



主要功能配置实例

ER2/3/5/6/7/8系列企业级路由器

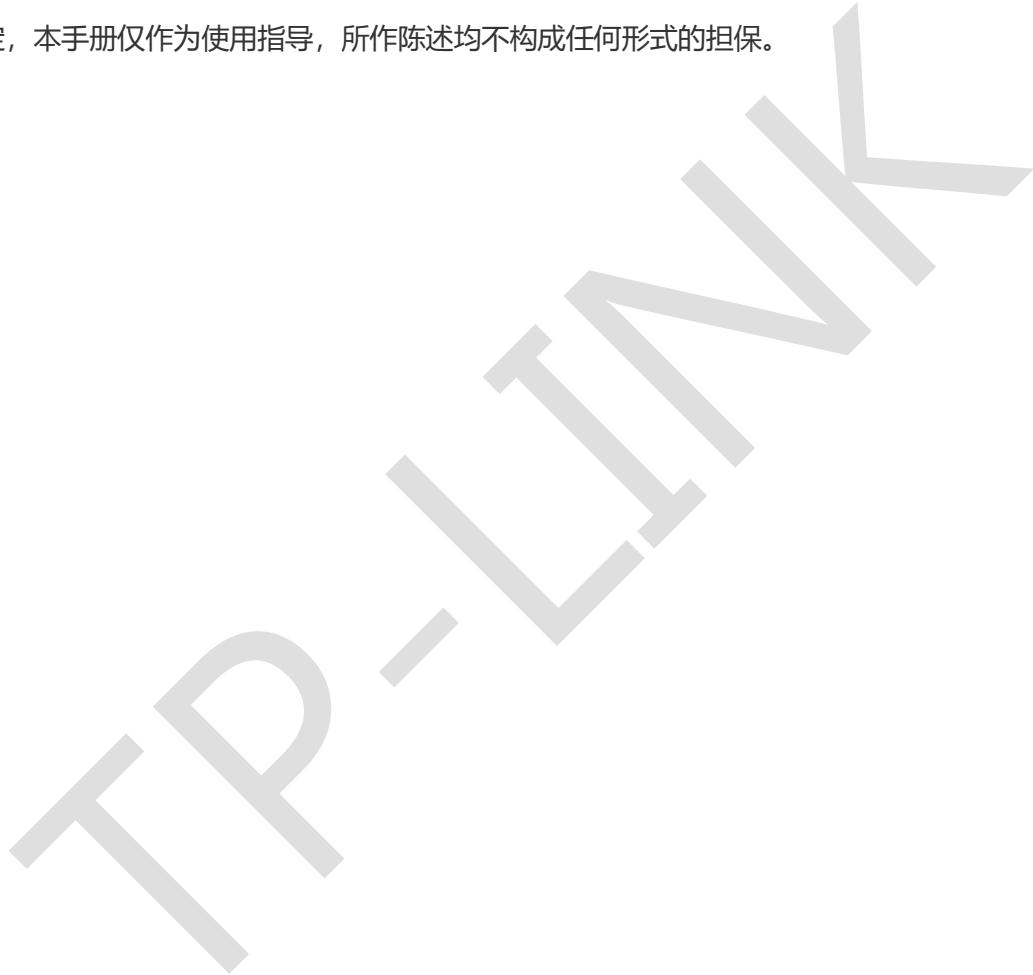
声明

Copyright © 2021 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
1.3	适用机型	1
第2章	基础联网设置	3
2.1	【ER3/5/6 系列】企业路由器基本设置指南	3
2.1.1	应用介绍	3
2.1.2	需求分析	3
2.1.3	线路连接	3
2.1.4	设置方法	3
2.2	【ER3/5/6 系列】企业路由器 IPv6 上网配置指导	9
2.2.1	应用介绍	9
2.2.2	需求介绍	9
2.2.3	设置方法	9
2.2.4	IPv6 常见问题解答	12
2.3	【ER7/8 系列】企业路由器基本设置指南	15
2.3.1	应用介绍	15

2.3.2	需求分析	15
2.3.3	设置方法	15
2.4	【ER7/8 系列】企业路由器 IPv6 上网配置指导	29
2.4.1	应用介绍	29
2.4.2	需求介绍	29
2.4.3	设置方法	29
2.4.4	IPv6 常见问题解答.....	34
2.5	【ER7/8 系列】如何设置实现一口多拨?	37
2.5.1	应用介绍	37
2.5.2	应用拓扑	37
2.5.3	设置方法	38
第 3 章	设备管理.....	48
3.1	如何在外网远程管理（控制）路由器?	48
3.1.1	应用介绍	48
3.1.2	设置方法 1-远程 WEB 管理	48
3.1.3	设置方法 2-商云管理	52
3.2	如何设置自动重启?	57
3.2.1	应用介绍	57

3.2.2	需求分析	57
3.2.3	设置方法	57
第4章	多带宽均衡.....	59
4.1	多 WAN 口路由器负载均衡的设置指南.....	59
4.1.1	应用介绍	59
4.1.2	需求介绍	59
4.1.3	工作原理	59
4.1.4	设置方法	60
第5章	路由转发模块	62
5.1	策略路由设置指南	62
5.1.1	应用介绍	62
5.1.2	需求分析	63
5.1.3	设置方法	63
5.2	ISP 选路设置指南	67
5.2.1	应用介绍	67
5.2.2	需求分析	68
5.2.3	设置方法	68
5.3	静态路由设置指南	70

5.3.1 应用介绍	70
5.3.2 需求分析	70
5.3.3 设置方法	71
5.4 线路备份设置指南	73
5.4.1 应用介绍	73
5.4.2 设置方法	73
5.5 虚拟服务器设置指南	75
5.5.1 应用介绍	75
5.5.2 需求分析	75
5.5.3 设置方法	76
5.6 NAT-DMZ 功能设置指南	78
5.6.1 应用介绍	78
5.6.2 需求分析	78
5.6.3 设置方法	79
第 6 章 AP 和易展管理	80
6.1 AP 管理设置指南	80
6.1.1 应用介绍	80
6.1.2 需求分析	80

6.1.3	设置方法	80
6.2	易展 AP 设置指南	86
6.2.1	应用介绍	86
6.2.2	需求分析	86
6.2.3	网络拓扑	87
6.2.4	设置方法	87
第 7 章	行为管控	92
7.1	连接数限制设置指南	92
7.1.1	应用介绍	92
7.1.2	需求分析	92
7.1.3	设置方法	92
7.1.4	疑问解答	93
7.2	URL 过滤设置指南	95
7.2.1	应用介绍	95
7.2.2	需求分析	95
7.2.3	设置方法	95
7.2.4	疑问解答	99
7.3	访问控制设置指南	101

7.3.1	应用介绍	101
7.3.2	需求分析	101
7.3.3	设置方法	101
7.3.4	疑问解答	105
7.4	应用限制设置指南	107
7.4.1	应用介绍	107
7.4.2	需求分析	107
7.4.3	设置方法	107
7.5	网址过滤设置指南	111
7.5.1	应用介绍	111
7.5.2	需求分析	111
7.5.3	设置方法	111
7.5.4	疑问解答	116
7.6	网页安全设置指南	118
7.6.1	应用介绍	118
7.6.2	需求分析	118
7.6.3	设置方法	118
第 8 章	安全防护.....	121

8.1	ARP 防护设置指南	121
8.1.1	应用介绍	121
8.1.2	设置方法	121
8.1.3	疑问解答	126
8.2	MAC 地址过滤设置指南	128
8.2.1	应用介绍	128
8.2.2	设置方法	128
第 9 章	VPN 模块	130
9.1	IPsec VPN 设置指南	130
9.1.1	应用介绍	130
9.1.2	需求介绍	130
9.1.3	设置方法	131
9.2	L2TP VPN 设置指南	138
9.2.1	应用介绍	138
9.2.2	需求介绍	138
9.2.3	应用拓扑	139
9.2.4	L2TP 站点到站点设置方法	139
9.2.5	L2TP PC 到站点设置方法	144

9.2.6	常见问题解答	145
9.3	PPTP VPN 设置指南	147
9.3.1	应用介绍	147
9.3.2	需求介绍	147
9.3.3	应用拓扑	148
9.3.4	PPTP 站点到站点设置方法	148
9.3.5	PPTP PC 到站点设置方法	153
9.3.6	常见问题解答	154
9.4	L2TP VPN 代理上网设置指南	156
9.4.1	应用介绍	156
9.4.2	需求介绍	156
9.4.3	应用拓扑	156
9.4.4	设置方法	156
9.5	PPTP VPN 代理上网设置指南	161
9.5.1	应用介绍	161
9.5.2	需求介绍	161
9.5.3	应用拓扑	161
9.5.4	设置方法	161

9.6	SSL VPN 功能设置指南	166
9.6.1	应用介绍	166
9.6.2	需求介绍	166
9.6.3	应用拓扑	166
9.6.4	设置方法	167
第 10 章	认证管理.....	173
10.1	一键上网设置指南	173
10.1.1	应用介绍	173
10.1.2	需求分析	173
10.1.3	应用拓扑	173
10.1.4	设置方法	174
10.2	短信认证设置指南	178
10.2.1	应用介绍	178
10.2.2	需求分析	178
10.2.3	应用拓扑	178
10.2.4	设置方法	179
10.3	Portal 认证设置指南—使用内置 WEB 服务器和内置认证服务器	187
10.3.1	应用介绍	187

10.3.2 需求分析	187
10.3.3 应用拓扑	187
10.3.4 设置方法	188
10.4 Portal 认证设置指南—使用内置 WEB 服务器和外部认证服务器	193
10.4.1 应用介绍	193
10.4.2 需求分析	193
10.4.3 应用拓扑	193
10.4.4 设置方法	194
10.5 Portal 认证设置指南—使用外置 WEB 服务器和内置认证服务器	199
10.5.1 应用介绍	199
10.5.2 需求分析	199
10.5.3 应用拓扑	199
10.5.4 设置方法	200
10.6 Portal 认证设置指南—使用外置 WEB 服务器和外置认证服务器	204
10.6.1 应用介绍	204
10.6.2 需求分析	204
10.6.3 应用拓扑	204
10.6.4 设置方法	205

10.7 免认证策略的使用方法.....	210
10.7.1 应用介绍	210
10.7.2 需求分析	210
10.7.3 应用拓扑	210
10.7.4 设置方法	211
10.8 Portal 认证中外部 WEB 服务器建立规范.....	214
10.8.1 应用介绍	214
10.8.2 流程规范	214
10.8.3 实现流程	215
第 11 章 工业级特性.....	219
11.1 如何使用工业级路由器?	219
11.1.1 应用介绍	219
11.1.2 需求分析	219
11.1.3 应用拓扑	220
11.1.4 设置方法	220
第 12 章 其他功能.....	226
12.1 地址组的设置与管理	226
12.1.1 应用介绍	226

12.1.2	需求分析	226
12.1.3	设置方法	226
12.1.4	疑问解答	229
12.2	带宽控制设置指南	230
12.2.1	应用介绍	230
12.2.2	需求分析	230
12.2.3	设置方法	230
12.2.4	疑问解答	233
12.3	PPPOE 服务器应用设置指南	234
12.3.1	应用介绍	234
12.3.2	需求分析	234
12.3.3	设置方法	235
12.3.4	疑问解答	238
12.4	网络唤醒功能的使用指南	240
12.4.1	应用介绍	240
12.4.2	需求分析	240
12.4.3	设置方法	240
12.5	诊断工具的使用指南	243

12.5.1 应用介绍	243
12.5.2 需求分析	243
12.5.3 设置方法	243
12.6 DDNS 的使用指南.....	248
12.6.1 应用介绍	248
12.6.2 需求分析	248
12.6.3 设置方法	248
12.6.4 疑难解答	251

第1章 前言

本手册旨在帮助您正确使用 TP-LINK ER 2/3/5/6/7/8 系列企业级路由器。内容包含配置路由器各个模块功能的配置实例和详细说明。请在操作前仔细阅读本手册。

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

- 用 >> 符号表示配置界面的进入顺序。默认为一级菜单 >> 二级菜单 >> 标签页，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字或图形，表示 Web 界面的按钮名称，如<确定>或< 新增 >。
- 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。

1.3 适用机型

本手册适用于以下路由器机型，部分功能仅特定型号支持，以产品实际页面为准。

产品型号	硬件版本
TL-ER2220G	1.0
TL-ER3210G	4.0、5.0
TL-ER3220G	4.0、5.0
TL-ER3229G	2.0
TL-ER5110G	4.0
TL-ER5120G	4.0
TL-ER5510G	4.0
TL-ER5520G	5.0
TL-ER6110G	4.0
TL-ER6120G	6.0
TL-ER6210G	3.0
TL-ER6220G	3.0
TL-ER6510G	3.0
TL-ER6520G	5.0
TL-ER6225G 工业级	1.0
TL-ER7520G	4.0
TL-ER8820T	1.0
TL-NR9202	1.0
TL-NR9302	1.0

第2章 基础联网设置

2.1 【ER3/5/6 系列】企业路由器基本设置指南

2.1.1 应用介绍

路由器已经成为家庭组网必备的产品，出厂设置下的路由器并不是买来就能够接入网络供终端上网，需要简单设置一下才能够上网，本文以 TL-ER6229GPE-AC 为例介绍 ER3/5/6 系列企业路由器的基本设置。

2.1.2 需求分析

路由器接入网络，电脑连接路由器能够正常上网。

2.1.3 线路连接

将前端上网的宽带线连接到路由器的 WAN 口，上网电脑连接到路由器任意一个 LAN 口。



2.1.4 设置方法

1、登录路由器管理界面

打开浏览器，清空地址栏并输入路由器的底部管理地址 192.168.1.1，在弹出的设置管理密码界面中，设置用户名及 6~15 位的管理密码，点击 **确定** 后路由器自动跳转到管理界面，输入设置的用户名和密码进入管理界面。

注意：请记住设置好的管理密码，用于后续管理路由器。





2、选择 WAN 口数量

按照快速设置向导设置 WAN 口数量，即外网线路数量。



3、选择 WAN 口上网方式

根据宽带类型选择 PPPoE、静态 IP 或者动态 IP 的上网方式。此处以**宽带拨号上网**为例，在对应设置框中选择 PPPoE 拨号，输入运营商提供的宽带账号和密码，并确定该账号密码输入正确，点击**下一步**。



4、设置 LAN 口上网参数及 AP 管理状态

根据网络规划设置 LAN 口的 IP 地址及子网掩码，同时选择设置 AP 管理状态为开启或者关闭。设置完成后点击连接网络，等待路由器完成配置并重启即可。



至此，路由器已经设置完成。电脑连接路由器后可以直接打开网页上网，**不用再使用电脑上的“宽带连接”来进行拨号了。**

如果您还有其他电脑需要上网，用网线直接将电脑连接在路由器任意一个空闲的 LAN 口即可上网。



2.2 【ER3/5/6 系列】企业路由器 IPv6 上网配置指导

2.2.1 应用介绍

全球所有 43 亿个 IPv4 地址已全部用完，意味着没有更多的 IPv4 地址可以分配给 ISP 和其它大型网络基础设施提供商，因此 Internet 研究组织发布新的主机标识方法，即 IPv6。目前国内的网络正在快速的向 IPv6 升级中，从网络基础设施如运营商骨干网、城域网，到互联网服务商如各类云服务，以及各类终端设备厂商如手机、电脑、路由器、交换机等。**目前运营商提供的 IPv6 线路主要分为支持前缀授权和不支持前缀授权两种，本文主要以 TL-ER6229GPE-AC 为例介绍 ER3/5/6 系列企业级路由器关于 IPv6 的上网配置和指导。**

2.2.2 需求介绍

终端获取到一个 IPv6 公网地址，实现端到端通信，减小网络转发开销；路由器 WAN 口可以同时获取到 IPv4 和 IPv6 地址，并且给支持双栈的终端分配 IPv4 和 IPv6 两个地址；终端访问 IPv4 的目标主机时走 IPv4，访问 IPv6 的目标主机时走 IPv6。

2.2.3 设置方法

支持前缀授权的 IPv6 线路上网设置方法

1、WAN 口参数设置

根据运营商提供的 IPv6 上网方式进行 WAN 口 IPv6 设置，并开启前缀授权功能，此处以 PPPoE 拨号为例（可以复用 IPv4 的拨号链路），拨号成功后可看到 WAN 口获取到 IPv6 地址。



2、LAN 口参数设置

IP 协议类型选择 IPv6，并点击启用，地址配置方式选择 EUI-64，前缀授权接口选择刚才设置好的 WAN 口 (EUI-64 表示自动获取 64 位 IPv6 的前缀地址)。



3、地址分配设置

根据需要设置 LAN 口 IPv6 地址分配方式, 可以选择 DHCPv6 或者 SLAAC (二选一), DNS 不填时默认为路由器的 IPv6 地址, 路由器作 DNS 代理。其中 DHCPv6 是路由器手动设置一个范围下发地址; SLAAC 是根据地址前缀路由器随机下发地址。

The screenshots show the configuration interface for IPv6 address allocation on the LAN interface.

Screenshot 1: DHCPv6 Service Configuration

- Basic Settings:**
 - Service Interface: LAN (selected)
 - Start Address: 240E:FE:3805:3900::1
 - End Address: 240E:FE:3805:3900::FF
 - Lease Time: 120 minutes (2-2880)
 - Primary DNS Server: 3:2000:56a7:3ff:fe3d:88ce (Optional)
 - Secondary DNS Server: (Optional)
 - Option 16: / (Optional)
 - Option 52: (Optional)
 - Status: Enabled (checked)

Screenshot 2: SLAAC Configuration

- Basic Settings:**
 - Service Interface: LAN
 - IPv6 Prefix: 240E:FE:380D:CE00::/64
 - DNS Configuration Method: DHCPv6
 - Primary DNS Server: (Optional)
 - Secondary DNS Server: (Optional)
 - Status: Enabled (checked)

4、电脑自动获取 IPv6 地址

设置好路由器的相关参数后，终端（电脑、手机等）勾选 IPv6 协议，并开启自动获取 IPv6 地址和 DNS 服务器即可，获取 IP 结果如下。



不支持前缀授权的 IPv6 线路上网设置方法

对于不支持前缀授权的运营商线路，无法由路由器给终端分配 IPv6 地址，终端 IPv6 地址统一由运营商进行分配，因此需要路由器支持 IPV6 桥模式，目前 ER3/5/6 系列暂不支持 IPv6 桥模式。

2.2.4 IPv6 常见问题解答

1、怎么判断宽带是否支持 IPv6？

有两种方式。①与宽带运营商确认线路是否支持 IPv6；②电脑直连猫拨号，看电脑是否获取到 IPv6 地址。

2、怎么判断 IPv6 线路是否支持前缀授权？

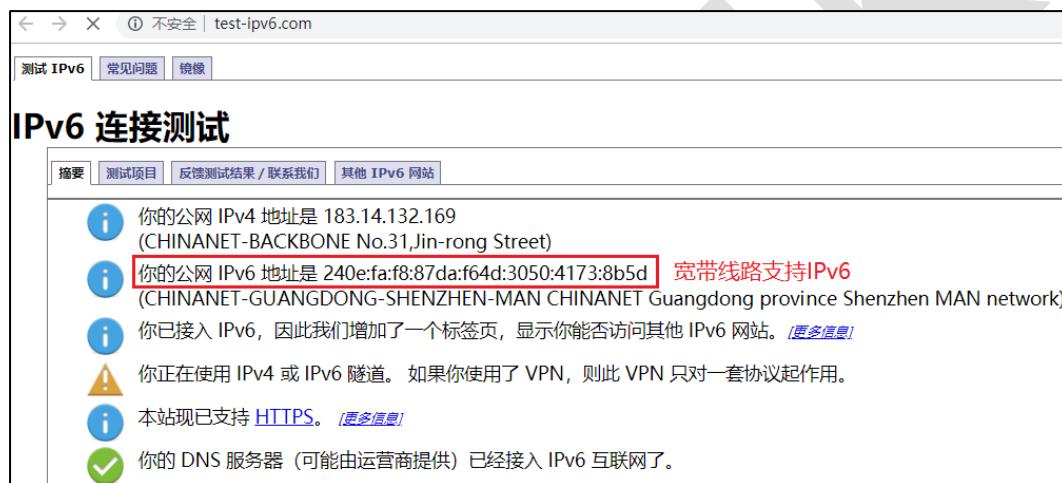
请致电宽带运营商确认。

3、怎么判断路由器是否支持 IPv6?

有两种方式。①登陆路由器管理界面→基本设置→有 IPv6 设置，则支持。②点击在线客服咨询人工客服。

4、怎么检测路由器获取的 IPv6 地址可以正常联网？

打开浏览器输入 www.test-ipv6.com，就可以看到线路是否支持 IPv6 了。



5、IPv6 支持哪些网络资源？

IPv6 目前还属于初步发展阶段，虽然多数网络资源都还未普及，但是校园教育资源和大型互联网企业资源（如谷歌、腾讯和百度等）已经铺展开来。

IPv6资源				
Baidu 百度	Tencent 腾讯	Google	Google Scholar	Microsoft 微软 学术
S 搜狗搜索	六维空间	阿里云	腾讯云	清华IPTV
YAHOO!	GitHub	爱奇艺	YOUKU 优酷	搜狐 视频
新华网 NEWS	凤凰网 ifeng.com	CNN	网易 NETEASE www.163.com	搜狐 SOHU.COM
淘宝网 Taobao.com	中国移动 China Mobile	中国电信 CHINA TELECOM	中国联通	CERNET
支付宝 ALIPAY	中国银行 BANK OF CHINA	Office 365	xkcd

6、IPv6 设置好上网后，能否通过 IPv6 地址远程访问路由器？

远程管理目前无法填写 IPv6 地址，推荐使用商云平台进行远程管理，更加方便。

7、IPv6 配置上网后，外网访问内网是否需要做映射？

不需要，每个 PC 是全球公网地址，IPv6 访问为纯路由模式，网络中直接访问设备即可。

8、开启 IPv6 后是否影响 IPv4 的资源访问？

不会，路由器支持 IPv4 和 IPv6 双栈协议，可以同时访问 IPv4 和 IPv6 的外网资源。

2.3 【ER7/8 系列】企业路由器基本设置指南

2.3.1 应用介绍

路由器已经成为家庭组网必备的产品，出厂设置下的路由器并不是买来就能够接入网络供终端上网，需要简单设置一下才能够上网，本文以 TL-ER7520G 为例介绍 ER7/8 系列企业路由器的基本设置。

2.3.2 需求分析

路由器接入网络，电脑连接路由器能够正常上网。

2.3.3 设置方法

TL-ER7520G 共有 5 个物理网络接口，支持 802.1Q VLAN，可以添加多个虚拟接口，通过自定义端口类型和参数实现多种组网需求。下面我们介绍常见的使用方式下，TL-ER7520G 的上网配置方法，主要包括以下类型：

1 个 WAN 口+4 个相同网段的 LAN 口

2 个 WAN 口+3 个相同网段的 LAN 口

1 个 WAN 口+4 个不同网段的 LAN 口

您可以根据自己的组网需求，选择查看对应类型。

1 个 WAN 口+4 个相同网段的 LAN 口

该类需求的网络拓扑如下，请按照设置步骤设置路由器：



1、登录路由器界面

TL-ER7520G 在出厂状态下未启用 DHCP 服务器，且必须通过 5 号接口来管理。请将管理电脑连接到路由器的 5 号接口，并且将电脑的本地连接手动配置为 192.168.1.X(2≤X≤254)。打开浏览器输入路由器的管理地址 192.168.1.1，输入默认用户名：admin、密码：admin。

2、设置 LAN 口

点击 **基本设置 > 接口设置 > 网桥设置**，点击，选择包含接口为 2、3、4、5，点击 确定，并重启，此时就可以将 2~5 号接口均添加为同一网段的 LAN 口：



注意：如果无法添加，确保路由器在出厂设置的状态。

3、设置 WAN 口上网

点击 **基本设置 > 接口设置**, 选择物理接口为 GE1, 若宽带上网方式为静态 IP/动态 IP,

请点击现有条目, 进行对应设置。

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
	1	物理接口	GE1	未连接 详细	---	---	---	

若宽带上网方式为 PPPoE 拨号, 请点击, 选择接口类型为 PPPoE, 填写对应的宽带账号密码, 点击 确定, 设置如下:

接口类型:	PPPoE
接口名称:	WAN_PPPoE (1-12个字符)
关联接口:	GE1
用户名:	075526611234@163.gd
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"/>
<input type="button" value="确定"/> <input type="button" value="取消"/>	

4、添加 DHCP 服务器

局域网电脑需要通过路由器自动获取 IP 地址上网, 请点击 基本设置 > DHCP 服务, 点击,

设置如下:

服务接口: LAN
开始地址: 192.168.1.100
结束地址: 192.168.1.199
地址租期: 120 分钟 (1-2880)
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)
状态: 启用
确定 取消

5、设置 NAPT 规则

点击 传输控制 > NAT 设置 > NAPT, 点击, NAPT 规则设置如下:

规则名称:	LAN_Internet
出接口:	WAN_PPPOE
源地址范围:	192.168.1.0 / 24
状态:	<input checked="" type="checkbox"/> 启用
备注:	
<button>确定</button> <button>取消</button>	

注意:出接口选择步骤 3 中配置联网的接口名称,此处以 WAN 口上网方式为 PPPoE 为例。

6、设置 DNS 代理

点击 系统服务 > DNS 代理, 点击, DNS 代理规则设置如下:

规则名称:	LAN_DNS
服务接口:	LAN
出接口:	auto
<button>确定</button> <button>取消</button>	

设置完成, 点击右上角 保存配置。电脑连接到任意一个 LAN 口下自动获取 IP 地址即可上网。

2 个 WAN 口+3 个相同网段的 LAN 口

该类需求的网络拓扑如下, 请按照设置步骤设置路由器:



1、登录路由器界面

TL-ER7520G 在出厂状态下未启用 DHCP 服务器，且必须通过 5 号接口来管理。请将管理电脑连接到路由器的 5 号接口，并且将电脑的本地连接手动配置为 192.168.1.X(2≤X≤254)。打开浏览器输入路由器的管理地址 192.168.1.1，输入默认用户名：admin、密码：admin。

2、设置 LAN 口

点击 基本设置 > 接口设置 > 网桥设置，点击，选择需要配置为 LAN 口的接口，点击 确定，添加后需要重启，如下：



3、设置 WAN 口上网

点击 基本设置 > 接口设置，选择物理接口为 GE1，若宽带上网方式为静态 IP/动态 IP，

请点击现有条目，进行对应设置。



选择物理接口:								
	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
	1	物理接口	GE1	未连接 详细	---	---	---	 

若宽带上网方式为 PPPoE 拨号，请点击，选择接口类型为 PPPoE，填写对应的宽带账号密码，点击 确定，设置如下：



接口类型:	PPPoE	
接口名称:	WAN_PPPoE	(1-12个字符)
关联接口:	GE1	
用户名:	075526611234@163.gd	
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"/>	
确定	取消	

同样的方法，选择物理接口为 GE2，并设置对应的上网方式。

4、添加 DHCP 服务器

局域网电脑需要通过路由器自动获取 IP 地址上网，点击 基本设置 > DHCP 服务，点击，

设置如下：

服务接口:	LAN
开始地址:	192.168.1.100
结束地址:	192.168.1.199
地址租期:	120 分钟 (1-2880)
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)
状态:	<input checked="" type="checkbox"/> 启用
<button>确定</button> <button>取消</button>	

5、设置 NAPT 规则

点击 传输控制 > NAT 设置 > NAPT，点击，NAPT 规则设置如下：

规则名称: LAN_Internet
出接口: WAN_PPPOE
源地址范围: 192.168.1.0 / 24
状态: 启用
备注:

确定 取消

同样的方法，添加出接口为 WAN2 的 NAPT 规则。添加完毕的 NAPT 规则列表如下：

NAPT规则列表							
	序号	规则名称	出接口	源地址范围	状态	备注	设置
	1	LAN_Internet_1	WAN1_PPPOE	192.168.1.0/24	已启用	---	
	2	LAN_Internet_2	WAN2_PPPOE	192.168.1.0/24	已启用	---	

6、设置 DNS 代理

点击 系统服务 > DNS 代理，点击，DNS 代理规则设置如下：

规则名称: LAN_DNS
服务接口: LAN
出接口: auto
确定 取消

设置完成，点击右上角 保存配置，接在 LAN 口下的电脑自动获取 IP 地址即可上网。

需要注意的是，如果其中一个 WAN 口连接专网（如企业内网或社保、教育专网），则需要在传输控制>路由设置>策略路由中添加出接口选路规则。

1 个 WAN 口+4 个不同网段的 LAN 口

该类需求的网络拓扑如下，请按照设置步骤设置路由器：



1、登录路由器界面

TL-ER7520G 在出厂状态下未启用 DHCP 服务器，且必须通过 5 号接口来管理。请将管理电脑连接到路由器的 5 号接口，并且将电脑的本地连接手动配置为 192.168.1.X(2≤X≤254)。打开浏览器输入路由器的管理地址 192.168.1.1，输入默认用户名：admin、密码：admin。

2、设置各个 LAN 口

5 口的默认 IP 为 192.168.1.1，即网段为 192.168.1.0/24，请保持不变。这一步需要做的是为 2、3、4 口配置不同网段的 IP 地址。

点击 基本设置 > 接口设置，选择物理接口为 GE2，并点击，对 2 口的配置如下：

The screenshot shows a configuration dialog for a network interface. The fields are as follows:

- 接口类型: 物理接口
- 接口名称: GE2 (1-12个字符)
- 连接方式: 静态IP
- IP地址: 192.168.2.1
- 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: 24-69-68-D5-5E-90
- 备注: (可选, 50个字符)
- 管理接口开启:

At the bottom are two buttons: 确定 (Confirm) and 取消 (Cancel).

