 设备的接口。
FTP 登录方式	可以选择匿名登录或账号登录。账号登录需要设置可登录的账号和密码。

USB 设备列表

点击移除设备，安全移除 USB 存储设备。

第13章 云管理

开启云管理后，AP 设置、射频设置、无线设置、认证设置可以在 TP-LINK 商用网络云平台上进行远程集中配置，后续管理维护更加方便。

TL-ER6225G 工业级支持两种云管理类型：

TP-LINK 商用网络云平台：基于公有云管理架构的 TP-LINK 网络设备云管理平台。访问 <https://www.tp-link.com.cn/act-smbcloud>，输入账号，进入云平台，进行管理。

TP-LINK 本地 NMS 管理平台：基于企业私有云管理架构的 TP-LINK 网络设备管理平台，可部署至企业本地物理服务器或虚拟机。

TL-ER6225G 工业级支持终端上网策略，基于 TP-LINK 统一管理平台，支持策略点及认证点功能。

13.1 基本配置

进入界面：云管理 >> 基本配置

选择启用云管理功能，选择 TP-LINK 本地 NMS 管理平台或者 TP-LINK 商用网络云平台，点击设置，使配置生效。

云管理

云管理： 启用 禁用

云类型：
TP-LINK商用网络云平台
TP-LINK本地NMS管理平台
TP-LINK商用网络云平台

设置



注意：

- 开启云管理，设备需连接至 Internet。若未连接，请前往“基本设置->接口设置”检查网络。
- 设备使用云管理后，本地 AP、射频、无线和认证配置将被清空，建议您先备份本地配置。

TP-LINK 本地 NMS 管理平台

云管理

云管理: 启用 禁用

云类型: TP-LINK本地NMS管理平台 ▼

设置

设备未连接到internet, 请前往 [基本设置](#) -> [接口设置](#) 检查网络连接。

TP-LINK本地NMS管理平台设置

服务器地址: (IP或者域名)

端口: (1024-65534)

描述: (可选,1-256个字符)

设置

服务器地址	TP-LINK 本地 NMS 管理平台服务器的地址。
端口	TP-LINK 本地 NMS 管理平台服务器的端口。
描述	TP-LINK 本地 NMS 管理平台服务器的描述信息。



注意:

- 修改云管理配置, 设备将自动保存云管理、AP、射频、无线和认证等相关配置。

TP-LINK 商用网络云平台

云管理

云管理: 启用 禁用

云类型: TP-LINK商用网络云平台 ▼

设置

设备未连接到Internet, 请前往 **基本设置** -> **接口设置** 检查网络连接。

注意:

1. 开启云管理后, 可以登录“TP-LINK商用网络云平台”配置AP、射频、无线和认证等参数, 其余功能参数仍需在本地管理界面设置。
2. 请记住本设备MAC地址(54-A7-03-2F-53-1C), 在“TP-LINK商用网络云平台”添加设备时需要使用该MAC地址。
3. 为保证设备能正常使用云管理功能, 请确保系统时间与当前时间保持一致。
4. 还未下载TP-LINK商云APP? 请扫描以下二维码:



注意:

- 开启云管理后, 可以登录 “<https://smbcloud.tp-link.com.cn/>” 配置 AP、射频、无线和认证等参数, 其余功能参数仍需在本地管理界面设置。
- 请记住设备的 MAC 地址, 在 “TP-LINK 商用网络云平台” 添加设备时需要使用该 MAC 地址。
- 为保证设备能正常使用云管理功能, 请确保系统时间与当前时间保持一致。
- 扫描如下二维码, 添加商云 APP, 也可实现云管理功能。



13.2 终端上网策略

13.2.1 策略点

进入界面：云管理 >> 终端上网策略 >> 策略点

您可以选择是否开启终端上网策略的策略点功能。

策略点

策略点： 启用 禁用

[设置](#)

策略列表

[清空策略列表](#) [搜索](#) [全局搜索](#) [刷新](#)

序号	名称	用户组	访问规则	上下行带宽	生效时间
--	--	--	--	--	--

共0条，每页：条 | 当前：0/0页，0~0条 | [<](#) [>](#)

策略点

关闭功能保留当前终端上网策略的策略点配置但不生效，开启功能原终端上网策略配置自动生效。选择完成后，点击设置，保存配置。



注意：

- 终端上网策略功能与带宽控制、url 过滤、应用控制、访问控制等功能互斥。
- 开启终端上网策略功能后，带宽控制、url 过滤、应用控制、访问控制的本地配置保留但不生效，且不允许修改。
- 关闭终端上网策略功能后，原带宽控制、url 过滤、应用控制、访问控制的本地配置自动生效。

策略列表

名称	策略名称。
用户组	生效用户组
访问规则	用户组允许/禁止访问的规则。
上下行带宽	用户组的上下行带宽（单位为 Kbps）。
生效时间	策略生效时间。

清空策略列表	将终端上网策略的所有策略清空。
搜索	根据列名内容进行指定方式的搜索。
全局搜索	根据列名内容进行全局搜索。
刷新	刷新本地终端上网策略的策略条目。

13.2.2 认证点

进入界面：云管理 >> 终端上网策略 >> 认证点

您可以通过本页面来配置认证点，选择启用认证点或禁用认证点，选择完成后，点击设置，存储配置。

认证点

认证点: 启用 禁用

设置

第14章 系统工具

14.1 管理账号

14.1.1 管理帐号

在此可以修改登录时使用的用户名和密码。

进入界面：系统工具 >> 管理账号 >> 管理账号

修改管理账户

原用户名:

原密码:

新用户名:

新密码:

低 中 高

确认新密码:

设置

图 14-1 修改管理帐户界面

原用户名	本次登录路由器的用户名。
原密码	本次登录路由器使用的密码。
新用户名	重新设置登录路由器的用户名。
新密码	重新设置登录路由器的密码。“低、中、高”表示密码的复杂程度。
确认新密码	再次输入新密码。

表 14.1 修改管理帐户



说明：

- 出厂的用户名和密码均为 admin。更改用户名及密码并保存生效后，后续登录时请使用新用户名及新密码。用户名和密码最多支持 50 个字符，且只能是数字和字母，区分大小写。

14.1.2 远程管理

进入界面：系统工具 >> 管理账号 >> 远程管理

点击  新增，新增远程管理的地址范围。

<input type="checkbox"/>	序号	远程地址范围	状态	设置
<input type="checkbox"/>	--	--	--	--

远程地址范围: /

状态: 启用

图 14-2 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 14.2 远程管理设置界面项说明

新增的条目会在地址列表里显示出来，如下图所示。

<input type="checkbox"/>	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 14-3 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。

 **说明：**

- 包含局域网地址的远程管理地址条目无效。
- 如果添加 0.0.0.0/0 的条目，将允许所有远程计算机访问设备，有可能在非法攻击情况下无法访问设备。

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：

<input type="checkbox"/>	序号	远程地址范围	状态	设置
<input type="checkbox"/>	--	--	--	--

远程地址范围: /

状态: 启用

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)

SSH服务端口: (22、1024-65535)

Web会话超时时间: 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。

14.1.3 系统管理设置

您可以通过本页面进行服务端口和会话超时时间的管理。

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: 开启

Http服务端口: (80、1024-65534)

Https服务端口: (443、1024-65534)

Web会话超时时间: 分钟(5-60)

最大登录尝试次数: 次(0-5,0表示无限制)

登录锁定时长: 分钟(1-60)

图 14-4 系统管理设置界面

Http 服务	Http 服务默认打开，当取消勾选该项时，将无法通过 Http 的方式对 WEB 进行管理。
Http 服务端口	设置路由器的 Http 服务端口。
Https 服务端口	设置路由器的 Https 服务端口。
Web 会话超时时间	设置通过 Web 访问路由器的超时时间，Web 登录路由器后，用户在该设定时间内如无任何指令，路由器将自动断开连接。 设置超时时间后，新的超时时间将在下一次登录时生效。
最大登录尝试次数	当连续尝试登陆失败达到该次数时，将会在一段时间内锁定设备不允许继续登录。为 0-5 次，0 表示无限制。
登录锁定时长	当连续登陆失败次数达到最大登录尝试次数后，将会在锁定时长期间无法进行登录。

表 14.3 系统管理设置界面项说明

14.2 设备管理

14.2.1 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 14-5 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。

14.2.2 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 14-6 备份与导入配置界面

版本信息

显示当前路由器软件版本。

备份配置信息

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

导入配置信息

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



说明：

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

14.2.3 重启设备

进入界面：系统工具 >> 设备管理 >> 重启设备



图 14-7 重启路由器界面

单击<重启设备>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。

14.2.4 软件升级

进入界面：系统工具 >> 设备管理 >> 软件升级

在线升级

当前软件版本: 1.0.0 Build 191221 Rel.68161n

检测新版本

本地升级

当前硬件版本: TL-ER6225G工业级 1.0

升级文件路径: 浏览

升级

图 14-8 软件升级界面

在线升级

点击<检测新版本>按钮向云端检测是否存在更新版本的软件。

本地升级

TL-ER6225G 工业级官方网站 (TL-ER6225G 工业级) 会不定期更新 TL-ER6225G 工业级的软件升级文件，可将升级文件下载保存在本地。登录路由器后进入软件升级界面，单击<选择文件>按钮，选择保存路径下的升级文件，点击<升级>进行软件升级。



说明：

- 使用在线升级的时候请确保设备正常联网。
- 请确保在设备升级过程中，不要将设备断电，不要对页面进行刷新。升级完毕，设备将自动重启。
- 您可以到网址 www.tp-link.com.cn 下载最新的升级软件。
- 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。

14.2.5 设备管理

进入界面：系统工具 >> 设备管理 >> 设备管理

设置路由器名称，点击设置，配置生效。

设备信息设置

设备名称: (1-20个字符)

14.3 流量统计

14.3.1 接口流量统计

接口流量界面显示路由器所有正在工作的接口的数据接收/发送速率，以及 WAN 口的附加信息统计。

进入界面：系统工具 >> 流量统计 >> 接口流量统计

流量统计列表

接口数量: 10 刷新

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

图 14-9 接口流量统计界面

发送/接收速率是以千比特每秒为单位进行统计的，通常所说的 1M 带宽即 1024Kbps。发送/接收包速率统计的是每秒发送/接收的数据包个数。发送/接收总字节数统计的则是所有数据包的总字节数。发送/接收总报文统计的是报文的总个数。

14.3.2 IP 流量统计

IP流量统计界面将显示指定IP范围之间各个IP的即时流量信息

进入界面：系统工具 >> 流量统计 >> IP流量统计



图 14-10 IP流量统计界面

勾选“启用IP流量统计”选项，相应的流量统计信息将显示在流量统计列表中。

14.4 诊断工具

14.4.1 诊断工具

进入界面：系统工具 >> 诊断工具 >> 诊断工具

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



图 14-11 PING通信检测界面

Ping 通信检测

目的 IP/域名	输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，路由器将发送 ping 包检测目的地址是否可以到达，并将检测结果显示在下面的方框中。
出接口	选择 PING 检测的出接口。
PING 次数	设置 PING 次数，范围为 1-50 次，默认为 4 次。
PING 数据包大小	设置 PING 数据包大小，范围为 4-1472 字节，默认为 64 字节。

表 14.4 PING 通信检测

诊断工具

诊断工具类型: PING 通信检测 路由跟踪检测

目的 IP/域名:

出接口:

路由跟踪最大 TTL: (1-30)

The Router is ready.