注意：勾选 管理接口开启，则该网段下的电脑可以通过该接口管理路由器。

同样的方法，将 GE3 的 IP 地址配置为 192.168.3.1，GE4 的 IP 地址配置为 192.168.4.1。

3、设置 WAN 口上网参数

点击 基本设置 > 接口设置，选择物理接口为 GE1，若宽带上网方式为静态 IP/动态 IP，

请点击现有条目，进行对应设置。

选择物理接口: GE1

	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
	1	物理接口	GE1	未连接 详细	---	---	---	 

若宽带上网方式为 PPPoE 拨号, 请点击, 设置如下:

接口类型:	PPPoE
接口名称:	WAN_PPPoE (1-12个字符)
关联接口:	GE1
用户名:	075526611234@163.gd
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"/>
确定	取消

4、设置 DHCP 服务器

局域网电脑需要通过路由器自动获取 IP 地址上网, 点击 基本设置 > DHCP 服务, 点击, 设置如下:

服务接口:	GE5
开始地址:	192.168.1.100
结束地址:	192.168.1.199
地址租期:	120 分钟 (1-2880)
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)
状态:	<input checked="" type="checkbox"/> 启用
<input type="button" value="确定"/> <input type="button" value="取消"/>	

同样的方法，分别配置 GE2、GE3、GE4 的 DHCP 服务器。

5、设置 NAPT 规则

点击 传输控制 > NAT 设置 > NAPT，点击，NAPT 规则设置如下：

规则名称:	GE5_Internet
出接口:	GE1
源地址范围:	192.168.1.0 / 24
状态:	<input checked="" type="checkbox"/> 启用
备注:	
<input type="button" value="确定"/> <input type="button" value="取消"/>	

同样的方法，添加 GE2、GE3、GE4 接口所属网段的 NAPT 规则。

6、设置 DNS 代理

点击 系统服务 > DNS 代理，点击，DNS 代理规则设置如下：



同样的方法，添加 GE3、GE4、GE5 的 DNS 代理规则。

设置完成，点击右上角 保存配置。电脑自动获取 IP 地址即可上网。

如果您有更多配置需求，比如接口下需要连接三层交换机或者 LAN 口添加多个网段对接二层交换机（划分 802.1Q VLAN），请按照接口规则的提示操作，也可以咨询 400 客服热线进行咨询。

2.4 【ER7/8 系列】企业路由器 IPv6 上网配置指导

2.4.1 应用介绍

全球所有 43 亿个 IPv4 地址已全部用完，意味着没有更多的 IPv4 地址可以分配给 ISP 和其它大型网络基础设施提供商，因此 Internet 研究组织发布新的主机标识方法，即 IPv6。目前国内的网络正在快速的向 IPv6 升级中，从网络基础设施如运营商骨干网、城域网，到互联网服务商如各类云服务，以及各类终端设备厂商如手机、电脑、路由器、交换机等。目前运营商提供的 IPv6 线路主要分为支持前缀授权和不支持前缀授权两种，本文主要以 TL-ER7520G 为例介绍 ER7/8 系列企业级路由器关于 IPv6 的上网配置和指导，请在设置 IPv6 线路上网之前完成路由器基本设置，参考本文档 2.3 章节 [【ER7/8 系列】企业路由器基本设置指南](#)

2.4.2 需求介绍

终端获取到一个 IPv6 公网地址，实现端到端通信，减小网络转发开销；路由器 WAN 口可以同时获取到 IPv4 和 IPv6 地址，并且给支持双栈的终端分配 IPv4 和 IPv6 两个地址；终端访问 IPv4 的目标主机时走 IPv4，访问 IPv6 的目标主机时走 IPv6。

2.4.3 设置方法

支持前缀授权的 IPv6 线路上网设置方法

1、WAN 口参数设置

在基本设置->接口设置中，选择物理接口为 GE1，根据运营商提供的 IPv6 上网方式进行 WAN 口 IPv6 设置，并开启前缀授权功能，此处以 PPPoE 拨号为例（可以复用 IPv4 的拨号链路），拨号成功后可看到 WAN 口获取到 IPv6 地址。

□	序号	接口类型	接口名称	连接状态	IP地址/子网掩码 (或前缀长度)	网关地址	设置
--	--	--	--	--	--	--	--

接口类型: **PPPoE** 选择PPPoE

接口名称: **dianxin** (1-11个字符)

关联接口: **GE1**

IP协议类型: **IPv4** **IPv6** 选择IPv6

状态: 启用 禁用 启用，并复用IPv4拨号链路

用户名:

密码:

IPv6地址获取协议: 自动 DHCPv6 SLAAC 静态IP

前缀授权: 开启 开启前缀授权

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 (或前缀长度)	网关地址	设置
	1	物理接口	GE1	已连接 详细	IPv4: / IPv6:	IPv4: IPv6:	编辑 删除
	2	PPPoE	dianxin	已连接 详细	IPv4: 100.64.90.41/255.255.255.255 IPv6: 240e:3b0:302b:832c:fa8c:21e4:f142:5530/64	IPv4: 100.64.0.1 IPv6: fe80::3826:69ff:fe0a:ff09	编辑 删除

2、LAN 口参数设置

在基本设置->接口设置中，选择物理接口为 LAN 口，IP 协议类型选择 IPv6，并点击启用，地址配置方式选择 EUI-64，前缀授权接口选择刚才设置好的 PPPoE 口（EUI-64 表示自动获取 64 位 IPv6 的前缀地址）。

--	1	网桥接口	LAN	已连接 详细	IPv4: 192.168.1.1/255.255.255.0 IPv6:	IPv4: IPv6:
接口类型: 网桥接口 接口名称: LAN (1-11个字符) 连接方式: 静态IP IP协议类型: IPv4 IPv6 状态: <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 地址配置方式: <input checked="" type="radio"/> EUI-64 <input type="radio"/> 手动 前缀授权接口: dianxin IPv6地址前缀: 240e:3b3:30b0:7010:: 状态启用 选择地址分配方式 选择前缀授权接口						

3、地址分配设置

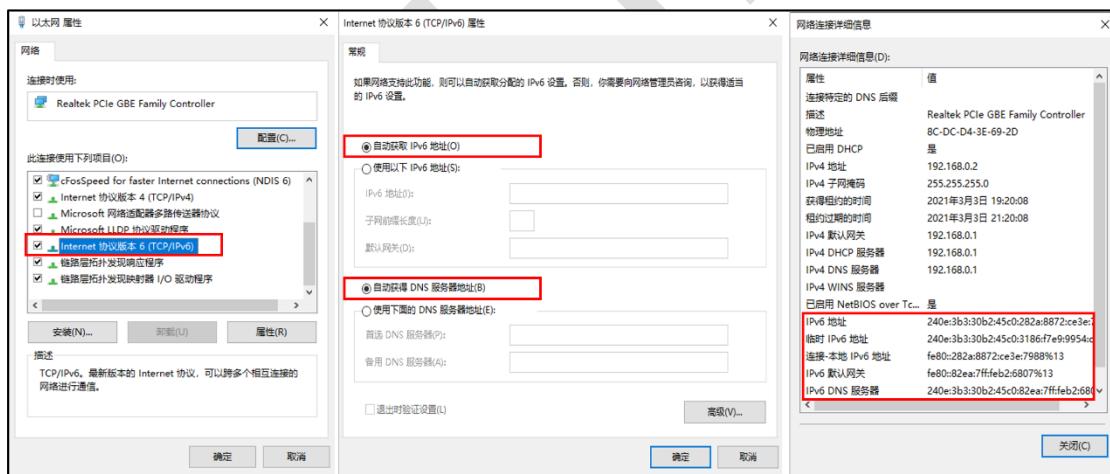
在基本设置->DHCP 服务中, 根据需要设置 LAN 口 IPv6 地址分配方式, 可以选择 DHCPv6 或者 SLAAC (二选一), DNS 不填时默认为路由器的 IPv6 地址, 路由器作 DNS 代理。其中 DHCPv6 是路由器手动设置一个范围下发地址; SLAAC 是根据地址前缀路由器随机下发地址。

DHCP服务	客户端列表	静态地址分配	DHCPv6服务	SLAAC	IPv6客户端列表	IPv6静态地址分配																		
DHCPv6服务列表 <div style="text-align: right;"> <input checked="" type="checkbox"/> 启用 <input type="checkbox"/> 禁用 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除 <input type="checkbox"/> 搜索 </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>□</th> <th>序号</th> <th>服务接口</th> <th>开始地址</th> <th>结束地址</th> <th>地址租期</th> <th>首选DNS服务器</th> <th>状态</th> <th>设置</th> </tr> </thead> <tbody> <tr> <td>--</td> <td>--</td> <td>--</td> <td>--</td> <td>--</td> <td>--</td> <td>--</td> <td>--</td> <td>--</td> </tr> </tbody> </table> <div style="margin-top: 10px;"> 服务接口: LAN 选择对应服务接口 开始地址: 240e:3b3:30b0:7010:: 配置IPv6地址段、租期和DNS服务器 结束地址: 240e:3b3:30b0:7010::1ff 地址租期: 120 分钟 (2-2880) 首选DNS服务器: <input type="text"/> 备用DNS服务器: <input type="text"/> Option16: <input type="text"/> / <input type="text"/> Option52: <input type="text"/> 状态: <input checked="" type="checkbox"/> 启用 </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="确定"/> <input type="button" value="取消"/> </div>							□	序号	服务接口	开始地址	结束地址	地址租期	首选DNS服务器	状态	设置	--	--	--	--	--	--	--	--	--
□	序号	服务接口	开始地址	结束地址	地址租期	首选DNS服务器	状态	设置																
--	--	--	--	--	--	--	--	--																



4、电脑自动获取 IPv6 地址

设置好路由器的相关参数后，终端（电脑、手机等）勾选 IPv6 协议，并开启自动获取 IPv6 地址和 DNS 服务器即可，获取 IP 结果如下。



不支持前缀授权的 IPv6 线路上网设置方法

对于不支持前缀授权的运营商线路，无法由路由器给终端分配 IPv6 地址，终端 IPv6 地址统一由运营商进行分配，因此需要路由器支持 IPV6 桥模式，目前 ER7/8 系列企业路由器支持 IPv6 桥模式，具体配置方法如下：

在基本设置->IPv6 桥模式中启用 IPv6 桥模式，点击保存。



开启桥模式后 WAN 口和 LAN 口的 IPv6 参数均不可设置





2.4.4 IPv6 常见问题解答

1、怎么判断宽带是否支持 IPv6?

有两种方式。①与宽带运营商确认线路是否支持 IPv6；②电脑直连猫拨号，看电脑是否获取到 IPv6 地址。

2、怎么判断 IPv6 线路是否支持前缀授权？

请致电宽带运营商确认。

3、怎么判断路由器是否支持 IPv6?

有两种方式。①登陆路由器管理界面→基本设置→有 IPv6 设置，则支持。②点击[在线客服](#)咨询人工客服。

4、怎么检测路由器获取的 IPv6 地址可以正常联网？

打开浏览器输入www.test-ipv6.com，就可以看到线路是否支持 IPv6 了。

The screenshot shows a web interface for testing IPv6 connectivity. At the top, it displays the URL 'test-ipv6.com' and a status message '① 不安全'. Below this, there are tabs for '测试 IPv6', '常见问题', and '镜像'. The main content area is titled 'IPv6 连接测试' (IPv6 Connection Test). It includes a navigation bar with '摘要', '测试项目', '反馈测试结果 / 联系我们', and '其他 IPv6 网站'. The results section contains several items:

- 你的公网 IPv4 地址是 183.14.132.169 (CHINANET-BACKBONE No.31,Jin-rong Street)
- 你的公网 IPv6 地址是 240e:fa:f8:87da:f64d:3050:4173:8b5d | 宽带线路支持IPv6 (CHINANET-GUANGDONG-SHENZHEN-MAN CHINANET Guangdong province Shenzhen MAN network)
- 你已接入 IPv6, 因此我们增加了一个标签页, 显示你能否访问其他 IPv6 网站。([更多信息](#))
- ⚠️ 你正在使用 IPv4 或 IPv6 隧道。如果你使用了 VPN, 则此 VPN 只对一套协议起作用。
- 本站现已支持 [HTTPS](#). ([更多信息](#))
- 你的 DNS 服务器 (可能由运营商提供) 已经接入 IPv6 互联网了。

5、IPv6 支持哪些网络资源？

IPv6 目前还属于初步发展阶段，虽然多数网络资源都还未普及，但是校园教育资源和大型互联网企业资源（如谷歌、腾讯和百度等）已经铺展开来。

IPv6资源				
Baidu 百度	Tencent 腾讯	Google	Google Scholar	Microsoft 微软 学术
Sogou 搜狗搜索	Qzone 大维空间	Aliyun 阿里云	Tencent Cloud 腾讯云	Tsinghua IPTV 清华IPTV
YAHOO!	GitHub	iQIYI 爱奇艺	YOUKU 优酷	Sohu 搜狐 视频
Xinhua News 新华网	Ifeng 凤凰网 ifeng.com	CNN	NetEase 网易 www.163.com	Sohu.com 搜狐
Taobao 淘宝网 Taobao.com	China Mobile 中国移动 China Mobile	China Telecom 中国电信 CHINA TELECOM	China Unicom 中国联通	CERNET
Alipay 支付宝 ALIPAY	Bank of China 中国银行 BANK OF CHINA	Office 365	xkcd

6、IPv6 设置好上网后，能否通过 IPv6 地址远程访问路由器？

远程管理目前无法填写 IPv6 地址，推荐使用商云平台进行远程管理，更加方便。

7、IPv6 配置上网后，外网访问内网是否需要做映射？

不需要，每个 PC 是全球公网地址，IPv6 访问为纯路由模式，网络中直接访问设备即可。

8、开启 IPv6 后是否影响 IPv4 的资源访问？

不会，路由器支持 IPv4 和 IPv6 双栈协议，可以同时访问 IPv4 和 IPv6 的外网资源。



2.5 【ER7/8 系列】如何设置实现一口多拨?

2.5.1 应用介绍

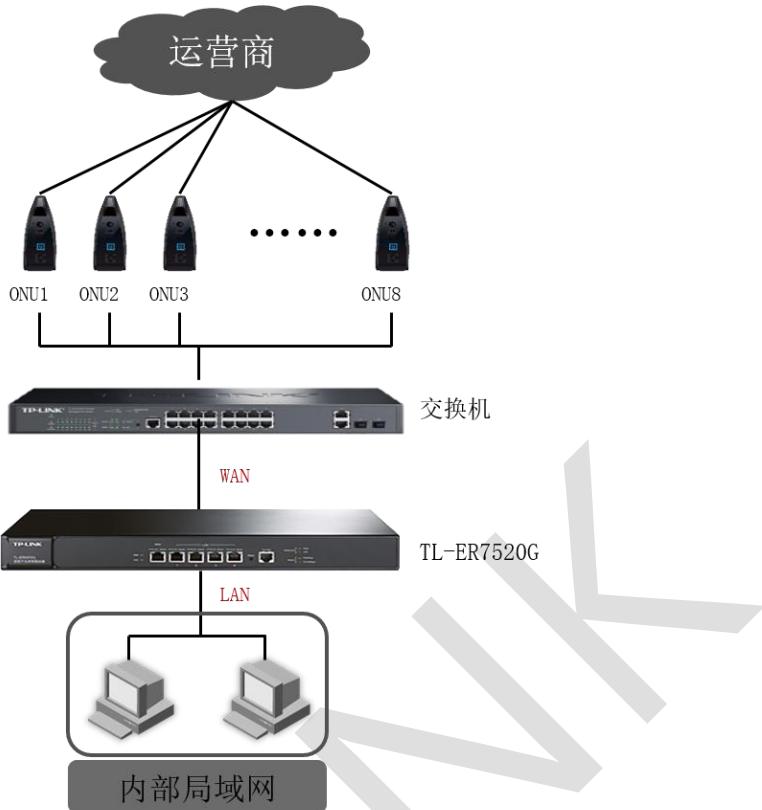
多 WAN 口路由器可以起到叠加带宽、链路备份等作用。在实际生活中多 WAN 口路由器得到了广泛的应用，但是由于端口数量限制，通常仅能使用 2~4 个 WAN 口进行通信。

TL-ER7520G/ TL-ER8820T 可在一个物理端口上划分多个虚拟子接口，同时向多个猫进行拨号，在一个物理端口上实现多 WAN 口路由器的功能。

下面以 TL-ER7520G 和二层简单网管交换机 TL-SG2024D 为例，介绍一口多拨的设置方法。TL-ER8820T 设置方法相同。

2.5.2 应用拓扑

如下图所示，TL-ER7520G 的 1 口接在前端交换机的 24 端口，交换机的 1-8 端口接了 8 台光猫，通过设置实现在 TL-ER7520G 的 1 口同时拨通这 8 条线路。



2.5.3 设置方法

设置路由器 (以 TL-ER7520G 为例)

1、登录路由器界面

TL-ER7520G 在恢复出厂的状态下，电脑通过网线连接到路由器的 5 口，本地连接手动配置 192.168.1.X (X 位于 2-254 之间) 的 IP 地址，登录到 192.168.1.1 的管理界面，登录用户名及密码默认均为 admin。

2、网桥设置-设置 LAN 口

点击“基本设置>接口设置>网桥设置”，点击 新增，设置如下：



点击“确定”，提示重启路由器，点击“是”。

3、接口设置-为 WAN 口设置多个虚接口

设置向 modem1 拨号的虚接口

点击“基本设置>接口设置”，选择物理接口为“GE1”，并点击 新增，添加 Ethernet 接口，

VLAN ID 为 10，设置如下：

接口设置 网桥设置 SFP+设置

接口类型:	Ethernet	接口类型选择Ethernet
接口名称:	WAN_eth10	(1-12个字符)
关联接口:	GE1	关联接口选择GE1
关联VLAN:	10 设置VLAN ID为10	<input type="checkbox"/> UNTAG 不勾选, 即加TAG
连接方式:	静态IP	
IP地址:	192.168.100.2	填写非LAN网段, 且各接口设置不同地址
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:	78-44-FD-F1-77-46	
备注:		(可选,50个字符)
管理接口开启:	<input type="checkbox"/>	
<input type="button" value="确定"/> <input type="button" value="取消"/>		

再次点击 新增 , 添加 VLAN10 的 PPPoE 拨号接口, 设置如下:

接口类型:	PPPoE	接口类型选择为PPPoE
接口名称:	WAN_PPPOE10	(1-12个字符)
关联接口:	WAN_eth10	关联接口选择为VLAN10 的eth口，即WAN_eth10
用户名:	sztp1@163.gd	
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"/>	
<input type="button" value="确定"/> <input type="button" value="取消"/>		

按照同样的方法,依次添加向 modem2~modem8 拨号的虚接口、且 VLAN ID 依次为 11、12、13、14、15、16、17。

4、设置 DHCP 服务器

点击“基本设置>DHCP 服务”，点击 新增，设置如下：

服务接口:	LAN
开始地址:	192.168.1.100
结束地址:	192.168.1.199
地址租期:	120 分钟 (1-2880)
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)
状态:	<input checked="" type="checkbox"/> 启用
<input type="button" value="确定"/> <input type="button" value="取消"/>	

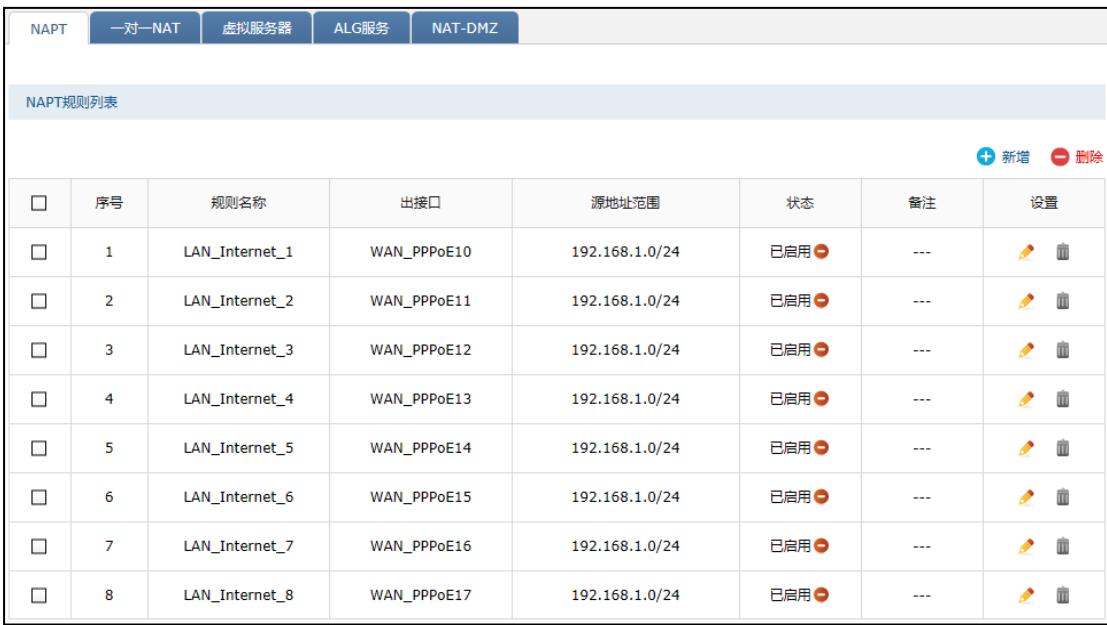
5、设置 NAPT 规则

点击“传输控制>NAT 设置>NAPT”，点击  新增，NAPT 规则设置如下：

规则名称:	LAN_Internet_1	
出接口:	WAN_PPPOE10	出接口选择PPPoE拨号的虚接口
源地址范围:	192.168.1.0 / 24	
状态:	<input checked="" type="checkbox"/> 启用	
备注:		
<input type="button" value="确定"/> <input type="button" value="取消"/>		

同样的方法，依次添加出接口为向 modem2~modem8 拨号的 PPPOE 接口的 NAPT 规则。

添加完毕的 NAPT 规则列表如下：

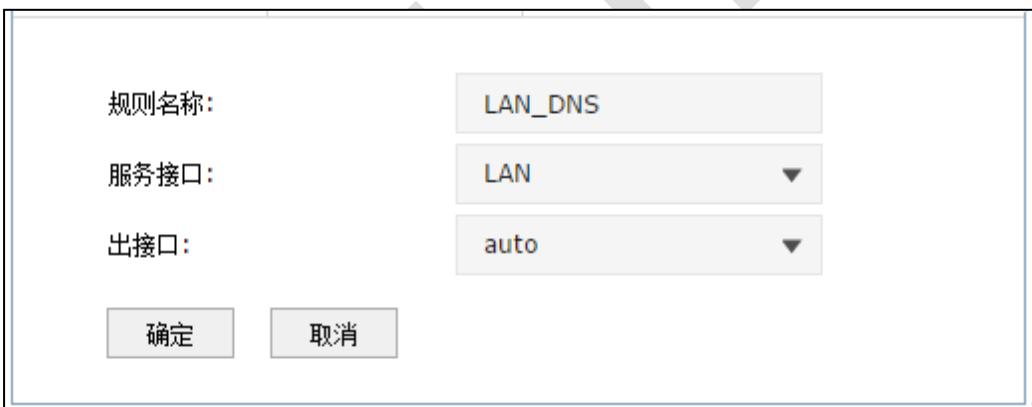


The screenshot shows a table titled "NAPT规则列表" (NAPT Rule List) with 8 rows. The columns are: 序号 (Index), 规则名称 (Rule Name), 出接口 (Interface), 源地址范围 (Source Address Range), 状态 (Status), 备注 (Remarks), and 设置 (Actions). Each row contains a checkbox, the index, the rule name, the interface, the source address range (192.168.1.0/24), the status (已启用 - Enabled), the remarks (---), and edit/delete icons.

<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	LAN_Internet_1	WAN_PPPOE10	192.168.1.0/24	已启用	---	
<input type="checkbox"/>	2	LAN_Internet_2	WAN_PPPOE11	192.168.1.0/24	已启用	---	
<input type="checkbox"/>	3	LAN_Internet_3	WAN_PPPOE12	192.168.1.0/24	已启用	---	
<input type="checkbox"/>	4	LAN_Internet_4	WAN_PPPOE13	192.168.1.0/24	已启用	---	
<input type="checkbox"/>	5	LAN_Internet_5	WAN_PPPOE14	192.168.1.0/24	已启用	---	
<input type="checkbox"/>	6	LAN_Internet_6	WAN_PPPOE15	192.168.1.0/24	已启用	---	
<input type="checkbox"/>	7	LAN_Internet_7	WAN_PPPOE16	192.168.1.0/24	已启用	---	
<input type="checkbox"/>	8	LAN_Internet_8	WAN_PPPOE17	192.168.1.0/24	已启用	---	

6、设置 DNS 代理

点击“系统服务>DNS 代理”，点击 新增，DNS 代理规则设置如下：



The dialog box shows the following settings:

- 规则名称 (Rule Name): LAN_DNS
- 服务接口 (Service Interface): LAN
- 出接口 (Outer Interface): auto

Buttons at the bottom: 确定 (Confirm) and 取消 (Cancel).

设置完成，点击右上角“保存配置”。

备注：TL-ER8820T 设置方法相同。

设置交换机 (以 TL-SG2024D 为例)

1、配置 802.1Q VLAN

登录交换机管理界面，打开 VLAN——802.1Q VLAN 页面，依次添加如下 VLAN：

vlan10，端口为 1 untagged、24 tagged；

vlan11，端口为 2 untagged、24 tagged；

vlan12，端口为 3 untagged、24 tagged；

vlan13，端口为 4 untagged、24 tagged；

vlan14，端口为 5 untagged、24 tagged；

vlan15，端口为 6 untagged、24 tagged；

vlan16，端口为 7 untagged、24 tagged；

vlan17，端口为 8 untagged、24 tagged。

如下图所示：

选择VLAN10

VLAN	10 (1-4094)	VLAN描述	
端口	Untagged端口	Tagged端口	非成员端口
全选	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
端口 1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
端口 2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 5	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 6	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 7	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 8	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 9	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 10	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 11	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 12	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 13	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 14	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 15	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 16	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 17	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 18	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 19	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 20	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 21	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 22	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 23	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
端口 24	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

添加/编辑 帮助 选择端口24为Tagged端口

VLAN	VLAN描述	成员端口	Tagged端口	Untagged端口	删除
1	Default	1-24	24	1-23	<input type="checkbox"/>
10		1,24	24	1	<input type="checkbox"/>

设置完成后VLAN10条目 全选 删除

配置完成后列表如下：

VLAN	VLAN描述	成员端口	Tagged端口	Untagged端口	删除
1	Default	1-24	24	1-23	<input type="checkbox"/>
10		1,24	24	1	<input type="checkbox"/>
11		2,24	24	2	<input type="checkbox"/>
12		3,24	24	3	<input type="checkbox"/>
13		4,24	24	4	<input type="checkbox"/>
14		5,24	24	5	<input type="checkbox"/>
15		6,24	24	6	<input type="checkbox"/>
16		7,24	24	7	<input type="checkbox"/>
17		8,24	24	8	<input type="checkbox"/>

[全选](#) [删除](#)

2、修改 802.1Q PVID 设置

打开 VLAN——802.1Q PVID 设置页面，根据 802.1Q VLAN 设置，修改各端口对应 PVID 值如下：

802.1Q VLAN PVID设置

选择	端口	PVID
<input type="checkbox"/>	端口1	10
<input type="checkbox"/>	端口2	11
<input type="checkbox"/>	端口3	12
<input type="checkbox"/>	端口4	13
<input type="checkbox"/>	端口5	14
<input type="checkbox"/>	端口6	15
<input type="checkbox"/>	端口7	16
<input type="checkbox"/>	端口8	17
<input type="checkbox"/>	端口9	1
<input type="checkbox"/>	端口10	1
<input type="checkbox"/>	端口11	1
<input type="checkbox"/>	端口12	1
<input type="checkbox"/>	端口13	1
<input type="checkbox"/>	端口14	1
<input type="checkbox"/>	端口15	1
<input type="checkbox"/>	端口16	1
<input type="checkbox"/>	端口17	1
<input type="checkbox"/>	端口18	1
<input type="checkbox"/>	端口19	1
<input type="checkbox"/>	端口20	1
<input type="checkbox"/>	端口21	1
<input type="checkbox"/>	端口22	1
<input type="checkbox"/>	端口23	1
<input type="checkbox"/>	端口24	1

对应修改各端口PVID值

应用 **帮助**

注意：

1、缺省情况下所有端口的PVID都是1。
2、当802.1Q VLAN被禁用后，所有端口的PVID会被恢复到1。

至此，使用 TL-ER7520G 通过一个 WAN 口向多条 ADSL 线路拨号的设置完成。

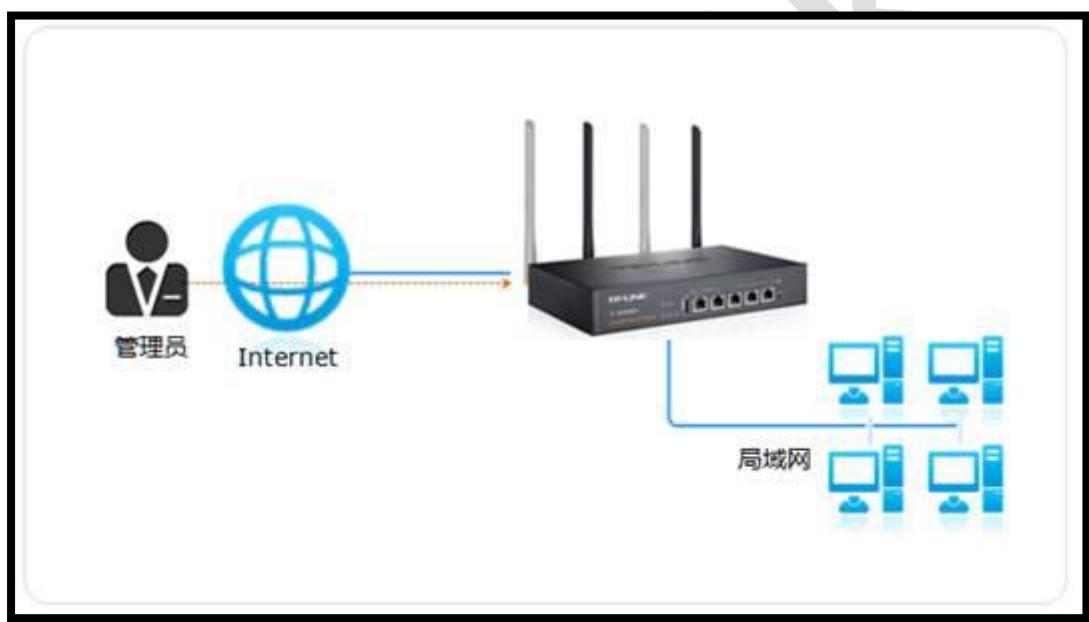
备注：其他管理型交换机的设置方法相同。

第3章 设备管理

3.1 如何在外网远程管理（控制）路由器？

3.1.1 应用介绍

企业网络管理员希望在网络任何地方都可以管理到路由器，从而可以实时、安全的进行管控配置。远程 WEB 管理功能和商云功能，可以实现在接入互联网的地方即可远程管理路由器。



本文介绍企业路由器远程管理路由器的设置方法：远程 WEB 管理和商云管理。

3.1.2 设置方法 1-远程 WEB 管理

1、如何设置路由器

登录路由器界面，在“系统工具>系统管理/管理账号>远程管理”，新增一条 0.0.0.0/0 的条目，(0.0.0.0/0 代表所有外网电脑均可以访问路由器)，如下。



同时在“系统工具>系统管理/管理账号>系统管理设置”中设置 WEB 服务端口。

设置Http服务端口为不常用端口		
Http服务端口:	9090	(80、1024-65535)
Https服务端口:	443	(443、1024-65535)
认证服务端口:	8080	(8080、1024-65535)
Web会话超时时间:	6	分钟(5-60)



说明:

- 1、80、8080 等常用端口容易被宽带服务商屏蔽，因此建议将 WEB 服务端口设置为不常用端口，如 9000 以上的端口。
- 2、修改 WEB 服务端口后，局域网电脑需要使用 LAN 口 IP:端口(如 http://192.168.1.1:9090)来登录路由器。
- 3、部分企业路由器界面有保存配置的提示，请务必保存配置。

- (1) 老平台企业路由器需要添加 0.0.0.0/32 的远程地址条目（具体以路由器界面中的“帮助”说明为准）。
- (2) 早期的 ER51XX (不带 G) 系列网吧路由器点击“系统服务>Web 服务器”，在“远程管理”和“服务设置”中分别设置，也是需要添加 0.0.0.0/32 的远程地址条目。

2、如何远程访问

在“运行状态/基本设置>系统状态”中，查看到 WAN 口 IP 地址。

WAN口信息						
WAN1信息						
接口名称	连接方式	连接状态	IP地址	子网掩码	网关地址	首选DNS服务器
WAN1	固定IP地址	已连接	121.201.33.100	255.255.255.0	121.201.33.1	202.96.134.133

外网电脑在浏览器地址栏输入 http://WAN 口 IP:端口来访问。如下图：



备注：如果路由器上登录了动态域名，还可以使用 <http://域名:端口> 来访问。

3、疑问解答

Q1、WAN 口的 IP 地址一直在变，怎么办？

当 WAN 口的上网方式为 PPPoE 时，WAN 口 IP 地址往往不是固定的公网 IP，每次在外网访问时都需要先确认路由器 WAN 口的 IP 地址，比较麻烦。使用动态域名功能即可解决该问题。在“系统服务>动态 DNS”，以 TP-LINK 动态域名为例，输入 TP-LINK ID 及密码登录。

The screenshot shows the TP-LINK Dynamic Domain Management interface. At the top, there are tabs for 'TP-LINK 动态域名' (selected), '花生壳动态域名', '科迈动态域名', and '3322动态域名'. Below the tabs, a header bar says 'TP-LINK ID的登录/注册/密码重置'. It displays 'TP-LINK ID:' (1813828) and a password field. A '登出' (Logout) button is present with a note: '(注意, 登出后, 绑定到本设备的域名将会自动解绑, 即变为“未绑定”状态)'. The main content area is titled 'TP-LINK动态域名' and shows a table of created domains:

序号	域名	绑定状态	绑定信息	设置
1	test'...tpddns.cn	绑定到本设备	WAN1	
2	...tpddns.cn	绑定到本设备	WAN1	

TP-LINK 动态域名登录成功后，在上图列表中可以查看到动态域名，外网电脑使用动态域名可以访问路由器。



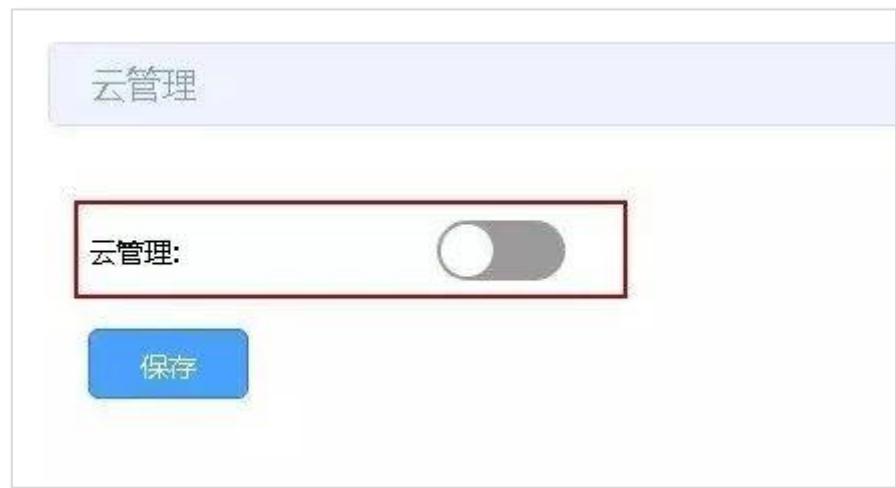
Q2、多 WAN 口路由器连接了多条宽带，外网访问时该使用哪个 WAN 口的 IP 地址？

在确认 WAN 口 IP 是公网 IP 的情况下，可以使用任意一个 WAN 口的 IP 地址访问路由器。

3.1.3 设置方法 2-商云管理

1、如何设置路由器

登录本地 Web 管理界面，进入系统工具>云管理页面，点击开启云管理功能。



备注：在开启云管理之前，建议先备份配置文件。

2、登录 TP-LINK 商云平台

打开浏览器，访问 TP-LINK 商用网络云平台：smbcloud.tp-link.com.cn，如下图：



输入 TP-LINK ID 和密码，点击“登录”。

注意：如果还没有 TP-LINK ID，请点击“创建 TP-LINK ID”，根据提示创建 TP-LINK ID，创建完成后可自动登录。

3、通过设置向导创建项目

登录成功后，请输入一个项目名称，该项目名称可根据实际情况自定义，如：XX 酒店、XX 商场。



输入项目名称后，请点击页面右下角的“保存并下一步”，进入“添加设备”页面。

4、添加设备

在“添加设备”页面中，根据提示输入设备 ID、设备 MAC 地址、设备名称、用户名、密码等信息。



输入完成后，点击“添加设备”，添加成功后设备的相关信息会在商云显示，如下图：

序号	设备名称	设备分组	设备类型	工作模式	软件版本	硬件版本	安装位置	设备状态	设备型号
1	1200G	a	无线路由器	---	1.1.1 Build 200630 Rel.8684n	4.0	---	● 在线	TL-WVR120C
2	TL-XAP6009GC-PoE/DC-0000	a	AP	---	1.0.0 Build 20200329 Rel.61843	1.0	---	● 在线	TL-XAP6009I

至此，便可以在外网通过商云平台管理 AC 以及 AC 管理的 AP。另外，支持商云远程管理的设备也可以在商云平台直接远程管理，如下图所示：

设备信息										名称, 型号, IP, MAC	筛选	
	内容	删除设备	修改分组	重启	升级	LED设置	固化IP地址	导出设备信息	刷新			
<input type="checkbox"/>	序号	设备名称 ↓	设备分组	设备类型 ↓	设备状态 ↓	设备型号 ↓	IP地址 ↓	MAC地址 ↓	工作模式	LED状态	关联设备 ↓	操作
<input type="checkbox"/>	1	TL-ER8820IT 1.0	222	有线路由器	● 在线	TL-ER8820T	27.46.93.183	00-00-FF-FF-14-E7	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	2	TL-SL3226P-Combo	2栋室内	L2交换机	● 在线	TL-SL3226P-Combo	172.26.0.121	80-8F-1D-3C-8B-CA	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	3	宿舍2栋4楼	2栋室内	L2交换机	● 在线	TL-SL3226P-Combo	172.26.0.122	80-8F-1D-3C-8B-C3	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	4	宿舍2栋5、6楼	2栋室内	L2交换机	● 离线	TL-SL3226P-Combo	172.26.0.123	80-8F-1D-3C-8B-C2	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	5	宿舍9楼10楼	内销工厂网络	L2交换机	● 在线	TL-SL3226P-Combo	172.26.0.125	80-8F-1D-3C-8B-B3	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	6	宿舍2栋11、12楼	2栋室内	L2交换机	● 在线	TL-SL3226P-Combo	172.26.0.126	80-8F-1D-3C-8B-C0	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	7	TL-SL3226P-Combo	内销工厂网络	L2交换机	● 在线	TL-SL3226P-Combo	172.26.0.127	80-8F-1D-3C-8B-B4	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	8	TL-SL3226P-Combo	内销工厂网络	L2交换机	● 在线	TL-SL3226P-Combo	172.26.0.128	80-8F-1D-3C-8B-B1	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	9	2栋7、8楼	2栋室内	L2交换机	● 在线	TL-SL3226P-Combo	172.26.0.124	80-8F-1D-3C-8B-98	---	---	---	远程管理 重启 升级 编辑
<input type="checkbox"/>	10	AC10000	内销工厂网络	AC	● 在线	TL-AC10000	172.20.0.1	00-00-FF-FF-02-01	---	---	---	远程管理 重启 升级 编辑

3.2 如何设置自动重启?