图 14-12 路由跟踪检测

路由跟踪检测

目的 IP/域名	输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，路由器将发送 tracert 包检测经过哪些路由到达目的地址，并将检测结果显示在下面的方框中。
出接口	选择路由跟踪检测的出接口。
路由跟踪最大 TTL	设置路由跟踪的最大 TTL 值，默认值为 20。

表 14.5 路由跟踪检测

14.4.2 故障诊断

可以通过诊断工具来检测和诊断当前的网络状况。

进入界面：系统工具 >> 诊断工具 >> 故障诊断

故障诊断模式

一般情况下请勿开启，需要故障诊断时请在技术支持人员的帮助下开启本功能。

故障诊断模式: 开启

设置

AP调试日志收集

发送至本设备

日志上报等级: 警告信息 及以上等级

发送至日志服务器

日志上报等级: 警告信息 及以上等级

日志上报间隔: (20-600秒)

远程服务器地址:

设置

诊断信息

您可以导出诊断信息并将其发给技术支持人员进行分析并协助解决问题。

导出诊断信息

一键清理

您可以在技术支持人员的指导下使用一键清理功能协助解决问题。

一键清理

故障诊断和诊断信息

勾选以开启诊断模式，取消勾选表示诊断模式关闭。开启本功能后可以配合技术支持人员对设备进行诊断。点击设置，配置生效。点击<导出诊断信息>按钮下载基本的诊断信息，将其提供给技术人员以协助您分析和解决问题。

AP 调试日志收集

开启/关闭 AP 调试日志收集功能，方便定位 AP 问题。

发送至本设备/日志服务器	AP 是否需要将日志发送给本设备或指定的日志服务器。
--------------	----------------------------

日志上报等级	设置 AP 上报的日志等级，AP 将不会上报小于该等级的日志。
日志上报间隔	设置 AP 上报给日志服务器的时间间隔。
远程服务器地址	设置 AP 上报的日志服务器地址。

一键清理

点击按钮进行设备清理，以协助解决问题。该功能需在技术支持人员的协助下使用。



说明：

- 一般情况下请不要随意开启本功能。
- 需要诊断时，请先联系技术支持人员，在其协助下打开并使用本功能。

14.5 时间设置

14.5.1 时间设置

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

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

进入界面：系统工具 >> 时间设置 >> 时间设置

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

时间设置

当前时间: 2019/12/21 09:29:01

设置时间: 通过网络获取系统时间 手动设置系统时间

时区: (GMT+08:00)北京, 乌鲁木齐, 香港特别行政区, 台北 ▼

首选NTP服务器: 0.0.0.0

备选NTP服务器: 0.0.0.0 (可选)

图 14-13 通过网络获取系统时间

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

表 14.6 时间设置界面项说明

若路由器暂时不能访问互联网，可以选择对系统时间进行手动设置设置完毕后点击<设置>生效。

The screenshot shows the 'Time Settings' (时间设置) interface. It displays the current time as 2019/12/21 09:30:00. Under 'Set Time' (设置时间), the 'Manually Set System Time' (手动设置系统时间) option is selected. The date is set to 2019/12/21 (YYYY/MM/DD) and the time is set to 09:27:08 (HH:MM:SS). There are buttons for 'Get Management Host Time' (获取管理主机时间) and 'Set' (设置).

图 14-14 手动设置系统时间

当前时间	显示当前系统时间。
设置时间	选择“手动设置系统时间”。
日期	手动设置系统日期。
时间	手动设置系统时间。
获取管理主机时间	点击按钮可以获取当前主机的系统时间。

表 14.7 时间设置界面项说明



说明：

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

14.6 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

日志设置

选择系统日志等级

所有等级 ▼

选择系统日志模块类别

所有模块 ▼

发送日志

服务器地址: 0.0.0.0

日志列表

🔄 刷新
☑️ 自动刷新
🗑️ 全部删除
📄 导出日志

序号	时间	功能模块	日志等级	日志内容
1	2019-12-21 08:57:56	CLOUD	通知信息	从云端获取固件列表：-3002
2	2019-12-21 08:04:15	WEB	通知信息	admin(IP:192.168.1.3) 成功登陆设备Web管理系统!