3.2.1 应用介绍

路由器长时间工作时，可能会出现路由器系统开销过大从而引起网络异常，就像电脑一样，长时间一直在工作可能会出现系统响应越来越慢，此时重启一下就好了。但由于路由器放置或其它因素，不方便手动重启。此时通过企业路由器的“自动清理”功能实现在指定时间段内让路由器自动重启。

本文介绍 ER 系列路由器的自动清理功能的配置步骤。

3.2.2 需求分析

某小型企业需要设置路由器在每周日的凌晨 3 点进行自动重启。

3.2.3 设置方法

登录到路由器界面，点击“系统工具>设备管理>自动清理”，点击开启自动清理功能，设置自动重启的时间，点击“确定”，添加规则如下：



注意：自动清理功能仅在获取到网络时间或者手动设置时间后生效；一般推荐重启时间设置在网络使用率不高时。

至此，自动清理设置完成，路由器可以在设置的时间点进行自动重启。



第4章 多带宽均衡

4.1 多 WAN 口路由器负载均衡的设置指南

4.1.1 应用介绍

多 WAN 口路由器连接多条宽带的目的主要有以下 2 个：

- (1) 增加带宽：上网主机可以通过任意宽带上网，从应用角度讲，相当于一条更高速的带宽。
- (2) 冗余备份：如果其中一条宽带出现故障，可以使用其他宽带上网，保证网络畅通无中断。

4.1.2 需求介绍

某企业接入两条电信的线路，一条 500M，另一条 300M。需要充分利用两条线路的带宽。

4.1.3 工作原理

在接入多条宽带时，多 WAN 口企业路由器可以通过设置流量均衡策略，充分利用各 WAN 口的带宽。均衡模式分为连接均衡和宽带均衡两种。

- (1) 连接均衡：根据总连接数合理分配给各个 WAN 口，保证每个 WAN 口利用率相同（路由器默认设置为连接均衡）。



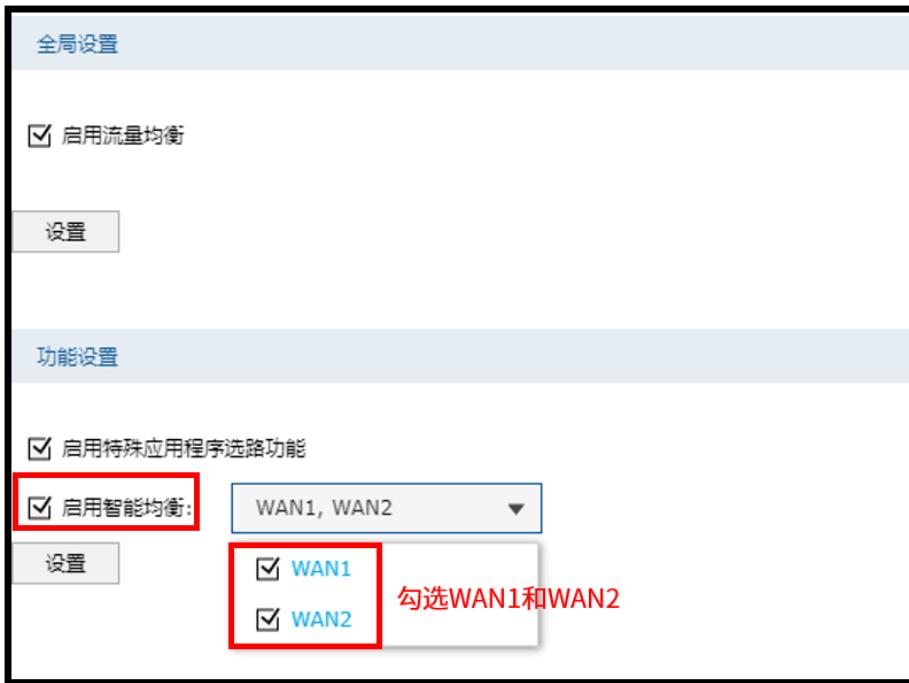
(2) 带宽均衡：各条宽带的流量比等于设置的各接口带宽比。如果接口 1 和接口 2 带宽比为 5:3，那么启用“带宽均衡”后，通过接口 1 和接口 2 的实际流量比约为 5:3。



4.1.4 设置方法

系统默认情况下是连接均衡，如果需要设置带宽均衡，

1、进入路由器，点击“传输控制>流量均衡>基本设置”，勾选“启用智能均衡”，勾选 WAN1 和 WAN2，点击设置。



2、点击 WAN 口列表的编辑设置，将 WAN1 口权重设置为 500，将 WAN2 口权重设置为 300.

序号	接口	权重	设置
1	WAN1	500	点击设置，将权重设置为500
2	WAN2	300	点击设置，将权重设置为300

至此，策略路由功能设置完成，如果玩游戏，浏览网页和服务器的行为较多，建议选择连接均衡模式。如果看视频，下载和上传大文件的行为较多，建议选择带宽均衡模式。两种模式各有优缺点，建议根据实际使用场景选择合适的均衡模式。

第5章 路由转发模块

5.1 策略路由设置指南

5.1.1 应用介绍

一些企业的应用环境中会接入多条宽带线路，不同的资源只能通过指定的线路才能正常访问。确保访问特定目标的数据走指定的线路是保证这种应用成功访问的前提。策略路由功能可以实现访问指定的 IP 或者端口时走指定的接口。



本文详细介绍 ER 系列路由器的策略路由功能设置方法。

5.1.2 需求分析

某企业接入了两条外网线路，WAN1 口接运营商拨号宽带线路，用于连接互联网；WAN2 口接企业内部专网，专网网络是 10.17.0.0/16，只能用于访问内网资源，无法访问互联网。需要实现下接的终端既能访问互联网，也能正常访问企业内部网络。



5.1.3 设置方法

1、设置 WAN 口参数

登录到路由器界面，点击“基本设置>WAN 设置”，分别设置 WAN1 和 WAN2 的上网参数。

Internet网络 企业内网

连接设置

连接方式:	固定IP地址
IP协议类型:	IPv4
IP地址:	10.17.0.100
子网掩码:	255.255.0.0
网关地址:	10.17.0.1 (可选)
MTU:	1500 (576-1500)
首选DNS服务器:	10.17.0.1 (可选)
备用DNS服务器:	10.17.0.2 (可选)
上行带宽:	1000000 Kbps (100-1000000)
下行带宽:	1000000 Kbps (100-1000000)
运营商:	不设置

设置

2、添加内网地址组

在路由器界面，点击“对象管理>地址管理>地址”，点击“新增”，添加内网 IP。

地址名称:

IP类型: IP段 IP/Mask

172.17.0.0 / 16

备注: (可选)

确定 **取消**

在路由器界面，点击“对象管理>地址管理>地址组”，点击“新增”，将内网 IP 添加到内网地址组中：



3、设置策略路由

登录到路由器 WEB 界面，点击“传输控制>路由设置>策略路由”，点击“新增”，进行设置。

1) 设置规则：访问专网 10.17.0.0/16 的数据只能从 WAN2 口转发，如下图：



2) 再设置一条规则：访问外网的数据只能从 WAN1 口转发，如下图：

规则名称:	Internet	
服务类型:	ALL	
源地址:	IPGROUP_LAN	源地址选择局域网地址段
目的地址:	IPGROUP_ANY	目的地址选择所有地址
生效接口:	WAN1	出接口选择Internet连接的WAN口
生效时间:	Any	规则生效的时间
强制:	<input checked="" type="checkbox"/> 接口不在线时仍应用此规则	外网不在线也不走内网口
备注:	(可选)	
添加到指定位置:	2	(可选)
状态:	<input checked="" type="checkbox"/> 启用	
<button>确定</button> <button>取消</button>		

注意：策略路由规则是由上往下逐条匹配的，两条规则必须按照以上添加顺序添加。

至此，策略路由功能设置完成，路由器 LAN 网段的终端访问企业内网或访问 Internet 都将按照规则来实现。

5.2 ISP 选路设置指南

5.2.1 应用介绍

多 WAN 口路由器接入多条宽带线路可以实现带宽叠加、线路备份的作用，从而提高网络的稳定性。但是，如果接入的多条宽带线路不是同一运营商（宽带服务商），则可能引起访问瓶颈（例如访问电信网络的数据走联通网络），导致网络延迟大、丢包等现象。多 WAN 口路由器的 ISP 选路功能可以避免以上问题发生，实现访问对应 ISP 网络的数据走正确的出接口。



本文详细介绍 ER 系列路由器的 ISP 选路功能设置方法。

5.2.2 需求分析

某企业使用 ER 系列路由器，连接两条宽带线路，WAN 口 1 是电信宽带，WAN2 口是联通宽带。需要实现访问电信服务器的流量走电信线路，所有访问联通服务器的流量走联通线路。

5.2.3 设置方法

登录到路由器 WEB 界面，点击“基本设置>WAN 设置”，分别设置 WAN1 和 WAN2 的上网参数，勾选对应的运营商。

The screenshot shows the 'WAN1设置' (WAN1 Settings) tab selected in the top navigation bar. Below it, the '连接设置' (Connection Settings) section is visible. The '运营商' (Operator) dropdown menu is highlighted with a red border, and the text '选择正确的运营商' (Select the correct operator) is displayed to its right. Other fields in the form include:

连接方式:	固定IP地址
IP协议类型:	IPv4
IP地址:	121.201.33.102
子网掩码:	255.255.255.0
网关地址:	121.201.33.1 (可选)
MTU:	1500 (576-1500)
首选DNS服务器:	202.96.134.133 (可选)
备用DNS服务器:	119.29.29.29 (可选)
上行带宽:	1000000 Kbps (100-1000000)
下行带宽:	1000000 Kbps (100-1000000)

运营商: 电信

选择正确的运营商

设置

目前 TP-LINK 路由器将国内 IP 分为“电信”、“联通”、“教育网”、“移动”、“国内其他”（如长城宽带，广电宽带等）这几类，国外的 IP 则放在“其他”类中。

备注：路由器 ISP 选路功能默认开启，仅需要在 WAN 口设置时选择 WAN 口宽带对应的运营商即可。

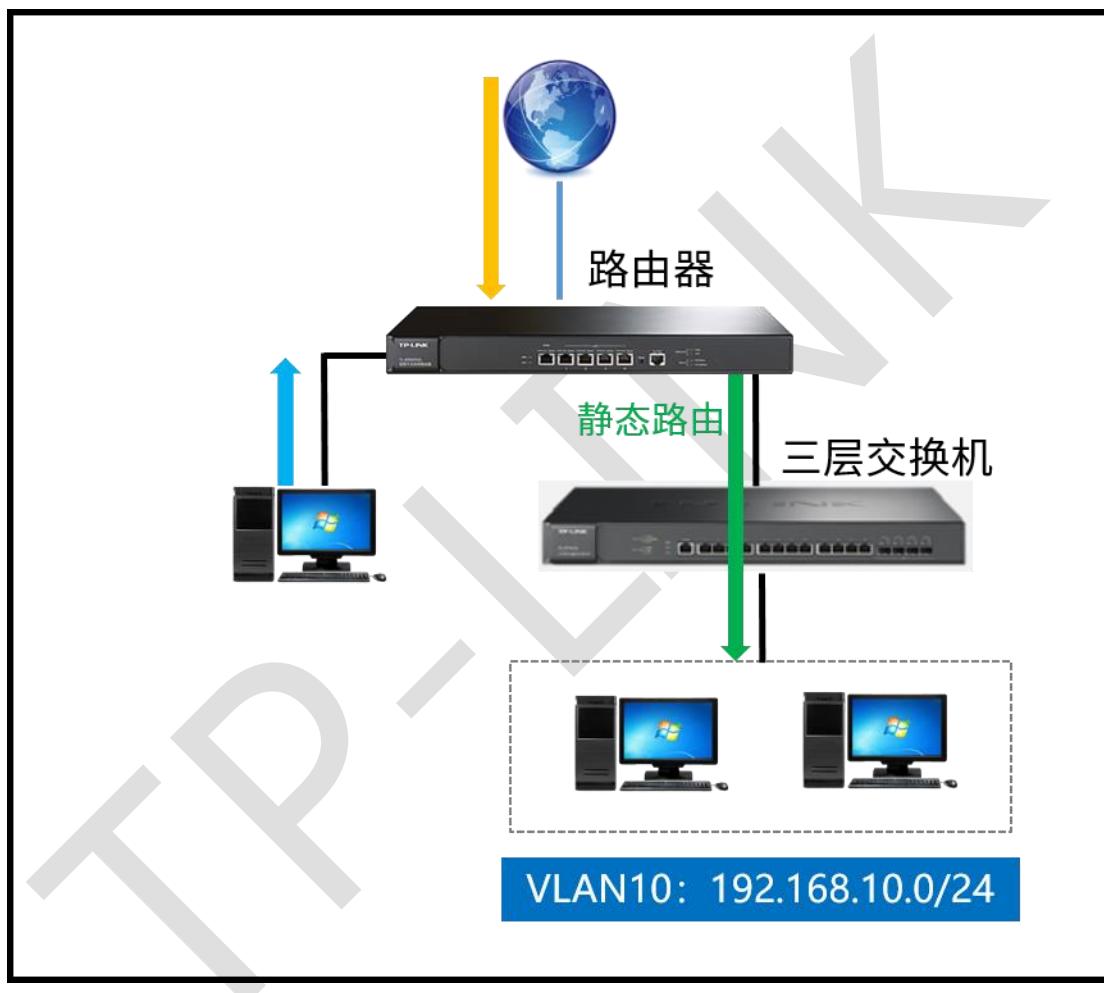
至此，ISP 选路功能设置完成，访问电信站点的流量由电信线路转发，访问联通站点的流量由联通线路转发。实现更快速的访问网络资源。



5.3 静态路由设置指南

5.3.1 应用介绍

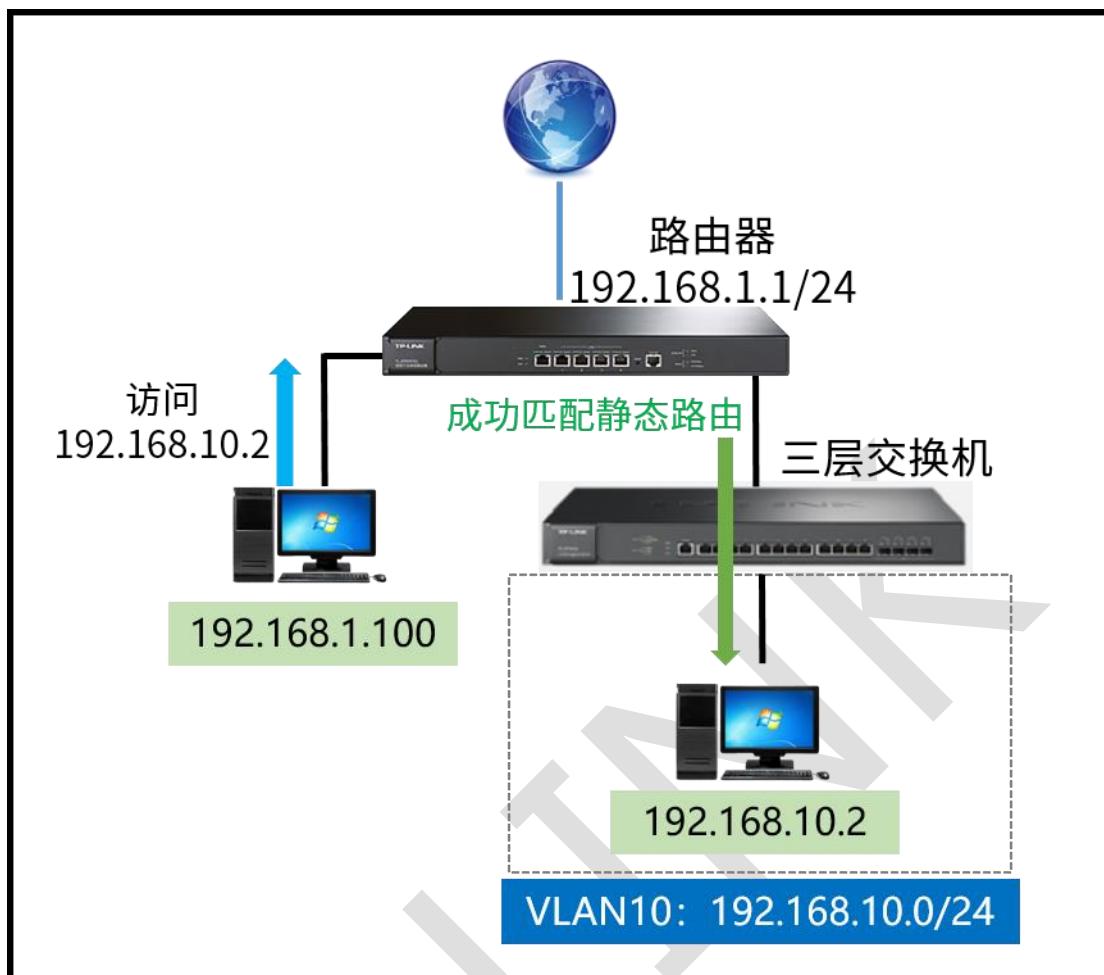
静态路由是在路由器中手工设置的固定的路由条目，当数据包与静态路由条目匹配成功时，将按照指定的出接口进行转发。



本文详细介绍 ER 系列路由器的静态路由功能设置方法。

5.3.2 需求分析

某企业使用 ER 系列路由器，下接三层交换机，交换机划分了 VLAN10，需要实现路由器 LAN 网段的终端可以与三层交换机下的 VLAN10 网段进行互访。



5.3.3 设置方法

登录到路由器 WEB 界面，点击“传输控制>路由设置>静态路由”，点击“新增”，进行设置。

规则名称:	VLAN10	填写目的网络的IP地址和子网掩码
目的地址:	192.168.10.0	
子网掩码:	255.255.255.0	填写路由的下一跳IP
下一跳:	192.168.1.254	选择路由使用的出接口
出接口:	LAN	
Metric:	0	(0-15)
备注:		(可选, 1-50个字符)
启用/禁用规则:	<input checked="" type="checkbox"/> 启用	
确定 取消		

至此，静态路由功能设置完成，路由器 LAN 网段的终端可以与三层交换机下的 VLAN10 网段进行互访了。

5.4 线路备份设置指南

5.4.1 应用介绍

多 WAN 口路由器的线路备份功能可以在其中某一个 WAN 口出现异常时，路由器能及时地把数据切换到其它正常的 WAN 口上，为网络稳定性提供强大保证。

本文介绍 ER 系列多 WAN 口路由器线路备份的配置方法。

5.4.2 设置方法

在路由器 WEB 界面，点击“传输控制>流量均衡>基本设置”，确认“启用流量均衡”已勾选。

点击“传输控制>流量均衡>线路备份”，点击  新增，设置线路备份规则。



说明：

1、定时备份：在设置的生效时间内，所有上网数据均由备接口转发。（生效时间在“对象管理>时间管理”中进行设置）

2、故障备份：主接口未联网时，所有上网数据均由备接口转发。

注意：大多数应用程序和服务器建立的是一对一的连接，如果主接口的宽带线路故障，连接就会断开。然后需要重新在备接口建立连接。此时会出现程序短暂掉线再次重连的现象。



5.5 虚拟服务器设置指南

5.5.1 应用介绍

企业在内部可能会搭建各种服务器，如 FTP 服务器、WEB 服务器、邮件服务器、监控服务器等。而这些服务器并不仅仅是针对内网用户开放的，外网的用户也需要通过互联网来访问。虚拟服务器功能可以实现将内网的服务器映射到 Internet，从而实现外网的访问。

本文介绍 ER 系列路由器的虚拟服务器功能的配置步骤。



5.5.2 需求分析

某小型企业需要将网页服务器对外网开放。通过虚拟服务器功能实现该需求。用户网络参数如下：

服务器类型	外部端口	内部端口	服务器 IP 地址
WEB 服务器	9000	80	192.168.1.10

外部端口：外网用户访问服务器使用的端口。

注意：以上参数仅供本文指导参考，请以实际为准。

5.5.3 设置方法

1、确认服务器搭建成功

设置虚拟服务器之前，请务必确认以下操作：

服务器	服务器设置为固定IP地址，默认网关为路由器的管理地址。
防火墙	建议关闭服务器的防火墙与杀毒软件。
局域网	确认局域网的电脑可以通过服务器的IP地址和开放的端口访问到服务器。

2、添加虚拟服务器规则

登录路由器的管理界面，点击“传输控制>NAT 设置>虚拟服务器”，点击“新增”，添加如下映射规则，并点击“确定”。

规则名称:	WEBSERVER	生效接口选择为端口映射的出接口，外网用户 使用该接口的IP来访问服务器	
生效接口:	WAN1	(1-65535,格式为X或X-X或X,X) 外部端口为外网用户访问服务器使用的端口	
外部端口:	9000	(1-65535,格式为X或X-X或X,X) 内部端口为服务器使用的端口	
内部端口:	80		
内部服务端IP:	192.168.1.10		
服务协议:	ALL		
环回地址:	/	+	(可选)
状态:	<input checked="" type="checkbox"/> 启用		
<input type="button" value="确定"/> <input type="button" value="取消"/>			

注意：由于宽带运营商可能会屏蔽 80、8080 等常用端口，因此建议外部端口不使用这些端口，外部端口可以设置为 9000 以上的端口。

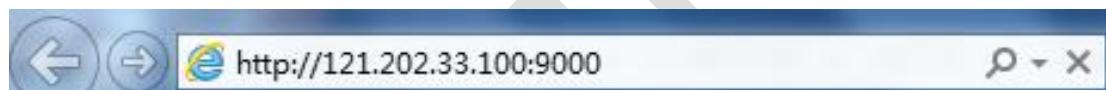
添加之后的条目如下：

	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
	1	WEBServer	WAN1	9000	80	192.168.1.10	ALL	已启用	

至此，虚拟服务器规则设置完成。

3、外网访问服务器

根据以上设置，外网的用户通过浏览器访问 WEB 服务器，访问形式如下：



说明：

- 1) 具体的访问形式以实际服务器要求为准。
- 2) 如果您的宽带并非静态IP地址，可以在“动态DNS”中申请域名账号并在路由器中登录该账号，登录成功后使用域名和开放的端口访问服务器。

5.6 NAT-DMZ 功能设置指南

5.6.1 应用介绍

企业在内部搭建各种服务器，如 FTP 服务器、WEB 服务器、邮件服务器、监控服务器等。而这些服务器并不仅仅是针对内网用户开放的，外网的用户也需要通过互联网来访问。NAT-DMZ 功能可以实现将内网的服务器映射到 Internet，从而实现外网的访问。

本文介绍 ER 系列路由器的虚拟服务器功能的配置步骤。



5.6.2 需求分析

某小型企业需要将 WEB 服务器、FTP 服务器、监控服务器对外网开放，且希望内外网都可以使用协议默认的端口进行访问。用户网络参数如下：

服务器类型	默认端口	服务器 IP 地址
WEB 服务器	80/443	192.168.1.199
FTP 服务器	20/21	192.168.1.199

监控服务器	8888	192.168.1.199
-------	------	---------------

注意：以上参数仅供本文指导参考，请以实际为准。

5.6.3 设置方法

1、确认服务器搭建成功

设置 NAT-DMZ 之前，请务必确认以下操作：

服务器	服务器设置为固定IP地址，默认网关为路由器的管理地址。
防火墙	建议关闭服务器的防火墙与杀毒软件。
局域网	确认局域网的电脑可以通过服务器的IP地址和开放的端口访问到服务器。

2、添加 NAT-DMZ 规则

登录路由器的管理界面，点击“传输控制>NAT 设置>NAT-DMZ”，点击“新增”，添加如下规则，并点击“确定”。



The screenshot shows a configuration dialog for adding a new NAT-DMZ rule. The fields are as follows:

- 规则名称: DMZ
- 出接口: WAN1
- 主机地址: 192.168.1.199
- 状态: 启用

Two red annotations are present on the right side of the dialog:

- A red box highlights "WAN1" with the text "外网用户使用该接口的IP访问服务器" (External network users access the server via this interface's IP).
- A red box highlights "192.168.1.199" with the text "内网服务器的IP地址" (Internal network server's IP address).