图 14-15 日志界面

日志设置

<p>选择系统日志等级</p>	<p>勾选后，将弹出系统日志等级复选框以供您查看特定等级的系统日志信息。</p> <ul style="list-style-type: none"> • 所有等级：查看所有等级的日志信息。 • 致命错误：导致系统不可用的错误。 • 紧急错误：必须对其采取紧急措施的错误。 • 严重错误：导致系统处于危险状态的错误。 • 一般错误：一般性的错误提示。 • 警告信息：系统仍然正常运行，但可能存在隐患的提示信息。 • 通知信息：正常状态下的重要提示信息。 • 信息报告：一般性的提示信息。 • 调试信息：调试过程中产生的信息。
<p>选择系统日志模块类别</p>	<p>勾选后，可查看特定模块的日志信息</p>
<p>发送日志</p>	<p>勾选后，将日志信息发送到特定的服务器中</p>

日志列表

启用自动刷新后，日志列表将每隔5秒刷新一次；选择日志等级可使日志列表中列出指定等级的日志记录。

14.7 系统参数

进入界面：系统工具 >> 系统参数 >> Metric 设置

您可以通过本页面设置逻辑接口的路由Metric信息。

metric设置

静态IP接口: (0-15)

DHCP接口: (0-15)

PPPOE接口: (0-15)

L2TP接口: (0-15)

PPTP接口: (0-15)

静态 IP 接口	填写静态拨号时的路由Metric信息。
----------	---------------------

图 14-16 系统参数设置界面

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

表 14.8 系统参数界面项说明

14.8 告警器

进入界面：系统工具 >> 告警器

路由器带有报警输出端口，正常工作时，继电器短路；报警事件出发后，继电器断路。满足以下三个条件中的任意一个，继电器输出报警信号：

- 电源告警：两路或以上电源接入正常供电时，告警器不会告警，只有一路电源或无电源接入时，告警器会告警。
- DI 报警：外部通过数字输入端口输入高店铺或低电平报警。
- 端口终端故障报警功能开启，且对应端口出现中断故障。

通过 web 管理页面可配置电源告警和 DI 告警，通过路由器的拨码开关可配置端口终端故障报警。

告警器设置

电源告警: 开启 关闭

DI告警: 开启 关闭

DI状态: 高状态告警 低状态告警

电源告警	开启后，两路或以上电源接入正常供电时，告警器不会告警，只有一路电源或无电源接入时，告警器会告警。
DI 告警	开启或关闭DI告警功能。
DI 状态	DI 高状态：当 DI 接口监测的电压值为 13V-30V 时，告警器告警，其余电压值不确保是否告警。 DI 低状态：当 DI 接口监测的电压值为-30V-3V 时，告警器告警，其余电压值不确保是否告警。

第15章 典型配置举例

15.1 组网需求

某制造工厂约有500人，需要组建一个安全、稳定的网络来保证车间产线的自动化生产，详细需求如下：

- 3) 企业有销售部和生产车间两个主要部分，生产车间分为车间1和车间2两个小部份，为了信息安全要求各部门网络相互隔离；
- 4) 各地分工厂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；
- 5) 公司从电信、联通各办理了10M光纤接入，为销售部员工提供上网服务，同时要求对上网流向做选路，实现“电信走电信，联通走联通”；
- 6) 公司有两个服务器群，一个位于广域网区，对广域网用户和销售部职员全天候开放，对车间职员在非工作时间开放；另一个位于工作区，供工厂职工工作中使用；
- 7) 需要防范来自企业内部的ARP欺骗和攻击；
- 8) 需要防范DoS等常见攻击；
- 9) 需要防止某些员工使用迅雷、BT等P2P软件占用网络资源；
- 10) 需要对网络各种流量进行实时监控以确保网络稳定运行；