注意：由于宽带运营商可能会屏蔽 80、8080 等常用端口，因此需要确认所使用的端口在当前宽带线路下是可以在互联网上进行访问的。

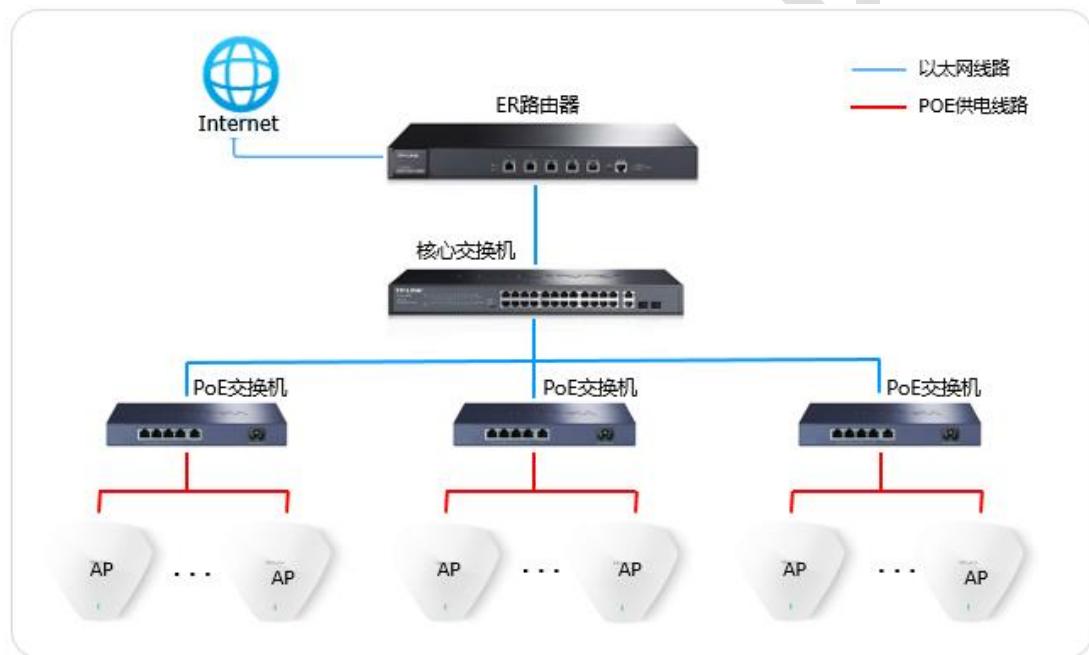
至此，NAT-DMZ 设置完成，终端在内外网都可以使用协议默认的端口进行访问。

第6章 AP 和易展管理

6.1 AP 管理设置指南

6.1.1 应用介绍

ER 系列路由器，内置 AC 功能，既是路由器又是无线控制器，可以统一管理 TP-LINK AP，轻松扩展企业无线网络。本文介绍 ER 系列新平台路由器 AP 管理功能的配置方法。



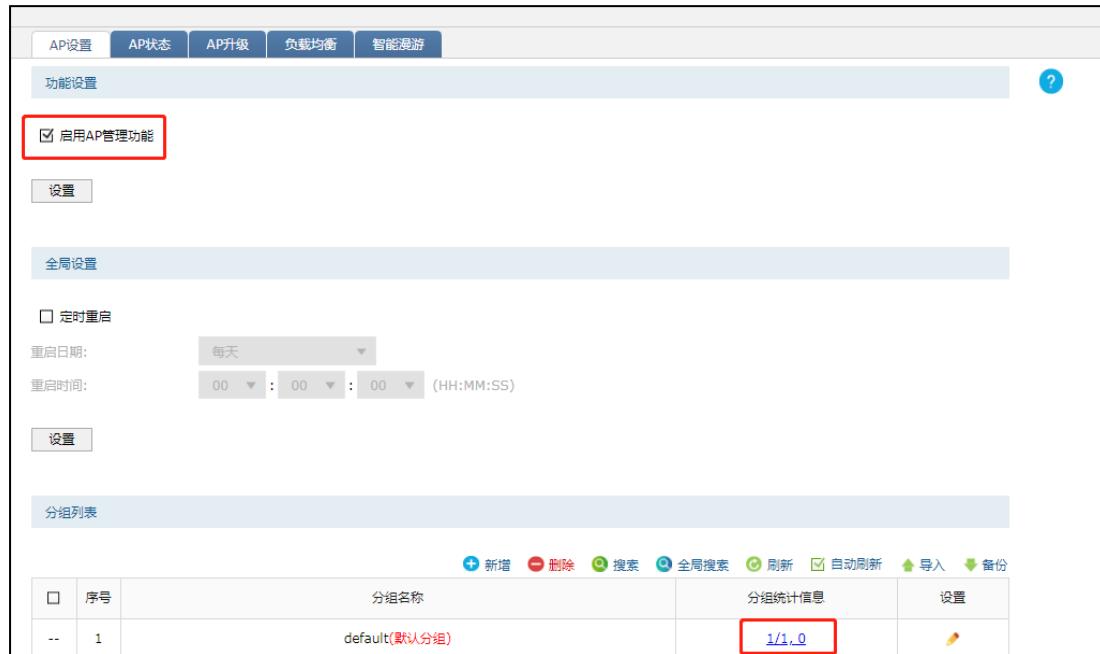
6.1.2 需求分析

某企业使用无线 AP 进行无线组网，通过主路由器集中管理无线 AP。需要设置员工无线网络供企业员工使用。

6.1.3 设置方法

1、启用 AP 管理功能

登录到路由器界面，点击“AP 管理>AP 设置”，启用“AP 管理功能”，分组列表中将会显示当前在线的 AP，点击分组确认路由器已经发现所有 AP，接下来可以对 AP 进行管理。



【温馨提示】若部分 AP 无法发现，请确认 AP 的模式开关已拨到 FIT 模式、同时检查 AP 与交换机之间的网线已接好。

2、设置 AP 的无线网络

点击“AP 管理>无线服务设置”，点击 新增，设置员工无线网络，如下图：

无线服务设置							
□	序号	SSID	描述	安全选项	状态	射频绑定	设置
--	--	--	--	--	--	--	--
状态: <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 SSID: Office (1-32个字符) 设置无线名称 描述: 员工网络 (1-50个字符, 可选) 无线网络内部隔离: <input type="radio"/> 启用 <input checked="" type="radio"/> 禁用 隐藏无线网络: <input type="radio"/> 启用 <input checked="" type="radio"/> 禁用 安全选项: WPA-PSK/WPA2-PSK 选择无线加密方式 认证类型: 自动 加密算法: 自动 组密钥更新周期: 86400 (30-604800) 秒, 不更新则为0 PSK密码: 1a2b3c4d (8-63个ASCII码字符或64个十六进制字符) 设置无线密码 带宽控制: <input type="radio"/> 启用 <input checked="" type="radio"/> 禁用 自动绑定所有AP: <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 选择是否自动绑定所有AP 射频选择: 全部, 2.4G1, 2.4G2, 5G 绑定VLAN: (1-4094, 可选)							
<input type="button" value="确定"/> <input type="button" value="取消"/>							

【温馨提示】“自动绑定所有 AP”的选项，如果启用，则接入的所有 AP 都将自动绑定该无线设置，此时需要选择所要绑定的射频，不需要进行下方第三步操作；如果禁用该功能，则需要手动去绑定射频，也就是需要进行第三步操作。

3、射频绑定

如果设置无线服务时禁用了自动绑定所有 AP 功能，则需要手动进行射频绑定。

点击“AP 管理>无线服务设置”，点击“射频绑定”，选择需要绑定的 AP，如下图：

无线服务设置

序号	SSID	描述	安全选项	状态	射频绑定	设置
1	Office	---	WPA-PSK/WPA2-PSK	已启用	<input checked="" type="radio"/>	<input type="button" value="绑定"/>

先勾选需要绑定的射频，再点击<绑定>即可。

'Office'的自动绑定设置

自动绑定所有AP: 启用 禁用 禁用该功能后才可以进行射频绑定

射频选择: 全部, 2.4G1, 2.4G2, (1-4094, 可选)

绑定VLAN: (1-4094, 可选)

设置

'Office'的手动绑定设置

选择AP分组: default

绑定VLAN: (1-4094, 可选)

点击绑定

返回无线服务 取消绑定 搜索 全局搜索

序号	AP名称	射频单元	射频模式	绑定状态	绑定VLAN
1	TL-AP1908GC-PoE/DC-0001	1(2.4GHz)	802.11b/g/n	未绑定	---
2	TL-AP1908GC-PoE/DC-0001	2(5GHz)	802.11a/n/ac	未绑定	---

绑定完成后，射频的“绑定状态”显示为“绑定”。

The screenshot shows the TP-LINK web configuration interface for the ER series routers. The left sidebar navigation includes: 运行状态, 基本设置, 对象管理, AP管理 (selected), AP设置, 射频设置 (selected), 无线服务设置, 客户端状态, 传输控制, 安全管理, 行为管控, VPN, 认证管理, 系统服务, and 系统工具. The main content area has tabs for 无线服务设置 and 'Office'的自动绑定设置. Under '自动绑定所有AP':

- 启用 (radio button selected)
- 禁用 (radio button)
- 射频选择: 全部, 2.4G1, 2.4G2, ... (dropdown menu)
- 绑定VLAN: (1-4094, 可选) (input field)

 A note below says: 注意: 如果需要手动绑定射频, 请禁用当前无线服务的自动绑定所有AP功能.
 Below is the 'Office'的手动绑定设置 section with:

- 选择AP分组: default (dropdown menu)
- 绑定VLAN: (1-4094, 可选) (input field)

 At the bottom is a table of bound APs:

	序号	AP名称	射频单元	射频模式	绑定状态	绑定VLAN
<input type="checkbox"/>	1	TL-AP1908GC-PoE/DC-0001	1(2.4GHz)	802.11b/g/n	绑定	---
<input type="checkbox"/>	2	TL-AP1908GC-PoE/DC-0001	2(5GHz)	802.11a/n/ac	绑定	---

 Other interface elements include: 返回无线服务 (Return to Wireless Service), 绑定 (Bind), 取消绑定 (Unbind), 搜索 (Search), 全局搜索 (Global Search), and pagination: 共2条, 每页: 10 条 | 当前: 1/1页, 1~2条 | (1) 1 (2).

4、射频调优

无线配置完成后，使用路由器自带射频调优功能，可以对 AP 的无线信道和发射功率进行自动调整，以保障良好的无线体验。

点击“AP 管理>射频设置>射频调优”，进行 AP 频段带宽和信道调整，同时可选择启用功率调优和自动调优，配置完成后点击立即调优即可：

射频设置 频谱导航 射频调优

调优参数设置

信道调优: 启用 禁用 **选择启用信道调优**

2.4G信道调优

频段带宽: 20MHz **选择固定2.4G频段带宽**

2.4G信道集合: 1,6,11 **选择固定2.4G信道集合**

5G信道调优

频段带宽: 40MHz **选择固定5G频段带宽**

5G信道集合: 36,44,149,157 **选择固定5G信道集合**

功率调优: 启用 禁用 **选择启用功率调优**

覆盖阈值: -65 dBm (-80~-50, 缺省值=-65)

最大功率: 50 dBm (10-50, 缺省值=50)

最小功率: 10 dBm (3-30, 缺省值=10)

定时调优: 启用 禁用 **选择启用定时调优**

日期: 每天

时间: 00 : 00 : 00 (HH:MM:SS)

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。

无线配置和 AP 射频调优设置完成，所有 AP 都能同时发射 Office 的无线信号，供企业员工使用。

至此，ER 系列新平台路由器搭配 AP 无线组网设置完成。

6.2 易展 AP 设置指南

6.2.1 应用介绍

随着互联网技术的快速发展，需求无线网络覆盖的地方越来越多，此时出现了一些传统网络无法解决的复杂区域和快速完成组网的需要，也有个人用户不想破坏原有的装修环境来进行网络覆盖。对于一些区域来说传统网络的组网方案不仅复杂且成本较高。为了解决这些问题，TP-LINK 新推出了带有“易展”功能的 AP，能够实现快速组网，无需布线，简单实现组网，且可以替换某些传统组网，优化整个网络。

6.2.2 需求分析

某多层写字楼想要在已有的 AP 组网中增加部分区域的无线覆盖范围，但是想要覆盖的区域不方便布线，区域的终端接入数和流量不大。

组网特点：

不方便布线；

不想破坏办公环境；

有临时增加网络位点的需求；

需要对设备统一管理，方便维护。

6.2.3 网络拓扑



6.2.4 设置方法

1、如何配对

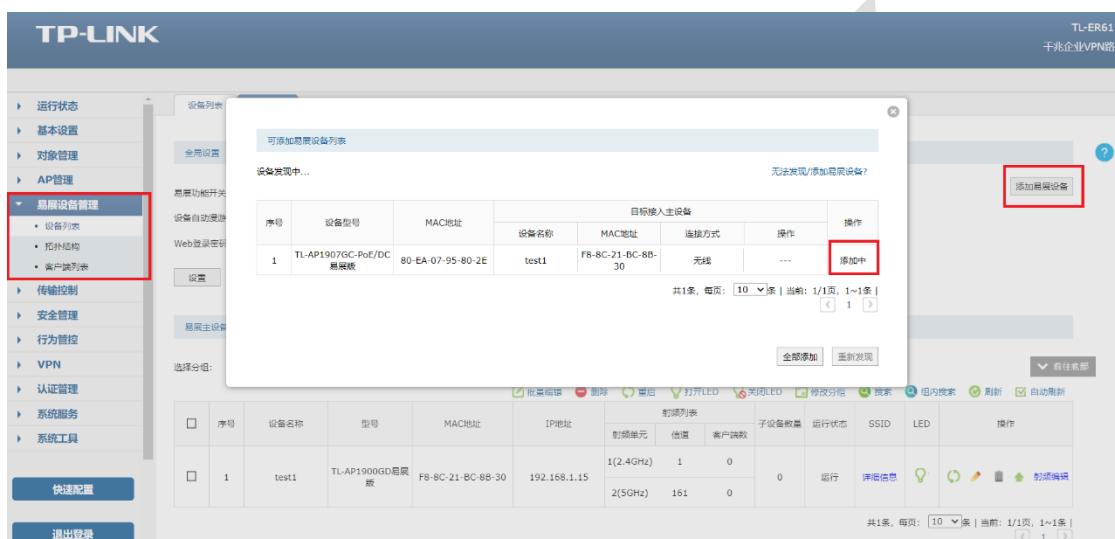
需要使用 FIT 模式下进行多个 MESH 单元组网，出厂状态下，将设备接入局域网中，若局域网中存在开启 AP 管理功能的 AC 或路由器，易展 AP 将自动识别并工作在 FIT 模式；同时 AC 或路由器需要开启易展管理功能，即可发现并管理易展 AP。



添加易展 AP 子设备，点击设备列表或拓扑结构页面右上角的“添加易展设备”按钮，此时主 AP 会自动搜索周围待配对的子 AP，发现设备后点击全部添加，等待一会儿即可完成配对。

 **相关说明:**

- 1) 通过 Web 页面搜索可以同时和多台子 AP 进行易展配对。
- 2) 配对过程需要保持子设备处于出厂的待配对状态。



2、如何使用

(1) 设备列表

在 FIT 模式下，易展 AP 的功能和普通 AP 基本是一样的，例如 LED 开关、射频编辑、设备升级、AP 列表查看等等；易展 AP 特有的功能主要有“易展主子 AP 列表分开展示”、“主设备冗备”和“子设备更换主 AP”。

首先是主子 AP 的列表页面，可以在此页面对主子设备做相应的操作。

The screenshot shows the TP-LINK ER series management interface. On the left, there is a navigation sidebar with various management options like '运行状态', '基本设置', '对象管理', 'AP管理', etc. The 'Easy Device Management' section is currently selected. It contains two tables: one for '易用设备列表' (main AP) and one for '易用子设备列表' (client device). The main AP table has a single row for 'test1'. The client device table also has a single row for 'test1'. A red box highlights the 'TL-AP1900GD 普通版' entry in the main AP's device list.

主设备冗备，可以通过此功能，将某个主 AP 的设备备份到新加入的主 AP，主要是用于主 AP 故障/替换的场景。

The screenshot shows the TP-LINK ER series management interface. The 'Easy Device Management' section is selected. A modal dialog box titled '备选设备列表' (Backup Device List) is open, showing a table with one row for 'test1'. A red box highlights the '目标设备' (Target Device) column. Below the table, a note says: '注意：执行替换操作后，目标设备将被删除，备选设备将继承目标设备的配置并重启。' (Note: After performing the replacement operation, the target device will be deleted, and the backup device will inherit the configuration of the target device and restart.)

子设备更换主设备，灵活调整组网，可以通过手动设置将子 AP 关联到信号更好的主 AP 上。

TP-LINK

TL-ER6...
千兆企业VPN

运行状态 基本设置 对象管理 AP管理 易展设备管理 传输控制 安全管理 行为管控 VPN 认证管理 系统服务 系统工具 快速配置

设备列表 设备升级

选择主AP列表

序号	设备名称	MAC地址	状态	操作
1	test1	F8-8C-21-BC-8B-30	运行	当前主易展设备

共1条, 每页: 10 条 | 当前: 1/1页, 1~1条 | 1

易展子设备

序号	设备名称	型号	MAC地址	IP地址	射频列表	运行状态	SSID	LED	主设备信息	操作
1	TL-AP1907GC-PoE/DC 易展版-0003	TL-AP1907GC-PoE/DC 易展版	80-EA-07-95-80-2E	192.168.1.10	1(2.4GHz) 2(5GHz)	运行	test1 (F8-8C-21-BC-8B-30)	<input checked="" type="checkbox"/>	详细信息	刷新 脚本编辑

共1条, 每页: 10 条 | 当前: 1/1页, 1~1条 | 1

(2) 拓扑结构

能够显示设备的网络拓扑，型号（名称）、IP 地址等参数。

TP-LINK

TL-ER6110G
千兆企业VPN路由器

运行状态 基本设置 对象管理 AP管理 易展设备管理 拓扑结构 传输控制 安全管理 行为管控 VPN 认证管理 系统服务 系统工具 快速配置 退出登录

拓扑图

设备名称 IP地址 刷新 放大 缩小

添加易展设备

TL-ER6110G 4.0 交换机 test1 TL-AP1907GC-P...

有线连接 无线连接

(3) 客户端列表

可以显示接入易展设备的终端情况，包括接入时间，设备 MAC，接入射频，信号强度、IP 地址等信息。

以上就是易展 AP 的 FIT 模式使用方法及配置方式。

备注：只有开启 AP 管理功能才能使用易展管理功能，开启易展管理功能才能使用 FIT 模式
的易展功能。

第7章 行为管控

7.1 连接数限制设置指南

7.1.1 应用介绍

通信过程中，点与点之间建立的任何一个独立连接均会在路由器上进行维护，从而确保通信数据正常转发。路由器内部维护着一张连接表，用来存放连接信息，该列表会动态占用内存、CPU 资源。由于表的总大小是固定的，如果某个时候，表中的连接达到最大数目，此时新的连接无法建立，导致数据转发异常。

简单理解为：路由器的连接总数是固定值（有上限的），如果其中的一部分电脑消耗了过多的连接数（如 BT、迅雷下载等），可能会导致其余的电脑无法正常上网。连接数限制功能可以控制主机占用的连接数，从而均衡网络应用，确保平稳使用。

7.1.2 需求分析

某公司网关路由器使用 ER 系列路由器，经常有电脑使用迅雷或 BT 下载，连接数可以达到上千，占用过多连接数，影响其他电脑的应用。

为了避免局域网部分主机占用过多的连接，通过设置连接数限制优化网络应用。

7.1.3 设置方法

登录到路由器界面，点击“传输控制>连接数限制”，勾选“启用连接数限制功能”



在连接数限制列表中，点击“新增”，添加连接数限制规则。



注意：如设置 300，所有受控用户的最大连接数均为 300；普通上网应用，建议设置最大连接数为 200-300。

至此，连接数限制功能设置完成。

7.1.4 疑问解答

Q1、为什么设置连接数限制功能后，打开网页很慢？

实际应用中，一些门户网站主页（如 www.sohu.com/www.sina.com.cn）及部分网页内容较多的网页，连接数接近或大于 200。

如果连接数设置的非常小（比如 50），会导致网页打开缓慢甚至显示不完整的情况。普通上网应用，建议设置为 200-300。

Q2、设置连接数限制功能后，为什么用户在下载时，还是占用大量带宽？

连接数限制的功能主要是限制病毒、攻击的影响，避免某个主机占用过多连接。如果要控制内网电脑的带宽，建议配合带宽控制功能使用。



7.2 URL 过滤设置指南

7.2.1 应用介绍

URL (统一资源定位符)是万维网资源定位标志，就是通常所讲的网址 (如 www.tp-link.com.cn)。URL 过滤功能即针对 URL 中的关键字或者完整的 URL 进行限制或允许，实现访问对应网站的权限的控制。ER 系列路由器的 URL 过滤针对地址组进行控制，可以实现网页访问限制、行为审计等功能。

本文介绍 ER 系列企业路由器的 URL 过滤功能的设置方法。

7.2.2 需求分析

某企业使用 ER 系列企业路由器，为了规范网络使用情况，制定不同部门的网络访问权限，权限如下：

部门	网络权限
市场部	只能访问公司官网 (https://www.tp-link.com.cn)
其他部门	禁止访问所有网页

7.2.3 设置方法

1、添加地址组

添加市场部的用户组，其他部门无需设置对应的用户组，后续的控制规则中针对用户组进行控制。

在路由器界面，点击“对象管理>地址管理>地址”，点击“新增”，添加市场部地址。

地址名称: Marketing

IP类型: IP段 IP/Mask

192.168.2.0 / 24

备注: (可选)

确定 取消

在路由器界面，点击“对象管理>地址管理>地址组”，点击“新增”，将市场部地址添加到市场部地址组中：

组名称: Marketing

地址名称: Marketing ▾

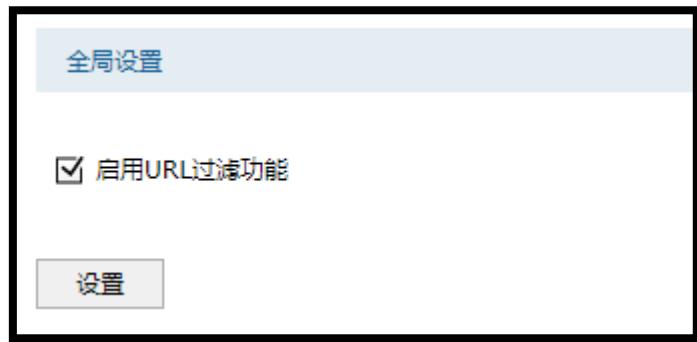
备注: (可选)

确定 取消

2、设置 URL 过滤规则

(1) 启用 URL 过滤功能

登录路由器的管理界面，点击 行为管控 > 网址过滤 > URL 过滤，勾选 启用 URL 过滤功能，点击 设置。



(2) 添加市场部规则

在 URL 地过滤规则中，用户组选择 Marketing，策略类型选择 允许访问下列的 URL，过滤内容列表输入公司官网的关键字，点击 确定。详细设置见下图：

用户组: Marketing

策略类型: 允许访问下列的URL

过滤方式: 关键字 (highlighted with a red box)

过滤内容列表: tp-link.com.cn (highlighted with a red box)

过滤内容列表输入网址的关键字 (highlighted with a red box)

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 (unchecked)

生效时间: Any

状态: 启用 (checked)

备注: (可选, 1-50个字符)

添加到指定位置(第几条): (可选)

确定 取消

注意：关键字指域名中的任何字符，比如 www.tp-link.com.cn 中的“www”、“tp-link”、“com”、“cn”、“.”等。如果网站域名中添加关键字，表示受控地址组中的成员可以访问带有该关键字的任何网址。

(3) 添加其它部门的规则

用户组选择 IPGROUP_ANY，策略类型选择 禁止访问下列的 URL，过滤内容列表的位置输入关键字“.”代表所有网址。如下图所示：



注意：如果需要记录所有用户访问的网页或拦截的网页，需要勾选以上规则中的“记录到系统日志”。

设置完成后，URL 过滤规则列表如下：

URL过滤规则列表										
	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	
<input type="checkbox"/>	1	Marketing	允许	关键字	tp-link.com.cn	Any	已启用 ×	---		
<input type="checkbox"/>	2	IPGROUP_ANY	禁止	关键字	.	Any	已启用 ×	---		

至此, URL 过滤规则设置完成, 局域网的所有电脑浏览网页的权限将按照 URL 规则来执行。

7.2.4 疑问解答

Q1、URL 过滤支持哪些格式的网站? 不支持哪些格式的网站?

输入格式 (支持)	输入格式 (不支持)
域名: www.baidu.com 通配符+后缀: *.baidu.com 关键字: baidu 完整 URL: https://service.tp-link.com.cn/detail_download_8363.html IP+端口: 10.10.10.10:80	无

Q2、URL 过滤关键字可以限制哪些字段?

企业路由器的 URL 过滤可以限制 URI 字段的内容, 也就是网页地址的任何关键字都可以限制。比如: https://service.tp-link.com.cn/detail_download_8363.html 这个域名, 可以限制该域名中的任何关键字 (_、t、v、8363、cn 等任何字符)。

Q3、URL 过滤设置完成后, 如何将访问过的网页记录下来?

该需求需要勾选规则中的“记录到系统日志”。但因为系统内存有限, 建议结合行为审计软件或者安全审计系统实现, 将访问内容记录到行为审计软件或者安全审计系统。

Q4、设置 URL 过滤后, 访问的网站显示不全, 怎么办?

常见门户网站存在域名之间的调用关系，并不是所有的网站都像我司官网那样一个*.tp-link.com.cn 就可以搞定的，如果只允许一个主域名（比如只允许 www.taobao.com 可能淘宝网的主页有很多部分无法正常显示）将无法完全打开该网页。下面整理了淘宝网的所有域名，仅供参考。



Q5、设置好 URL 过滤，限制不生效，怎么办？

设置完成 URL 过滤后，限制不生效，需要考虑以下几个方面：首先，检查被限制的电脑 IP 地址在受控组中；请确认针对受控组设置的控制规则正确，如关键字、禁用或允许、规则是否启用等；请确认设置的关键字合理，尝试修改关键字；请确认规则设置顺序正确，默认禁用规则需要放在最后一条。

7.3 访问控制设置指南

7.3.1 应用介绍

企业办公网络环境中，需要对内部办公电脑进行网络权限差异化设置，从而提升办公效率和网络安全。访问控制功能通过对源/目的 IP 地址、端口及访问时间进行控制，实现上网权限的差异化设置，满足企业用户的需求。

本文介绍 ER 系列路由器访问控制功能的设置方法。

7.3.2 需求分析

某企业使用 ER 系列路由器，需要实现市场部上网不受限制，其它部门只能浏览网页。根据需求，制定以下配置表：

部门	允许的上网行为
市场部	所有网络应用
其它部门	浏览网页

注意：上述参数仅供参考，具体以实际应用为准。

7.3.3 设置方法

1、添加市场部地址组

在路由器界面，点击“对象管理>地址管理>地址”，点击“新增”，添加市场部 IP 地址。

地址名称: Marketing

IP类型: IP段 IP/Mask

192.168.1.10 - 192.168.1.20

备注: (可选)

确定 取消

在路由器界面，点击“对象管理>地址管理>地址组”，点击“新增”，将市场部 IP 地址添加到市场部地址组中：

组名称: Marketing

地址名称: Marketing

备注: (可选)

确定 取消

2、设置 HTTPS 服务

访问控制的设置中，服务类型仅包含了 FTP、邮件服务、DNS 以及 HTTP 等常用服务。当要添加新的服务（或端口）时，需要在“对象管理>服务类型”中新增条目。本例需要添加 HTTPS 服务：

服务名称: HTTPS

协议类型/协议号: TCP UDP TCP/UDP ICMP Other

源端口范围: 0 - 65535 (0-65535) 源端口填写0-65535

目的端口范围: 443 - 443 (0-65535) 目的端口填写443

备注:

确定 取消

3、设置市场部的访问控制规则

点击“安全管理>访问控制”，点击  新增，添加策略规则：允许市场部访问所有网络应用，如下图所示：



The screenshot shows the configuration interface for a new policy rule:

- 规则名称:** Marketing (1-50个字符)
- 策略类型:** 允许 (策略类型选择允许)
- 服务类型:** ALL (服务类型选择所有)
- 生效接口域:** LAN (生效接口域选择LAN)
- 源地址范围:** Marketing (源地址选择所有市场部地址段)
- 目的地址范围:** IPGROUP_ANY (目的地址选择所有)
- 生效时间:** Any (时间选择所有)
- 添加到指定位置(第几条):** (可选)

Buttons at the bottom: 确定 (Confirm) and 取消 (Cancel).

4、设置其它部门的访问控制规则

其它部门的员工，只允许浏览网页，即需要开放 HTTP、HTTPS、以及 DNS 服务，添加规则如下：



The screenshot shows the configuration interface for a new policy rule:

- 规则名称:** Others_HTTP (1-50个字符)
- 策略类型:** 允许 (策略类型选择允许)
- 服务类型:** ALL (服务类型选择HTTP)
- 生效接口域:** LAN (生效接口域选择LAN)
- 源地址范围:** IPGROUP_LAN (源地址选择所有LAN网段)
- 目的地址范围:** IPGROUP_ANY (目的地址选择所有)
- 生效时间:** Any (时间选择所有)
- 添加到指定位置(第几条):** (可选)

Buttons at the bottom: 确定 (Confirm) and 取消 (Cancel).

规则名称:	Others_HTTPS	(1-50个字符)
策略类型:	允许	策略类型选择允许
服务类型:	HTTPS	服务类型选择HTTPS
生效接口域:	LAN	生效接口域选择LAN
源地址范围:	IPGROUP_LAN	源地址选择所有LAN网段
目的地址范围:	IPGROUP_ANY	目的地址选择所有
生效时间:	Any	时间选择所有
添加到指定位置(第几条):	(可选)	
<input type="button" value="确定"/> <input type="button" value="取消"/>		

规则名称:	DNS	(1-50个字符)
策略类型:	允许	策略类型选择允许
服务类型:	DNS	服务类型选择DNS
生效接口域:	LAN	生效接口域选择LAN
源地址范围:	IPGROUP_LAN	源地址选择所有LAN网段
目的地址范围:	IPGROUP_ANY	目的地址选择所有
生效时间:	Any	时间选择所有
添加到指定位置(第几条):	(可选)	
<input type="button" value="确定"/> <input type="button" value="取消"/>		

5、设置阻塞规则

由于访问控制规则默认为“允许”，所以需要再添加禁止访问一切的规则才可以实现需求，规则如下：

规则名称:	Block	(1-50个字符)
策略类型:	阻塞	策略类型选择阻塞
服务类型:	ALL	服务类型选择所有
生效接口域:	LAN	生效接口域选择LAN
源地址范围:	IPGROUP_LAN	源地址选择所有LAN网段
目的地址范围:	IPGROUP_ANY	目的地址选择所有
生效时间:	Any	时间选择所有
添加到指定位置(第几条):	(可选)	
<input type="button" value="确定"/> <input type="button" value="取消"/>		

添加完成后，规则列表如下：

访问控制规则列表									
	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	Marketing	Marketing	IPGROUP_ANY	允许	ALL	LAN	Any	
<input type="checkbox"/>	2	Others_HTTP	IPGROUP_LAN	IPGROUP_ANY	允许	HTTP	LAN	Any	
<input type="checkbox"/>	3	Others_HTTPS	IPGROUP_LAN	IPGROUP_ANY	允许	HTTPS	LAN	Any	
<input type="checkbox"/>	4	DNS	IPGROUP_LAN	IPGROUP_ANY	允许	DNS	LAN	Any	
<input type="checkbox"/>	5	Block	IPGROUP_LAN	IPGROUP_ANY	阻塞	ALL	LAN	Any	

至此，访问控制设置完成，局域网中所有电脑将拥有所属的部门对应的上网权限。

7.3.4 疑问解答

Q1：设置允许访问网页的规则，为什么依旧无法访问？

需要排查以下方面：受控电脑的 IP 地址必须在对应的受控组中，规则才能起作用；按照以上步骤检查规则设置是否正确，确定设置的源、目的地址正确（限制内网主机、生效接口域）

选择 LAN)；确认添加允许 HTTPS 服务，否则涉及 HTTPS 的网页将无法访问；确认添加允许 DNS 服务，否则涉及域名的网页将无法访问。



7.4 应用限制设置指南

7.4.1 应用介绍

企业网络环境中，经常需要实现对一些常见上网应用（如迅雷下载、QQ、电驴等）进行限制，通俗的理解就是实现“一键屏蔽”。通过企业路由器的应用控制功能可以实现管控。

本文介绍 ER 系列路由器应用控制功能的设置方法。

7.4.2 需求分析

某公司市场部由于工作需要，对网络访问没有任何限制，但部分员工在上班时间炒股、QQ 聊天、迅雷下载电影，影响了正常工作，并占用了大量的带宽。为提高员工的工作效率，网络管理员制定如下需求：

- 1、仅允许市场部员工登录企业 QQ、微信、阿里旺旺（相对于限制列表）；
- 2、允许市场部员工登录 12345678, 987654321 这两个 QQ 号码；
- 3、其它部门不做限制；

7.4.3 设置方法

1、添加市场部地址组

在路由器界面，点击“对象管理>地址管理>地址”，点击“新增”，添加市场部 IP 地址。

地址名称: Marketing

IP类型: IP段 IP/Mask

192.168.1.10 - 192.168.1.20

备注: (可选)

确定 取消

在路由器界面，点击“对象管理>地址管理>地址组”，点击“新增”，将市场部 IP 地址添加到市场部地址组中：

组名称: Marketing

地址名称: Marketing

备注: (可选)

确定 取消

2、启用并设置应用控制功能

登录路由器的管理界面，点击 “行为管控 >> 应用控制”，勾选“启用应用控制功能”，点击设置。

功能设置

启用应用控制功能

设置

在应用控制规则列表中，点击“新增”，为市场部设置如下规则：



3、启用并设置 QQ 白名单

点击“行为管控>应用控制>QQ 白名单”，勾选“启用 QQ 黑白名单”，点击设置：



在规则列表中，点击“新增”，设置允许市场部登录如下 QQ，选择规则生效时间，点击确定。

用户组: Marketing

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

填写允许登录的QQ号码
多个QQ号码以换行或者逗号隔开

QQ号码:

当使用上述QQ号码时: 记录到系统日志

生效时间: Any [选择生效时间](#)

备注: (可选)

状态: 启用 禁用

添加到指定位置(第几条): (可选)

[确定](#) [取消](#)

至此，应用控制功能设置完成，市场部的员工在使用网络过程中，视频软件、购物软件、P2P 软件、网络游戏、炒股等上网行为将会被禁止。

7.5 网址过滤设置指南

7.5.1 应用介绍

企业网络环境中，不同部门允许访问的网页权限也不同。如：市场部需要访问各类网站，但对游戏、视频、购物类的网站则无需求。企业路由器的网站过滤功能可以实现对不同类别的网页进行权限设置，从而实现合理管控网络权限的目的。

本文档详细介绍 ER 系列企业路由器的网站过滤的设置方法。

7.5.2 需求分析

某企业需要限制公司不同部门的网络权限，需求如下：

部门	网络权限
市场部	禁止访问视频、游戏、购物类网站
其他部门	仅允许访问公司网站及百度

7.5.3 设置方法

1. 添加地址组

添加市场部的用户组，其他部门无需设置对应的用户组，后续的控制规则中针对用户组进行控制。

在路由器界面，点击“对象管理>地址管理>地址”，点击“新增”，添加市场部地址。

This screenshot shows the configuration dialog for creating a new IP address group. The fields are as follows:

- 地址名称 (Address Name): Marketing
- IP类型 (IP Type): IP段 (IP Range) IP/Mask
- IP/Mask input field: 192.168.2.0 / 24
- 备注 (Remarks): (Optional) (可选)
- Buttons: 确定 (Confirm) and 取消 (Cancel)

在路由器界面，点击“对象管理>地址管理>地址组”，点击“新增”，将市场部地址添加到市场部地址组中：

This screenshot shows the configuration dialog for adding an IP address to a group. The fields are as follows:

- 组名称 (Group Name): Marketing
- 地址名称 (Address Name): Marketing (dropdown menu)
- 备注 (Remarks): (Optional) (可选)
- Buttons: 确定 (Confirm) and 取消 (Cancel)

2、添加网站分组

点击“行为管控>网址过滤>网站分组”，点击“新增”，添加其他部门允许访问的网站分组，如下：

组名称: 官网及百度 (1-28个字符)

组成员: *tp-link.com.cn
*baidu.com
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*只允许输入在最前面, 而不能夹杂在域名中间或后面
清空
请使用换行或者分号来分隔网址

文件路径: 浏览 (可选, 文件格式为txt)
导入 您还可以通过导入文件来配置组成员

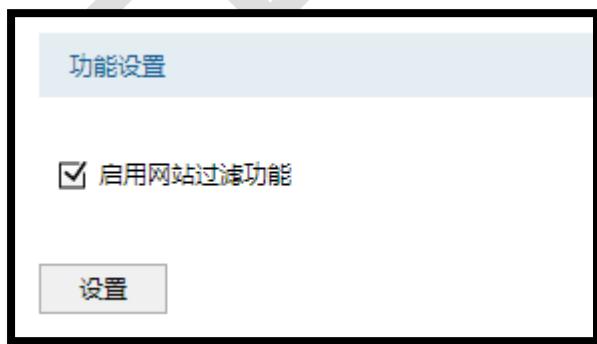
备注: (可选)

确定 取消

注意: 在组成员中可以使用通配符 (*) 的方式来添加网站 (例如*.baidu.com, 即可匹配 www.baidu.com、news.baidu.com、mp3.baidu.com 等网页。

3、设置网站过滤规则

登录路由器的管理界面, 点击 行为管控 > 网址过滤 > 网站过滤, 勾选 启用网站过滤功能, 点击 设置。



在“行为管控>网址过滤>网站过滤”, 点击“新增”, 添加市场部的过滤规则。

先添加禁止的规则, 禁止市场部访问视频、游戏、购物类的网站, 如下图:

用户组: Marketing

规则类型: 允许访问 禁止访问

选择网站: 视频, 游戏, 购物

访问上述网站时: 记录到系统日志

生效时间: Any

备注: (可选)

添加到指定位置(第几条): (可选)

状态: 启用

再添加允许的规则, 允许市场部访问其他网站, 如下图:

用户组: Marketing

规则类型: 允许访问 禁止访问

选择网站: 所有网站

访问上述网站时: 记录到系统日志

生效时间: Any

备注: (可选)

添加到指定位置(第几条): (可选)

状态: 启用

添加其他部门的规则

在“行为管控>网址过滤>网站过滤”，点击“新增”， 用户组选择 IPGROUP_ANY，添加其他部门的规则。

先添加一条允许的规则，允许其他部门访问官网及百度，如下图：



再添加禁止的规则，禁止其他部门访问所有网站，如下图：

用户组: IPGROUP_ANY

规则类型: 允许访问 禁止访问

选择网站: 所有网站

访问上述网站时: 记录到系统日志

生效时间: Any

备注: (可选)

添加到指定位置(第几条): (可选)

状态: 启用

设置完成，可以查看到网站过滤的列表如下：

规则列表								
	序号	用户组	规则类型	网站过滤列表	生效时间	状态	备注	设置
<input type="checkbox"/>	1	Marketing	禁止访问	视频,游戏,购物	Any	已启用 X	---	
<input type="checkbox"/>	2	Marketing	允许访问	所有网站	Any	已启用 X	---	
<input type="checkbox"/>	3	IPGROUP_ANY	允许访问	官网及百度	Any	已启用 X	---	
<input type="checkbox"/>	4	IPGROUP_ANY	禁止访问	所有网站	Any	已启用 X	---	

至此，网站过滤功能设置完成，企业所有部门员工将按照设置的规则来上网。

7.5.4 疑问解答

Q1、网站过滤支持哪些格式的网站？不支持哪些格式的网站？

输入格式 (支持)	输入格式 (不支持)
域名: www.baidu.com	单独关键字: baidu
通配符+后缀: *.baidu.com	IP+端口: 10.10.10.10:80

通配符+关键字：*baidu	
----------------	--

Q2、设置网站访问，不生效怎么办？

设置网站访问后，确保上网电脑的 IP 地址是在受控地址组内，电脑的 DNS 地址设置正确；

请检查限制的网站分组中是否包含被限制域名（分组默认包含主流的域名）；检查规则设置逻辑合理，针对某一个地址组，先设置允许规则，后设置禁止规则。

Q3、网站过滤设置完成后，如何将访问过的网页记录下来？

该需求需要勾选规则中的“记录到系统日志”。但因为系统内存有限，建议结合行为审计软件或者安全审计系统实现，将访问内容记录到行为审计软件或者安全审计系统。

Q4、设置网站访问后，允许访问的网页页面显示不完整，怎么办？

一般情况下，该类问题出现在对门户网站的访问权限管理上，比如网易、搜狐等主页。该类网页多数为嵌套域名，即并非只有 www.163.com 或 www.sohu.com 一个单独的域名构成。如果仅允许访问*.163.com 或*.sohu.com，则可能出现无法打开完整网页的问题。如果需要设置仅允许访问这些门户网站，需要添加所有嵌套域名。主流域名的嵌套如下：

域名	关键字
网易	163、126、netease、midia、127
搜狐	sohu、itc
新浪	sina
腾讯	qq、gtimg、tencent

7.6 网页安全设置指南

7.6.1 应用介绍

企业网络环境中，对于访问网络的安全性的要求较高，对上传和下载有严格的要求，尤其是对于一些 exe、rar、txt 等类型文件有严格限制。网页安全功能可以限制内网用户通过网络提交信息，同时可以对下载文件的扩展类型进行管控，对常见扩展类型的文件的下载权限进行限制，从而实现网络应用安全。

本文介绍 ER 系列路由器的网页安全功能的设置方法。

7.6.2 需求分析

某企业网络环境中，为了确保内部网络安全，需求如下：

- 1、禁止企业内部部分终端对网页内容的上传和网站、论坛等用户名密码的登录；
- 2、禁止企业内部部分终端从网页上下载 exe, rar 后缀的文件。

7.6.3 设置方法

1、添加用户组

添加受控终端的用户组，方便后续的控制规则针对用户组进行控制。在路由器界面，点击“对象管理>地址管理>地址”，点击“新增”，添加受控 IP 地址。

This screenshot shows the configuration dialog for adding an IP address group. It includes fields for 'Address Name' (IP_Control), 'IP Type' (IP Segment selected), 'Start IP' (192.168.1.100), 'End IP' (192.168.1.199), and an optional note field. At the bottom are 'Confirm' and 'Cancel' buttons.

地址名称:	IP_Control
IP类型:	<input checked="" type="radio"/> IP段 <input type="radio"/> IP/Mask
	192.168.1.100 - 192.168.1.199
备注:	(可选)
<input type="button" value="确定"/> <input type="button" value="取消"/>	

在路由器界面，点击“对象管理>地址管理>地址组”，点击“新增”，将受控 IP 地址添加到地址组中：

This screenshot shows the configuration dialog for adding an IP address group. It includes fields for 'Group Name' (IP_Control), 'Address Name' (IP_Control selected from a dropdown), and an optional note field. At the bottom are 'Confirm' and 'Cancel' buttons.

组名称:	IP_Control
地址名称:	IP_Control
备注:	(可选)
<input type="button" value="确定"/> <input type="button" value="取消"/>	

2、启用网页安全功能

登录路由器的管理界面，点击 “行为管控 >> 网页安全”，勾选“启用网页安全功能”。

This screenshot shows the 'Function Settings' section of the management interface. It has a checkbox for 'Enable Web Security Function' which is checked, and a 'Settings' button below it.

功能设置
<input checked="" type="checkbox"/> 启用网页安全功能
<input type="button" value="设置"/>

3、设置规则

在规则列表中，点击“新增”，选择相应的用户组，选择禁止网页提交（禁止上传和网站、论坛等用户名密码的登录），填写需要过滤文件的扩展类型，设置完成后，点击确定。如下图所示：



过滤文件扩展类型：即文件的类型，如压缩包 rar、zip 等，安装软件 exe 等。

至此，网页安全设置完成，局域网内的电脑在上网的过程中，将会按照上述的设置的规则使用网络。

第8章 安全防护

8.1 ARP 防护设置指南

8.1.1 应用介绍

ARP 是 IP 与 MAC 地址的解析协议，对网络通信至关重要。一般情况下，上网数据直接在主机和网关之间进行交互，ARP 欺骗主要针对网关和主机的 ARP 列表进行欺骗，导致通信异常。常见的 ARP 欺骗软件有“网络执法官”、“P2P 终结者”、“QQ 第六感”等。那么 ARP 防护就需要从两个方面着手，在网关上绑定主机的 ARP 信息，在主机上绑定网关的 ARP 信息，从而实现双向绑定，确保网络安全。

本文介绍 ER 系列路由器的 ARP 防护功能的设置方法。

8.1.2 设置方法

1、手动指定绑定电脑的 IP 地址

在设置 ARP 绑定之前，请给需要绑定的电脑手动指定 IP 地址。

如果不清楚如何设置，请参考：[如何给终端手动指定 IP 地址？](#)

同时，建议查看对应电脑的 MAC 地址，制作 IP、MAC、电脑的表格，便于后续维护，如下图所示：

使用人	IP 地址	MAC 地址	备注
张三	192.168.32.100	8C-16-45-9F-5B-B0	办公电脑
...

注意：以上表格仅供参考，具体信息请根据实际需要记录。

2、路由器上添加绑定条目

登录路由器的管理界面，点击“安全管理>ARP 防护>IP-MAC 绑定”，在 IP-MAC 绑定界面添加绑定条目。有两种添加方法：手动逐条添加和扫描添加。具体方法请根据实际需要来选择，方法如下：

(1) 手动添加方法：

手动添加操作复杂，但是安全性高。在网络中已经存在 ARP 欺骗或者不确定网络中是否存在 ARP 欺骗的情况下，建议使用手动添加的方式。手工进行添加，先点击  新增，填写需要绑定的电脑的 IP 和 MAC 地址，选择生效域，填写备注信息，并点击“确定”。如下图所示：



IP地址:	192.168.32.100
MAC地址:	8C-16-45-9F-5B-B0 (MAC地址格式:XX-XX-XX-XX-XX-XX)
生效域:	LAN
备注:	张三 (可选,0-50个字符)
状态:	<input checked="" type="checkbox"/> 启用

确定 **取消**

(2) 扫描添加方法：

简单快捷，但是要确定网络中没有 ARP 欺骗，否则绑定错误的 IP/MAC 条目可能导致内网部分主机无法上网。在扫描范围输入需要扫描的 IP 地址段后，点击“开始扫描”，此时等待一会，路由器会自动查找当前内网的主机，并显示主机的 IP 和 MAC 地址信息，如下图所示：



注意：ARP 扫描只能检测当前网络中的活动主机，如果主机处于关机状态，则 ARP 扫描无法发现该主机。

勾选所有条目，再点击“添加到绑定列表”，所有的绑定条目就设置完成了。

	序号	IP地址	MAC地址	生效域	备注	状态	设置
<input type="checkbox"/>	1	192.168.32.9	90-76-9F-E6-F4-6A	LAN	---	已启用	
<input type="checkbox"/>	2	192.168.32.3	8C-16-45-9F-5B-BC	LAN	---	已启用	

注意：ARP 扫描的功能也可以扫描 WAN 口的网段，可以通过扫描绑定 WAN 口网关地址防止前端 ARP 欺骗（宽带拨号无需绑定）。

3、启用 ARP 绑定功能

局域网中电脑的 IP 与 MAC 全部绑定完成后，在“安全管理> ARP 防护> IP-MAC 绑定”中，确认已勾选“启用 ARP 防欺骗功能”，点击“设置”。如下图所示：



注意：如果勾选仅允许 IP-MAC 绑定的数据包通过路由器，则不在绑定列表或与绑定列表冲突的电脑不能上网或管理路由器。

至此，路由器防止 ARP 欺骗设置完成。

4、电脑绑定网关 ARP 信息

仅在路由器上绑定主机的 MAC 地址并不能完全解决 ARP 欺骗的问题，在主机上绑定路由器的 MAC 地址，即双向绑定，就可以彻底解决欺骗问题。以下介绍不同操作系统电脑的绑定方法：

(1) Windows XP 系统：

在电脑上建立一个文本文件，写入 ARP 绑定命令：“arp -s IP MAC”，如下图所示：



注意：IP 是路由器的管理地址（192.168.1.1），MAC 是路由器 LAN 口的 MAC 地址（01-02-03-04-05-06）。

保存之后将该文件修改为.bat 后缀的批处理文件，比如“arp.bat”。然后将其放入系统启动项中，以后系统每次开机时都会执行该绑定命令。如下图所示：



(2) Windows 7/ Windows 8/ Windows 10 系统：

- 打开命令提示符，使用命令：“netsh i i show in”查看网卡 idx 编号；
- 查询到网卡 idx 编号后，再使用命令“ netsh -c i i add neighbors idx ip mac”进行 ARP 绑定，如下图所示：

```

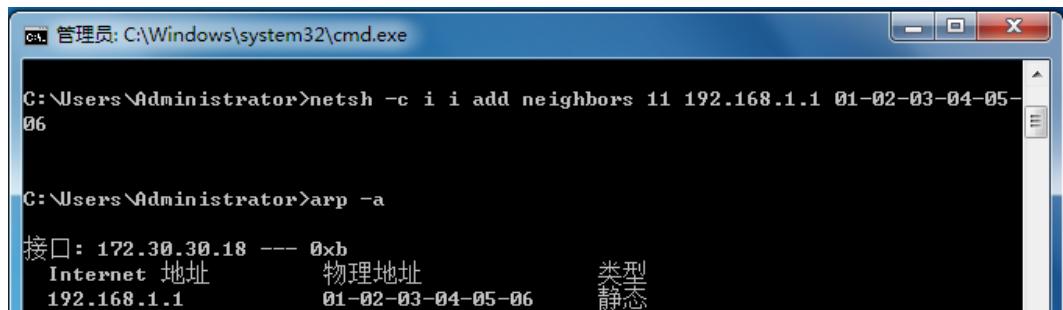
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 © 2009 Microsoft Corporation。保留所有权利。
C:\Users\Administrator>netsh i i show in 网卡Idx编号查询命令
Idx      Met          MTU        状态          名称
-----  --  -----  -----
  1          50    4294967295  connected  Loopback Pseudo-Interface 1
  11         20        1500  connected  本地连接

ARP绑定命令格式: netsh -c i i add neighbors Idx IP MAC
C:\Users\Administrator>netsh -c i i add neighbors 11 192.168.1.1 01-02-03-04-05-06

```

注意：Windows 8/ Windows 10 系统中以太网为有线网卡。Windows 8 系统中 Wi-Fi 为无线网卡，Windows 10 系统中 WLAN 为无线网卡。

- 使用 arp -a 的命令可以查询到绑定是否生效，如下图所示：



A screenshot of a Windows Command Prompt window titled "管理员: C:\Windows\system32\cmd.exe". The window shows two commands being run:

```
C:\Users\Administrator>netsh -c i i add neighbors 11 192.168.1.1 01-02-03-04-05-06  
C:\Users\Administrator>arp -a
```

The output of the "arp -a" command is displayed in a table:

接口: 172.30.30.18 --- 0xb	Internet 地址	物理地址	类型
	192.168.1.1	01-02-03-04-05-06	静态

设置完成后，电脑重启，ARP 绑定条目也不会失效。

注意：如果需要删除 ARP 绑定条目，只需要输入命令：

netsh -c i i delete neighbors idx(idx 表示编号)，重启电脑后，绑定删除。

至此全部的设置就完成了，后续无需担心 ARP 欺骗给网络带来的影响。

8.1.3 疑问解答

Q1、设置 ARP 绑定不生效，怎么办？

由于 ARP 欺骗是双向的，请确认已经在路由器及电脑上都做好 ARP 绑定，同时确保内网电脑的 IP 地址是手动指定的。

Q2、设置 ARP 绑定后，电脑上不了网怎么办？

确保上不了网的电脑 ARP 信息在路由器绑定列表，如果信息不一致，请修正设置；如果路由器上勾选了“禁止非 IP-MAC 绑定的数据包通过路由器”，请确保上不了网的电脑已经在路由器上做了绑定。

Q3、仅启用“ARP 防欺骗功能”与“禁止非 IP-MAC 绑定的数据包通过路由器”有什么区别？

两者都是防止 ARP 欺骗的，区别在于：启用禁止非 IP-MAC 绑定的数据包通过路由器，则没有做绑定或绑定信息与路由器设置的条目不符的电脑，无法上网，也不可以管理路由器。

仅设置启用 ARP 防欺骗，没有设置绑定的电脑还是可以上网的（但电脑 MAC 参数与绑定条目不符的，同样无法上网及管理路由器）。

Q4、为何开启绑定后，界面卡死（无法操作）？

设置 ARP 绑定的时候，建议先添加绑定条目，然后再开启绑定开关。如果先开启强制绑定的开关，那么当列表为空时，会导致管理主机无法管理路由器，表现出来管理页面卡死的现象。

8.2 MAC 地址过滤设置指南

8.2.1 应用介绍

每个网络设备都有一个唯一的标识，即 MAC 地址。MAC 地址过滤功能可以有效控制电脑的网络接入权限，并且还可以避免因电脑 IP 地址变化而导致规则不生效的问题。

本文介绍 ER 系列路由器的 MAC 地址过滤功能的设置方法。

8.2.2 设置方法

1、启用 MAC 地址过滤功能

在路由器界面，点击“安全管理>MAC 地址过滤”，启用 MAC 地址过滤功能，选择对应的规则类型和生效接口域，点击“保存”。



2、添加 MAC 地址

点击“新增”，添加受控电脑的 MAC 地址。



上述设置完成后，只有规则列表中 MAC 地址的电脑如“zhangsan”才能上网，列表外的均无法上网。

注意：如果您的需求为列表中 MAC 地址的电脑不能上网，列表外的均能上网。那么需要将步骤 1 中的规则类型选择为“仅禁止规则列表内的 MAC 地址访问外网”。

第9章 VPN 模块

9.1 IPsec VPN 设置指南

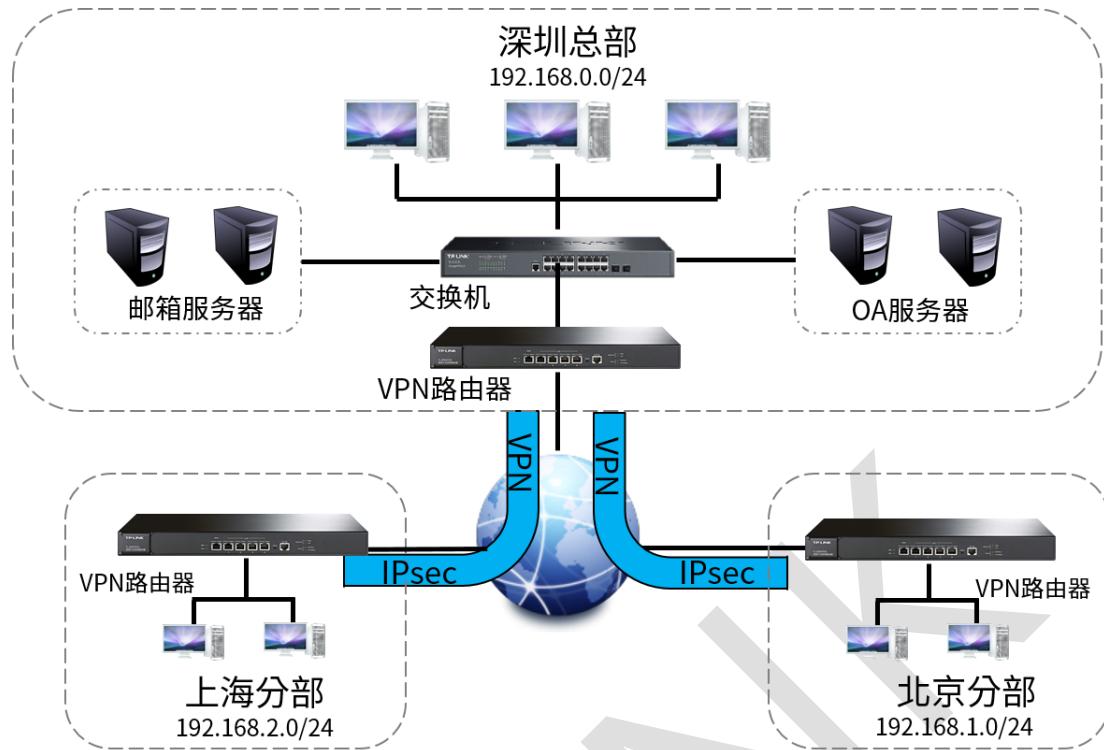
9.1.1 应用介绍

企业级路由器提供多类 VPN 功能。其中 IPSec VPN 可以实现企业站点之间搭建安全的数据传输通道，将接入 Internet 的企业分支机构与总部网络通过安全隧道互联，实现资源、信息共享。权限。

9.1.2 需求介绍

某公司总公司位于深圳，在北京、上海两地有分公司，现需要组建一个网络，达到三个机构能资源共享的目的，本文将通过一个实例来展示 TL-ER6520G 与 TL-ER3220G 搭建 IPsec VPN 的解决方案和配置过程。

深圳总公司局域网网段为“192.168.0.0/24”，WAN 口为公网 IP：183.15.15.15；北京分公司为“192.168.1.0/24”，WAN 口为公网 IP：183.15.15.30；上海分公司为“192.168.2.0/24”；



9.1.3 设置方法

深圳总部 TL-ER6520G 设置步骤

第一步、基本设置

1、设置路由器的 WAN 口模式：基本设置>> WAN 口设置，进入 WAN 口模式 标签页，

根据需求设置 WAN 口数量，此处我们保持默认为“双 WAN 口”，保存。

2、设置 WAN 口网络参数：基本设置>> WAN 口设置，在 WAN1 设置 标签页，设置 WAN

口网络参数以及该线路的上下行带宽值。此处设置 WAN 口为固定 IP：183.15.15.15.

注意：VPN 两端路由器 WAN 口需要公网 IP，如没有公网 IP 则需要考虑 NAT 下的 IPsec 应用，见链接：

[NAT 下的 IPSEC VPN 配置实例](#)

第二步、IPsec VPN 设置

此处以配置北京分公司与深圳总公司间的 IPsec VPN 为例，首先配置深圳总公司的 TL-

ER6520G：

(1) 配置 IPsec 安全策略基本设置: VPN >> IPsec, 进入 IPsec 安全策略 标签页, 点击新增。

The screenshot shows the 'IPsec安全策略' (IPsec Security Policy) configuration page. The 'IPsec安全策略' tab is selected. A table lists existing policies, all showing '-' in every column. Below the table, configuration fields are displayed:

- 策略名称: IPsec_sz (1-32个字符)
- 对端网关: 183.15.15.30 (IP地址或域名)
- 绑定接口: WAN1
- 本地子网范围: 192.168.0.0 / 24
- 对端子网范围: 192.168.1.0 / 24
- 预共享密钥: 123456 (1-128个字符) - This field is highlighted with a red border, and a note says '设置预共享密钥，双方的预共享密钥必须相同' (Set pre-shared key, both parties' pre-shared keys must be the same).
- 状态: 启用

At the bottom are '确定' (Confirm) and '取消' (Cancel) buttons.



相关参数说明如下:

- 1) 策略名称: 设置 IPsec 安全策略名称。
- 2) 对端网关: 填写对端 IPsec VPN 服务器的 IP 地址或者域名, 此处为北京分公司 TL-ER3220G WAN 口 IP 地址“183.15.15.30”。
- 3) 绑定接口: 从下拉列表中指定本地使用的接口; 对端网关设置的“对端网关地址”必须与该接口的 IP 地址相同。
- 4) 本地子网范围: 设置本地子网范围, 即深圳总公司局域网“192.168.0.0 /24”。
- 5) 对端子网范围: 设置对端子网范围, 即北京分公司局域网“192.168.1.0 /24”。
- 6) 预共享密钥: 设置 IKE 认证的预共享密钥, 通信双方的预共享密钥必须相同。

7) 状态：设置勾选启用时，当前策略生效。

(2) 配置 IPsec 安全策略高级设置：在基本设置完成后，点击高级设置，包括两个部分：

阶段 1 设置和阶段 2 设置。一般不需要配置高级设置，采用默认值即可。

阶段1设置

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

阶段2设置

封装模式:	<input checked="" type="radio"/> 隧道模式 <input type="radio"/> 传输模式	选择封装模式
安全提议:	esp-md5-3des	选择安全提议
安全提议:	---	
安全提议:	---	
安全提议:	---	
PFS:	none	选择PFS
生存时间:	28800	秒(120-604800)



相关参数说明如下：

阶段一设置：设定 IKEv1 的第一阶段的相关参数。

- 1) 安全提议：选择合适的的 IPsec 安全提议，注意需要与对端保持一致。
- 2) 交换模式：主模式（Main mode）适用于对身份保护要求较高的场合；野蛮模式（Aggressive mode）适用于对身份保护要求较低的场合，推荐使用主模式。
- 3) 协商模式：初始者模式会主动向对端发起连接，此时要求对端网关是路由可达，而响应者模式仅仅会等待对端发起连接。
- 4) 本地 ID 类型：作为对端的身份标识，支持两种类型：IP 地址和 NAME，默认选择"IP 地址"，如果选择 NAME 类型，则需要输入任意的字符串。
- 5) 生存时间：用于 IKE 协商方式下 IPsec 会话密钥的生存时间。
- 6) DPD 检测：Dead Peer Detect，检测对端在线状态，建议启用。

阶段 2 设置：设定 IKEv1 的第二阶段的相关参数

- 1) 封装模式：指定该策略是隧道模式还是传输模式，两者的区别在于：前者会在原始 IP 报文外多增加一个 IP 头，后者则不会。
- 2) 安全提议：选择 IKEv1 第二阶段合适的的 IPsec 安全提议，注意需要与对端保持一致。
- 3) PFS：用于 IKE 协商方式下设置 IPsec 会话密钥的 PFS 属性，本地与对端的 PFS 属性必须一致。
- 4) 生存时间：用于 IKE 协商方式下 IPsec 会话密钥的生存时间。

上海、北京公司 TL-ER3220G VPN 配置方法

第一步、基本设置

设置路由器的 WAN 口模式：网络参数 >> WAN 口设置，根据需求设置 WAN 口连接类型，此处我们设置为静态 IP：183.15.15.30。

第二步、IPsec VPN 设置

此处以配置北京分公司与深圳总公司间的 IPsec VPN 为例，首先要先配置深圳总公司的 TL-ER6520G，再进行配置分部 TL-ER3220G：

- (1) 配置 IPsec 安全策略基本设置：VPN >> IPsec >> IPsec 安全策略

点击 新增，进行基本设置配置，填写策略名称、对端网关，选择绑定接口、填写本地子网范围、对段子网范围、预共享密码需要与总部相同，选择启用。

上图中各个选项意义上文 TL-ER6520G 中的意义相同。点击保存，生成 IPsec 条目。

(2) 配置 IPsec 安全策略高级设置：VPN >> IPsec

点击 高级设置，进行 IKEv1 阶段 1 和阶段 2 配置。如果总部保持的默认配置，分部也保存默认配置即可，如果总部做了修改，则分部应保持一致。

本例中总部高级设置均为默认参数，且分部与总部 web 界面相同，此处不再展示。

配置完成后点击保存，在 IPsec 安全策略列表中会出现一个条目：

配置完成，IPsec 安全联盟建立成功后，可以在 IPsec 安全联盟中看到相应条目，北京分公司的局域网“192.168.1.0/24”与深圳总公司局域网“192.168.0.0 /24 ”间可相互访问。

IPSec安全策略									IPSec安全联盟		
IPSec安全联盟列表									操作		
条目数量: 2									刷新		
序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法		
1	IPsec_bj	3222533904	in	183.15.15.30<->183.15.15.15	192.168.1.0/24 <-> 192.168.0.0/24	ESP	--	MD5	3DES		
2	IPsec_bj	3240553103	out	183.15.15.30-->183.15.15.15	192.168.1.0/24 --> 192.168.0.0/24	ESP	--	MD5	3DES		

共2条, 每页: 10 条 | 当前: 1/1页, 1~2条 | [上一页](#) [下一页](#) [1](#) [下一页](#)

9.2 L2TP VPN 设置指南

9.2.1 应用介绍

企业路由器提供多类 VPN 功能。其中 L2TP VPN 可以实现企业站点之间搭建安全的数据传输通道，将接入 Internet 的企业分支机构与总部网络通过安全隧道互联，实现资源、信息共享；并支持 PC 端建立 L2TP VPN 隧道，满足外出员工移动办公需求。

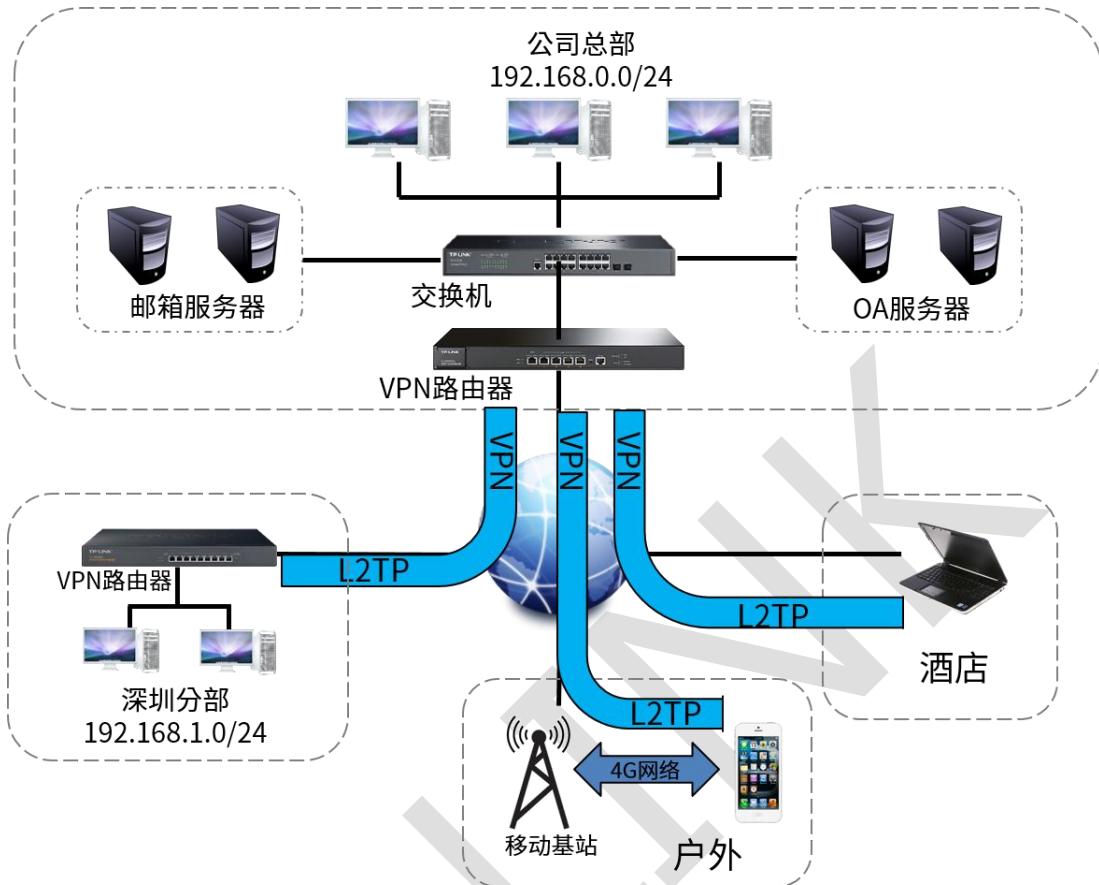
本文介绍使用 ER 系列新平台路由器搭建站点到站点以及 PC 到站点的 L2TP 安全隧道的方法。

9.2.2 需求介绍

某公司的总部与分部均使用 ER 系列新平台路由器。需要实现将北京总部与深圳分公司通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性。需求参数如下：

L2TP 账号/密码	123/123
地址池	10.10.10.11~10.10.10.200
加密	开启
总部网段	192.168.0.0/24
分部网段	192.168.1.0/24

9.2.3 应用拓扑



9.2.4 L2TP 站点到站点设置方法

服务器端的设置 (以 TL-ER6520G 为例)

1、进入管理界面

设置 LAN 口网段 (与客户端不在同一个网段) ,本例中将 LAN 网段设置为 192.168.0.0/24

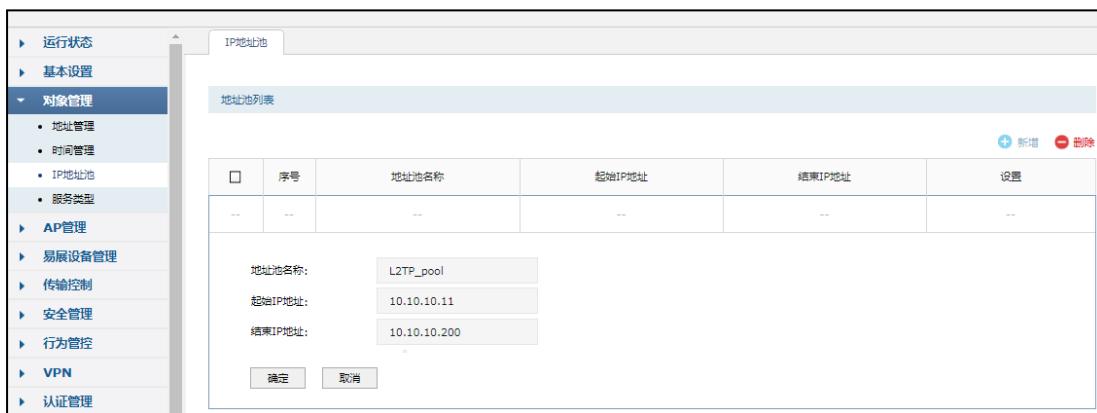
2、WAN 口设置

静态 ip 方式上网或者 PPPoE 方式上网 (如果使用的是 PPPoE 上网, 由于获取的 IP 地址会变化, 此时建议使用动态域名 DDNS), 本例使用静态 IP: 183.15.15.15。