15.2 组网方案及特点

为满足上述网络需求，使用 TL-ER6225G 工业级进行组网，网络拓扑如下图所示。

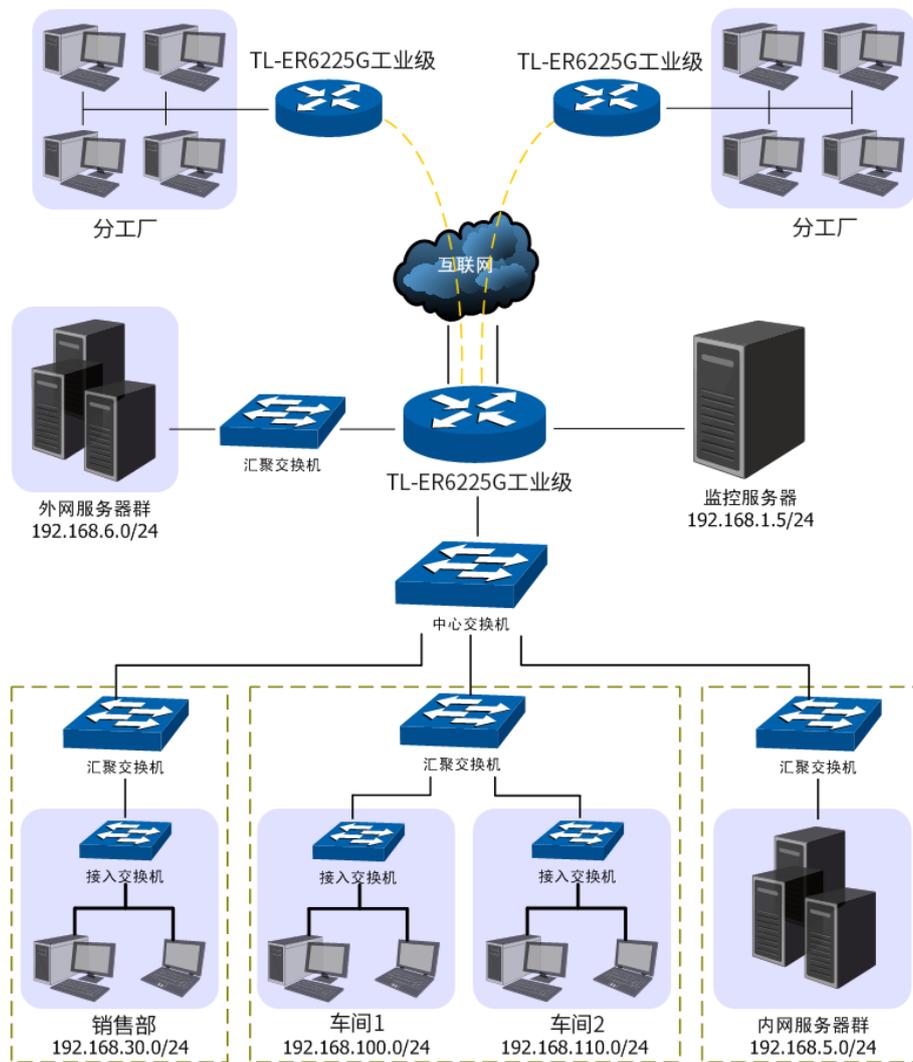


图 15-1 企业整体组网应用

现根据网络需求做简单的分析：

- 11) 为了实现各部门网络相互隔离，可以在各交换机上通过VLAN相互隔离，在TL-ER6225G工业级上分别属于相应接口并通过访问策略功能进一步限制各部门之间的网络通信；
- 12) 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；
- 13) 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；
- 14) 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；
- 15) 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；

- 16) 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；
- 17) 启用发送免费ARP包功能，实现局域网ARP防欺骗；
- 18) 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；
- 19) 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；
- 20) 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；

15.3 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 15.1，在后面的配置步骤中将使用表格中的参数进行举例。

接口名称	描述	物理端口	VLAN	网段
Dep1	车间 1	1	100	192.168.100.0/24
Dep2	车间 2	1	110	192.168.110.0/24
sell	销售部门	1	30	192.168.30.0/24
server	办公服务器群	1	5	192.168.5.0/24
dmz	公网服务器群	2	6	192.168.6.0/24
isp1	电信	3	10	201.1.1.1/24
isp2	联通	4	20	/

表 15.1 网络参数说明

初始状态下计算机可以连接到路由器的端口5来对路由器进行配置。请确保计算机IP地址与路由器的管理接口在同一网段。出厂情况下，路由器上已建立有唯一的物理接口GE5，IP地址为192.168.1.1/24，请将管理计算机的IP地址设为同一网段。访问路由器时，在Web浏览器的地址栏中输入“http://192.168.1.1”，按下回车键后出现登录窗口，输入用户名：admin，密码：admin，点击<登录>按钮即可进入路由器Web配置界面。



说明：

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

根据15.2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。

15.3.1 配置 VLAN

由表 15.1可知，本组网需要创建VLAN 5 /6 /10 /20 /30 /100 /110，请在交换机上进行创建。

15.3.2 配置接口

根据网络分析可知，本组网需要根据业务特性将网络划分成DEP、SELL、SERVER、DMZ、ISP1和ISP2六个部分。其中DEP需要创建两个Ethernet类型接口，分别指向局域网中的车间1和车间2，而ISP1和ISP2则分别需要根据网络接入方式来创建接口，下面将详细介绍此组网中所需要建立的接口。

■ 创建Ethernet接口

进入界面：基本设置 >> 接口设置>>接口设置

选择物理接口GE1，点击<  新增 >按钮，为车间1创建Ethernet接口dep1。具体参数设置如下图所示。

接口设置

1  2  3  4  5 

选择物理接口: GE1

+ 新增 - 删除

□	序号	接口类型	接口名称	连接状态	IP地址	子网掩码	网关地址	设置
--	--	--	--	--	--	--	--	--

接口类型: Ethernet ▼

接口名称: dep1 (1-12个字符)

关联接口: GE1 ▼

关联VLAN: 100 UNTAG

连接方式: 静态IP ▼

IP地址: 192.168.100.0

子网掩码: 255.255.255.0

网关地址: (可选)

上行带宽: 1000000 Kbps (100-1000000)

下行带宽: 1000000 Kbps (100-1000000)

MTU: 1500 (576-1500)

首选DNS服务器: (可选)

备用DNS服务器: (可选)

MAC地址: 54-A7-03-2F-53-22

备注: (可选,50个字符)

管理接口开启:

确定 取消

1	物理接口	GE1	未连接 详细	---	---	---	 
---	------	-----	------------------------	-----	-----	-----	---

图 15-2 接口设置界面-创建车间1Ethernet接口

根据表 15.1中的参数，重复上述操作为各部门创建Ethernet类型接口，此处将不重复介绍。



说明：

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

■ 创建其他接口

进入界面：基本设置 >> 接口设置 >> 接口设置

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

接口设置

选择物理接口: GE4

□	序号	接口类型	接口名称	连接状态	IP地址	子网掩码	网关地址	设置
--	--	--	--	--	--	--	--	--

新增 删除

接口类型: PPPoE

接口名称: isp2 (1-12个字符)

关联接口: GE4

用户名: user

密码: ●●●●

连接方式: 自动连接

上行带宽: 10000 Kbps (100-1000000)

下行带宽: 10000 Kbps (100-1000000)

MTU: (576-1492)

服务名: (1-128个字符, 可选)

首选DNS服务器: (可选)

备用DNS服务器: (可选)

备注: (可选, 50个字符)

管理接口开启:

确定 取消

图 15-3 创建联通网络接口

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

15.3.3 配置流量均衡

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

■ 配置智能均衡

进入界面：传输控制 >> 流量均衡 >> 基本设置

在界面中选择两个外线接口进行流量均衡，点击<设置>按钮完成配置。

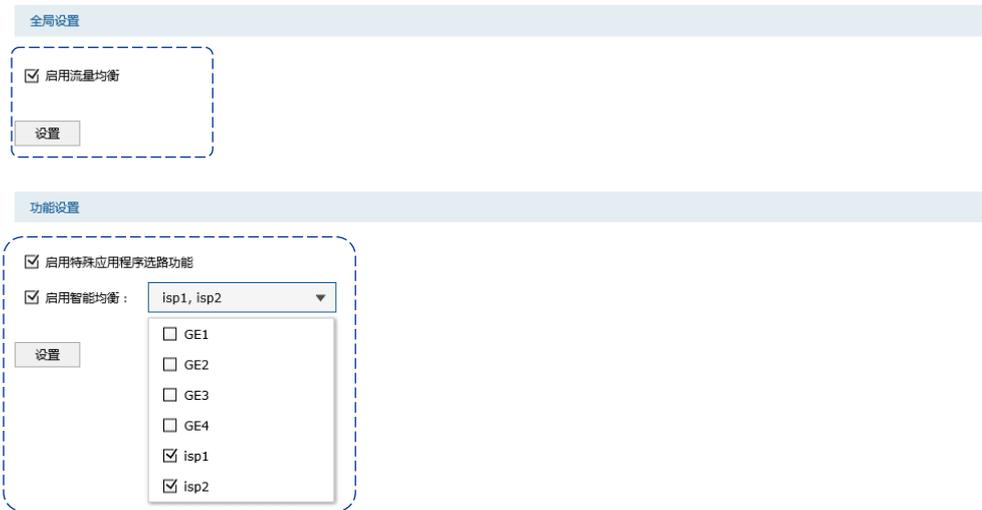


图 15-4 设置智能均衡

■ 配置ISP选路

进入界面：传输控制 >> 流量均衡 >> ISP选路

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



图 15-5 全局启用 ISP 选路功能



图 15-6 设置 ISP 选路

配置在线检测

进入界面：传输控制 >> 流量均衡 >> 在线检测

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



图 15-7 设置isp1在线检测



图 15-8 设置isp2在线检测

15.3.4 配置对象

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

■ 创建用户对象

进入界面：对象管理 >> 地址管理 >> 地址

输入用户地址段名称，设置地址段，如下图所示操作，点击<确定>按钮完成配置。

<input type="checkbox"/>	序号	地址名称	IP类型	IP段	备注	设置
--	--	--	--	--	--	--

地址名称： (1-32个字符)

IP类型： IP段 IP/Mask

/

备注： (可选，1-50个字符)

图 15-9 地址设置界面-创建软件职员地址段

进入界面：对象管理 >> 地址管理 >> 地址组

点击<+ 新增>按钮，创建新的地址组。

<input type="checkbox"/>	序号	地址名称	IP类型	IP段	备注	设置
--	--	--	--	--	--	--

组名称： (1-28个字符)

地址名称：

备注： (可选，1-50个字符)

- dep1
- dep2
- sell
- server
- dmz
- ips1

--	1			---	IPGROUP_ANY	---
--	2			---	中国所有IP地址	---
--	3	ISP_CHINA_TELECOM		---	中国电信	---
--	4	ISP_UNICOM_CNC		---	中国联通/网通	---
--	5	ISP_CMCC_CRTC		---	中国移动/铁通	---
--	6	ISP_CERNET		---	中国教育网	---
--	7	ISP_CN_OTHERS		---	中国其他ISP	---
<input type="checkbox"/>	8	dep1_IP		dep1	---	

图 15-10 地址组设置界面-创建地址组

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

■ 创建时间对象

进入界面：对象管理 >> 时间管理 >> 时间管理

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

□	序号	时间对象名称	工作时间	备注	设置
--	--	--	--	--	--

时间对象名称:

时间设置: 工作日历 手动设置

工作日历: 

备注: (可选)

图 15-11 时间对象设置界面-创建日常工作日历

系统时间: 2016年 1月 28日 星期四 10:44:45 GMT+08:00

	星期一	星期二	星期三	星期四	星期五	星期六	星期日
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00	■	■	■	■	■		
09:00	■	■	■	■	■		
10:00	■	■	■	■	■		
11:00	■	■	■	■	■		
12:00	■	■	■	■	■		
13:00	■	■	■	■	■		
14:00	■	■	■	■	■		
15:00	■	■	■	■	■		
16:00	■	■	■	■	■		
17:00	■	■	■	■	■		
18:00	■	■	■	■	■		
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							

■ 时间

图 15-12 工作日历设置界面-设置工作时间对象

15.3.5 配置访问策略

在本网络中，对各网段间的访问有严格的限制，因此需要设置丰富的访问策略规则。

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

网段通信；ISP1和ISP2网段不能与SERVER、DEP网段通信；DMZ网段不能与SERVER网段通信，工作时间不能与DEP网段通信。

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

■ 配置地址对象和时间对象

在对象管理中，为车间部门创建一个地址组“DEP_IP”，为外网服务器群创建一个地址组“dmz_IP”，并创建时间对象“worktime”。

■ 配置访问规则

进入界面：安全管理 >> 访问控制 >> 访问控制

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

<input type="checkbox"/>	序号	规则名称	源地址范围	目的地址范围	策略类型	服务类型	生效接口域	生效时间	设置
<input type="checkbox"/>	--	--	--	--	--	--	--	--	--

规则名称: (1-50个字符)

策略类型: 阻塞 ▼

服务类型: ALL ▼

生效接口域: GE1 ▼

源地址范围: DEP_IP ▼

目的地址范围: dmz_IP ▼

生效时间: worktime ▼

添加到指定位置(第几条): (可选)