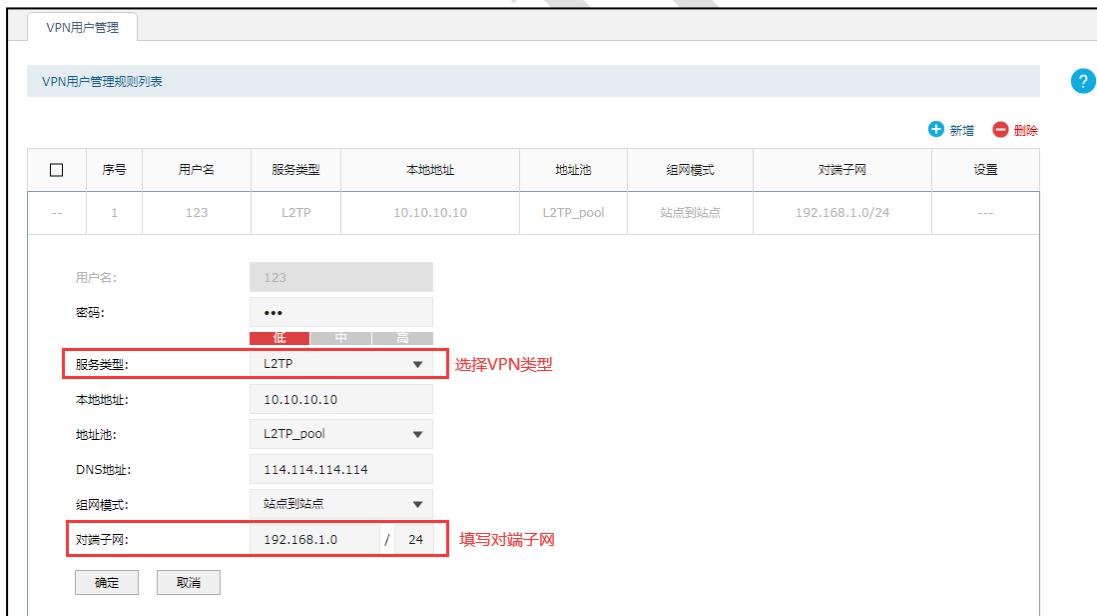
注: 服务器端 WAN 口 IP 推荐为公网 IP, 若非公网 IP, 需要在前端设备做映射。

3、L2TP 服务器的设置

- A. 打开 对象管理->IP 地址池 页面：新增隧道地址池(L2TP vpn 隧道通信时使用的 ip 地址)：



- B. 打开 VPN->用户管理 页面，进行用户管理配置，点击新增。



参数说明：

- 1) 用户名：客户端与服务器端建立连接的用户名。
- 2) 密码：客户端与服务器端建立连接的密码。

- 3) 服务类型: L2TP: 本用户只用于 L2TP; L2TP: 本用户只用于 L2TP; 自动: 本用户既可用于 L2TP 也可用于 L2TP。
- 4) 本地地址: VPN 隧道的本地虚拟 IP 地址。
- 5) 地址池: 就是 A 步骤建立的隧道地址池, 选择即可。
- 6) 组网模式: 可选择站点到站点或 PC 到站点。
- 7) 对端子网范围: 客户端 LAN 口的网段 (服务器端和客户端 LAN 口地址不能在同一网段)。
- 8) 最大连接数: 这种模式下不能填写 (PC 到站点的模式时可以填写 1-10)。

C. 打开 VPN->L2TP 页面, 设置 L2TP VPN 服务器:

口	序号	服务接口	IPSec加密	状态	设置
--	--	--	--	--	--



参数说明:

- 1) 服务接口: L2TP 服务器监听的接口, 只有来自服务接口的报文才会被处理。
- 2) IPSec 加密: 是否对隧道进行加密, 可选择加密、不加密、可选加密。

- 3) 预共享密钥：设置 IPSec 加密时的预共享密钥，VPN 两端需要保持一致。
- 4) MTU：MTU (Maximum Transmission Unit, 最大传输单元)，在一定物理网络中能传送的最大数据单元。可选设置。

客户端的设置（以 TL-ER3220G 为例）

1、进入管理界面

设置 LAN 口网段（与服务器端不在同一个网段），本例为 192.168.1.0/24

2、WAN 口设置

正确设置 WAN 口上网方式，保证路由器可以正常上网。

3、L2TP 客户端的设置

打开 VPN->L2TP ->L2TP 客户端 页面，新增填写客户端配置信息。

L2TP服务器 L2TP客户端 隧道信息列表

隧道名称:	sz_bj	(1-12个字符)
用户名:	123	
密码:	***	
出接口:	WAN1	
服务器地址:	183.15.15.15	填写服务器地址
IPSec加密:	加密	
预共享密钥:	123456789	(1-128个字符)
对端子网:	192.168.0.0 / 24	
上行带宽:	1000000	Kbps (100-1000000)
下行带宽:	1000000	Kbps (100-1000000)
MTU:		(可选)
工作模式:	<input checked="" type="radio"/> NAT <input type="radio"/> 路由	
状态:	<input checked="" type="checkbox"/> 启用	
运营商:	---	
<input type="button" value="确定"/> <input type="button" value="取消"/>		



参数说明:

- 1) 用户名: 服务器端设置的用户名。
- 2) 密码: 服务器端设置的密码。
- 3) 出接口: 选择已经设置上网的 WAN 口。
- 4) 服务器地址: 服务器 WAN 口地址, 或者填域名: 例如 vs.yueshen.gd (服务器端申请的动态域名)。
- 5) IPSec 加密: 选择是否加密, 与服务器端设置一致。
- 6) 预共享密钥: 选择加密时需要填写预共享密钥, 与服务器端保持一致。
- 7) 对端子网范围: 服务器端 LAN 口的网段 (与本地 LAN 不同网段)。

- 8) 工作模式： NAT：对经过此 L2TP 隧道的数据包进行 NAT 转换（数据包的源 IP 替换为 L2TP 隧道的本地虚拟 IP）。路由：对经过此 L2TP 隧道的数据包进行路由转发。

服务器端和客户端条目建立后，都选择启用，成功建立后在服务器端和客户端的 L2TP 隧道信息中将有对应的条目。

服务器隧道条目：

序号	用户名	服务器/客户端	隧道名称	虚拟本地IP	接入服务IP	对端虚拟IP	DNS
1	123	服务器	---	10.10.10.10	183.15.15.30	10.10.10.11	---

共1条，每页：10 条 | 当前：1/1页，1~1条 | < 1 >

客户端条目：

序号	用户名	服务器/客户端	隧道名称	虚拟本地IP	接入服务IP	对端虚拟IP	DNS
1	123	客户端	sz_bj	10.10.10.11	183.15.15.15	10.10.10.10	114.114.114.114

共1条，每页：10 条 | 当前：1/1页，1~1条 | < 1 >

9.2.5 L2TP PC 到站点设置方法

服务器端的设置（以 TL-ER6520G 为例）

需要在用户管理配置中添加 PC 到站点的用户账号密码，组网模式选择 PC 到站点，其余设置步骤与上面相同：

The screenshot shows a 'VPN User Management' interface with a 'VPN User Management Rule List' table. The table has columns:序号 (Index), 用户名 (Username), 服务类型 (Service Type), 本地地址 (Local Address), 地址池 (Address Pool), 组网模式 (Networking Mode), 对端子网 (Peer Subnet), and 设置 (Settings). A single row is present with all fields empty. Below the table is a configuration form:

用户名:	456
密码:	...
服务类型:	L2TP
本地地址:	10.10.10.10
地址池:	L2TP_pool
DNS地址:	114.114.114.114
组网模式:	PC到站点
最大会话数:	1 (1-100)

Buttons at the bottom: 确定 (Confirm) and 取消 (Cancel).

客户端的设置

不同 L2TP 客户端的配置方式有所差异, 请选择客户端操作系统, 参考对应指导文档:

[\[Windows XP\] L2TP VPN 客户端拨号操作步骤](#)

[\[Windows 7\] L2TP VPN 客户端拨号操作步骤](#)

[\[Windows 8\] L2TP VPN 客户端拨号操作步骤](#)

[\[Android\] L2TP VPN 客户端拨号操作步骤](#)

客户端拨号成功后, 可以在 L2TP 服务器隧道信息显示客户端信息。

9.2.6 常见问题解答

Q: 电脑拨号成功后, 如何访问分支机构网络?

电脑拨号成功后, 系统默认勾选了 VPN 连接 IPv4 高级设置中的“在远程网络上使用默认网关”, 则电脑所有数据优先从 VPN 接口转发, 即可正常访问总部资源。

如果需要通过总部进行代理转发访问分部资源，可在分部路由器上设置静态路由如下即可：

策略路由 静态路由 IPv6静态路由 系统路由

静态路由

启用 禁用 新增 删除 搜索 全局搜索

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: vpn_back
目的地址: 10.10.10.10 填写总部VPN地址池
子网掩码: 255.255.255.0
下一跳: 10.10.10.10 填写总部虚拟本地IP
出接口: sz_bj 选择对应VPN接口
Metric: 0 (0-15)
备注: (可选, 1-50个字符)
启用/禁用规则: 启用

确定 取消

9.3 PPTP VPN 设置指南

9.3.1 应用介绍

企业路由器提供多类 VPN 功能。其中 PPTP VPN 可以实现企业站点之间搭建安全的数据传输通道，将接入 Internet 的企业分支机构与总部网络通过安全隧道互联，实现资源、信息共享；并支持 PC 端建立 PPTP VPN 隧道，满足外出员工移动办公需求。

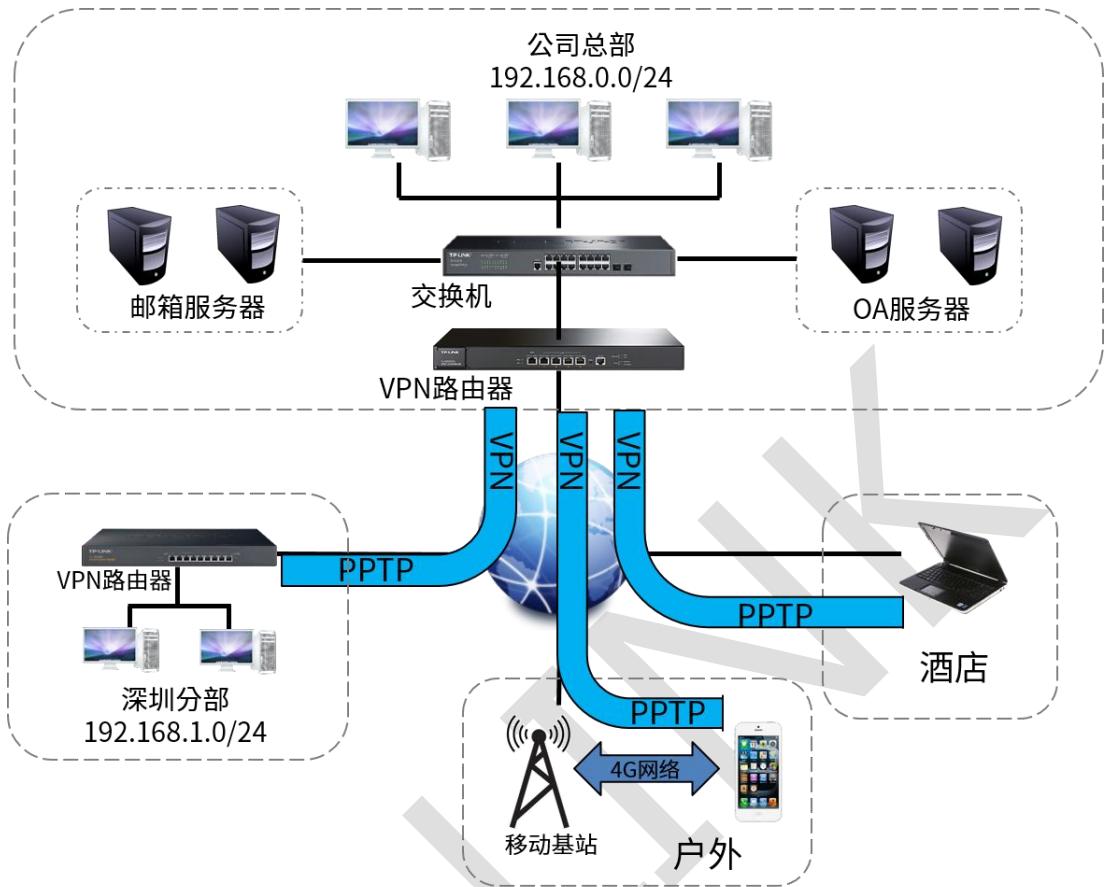
本文介绍使用 ER 系列新平台路由器搭建站点到站点以及 PC 到站点的 PPTP 安全隧道的方法。

9.3.2 需求介绍

某公司的总部与分部均使用 ER 系列新平台路由器。需要实现将北京总部与深圳分公司通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性。需求参数如下：

PPTP 账号/密码	123/123
地址池	10.10.10.11~10.10.10.200
加密	开启
总部网段	192.168.0.0/24
分部网段	192.168.1.0/24

9.3.3 应用拓扑



9.3.4 PPTP 站点到站点设置方法

服务器端的设置（以 TL-ER6520G 为例）

1、进入管理界面

设置 LAN 口网段（与客户端不在同一个网段），本例中将 LAN 网段设置为 192.168.0.0/24

WAN 口设置

静态 ip 方式上网或者 PPPoE 方式上网（如果使用的是 PPPoE 上网，由于获取的 IP 地址会变化，此时建议使用动态域名 DDNS），本例使用静态 IP：183.15.15.15。

2、PPTP 服务器的设置

- A. 打开 对象管理->IP 地址池 页面：新增隧道地址池(PPTP vpn 隧道通信时使用的 ip 地址)：

序号	地址池名称	起始IP地址	结束IP地址	设置
1	PPTP_pool	10.10.10.11	10.10.10.200	---

地址池名称: PPTP_pool
起始IP地址: 10.10.10.11
结束IP地址: 10.10.10.200

对象管理

- 地址管理
- 时间管理
- IP地址池
- 服务类型

VPN

- B. 打开 VPN->用户管理 页面，进行用户管理配置，点击新增。

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
--	123	PPTP	10.10.10.10	pptp_pool	站点到站点	192.168.1.0 / 24	--

用户名: 123
密码: ***
服务类型: PPTP
本地地址: 10.10.10.10
地址池: pptp_pool
DNS地址: 114.114.114.114
组网模式: 站点到站点
对端子网: 192.168.1.0 / 24

VPN用户管理

VPN用户管理规则列表

参数说明:

- 1) 用户名：客户端与服务器端建立连接的用户名。
2) 密码：客户端与服务器端建立连接的密码。

- 3) 服务类型: L2TP: 本用户只用于 L2TP; L2TP: 本用户只用于 L2TP; 自动: 本用户既可用于 L2TP 也可用于 L2TP。
- 4) 本地地址: VPN 隧道的本地虚拟 IP 地址。
- 5) 地址池: 就是 A 步骤建立的隧道地址池, 选择即可。
- 6) 组网模式: 可选择站点到站点或 PC 到站点。
- 7) 对端子网范围: 客户端 LAN 口的网段 (服务器端和客户端 LAN 口地址不能在同一网段)。
- 8) 最大连接数: 这种模式下不能填写 (PC 到站点的模式时可以填写 1-10)。

C. 打开 VPN->PPTP 页面, 设置 PPTP VPN 服务器:



服务器列表					
	序号	服务接口	MPPE加密	状态	设置
--	--	--	--	--	--

服务接口: WAN1 选择服务接口

MPPE加密: 加密 选择是否加密

MTU: (可选)

状态: 启用

确定 **取消**



参数说明:

- 1) 服务接口：PPTP 服务器监听的接口，只有来自服务接口的报文才会被处理。
- 2) MPPE 加密：是否对隧道进行加密。若启用，则使用 MPPE 对 PPTP 隧道加密。
- 3) MTU：MTU (Maximum Transmission Unit, 最大传输单元)，在一定物理网络中能传送的最大数据单元。可选设置。

客户端的设置（以 TL-ER3220G 为例）

1、进入管理界面

设置 LAN 口网段（与服务器端不在同一个网段），本例为 192.168.1.0/24

2、WAN 口设置

正确设置 WAN 口上网方式，保证路由器可以正常上网，本例为静态 IP：183.15.15.30。

3、PPTP 客户端的设置

打开 VPN->PPTP ->PPTP 客户端 页面，新增填写客户端配置信息。

PPTP服务器 PPTP客户端 隧道信息列表

隧道名称:	sz_bj	(1-12个字符)
用户名:	123	
密码:	***	
出接口:	WAN1	
服务器地址:	183.15.15.15	填写服务器地址
MPPE加密:	加密	
对端子网:	192.168.0.0 / 24	填写对端子网范围
上行带宽:	1000000	Kbps (100-1000000)
下行带宽:	1000000	Kbps (100-1000000)
MTU:	(可选)	
工作模式:	<input checked="" type="radio"/> NAT <input type="radio"/> 路由	
状态:	<input checked="" type="checkbox"/> 启用	
运营商:	不设置	
<input type="button" value="确定"/> <input type="button" value="取消"/>		



参数说明:

- 1) 用户名: 服务器端设置的用户名。
- 2) 密码: 服务器端设置的密码。
- 3) 出接口: 选择已经设置上网的 WAN 口。
- 4) 服务器地址: 服务器 WAN 口地址, 或者填域名: 例如 vs.yueshen.gd (服务器端申请的动态域名)。
- 5) MPPE 加密: 与服务器端设置一致。
- 6) 对端子网范围: 服务器端 LAN 口的网段 (与本地 LAN 不同网段)。

7) 工作模式： NAT：对经过此 L2TP 隧道的数据包进行 NAT 转换（数据包的源 IP 替换为 L2TP 隧道的本地虚拟 IP）。路由：对经过此 L2TP 隧道的数据包进行路由转发。

服务器端和客户端条目建立后，都选择启用，成功建立后在服务器端和客户端的 PPTP 隧道信息中将有对应的条目。

服务器隧道条目：



The screenshot shows a table titled '隧道信息列表' (Tunnel Information List) under the 'PPTP服务器' (PPTP Server) tab. The table has columns: 序号 (Index), 用户名 (Username), 服务器/客户端 (Server/Client), 隧道名称 (Tunnel Name), 虚拟本地IP (Virtual Local IP), 接入服务IP (Access Service IP), 对端虚拟IP (Peer Virtual IP), and DNS. There is one entry:序号 1, 用户名 123, 服务器/客户端 服务器, 隧道名称 ---, 虚拟本地IP 10.10.10.10, 接入服务IP 183.15.15.30, 对端虚拟IP 10.10.10.11, DNS ---. Below the table, it says '共1条, 每页: [10] 条 | 当前: 1/1页, 1~1条 |' and has navigation buttons.

客户端条目：



The screenshot shows a table titled '隧道信息列表' (Tunnel Information List) under the 'PPTP客户端' (PPTP Client) tab. The table has columns: 序号 (Index), 用户名 (Username), 服务器/客户端 (Server/Client), 隧道名称 (Tunnel Name), 虚拟本地IP (Virtual Local IP), 接入服务IP (Access Service IP), 对端虚拟IP (Peer Virtual IP), and DNS. There is one entry:序号 1, 用户名 123, 服务器/客户端 客户端, 隧道名称 sz_bj, 虚拟本地IP 10.10.10.11, 接入服务IP 183.15.15.15, 对端虚拟IP 10.10.10.10, DNS 114.114.114.114. Below the table, it says '共1条, 每页: [10] 条 | 当前: 1/1页, 1~1条 |' and has navigation buttons.

9.3.5 PPTP PC 到站点设置方法

服务器端的设置 (以 TL-ER6520G 为例)

需要在用户管理配置中添加 PC 到站点的用户账号密码，组网模式选择 PC 到站点，其余设置步骤与上面相同：

其中最大会话数配置是指可同时使用该账号拨 VPN 的终端数量。

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: 456
 密码:
 服务类型: PPTP
 本地地址: 10.10.10.10
 地址池: PPTP_pool
 DNS地址: 114.114.114.114
 组网模式: **PC到站点** 选择PC到站点模式
 最大会话数: 1 (1-100)

确定 取消

客户端的设置

不同 PPTP 客户端的配置方式有所差异, 请选择客户端操作系统, 参考对应指导文档:

[\[Windows XP\] PPTP VPN 客户端拨号操作步骤](#)

[\[Windows 7\] PPTP VPN 客户端拨号操作步骤](#)

[\[Windows 8\] PPTP VPN 客户端拨号操作步骤](#)

[\[Android\] PPTP VPN 客户端拨号操作步骤](#)

[\[iOS\] PPTP VPN 客户端拨号操作步骤](#)

客户端拨号成功后, 可以在 PPTP 服务器隧道信息显示客户端信息。

9.3.6 常见问题解答

Q: 电脑拨号成功后, 如何访问分支机构网络?

电脑拨号成功后，系统默认勾选了 VPN 连接 IPv4 高级设置中的“在远程网络上使用默认网关”，则电脑所有数据优先从 VPN 接口转发，即可正常访问总部资源。

如果需要通过总部进行代理转发访问分部资源，可在分部路由器上设置静态路由如下即可：

□	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: 填写总部VPN地址池

子网掩码:

下一跳: 填写总部虚拟本地IP

出接口: 选择对应VPN接口

Metric: (0-15)

备注:

(可选, 1-50个字符)

启用/禁用规则: 启用

9.4 L2TP VPN 代理上网设置指南

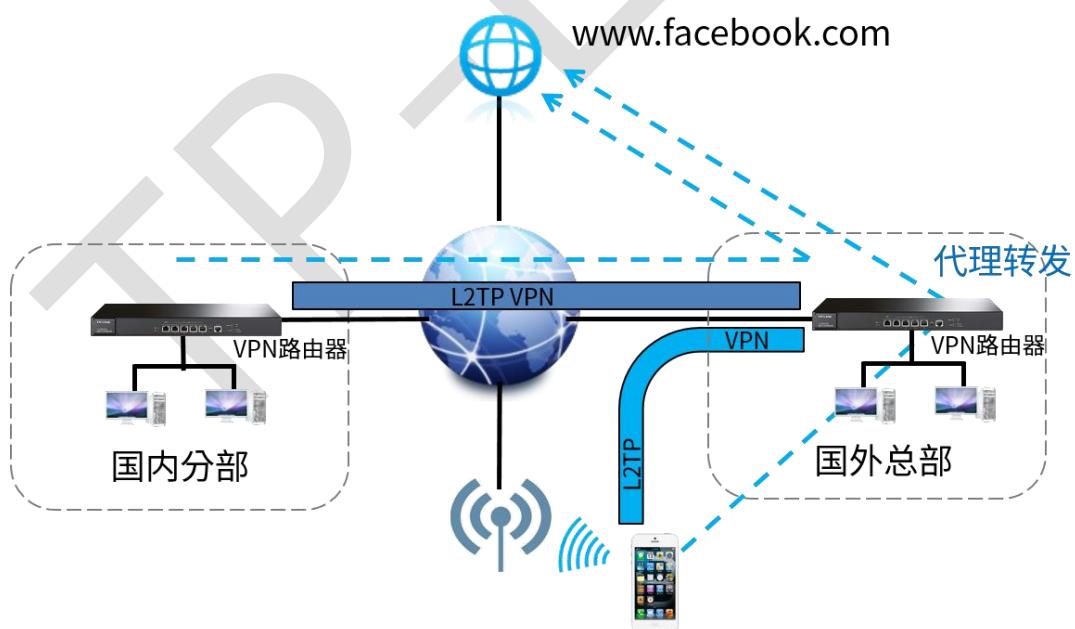
9.4.1 应用介绍

许多公司在海外也有承接业务，但有一些地址国内是无法直接访问的，需要通过 VPN 连接海外的服务器进行代理转发，实现海外业务、海外购物、国际邮件等需求。主要通过 PPTP 或 L2TP VPN 满足。

9.4.2 需求介绍

某公司的总部与分部均使用 ER 系列新平台路由器，需要实现将国内分部与国外总部通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性；且国内分部以及移动办公人员需要通过国外总部代理转发去访问一些国外的网站资源。

9.4.3 应用拓扑



9.4.4 设置方法

1、已搭建好 L2TP VPN 隧道。设置方法请参考本文档 [9.2 章 L2TP VPN 设置指南](#)

2、VPN 服务器端设置

在 VPN 服务器端路由器中设置针对 VPN 地址池的 NAPT 规则，出接口选择上网口：

The screenshot shows the 'NAPT' tab selected in a router's configuration interface. A table titled 'NAPT规则列表' displays one existing rule with columns: 序号 (Index), 规则名称 (Rule Name), 出接口 (Interface), 源地址范围 (Source Address Range), 状态 (Status), 备注 (Remarks), and 设置 (Settings). Below the table, a form is used to add a new rule:

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

Fields in the form:

- 规则名称: vpn_napt
- 出接口: WAN1 (selected from a dropdown menu labeled '选择上网口')
- 源地址范围: 10.10.10.0 / 24 (highlighted with a red box and labeled '填写VPN地址池')
- 状态: 启用
- 备注: (empty)
- 按钮: 确定 (Confirm) | 取消 (Cancel)

2、VPN 客户端设置

(1) 站点到站点客户端设置

在 VPN 客户端路由器界面，点击“VPN—L2TP—L2TP 客户端”，点击设置 VPN 条目，设置对端子网为 0.0.0.0/0，工作模式设置为 NAT 模式。

L2TP服务器 L2TP客户端 隧道信息列表

隧道名称: sz_bj (1-12个字符)

用户名: 123

密码: (1-128个字符)

出接口: WAN1

服务器地址: 183.15.15.15

IPSec加密: 加密

预共享密钥: 123456789 (1-128个字符)

对端子网: 0.0.0.0 / 0 设置对端子网为0.0.0.0

上行带宽: 1000000 Kbps (100-1000000)

下行带宽: 1000000 Kbps (100-1000000)

MTU: (可选)

工作模式: NAT 路由 选择工作模式为NAT模式

状态: 启用

运营商: 不设置

确定 取消

然后添加策略路由使所有数据优先走 VPN 接口，策略路由设置如下：

策略路由	静态路由	IPv6静态路由	系统路由				
□	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
--	--	--	--	--	--	--	--

规则名称: vpn_proxy

服务类型: ALL

源地址: IPGROUP_ANY

目的地址: IPGROUP_ANY

生效接口: sz_bj 出接口选择VPN接口

生效时间: Any

强制: 接口不在线时仍应用此规则

备注: VPN代理上网 (可选)

添加到指定位置: (可选)

状态: 启用

确定 **取消**

(2) PC 到站点客户端设置

不同 PPTP 客户端的配置方式有所差异, 请选择客户端操作系统, 参考对应指导文档:

[\[Windows XP\] L2TP VPN 客户端拨号操作步骤](#)

[\[Windows 7\] L2TP VPN 客户端拨号操作步骤](#)

[\[Windows 8\] L2TP VPN 客户端拨号操作步骤](#)

[\[Android\] L2TP VPN 客户端拨号操作步骤](#)

客户端拨号成功后，可以在 L2TP 服务器隧道信息显示客户端信息。PC 拨通 VPN 后，设置 VPN 连接—IPv4 选项—高级设置中，系统已经默认勾选“在远程网络上使用默认网关”，即可实现所有数据走 VPN 接口，实现 VPN 代理上网效果。

如果未能实现代理上网，可以检查确认 PC 端此处设置：



9.5 PPTP VPN 代理上网设置指南

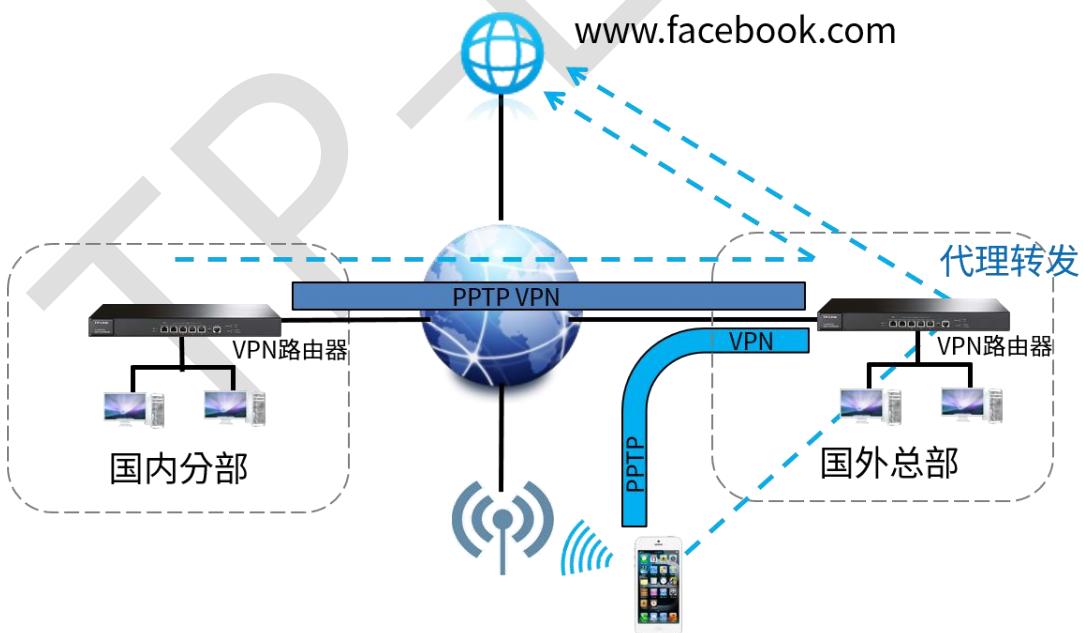
9.5.1 应用介绍

许多公司在海外也有承接业务，但有一些地址国内是无法直接访问的，需要通过 VPN 连接海外的服务器进行代理转发，实现海外业务、海外购物、国际邮件等需求。主要通过 PPTP 或 L2TP VPN 满足。

9.5.2 需求介绍

某公司的总部与分部均使用 ER 系列新平台路由器，需要实现将国内分部与国外总部通过 VPN 互联，实现资源相互访问，同时要求数据传输的安全性；且国内分部以及移动办公人员需要通过国外总部代理转发去访问一些国外的网站资源。

9.5.3 应用拓扑



9.5.4 设置方法

1、已搭建好 PPTP VPN 隧道。设置方法请参考本文档 [9.3 章 PPTP VPN 设置指南](#)

2、VPN 服务器端设置

在 VPN 服务器端路由器中设置针对 VPN 地址池的 NAPT 规则，出接口选择上网口：

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

2、VPN 客户端设置

(1) 站点到站点客户端设置

在 VPN 客户端路由器界面，点击“VPN—PPTP—PPTP 客户端”，点击设置 VPN 条目，设置对端子网为 0.0.0.0/0，工作模式设置为 NAT 模式。

PPTP服务器 PPTP客户端 隧道信息列表

隧道名称: sz_bj (1-12个字符)

用户名: 123

密码: ***

速率限制: 低 中 高

出接口: WAN1

服务器地址: 183.15.15.15

MPPE加密: 加密

对端子网: 0.0.0.0 / 0 设置对端子网为0.0.0.0/0

上行带宽: 1000000 Kbps (100-1000000)

下行带宽: 1000000 Kbps (100-1000000)

MTU: (可选)

工作模式: NAT 路由 选择工作模式为NAT模式

状态: 启用

运营商: 不设置

确定 取消

然后添加策略路由使所有数据优先走 VPN 接口，策略路由设置如下：

策略路由	静态路由	IPv6静态路由	系统路由				
□	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
--	--	--	--	--	--	--	--

规则名称: vpn_proxy

服务类型: ALL

源地址: IPGROUP_ANY

目的地址: IPGROUP_ANY

生效接口: sz_bj 出接口选择VPN接口

生效时间: Any

强制: 接口不在线时仍应用此规则

备注: VPN代理上网 (可选)

添加到指定位置: (可选)

状态: 启用

确定 **取消**

(2) PC 到站点客户端设置

不同 PPTP 客户端的配置方式有所差异, 请选择客户端操作系统, 参考对应指导文档:

[\[Windows XP\] PPTP VPN 客户端拨号操作步骤](#)

[\[Windows 7\] PPTP VPN 客户端拨号操作步骤](#)

[\[Windows 8\] PPTP VPN 客户端拨号操作步骤](#)

[\[Android\] PPTP VPN 客户端拨号操作步骤](#)

[\[iOS\] PPTP VPN 客户端拨号操作步骤](#)

客户端拨号成功后，可以在 PPTP 服务器隧道信息显示客户端信息。PC 拨通 VPN 后，设置 VPN 连接—IPv4 选项—高级设置中，系统已经默认勾选“在远程网络上使用默认网关”，即可实现所有数据走 VPN 接口，实现 VPN 代理上网效果。