图 15-13 网段间访问规则设置界面-选择网段

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

<input type="checkbox"/>	序号	规则名称	源地址范围	目的地址范围	策略类型	服务类型	生效接口域	生效时间	设置
<input type="checkbox"/>	1	rule1	DEP_IP	dmz_IP	阻塞	ALL	GE1	worktime	 
<input type="checkbox"/>	2	rule2	dmz_IP	DEP_IP	阻塞	ALL	GE2	worktime	 

图 15-14 网段间访问规则设置界面-设置DEP/DMZ访问规则

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

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

15.3.6 配置 NAT

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

■ 配置NAPT

进入界面：传输控制 >> NAT设置 >> NAPT

在界面的设置区域，设置销售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。

<input type="checkbox"/>	序号	规则名称	出接口	源地址范围	状态	备注	设置
<input type="checkbox"/>	--	--	--	--	--	--	--

规则名称:

出接口:

源地址范围: /

状态: 启用

备注:

图 15-15 NAPT设置界面-设置销售部共享上网

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

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

图 15-16 NAPT设置界面-查看销售部门NAPT转发规则

■ 配置一对一NAT

进入界面：传输控制 >> NAT设置 >> 一对一NAT

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

□	序号	规则名称	出接口	映射前地址	映射后地址	DMZ转发	备注	状态	设置
--	--	--	--	--	--	--	--	--	--

规则名称:

出接口:

映射前地址:

映射后地址:

DMZ转发: 启用

备注:

状态: 启用

图 15-17 一对一NAT设置界面-设置公网服务器的一对一NAT规则

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



说明：

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

15.3.7 配置 VPN

该企业有多个分工厂，假设某分工厂的路由器WAN口地址为116.31.85.133，LAN网段为172.31.10.0/24。分支机构中的主机希望能访问企业总部服务器，则可以通过在总部和分支机构部署TP-LINK企业VPN路由器来搭建VPN隧道，实现安全通信的需求。本文中以IPsec为例进行企业总部的VPN设置说明，以本地路由器的isp1接口与分公司的路由器配置IPsec隧道。



说明：

- 分公司的 VPN 路由器上也需要做对应的 IPsec 设置。

进入界面：VPN >> IPsec >> IPsec安全策略

□	序号	策略名称	对端网关	本地子网范围	对端子网范围	状态	设置
--	--	--	--	--	--	--	--

点击 <  新增 > 按钮并进行如下配置：

■ 创建IPSec安全策略

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

策略名称：	proposal_IKE_1	(1-32个字符)
对端网关：	116.31.85.133	(IP地址或域名)
绑定接口：	GE3	
本地子网范围：	192.168.6.0 / 24	
对端子网范围：	172.31.10.0 / 24	
预共享密钥：	12345678	(1-128个字符)
状态：	<input checked="" type="checkbox"/> 启用	

图 15-18 创建IPSec安全策略

■ 阶段1设置

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



说明：

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

阶段1设置

安全提议:	md5-3des-dh1	▼
安全提议:	---	▼
安全提议:	---	▼
安全提议:	---	▼
交换模式:	<input checked="" type="radio"/> 主模式	<input type="radio"/> 野蛮模式
协商模式:	<input checked="" type="radio"/> 初始者模式	<input type="radio"/> 响应者模式
本地ID类型:	<input checked="" type="radio"/> IP地址	<input type="radio"/> NAME
本地ID:	<input type="text"/>	(1-28个非空字符)
对端ID类型:	<input checked="" type="radio"/> IP地址	<input type="radio"/> NAME
对端ID:	<input type="text"/>	(1-28个非空字符)
生存时间:	3600	秒(60-604800)
DPD检测开启:	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
DPD检测周期:	30	秒(1-300)

图 15-19 设置 IKE 安全策略

■ 阶段2设置

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

阶段2设置

封装模式: 隧道模式 传输模式

安全提议: esp-md5-3des

安全提议: ---

安全提议: ---

安全提议: ---

PFS: modp768

生存时间: 3600 秒(120-604800)

图 15-20 设置IPSec安全提议

■ 查看IPsec安全联盟

进入界面：VPN >> IPSec >> IPSec 安全联盟

两端IPSec VPN连接成功后，可进入“IPSec安全联盟”标签页查看连接信息。

IPSec安全联盟列表

条目数量: 2 刷新

<input type="checkbox"/>	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

图 15-21 查看IPSec安全联盟

15.3.8 配置应用限制

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

■ 配置用户组

进入界面：对象管理 >> 地址管理 >> 地址

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

□	序号	地址名称	IP类型	IP段	备注	设置
--	--	--	--	--	--	--
<p>地址名称: <input type="text" value="sell"/> (1-32个字符)</p> <p>IP类型: <input type="radio"/> IP段 <input checked="" type="radio"/> IP/Mask</p> <p><input type="text" value="192.168.30.1"/> / <input type="text" value="24"/></p> <p>备注: <input type="text"/> (可选, 1-50个字符)</p> <p><input type="button" value="确定"/> <input type="button" value="取消"/></p>						

图 15-22 地址设置界面-创建销售部职员地址段

进入界面：对象管理 >> 地址管理 >> 地址组

输入销售部职员地址组的名称为SELL_IP，点击<  新增 >按钮完成配置。

□	序号	组名称	地址名称	备注	设置
--	--	--	--	--	--
<p>组名称: <input type="text" value="SELL_IP"/> (1-28个字符)</p> <p>地址名称: <input type="text" value="sell"/> ▼</p> <p>备注: <input type="text"/> (可选, 1-50个字符)</p> <p><input type="button" value="确定"/> <input type="button" value="取消"/></p>					

图 15-23 地址组设置界面-创建销售部职员地址组

■ 进入界面配置应用限制

进入界面：行为管控 >> 应用控制 >> 应用控制

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



图 15-24 设置应用限制

15.3.9 配置局域网 ARP 攻击防护

通过在路由器上绑定局域网设备的IP地址和MAC地址，可以避免局域网中的ARP攻击。在本路由器上，可以采用ARP扫描和手动设置两种方式绑定IP与MAC信息。首次设置时，可以使用ARP扫描来获取局域网大部分的ARP信息，然后通过手动设置绑定个别特殊条目。

■ ARP扫描并绑定

进入界面：安全管理 >> ARP防护 >> ARP扫描

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

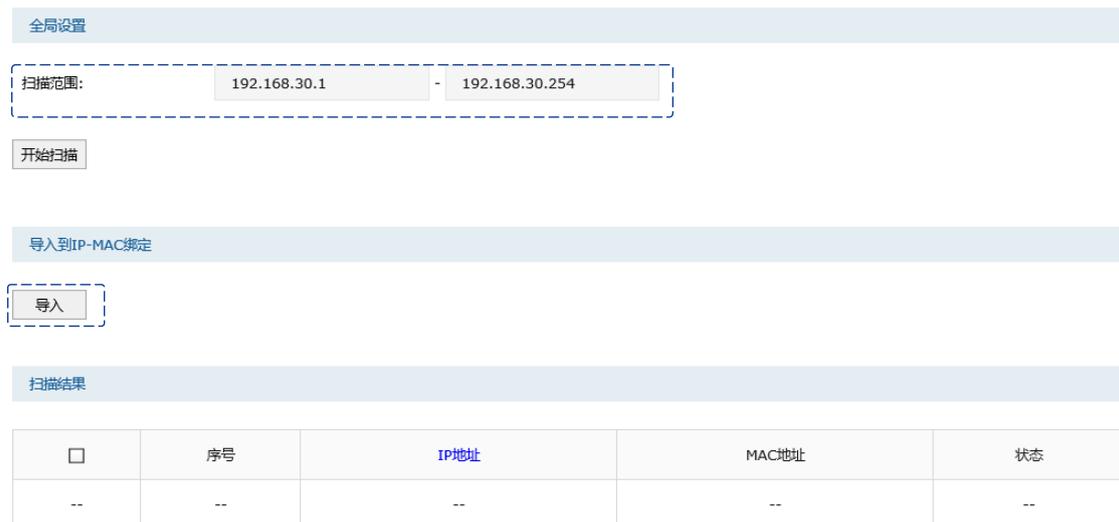


图 15-25 ARP扫描并绑定

■ 手动绑定ARP信息

进入界面：安全管理 >> ARP防护 >> IP-MAC绑定

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



图 15-26 手动绑定ARP信息

■ 设置ARP攻击防护功能

进入界面：安全管理 >> ARP防护 >> IP- MAC绑定

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



图 15-27 设置ARP防护功能

15.3.10 配置攻击防护

进入界面：安全管理 >> 攻击防护 >> 攻击防护

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



图 15-28 设置攻击防护功能

15.3.11 配置内网流量统计

■ 流量统计

进入界面：系统工具 >> 流量统计 >> 接口流量统计

在界面中，可以查看路由器各接口的流量统计结果，如下图所示。

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

图 15-29 查看接口流量统计结果

进入界面：系统工具 >> 流量统计 >> IP 流量统计

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

功能设置

启用IP流量统计

监控IP范围: 192.168.1.0 / 255.255.255.0

设置

流量统计列表

IP数量: 0 刷新

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

图 15-30 查看IP流量统计结果

第16章 附录 A 常见问题

问题 1：无法登录路由器 Web 管理界面该如何处理？

- 1) 观察指示灯的状态，检查相应端口线缆是否正常连接，同时确认端口没有被禁用，可以换另外一个物理端口登录路由器。
- 2) 如果是通过本地计算机管理路由器，请确保计算机IP地址与路由器IP地址处于同一网段。
- 3) 通过Ping命令检查网络连接。通过“开始” “运行”输入“cmd”命令，点击“确定”后，可以打开命令窗口。输入ping 127.0.0.1检查计算机的TCP/IP协议是否安装；输入ping 192.168.1.1(路由器管理接口的IP地址，如果路由器设有多个管理接口，也可以ping其它管理接口的IP地址) 检查计算机与路由器的连接是否正常。
- 4) 如果确认物理连接正常，但是还是无法管理，建议通过Console口管理路由器，检查路由器VLAN和管理IP相关配置信息。
- 5) 如果修改过路由器的管理端口，则注意下次登录时需要以“http://管理IP:XX”的方式登录，XX为修改后的端口号，如http://192.168.1.1:8080。
- 6) 如果恢复出厂配置后仍然无法登录或开始一段时间能登录，但过一段时间后又不能登录，则可能是遭受了ARP欺骗，建议查找欺骗源、查杀病毒或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。

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)。

第17章 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 802.3i、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x、IEEE 802.1x、IEEE 802.1q、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	PWR1/2/3电源指示灯、FAULT/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	DC输入电压：12/24/48VDC(9.6~ 60VDC) 输入电流：1.1A@24V
工作温度	-40℃ -75℃
存储温度	-40℃ -85℃
工作湿度	10% ~ 90%RH 不凝结
存储湿度	5% ~ 90%RH 不凝结