如果未能实现代理上网，可以检查确认 PC 端此处设置：



9.6 SSL VPN 功能设置指南

9.6.1 应用介绍

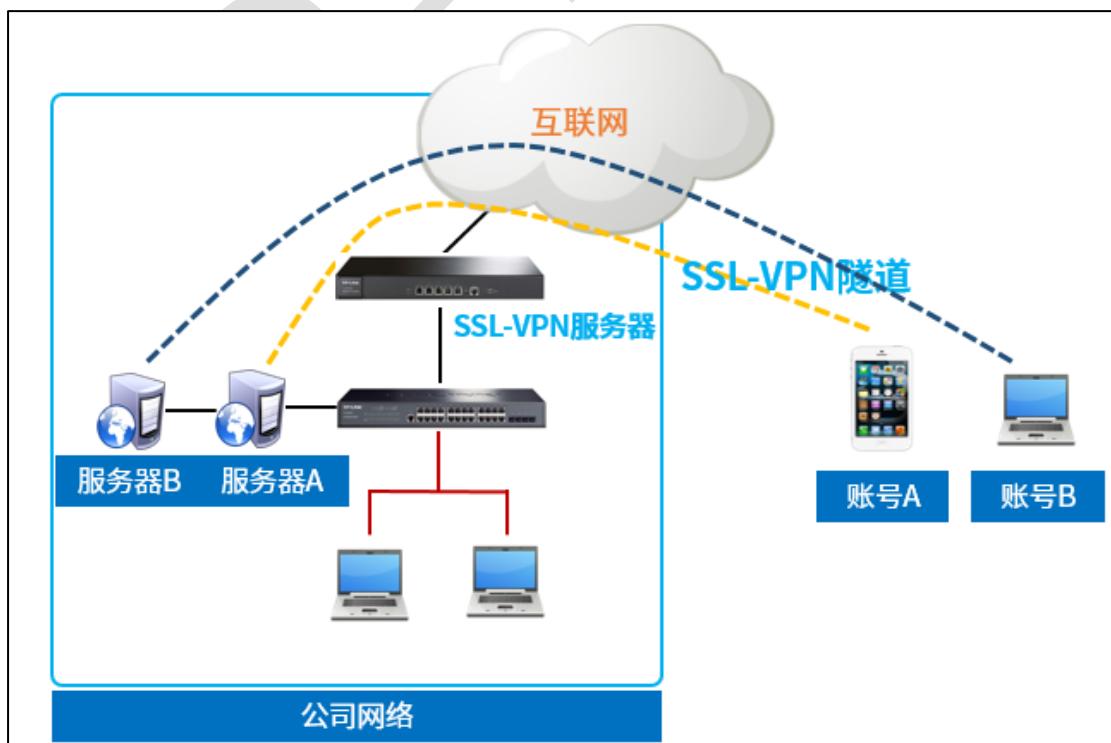
SSL VPN 是以 SSL 加密技术为基础的 VPN 技术，利用 SSL 提供的安全机制，为用户远程访问公司内部网络提供了安全保证，SSL VPN 可以针对不同账号分配不同的账号权限，不同账号可以访问不同的内网资源，权限控制方便灵活。

9.6.2 需求介绍

某企业使用 ER7 系列路由器，设置 SSL VPN 功能让在外出差的员工可以正常访问内网的服务器资源，且不同用户能访问的资源权限不同，需求如下：

拨上 VPN 后，账号 A 只能访问公司的服务器 A，账号 B 只能访问公司的服务器 B，除了对应该的服务器资源不能访问其它资源。

9.6.3 应用拓扑



9.6.4 设置方法

配置 SSL VPN 服务器：

登录到路由器界面，点击“对象管理”-“IP 地址池”，点击“新增”，设置 SSL VPN 的地址池：

序号	地址池名称	起始IP地址	结束IP地址	设置
--	1 SSL_VPN	10.0.0.10	10.0.0.100	---

地址池名称： (1-30个字符)

起始IP地址：

结束IP地址：

1. 点击“SSL VPN”-“服务器配置”，启用 VPN 服务器：

服务器设置

SSL VPN服务器： 启用 禁用 **启用VPN服务器功能**

服务接口： **选择对应的外网接口**

虚拟IP地址池： **为VPN客户端选择地址池**

首选DNS服务器地址： (X.X.X.X, 可选)

备选DNS服务器地址： (X.X.X.X, 可选)

如需继续，请点击“下一步”。如需退出本向导，请点击“退出”。

2. 点击“资源管理”，创建资源条目，本例条目为服务器 A 和服务器 B 的 IP 地址：

设置向导

隧道资源

+ 新增 **- 删除**

序号	资源名称	域名/IP地址	资源组	服务类型	端口范围	设置	
--	1	LAN	---	GROUP_LAN	ALL	---	
--	2	ALL	---	GROUP_ALL	ALL	---	
<input type="checkbox"/>	3	fuwuqiA	192.168.111.10/32	---	ALL	---	
<input type="checkbox"/>	4	fuwuqiB	192.168.111.20/32	---	ALL	---	

创建服务器资源

共4条, 每页: 10 条 | 当前: 1/1页, 1~4条 | < 1 >

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**

3. 点击“资源组”栏, 新增资源组条目, 将上一步创建的资源条目放在对应的资源组内, 方便下一步将资源组绑定账号:

资源组

+ 新增 **- 删除**

序号	资源组	资源	设置	
--	1	GROUP_LAN	LAN	
--	2	GROUP_ALL	ALL	
<input type="checkbox"/>	3	FUWUQI_A	fuwuqiA	
<input type="checkbox"/>	4	FUWUQI_B	fuwuqiB	

将资源分别放置在对应的资源组条目中

共4条, 每页: 10 条 | 当前: 1/1页, 1~4条 | < 1 >

4. 点击“用户管理”-“用户组”新增用户组, 分别给用户 A 和用户 B 使用, 并将用户组 A 绑定资源组服务器 A, 用户组 B 绑定资源 B:

用户 用户组

用户组列表

+ 新增 - 删除

□	序号	组名称	成员列表	资源组列表	设置
--	--	--	--	--	--

组名称: (1-50个字符) **用户组**

成员列表:

资源组列表:

成员列表暂时不添加，在添加用户时添加
绑定资源组

确定 取消

用户 用户组

用户组列表

+ 新增 - 删除

□	序号	组名称	成员列表	资源组列表	设置
	1	default			
□	2	A_zu		FUWUQI_A	
□	3	B_zu		FUWUQI_B	

5. 点击用户栏，新增用户 A 绑定到用户组 A 中，用户 B 绑定到用户组 B 中：

用户 用户组

用户列表

✓ 启用 ✗ 禁用 + 新增 - 删除

□	序号	用户类型	用户名	用户组	有效期	状态	设置
--	--	--	--	--	--	--	--

用户名: (1-100个英文字符、数字或下划线) **用户A的账号**

密码: (1-100个英文字符、数字或英文特殊字符)

用户组:

有效期: (格式: YYYY/MM/DD)

同时登录用户数: (1-100)

状态: 启用 禁用

确定 取消



<input type="checkbox"/>	序号	用户类型	用户名	用户组	有效期	状态	设置
<input type="checkbox"/>	1	管理员注册用户	adminA	A_zu	2021/12/31	已启用 	 
<input type="checkbox"/>	2	管理员注册用户	adminB	B_zu	2021/12/31	已启用 	 

至此，服务器端配置已经设置完成，用户也可根据服务器端提供的快速设置向导一步一步按照提示配置。

配置 SSL VPN 客户端：

手机或者电脑上安装客户端软件，打开客户端软件并输入服务器 WAN 口公网 IP 地址或者动态域名：



客户端输入用户 A 的用户名和密码，即可登录 SSL VPN 方位对应的内网资源：





备注：APP 端设置类似，这里就不详细叙述了。

至此，整个 SSL VPN 的配置完成，用户可以通过对应的账号访问对应的内网资源。

第10章 认证管理

10.1 一键上网设置指南

10.1.1 应用介绍

目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客接入网络的方式有很多，一键认证就是其中的一种。商户可以通过一键认证推送广告，而访客无需账号密码，一键免费上网。本文通过典型应用实例介绍 ER 系列路由器一键上网的应用与配置。

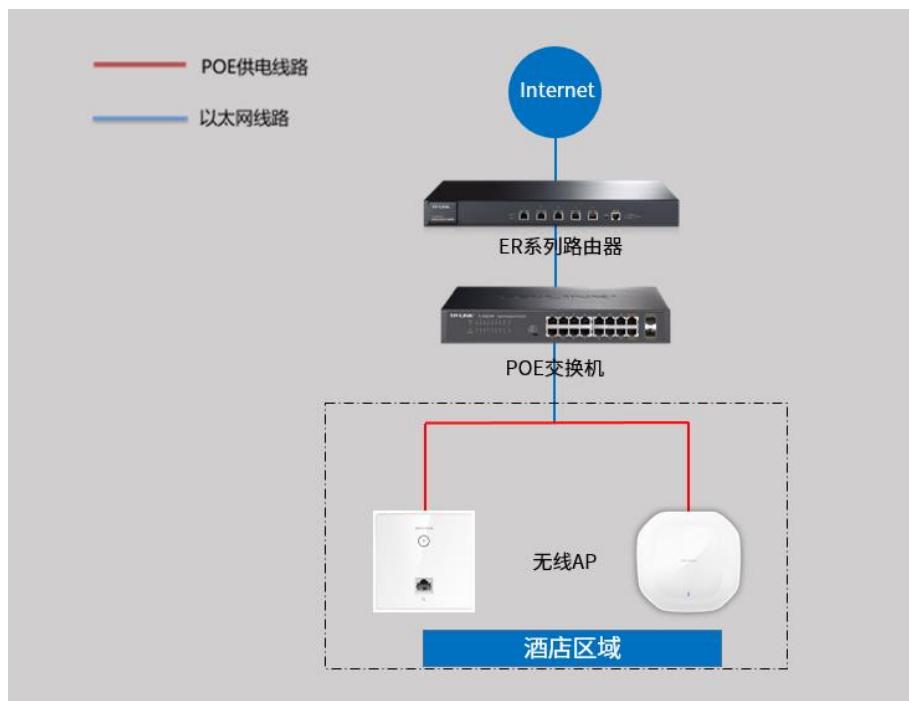
10.1.2 需求分析

某酒店需要实现无线覆盖，为顾客提供无线网络接入，有以下需求：

顾客连接无线后可以收到酒店推送的广告页面，且无需用户填写登录信息。

10.1.3 应用拓扑

根据用户需求，路由器和 AP 连接参考拓扑如下：



10.1.4 设置方法

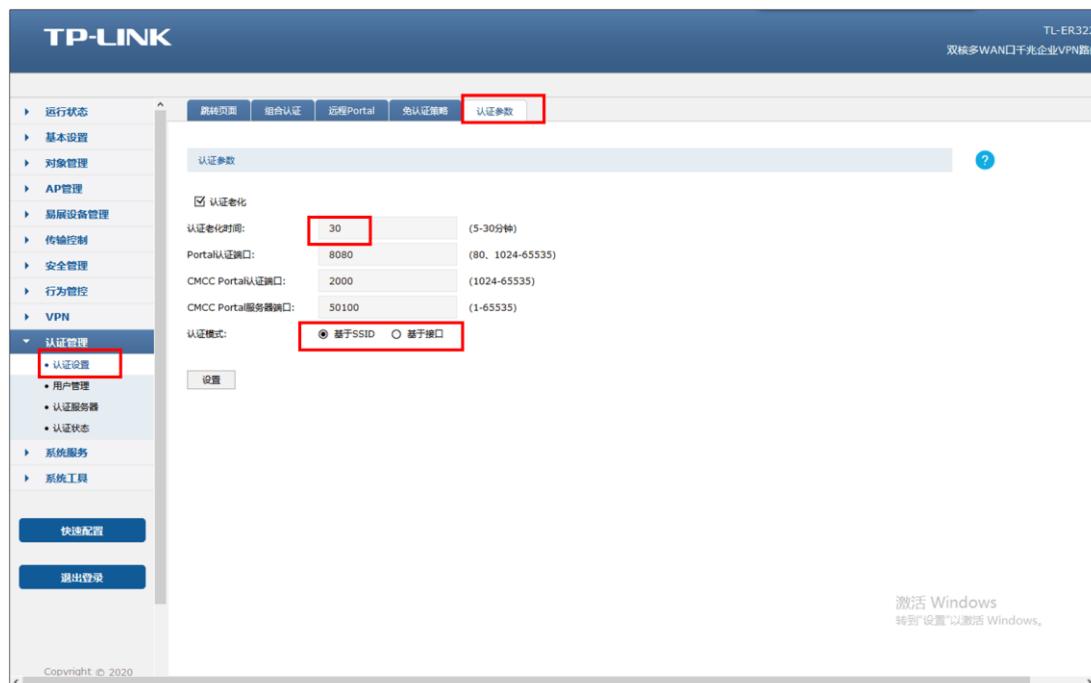
1、新增无线并进行射频绑定

点击“AP管理>无线网络设置”，设置酒店 SSID，如下图：



2、认证参数设置

点击“认证管理>认证设置>认证参数”，配置认证老化时间和认证模式，如下图：



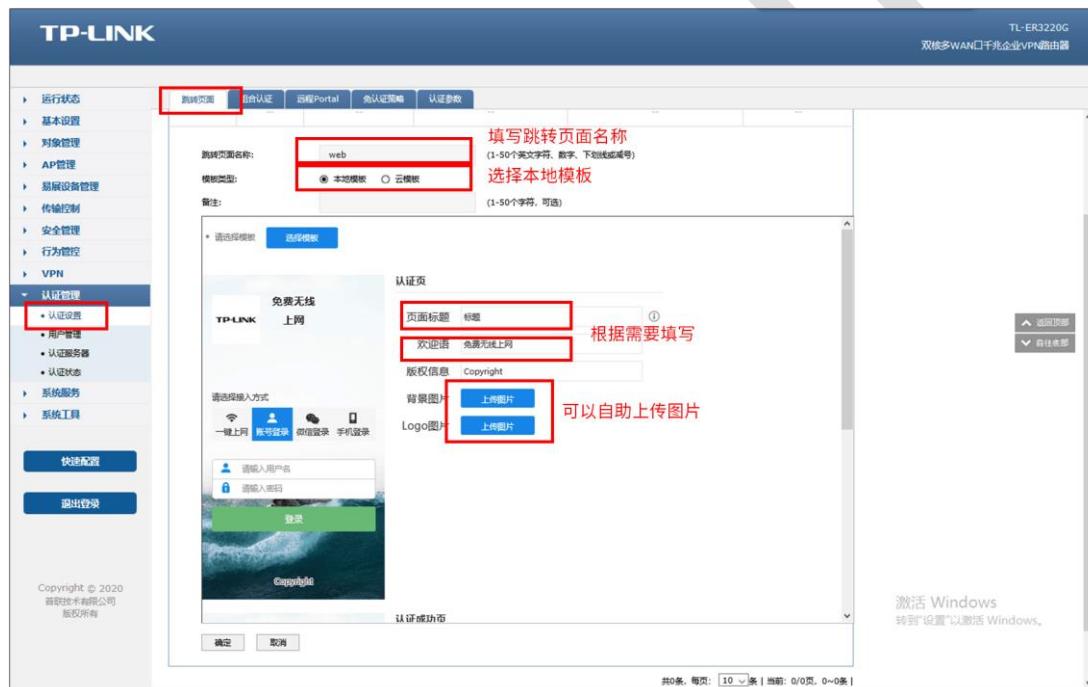
相关参数说明如下：

- 1) 认证老化时间：当已认证客户端断开连接后，对应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。
- 2) Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 3) CMCC Portal 认证端口：AC 的 CMCC Portal 认证端口，用于接收 Portal 服务器发送的认证报文。
- 4) CMCC Portal 服务器端口：CMCC Portal 服务器的端口号，用于 CMCC Portal 认证时 AC 发送 NTF_LOGOUT 报文的目的端口号。

5) 认证模式：设置 Portal 认证的认证模式，支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示连接到这个接口中的终端都需要认证才能上网。

4、配置内置 WEB 服务器和内置认证服务器

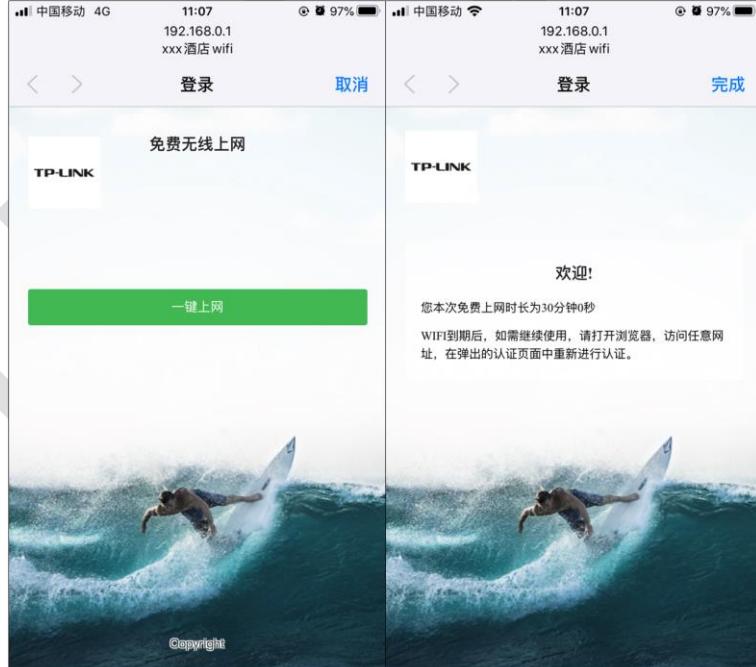
(1) 点击“认证管理>认证设置>跳转页面”，根据实际需求设置跳转页面标题、欢迎信息等，背景图片和 Logo 可以自助上传，如下图：



(2) 点击“认证管理>认证设置>组合认证”，点击新增，认证方式选择一键上网，如下图：



以上内容配置完毕，ER 系列路由器的一键上网设置成功，连接酒店的无线 SSID 即可一键上网。最终效果如下图：



10.2 短信认证设置指南

10.2.1 应用介绍

目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客连接网络后需要通过认证才可以免费使用网络。接入认证方式有很多，短信认证就是其中的一种，访客需要输入手机号获取验证码并通过验证后才能免费上网。我司 ER 系列路由器的短信认证功能支持和阿里云、腾讯云、百度云、网易云信以及第三方使用 HTTP 协议的服务器进行对接，从而实现短信认证上网的需求。本文通过典型应用实例介绍 ER 系列路由器短信认证的应用与配置。

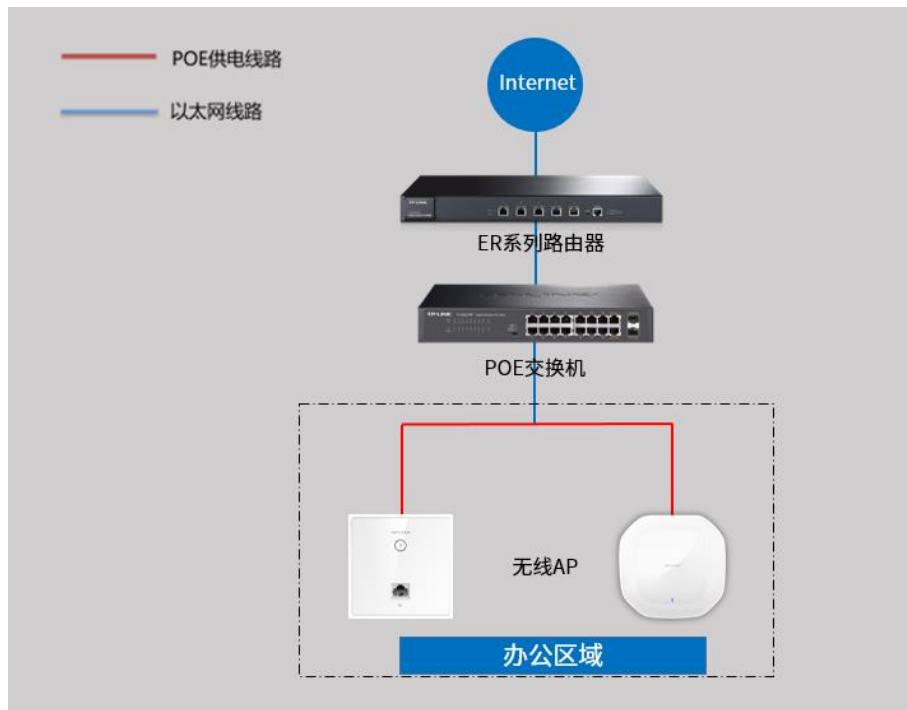
注意：使用短信认证时，短信服务平台会收取通信服务费，具体收费标准请参考云平台。

10.2.2 需求分析

某办公室需要实现无线覆盖，为员工提供无线网络接入，办公区员工连接无线后需要在 WEB 页面中输入手机号进行短信认证，认证通过之后才能上网。

10.2.3 应用拓扑

根据用户需求，路由器和 AP 连接参考拓扑如下：



10.2.4 设置方法

1、第三方平台中设置短信服务

详细的设置方法请点击参考：[不同平台短信服务的设置方法](#)

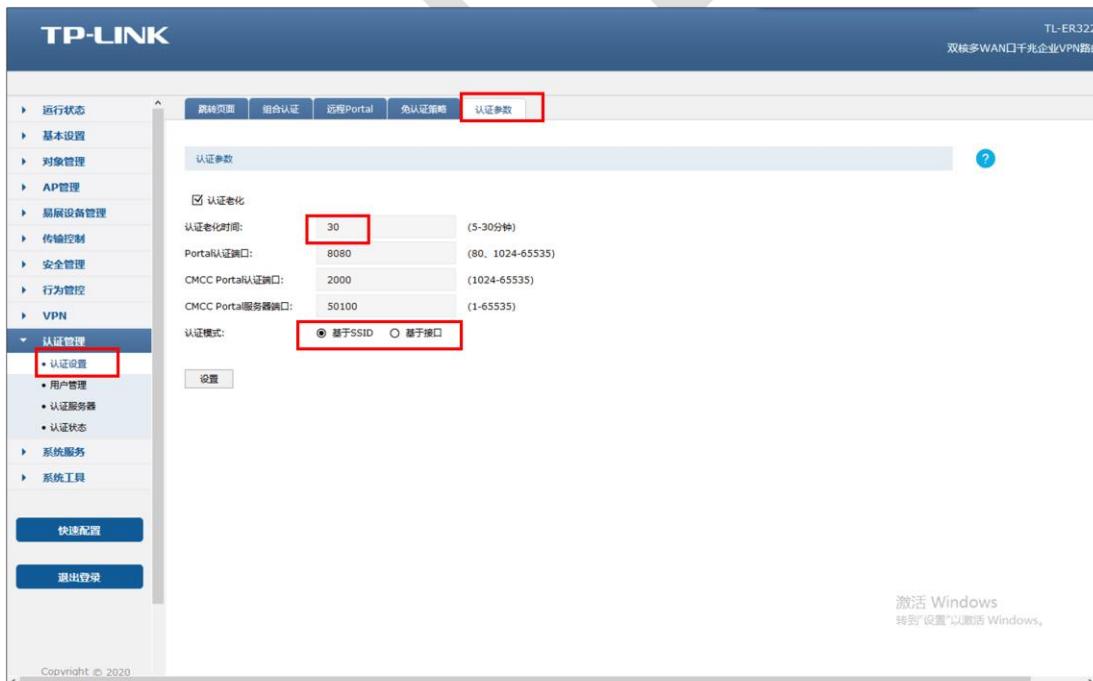
2、新增无线并进行射频绑定

点击“AP 管理>无线网络设置”，设置办公 SSID，如下图：



3、认证参数设置

点击“认证管理>认证设置>认证参数”，配置认证老化时间和认证模式，如下图：

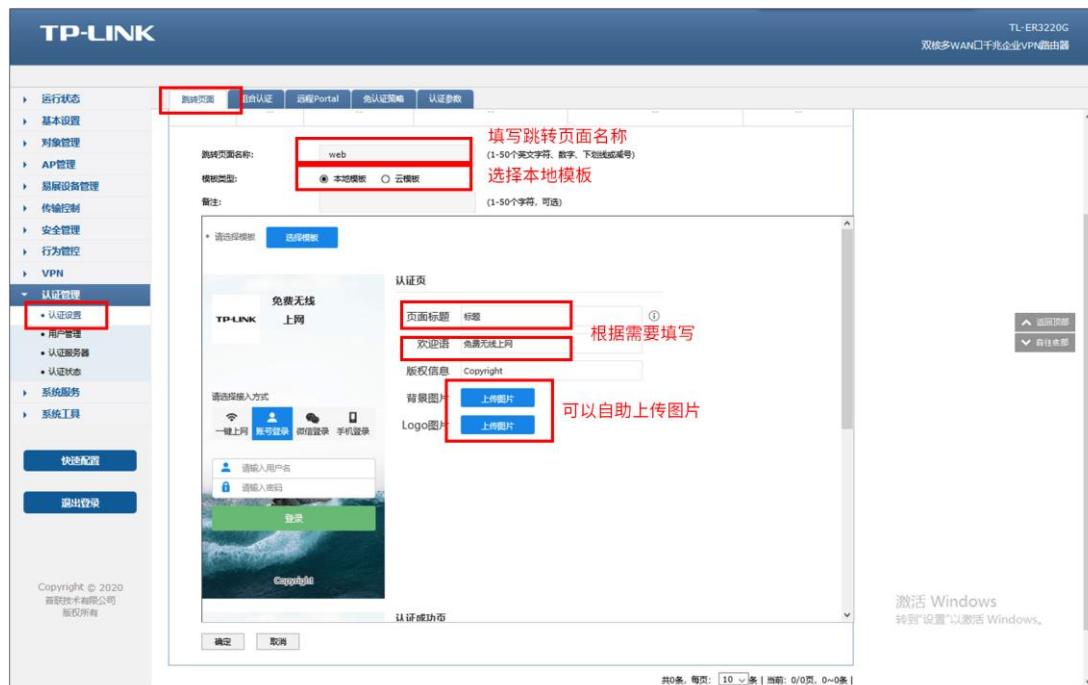


相关参数说明如下：

- 1) 认证老化时间：当已认证客户端断开连接后，对应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。
- 2) Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 3) CMCC Portal 认证端口： AC 的 CMCC Portal 认证端口，用于接收 Portal 服务器发送的认证报文。
- 4) CMCC Portal 服务器端口：CMCC Portal 服务器的端口号，用于 CMCC Portal 认证时 AC 发送 NTF_LOGOUT 报文的目的端口号。
- 5) 认证模式：设置 Portal 认证的认证模式，支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示连接到这个接口中的终端都需要认证才能上网。

4、配置内置 WEB 服务器和内置认证服务器

(1) 点击“认证管理>认证设置>跳转页面”，根据实际需求设置跳转页面标题、欢迎信息等，如下图：



(2) 点击“认证管理>认证设置>组合认证”，点击新增，选择短信认证，根据实际需要设置

免费上网时长和验证码有效期等信息，如下图：



通道类型填写所使用的第三方平台（阿里云、腾讯云、百度云、网易云信、HTTP 协议的服务器），以及填写相应的参数信息（可以参考链接不同平台短信服务的设置方法），填写完毕点击保存，下面给予介绍：

阿里云

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

腾讯云

认证方式

一键上网	Web认证	微信连Wi-Fi	短信认证
状态: <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 免费上网时长: 30 分钟 (1-43200) 验证码有效期: 1 分钟 (1-3) 通道类型: 腾讯云 SMK_App_ID: 填写SMK_APP_ID (1-50个字符) App Secret: 填写APP Secret (1-50个字符) 模板ID: 填写模板ID (1-50个字符) 签名: 填写短信签名 (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。			
<input type="button" value="确定"/> <input type="button" value="取消"/>			

百度云

认证方式

一键上网	Web认证	微信连Wi-Fi	短信认证
状态: <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 免费上网时长: 30 分钟 (1-43200) 验证码有效期: 1 分钟 (1-3) 通道类型: 百度云 Access Key ID: 填写Access Key ID (1-50个字符) Secret Access Key: 填写Secret Access Key (1-50个字符) 模板ID: 填写模板ID (1-50个字符) 短信签名: 填写短信签名 (1-50个字符) 签名ID: 填写签名ID (1-100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. 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。			
<input type="button" value="确定"/> <input type="button" value="取消"/>			

网易云信

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: 30 分钟 (1-43200)

验证码有效期: 1 分钟 (1-3)

通道类型: 网易云信

AppKey: 填写APP ID (1-50个字符)
App Secret: 填写Secret Access Key (1-50个字符)

模板ID: 填写模板ID (1-50个字符)

短信签名: 填写短信签名 (1-50个字符)

注意:

- 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。
- 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。
- 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。

确定 **取消**

HTTP 协议

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: 30 分钟 (1-43200)

验证码有效期: 1 分钟 (1-3)

通道类型: HTTP协议

URL地址: 填写接口请求地址
第三方短信平台提供相关参数
(1-120个英文字符、数字或英文特殊字符, 必填。
若链接包含IPv6地址, 需用[]包含, 例如: http://[2000::1]/index.html)

请求方式: GET POST **选择请求方式**

编码类型: UTF-8 **选择编码类型**

短信模板: 填写短信模板
(请将参数中的手机号与验证码用关键字'{PHONE}'和'{CODE}'进行替换, 详情请参考帮助文档或用户手册, 必填)

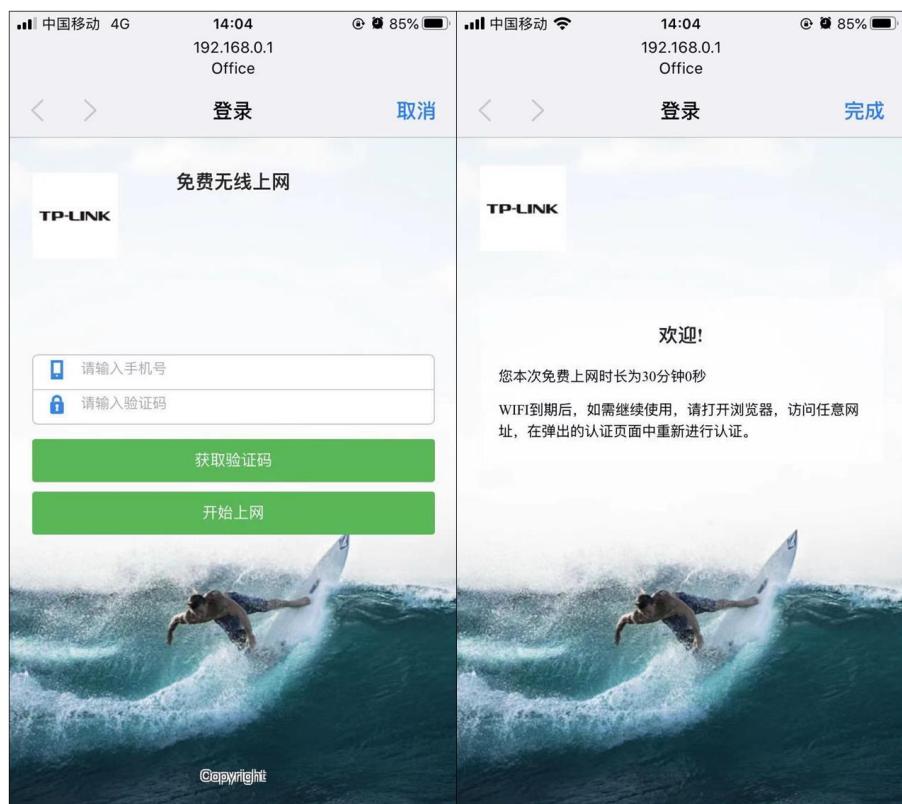
注意:

- 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。
- 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。
- 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。

确定 **取消**

以上内容配置完毕, ER 系列路由器的短信认证设置成功, 连接办公区的无线 SSID 输入手

机号获取验证码认证通过后即可上网。效果图如下:



10.3 Portal 认证设置指南—使用内置 WEB 服务器和内置认证服务器

10.3.1 应用介绍

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。ER 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 ER 系列路由器 Portal 认证功能的应用与配置。

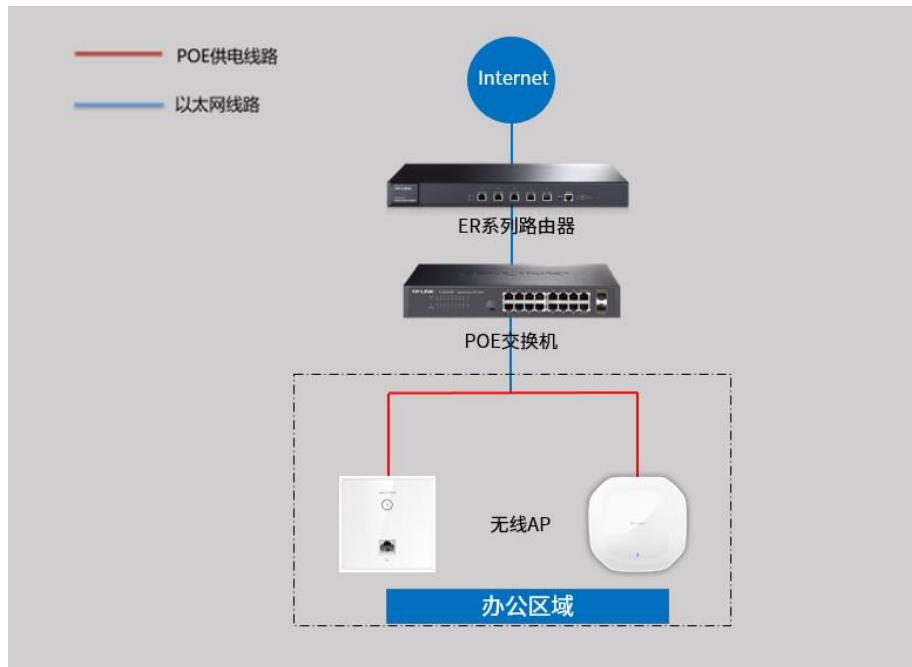
10.3.2 需求分析

某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

办公区员工连接无线后需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

10.3.3 应用拓扑

根据用户需求，路由器和 AP 连接参考拓扑如下：



10.3.4 设置方法

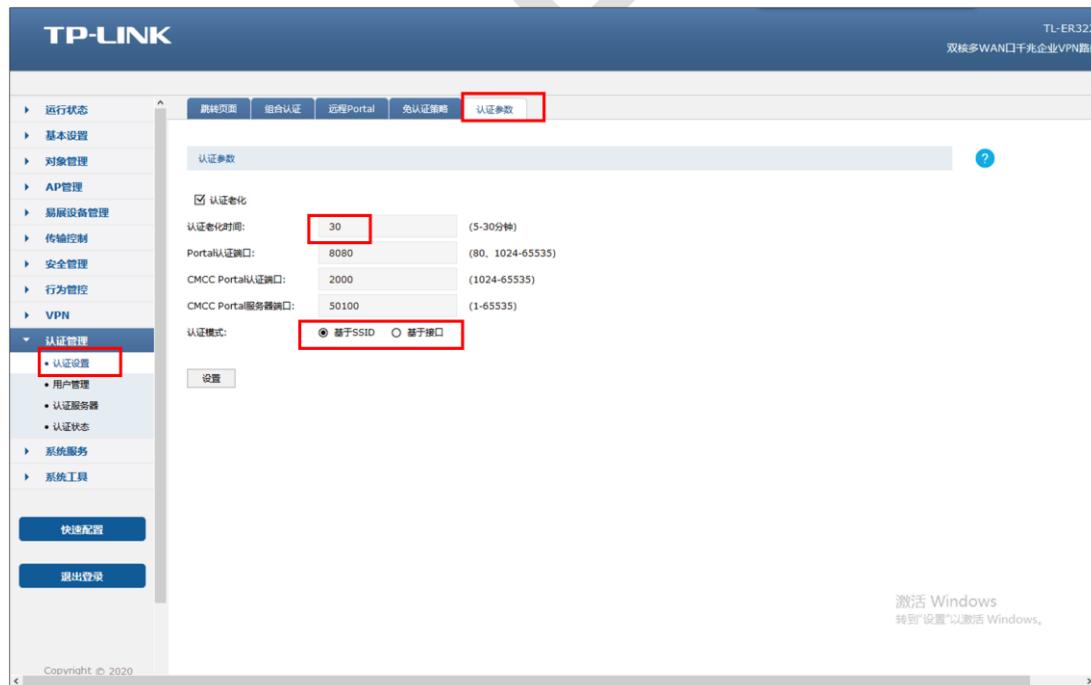
1、新增无线并进行射频绑定

点击“AP管理>无线网络设置”，设置办公 SSID，如下图：



2、认证参数设置

点击“认证管理>认证设置>认证参数”，配置认证老化时间和认证模式，如下图：

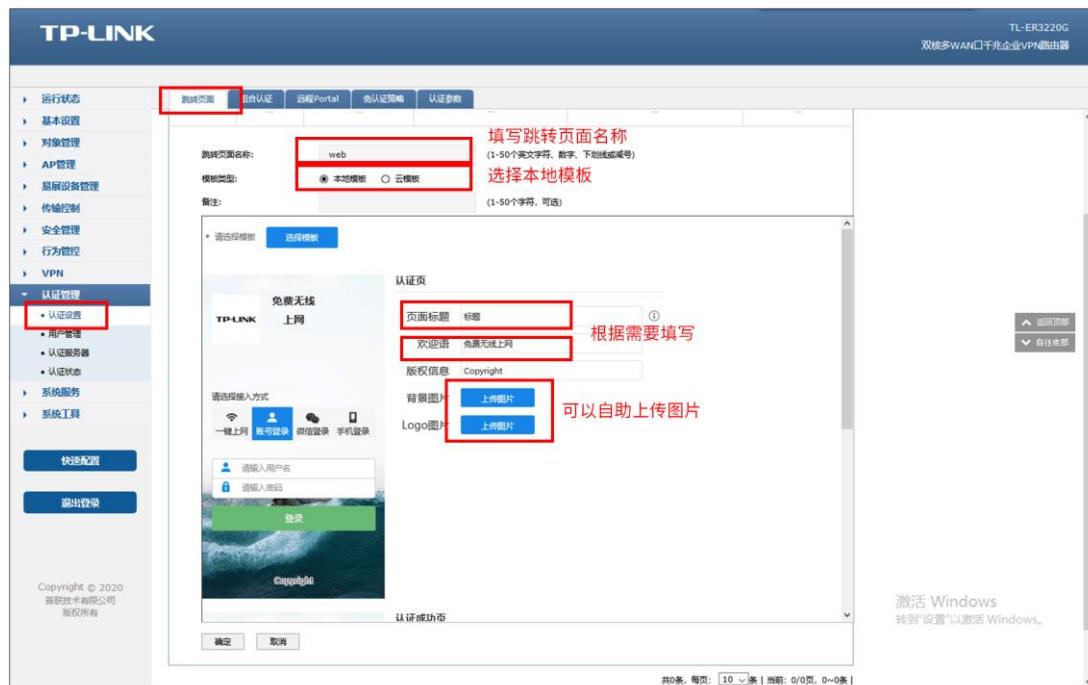


**相关参数说明如下：**

- 1) 认证老化时间：当已认证客户端断开连接后，对应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。
- 2) Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 3) CMCC Portal 认证端口： AC 的 CMCC Portal 认证端口，用于接收 Portal 服务器发送的认证报文。
- 4) CMCC Portal 服务器端口：CMCC Portal 服务器的端口号，用于 CMCC Portal 认证时 AC 发送 NTF_LOGOUT 报文的目的端口号。
- 5) 认证模式：设置 Portal 认证的认证模式，支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示连接到这个接口中的终端都需要认证才能上网。

3、配置内置 WEB 服务器和内置认证服务器

- (1) 点击“认证管理>认证设置>跳转页面”，根据实际需求设置跳转页面标题、欢迎信息等，如下图：



(2) 点击“认证管理>认证设置>组合认证”，点击新增，认证服务器类型选择本地服务器，

如下图：



4、创建用户管理条目

点击“认证管理>用户管理>认证用户管理”，点击新增，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，如下图：



以上内容配置完毕，ER 系列路由器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

10.4 Portal 认证设置指南—使用内置 WEB 服务器和外部认证服务器

10.4.1 应用介绍

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。ER 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 ER 系列路由器 Portal 认证功能的应用与配置。

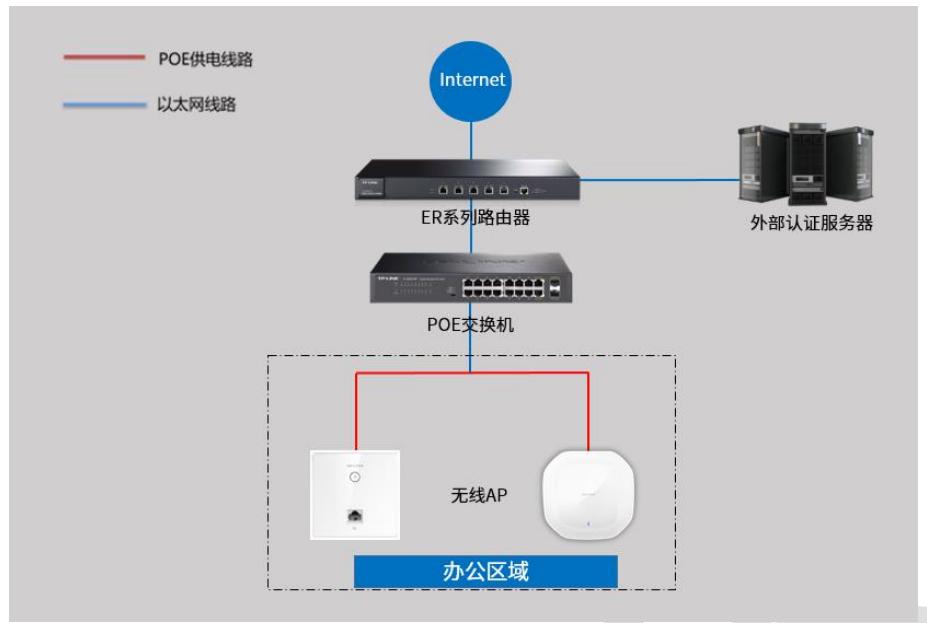
10.4.2 需求分析

某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

办公区员工接入无线后需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

10.4.3 应用拓扑

根据用户需求，路由器和 AP 以及服务器连接参考拓扑如下：



10.4.4 设置方法

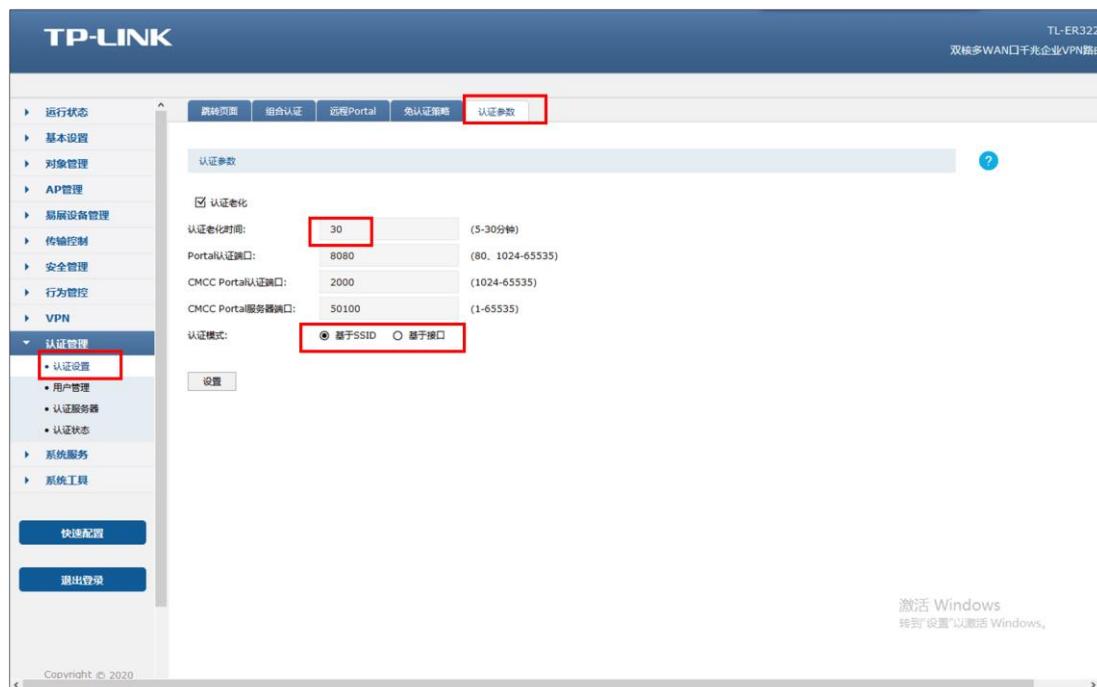
1、新增无线并进行射频绑定

点击“AP管理>无线网络设置”，设置办公 SSID，如下图：



2、认证参数设置

点击“认证管理>认证设置>认证参数”，配置认证老化时间和认证模式，如下图：



相关参数说明如下：

- 1) 认证老化时间：当已认证客户端断开连接后，对应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。
- 2) Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 3) CMCC Portal 认证端口：AC 的 CMCC Portal 认证端口，用于接收 Portal 服务器发送的认证报文。
- 4) CMCC Portal 服务器端口：CMCC Portal 服务器的端口号，用于 CMCC Portal 认证时 AC 发送 NTF_LOGOUT 报文的目的端口号。

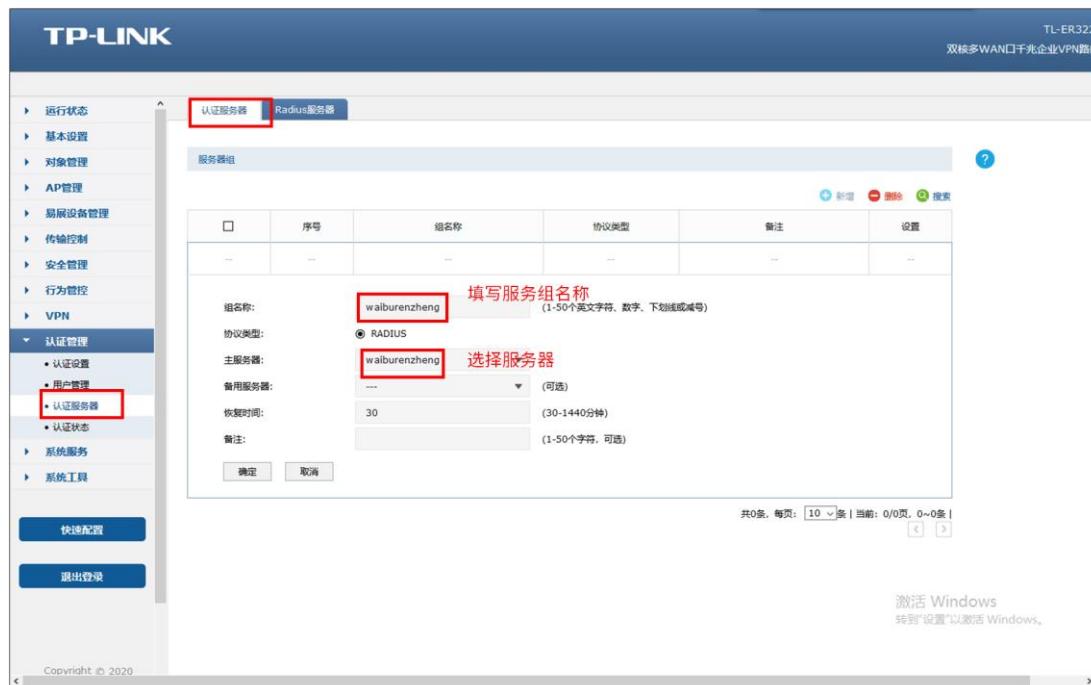
5) 认证模式：设置 Portal 认证的认证模式，支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示连接到这个接口中的终端都需要认证才能上网。

3、配置外部认证服务器并添加服务器组

(1) 点击“认证服务器>Radius 服务器”，根据自己设置的外部认证服务器在路由器添加条目



(2) 添加外部服务器组



4、配置内部 Web 服务器

(1) 点击“认证管理>认证设置>跳转页面”，根据实际需求设置跳转页面标题、欢迎信息等，如下图：



(2) 点击“认证管理>认证设置>组合认证”，点击新增，认证服务器类型选择远程服务器，

如下图：



以上内容配置完毕，ER 系列路由器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网，且此时用户提交的密码和账户是外部认证服务器设置的。

10.5 Portal 认证设置指南—使用外置 WEB 服务器和内置认证服务器

10.5.1 应用介绍

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。ER 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 ER 系列路由器 Portal 认证功能的应用与配置。

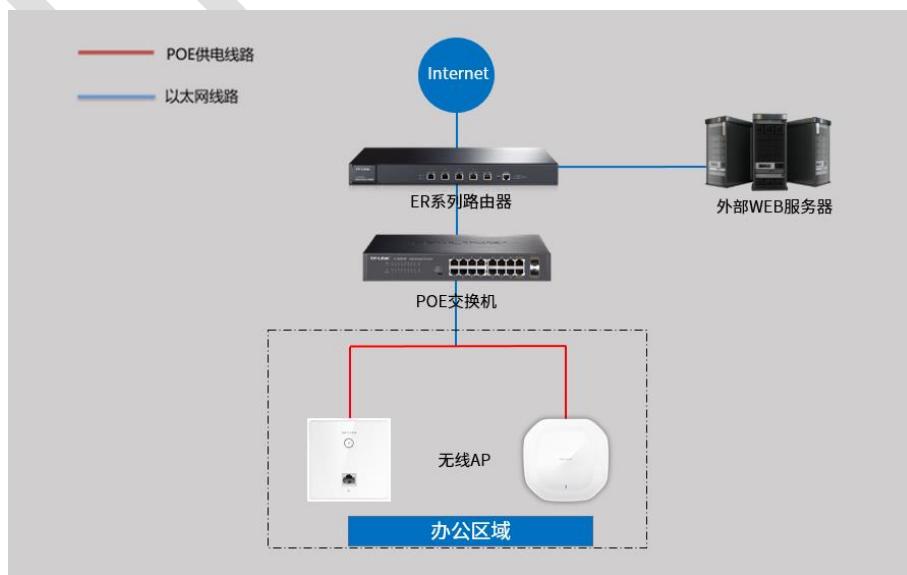
10.5.2 需求分析

某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

办公区员工连接无线后需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

10.5.3 应用拓扑

根据用户需求，路由器和 AP 以及服务器连接参考拓扑如下：



10.5.4 设置方法

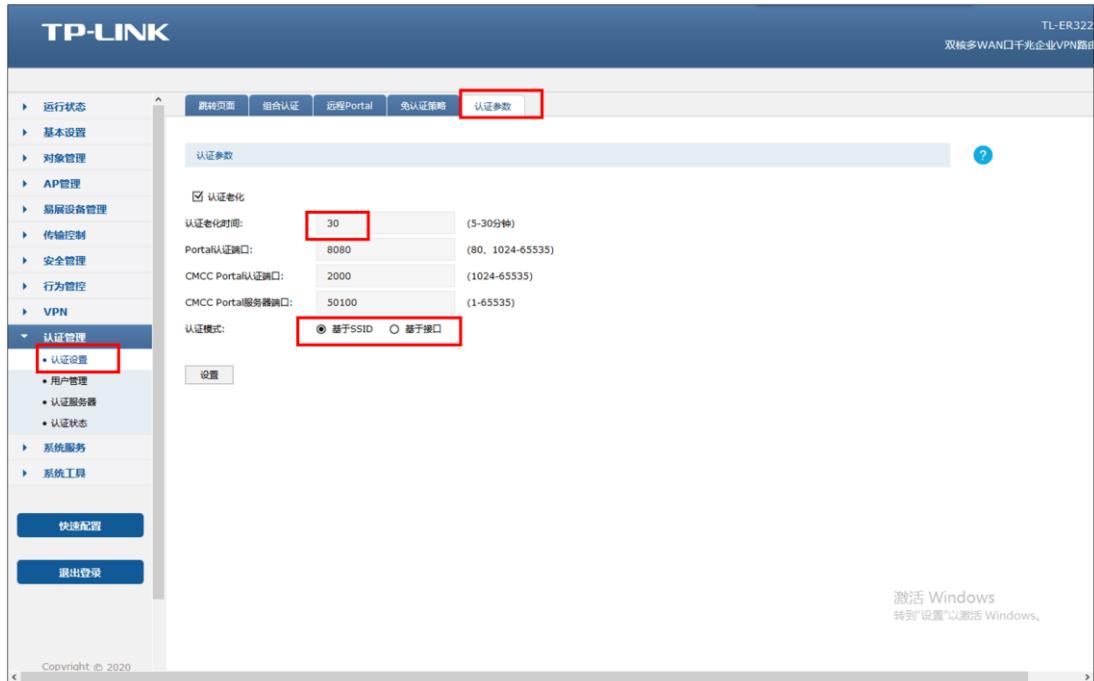
1、新增无线并进行射频绑定

点击“AP 管理>无线网络设置”，设置办公 SSID，如下图：



2、认证参数设置

点击“认证管理>认证设置>认证参数”，配置认证老化时间和认证模式，如下图：



相关参数说明如下：

- 1) 认证老化时间：当已认证客户端断开连接后，对应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。
- 2) Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 3) CMCC Portal 认证端口：AC 的 CMCC Portal 认证端口，用于接收 Portal 服务器发送的认证报文。
- 4) CMCC Portal 服务器端口：CMCC Portal 服务器的端口号，用于 CMCC Portal 认证时 AC 发送 NTF_LOGOUT 报文的目的端口号。

5) 认证模式：设置 Portal 认证的认证模式，支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示连接到这个接口中的终端都需要认证才能上网。

3、配置外部 Web 服务器

点击“认证管理>认证设置>远程 Portal”，点击新增，认证服务器类型选择本地服务器，如下图：



4、创建用户管理条目

点击“认证管理>用户管理>认证用户管理”，点击新增，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，如下图：



以上内容配置完毕，ER 系列路由器的 Portal 认证服务设置成功，连接办公区的无线 SSID
输入用户名和密码认证通过后即可上网。

10.6 Portal 认证设置指南—使用外置 WEB 服务器和外置认证服务器

10.6.1 应用介绍

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。ER 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 ER 系列路由器 Portal 认证功能的应用与配置。

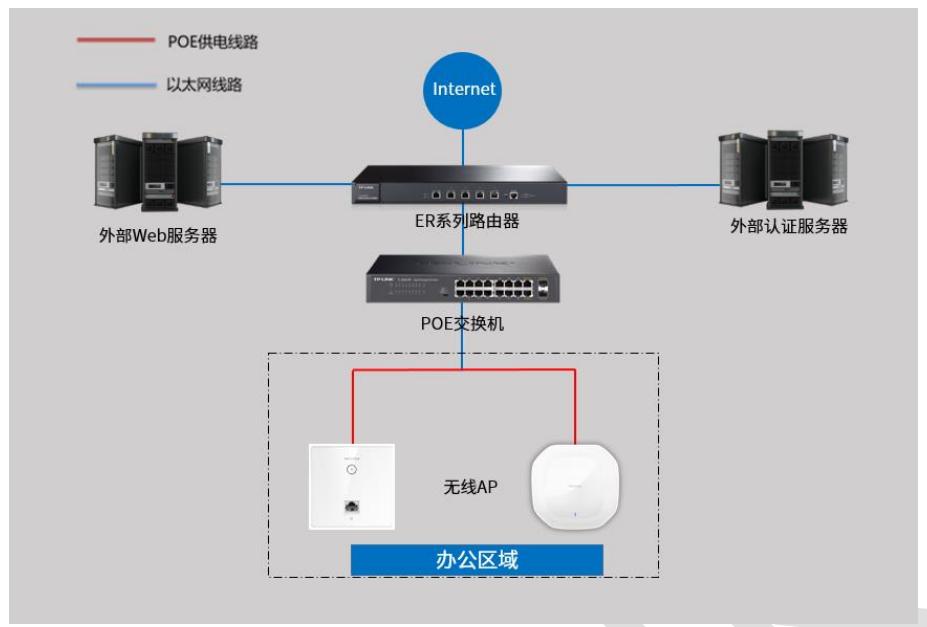
10.6.2 需求分析

某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

办公区员工连接无线后需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

10.6.3 应用拓扑

根据用户需求，路由器和 AP 以及服务器连接参考拓扑如下：



10.6.4 设置方法

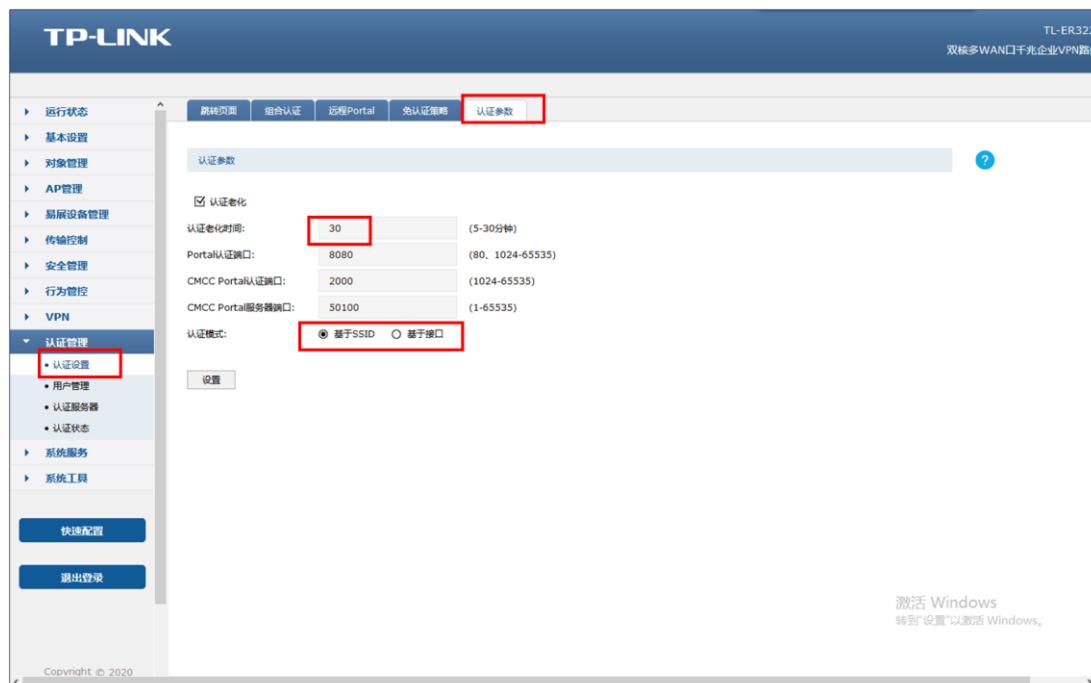
1、新增无线并进行射频绑定

点击“AP管理>无线网络设置”，设置办公 SSID，如下图：



2、认证参数设置

点击“认证管理>认证设置>认证参数”，配置认证老化时间和认证模式，如下图：



相关参数说明如下：

- 1) 认证老化时间：当已认证客户端断开连接后，对应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。
- 2) Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 3) CMCC Portal 认证端口：AC 的 CMCC Portal 认证端口，用于接收 Portal 服务器发送的认证报文。
- 4) CMCC Portal 服务器端口：CMCC Portal 服务器的端口号，用于 CMCC Portal 认证时 AC 发送 NTF_LOGOUT 报文的目的端口号。

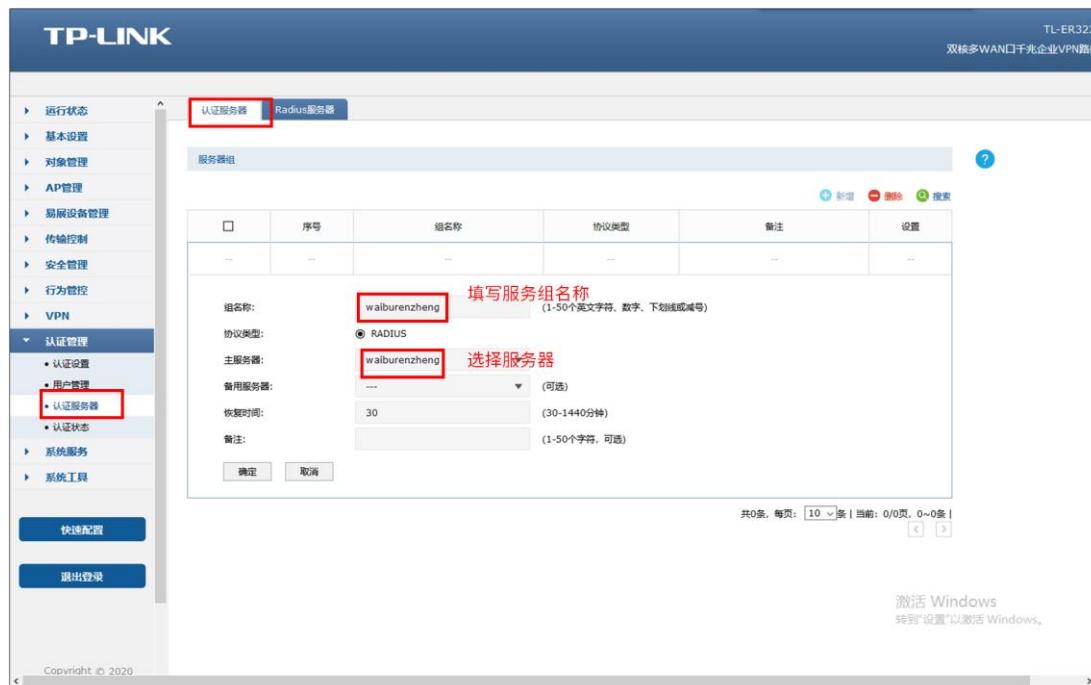
5) 认证模式：设置 Portal 认证的认证模式，支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示连接到这个接口中的终端都需要认证才能上网。

3、配置外部认证服务器并添加服务器组

(1) 点击“认证服务器>Radius 服务器”，根据自己设置的外部认证服务器在路由器添加条目



(2) 添加外部服务器组



4、配置外部 Web 服务器

点击“认证管理>认证设置>远程 Portal”，点击新增，认证服务器类型选择远程服务器，如
下图：



以上内容配置完毕，ER 系列路由器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网，且此时用户提交的密码和账户是外部认证服务器设置的。



10.7 免认证策略的使用方法

10.7.1 应用介绍

目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客连接网络后需要通过认证才可以免费使用网络。免认证策略可以实现客户端不需要认证就能访问指定的网站或者服务器。本文通过典型应用实例介绍 ER 系列路由器免认证策略的应用与配置。

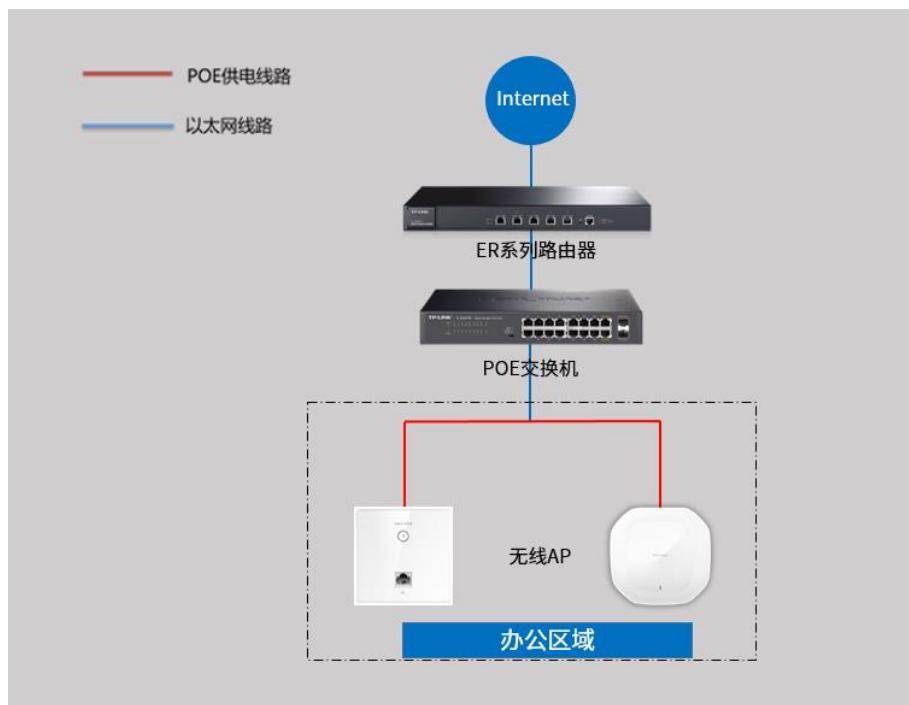
10.7.2 需求分析

某办公室需要实现无线覆盖，员工需要通过认证后才能上网，有以下需求：

- 特定终端如打印机不需要认证即可上网；
- 员工无需认证也可以访问公司外网服务器；
- 员工无需认证也可以访问公司网站；

10.7.3 应用拓扑

根据用户需求，路由器和 AP 连接参考拓扑如下：



10.7.4 设置方法

1、特定终端无需认证即可上网

进入路由器界面，点击“认证管理>认证设置>免认证策略”，添加免认证策略，如下图：

The screenshot shows the TP-LINK TL-ER322 router's configuration interface. The left sidebar has a tree view with "认证管理" (Authentication Management) selected, and "认证设置" (Authentication Settings) is highlighted with a red box. The main content area has tabs: "流转页面" (Flowchart Page), "组合认证" (Combined Authentication), "远程Portal" (Remote Portal), "免认证策略" (Exemption Strategy) which is highlighted with a red box, and "认证参数" (Authentication Parameters). The "免认证策略设置" (Exemption Strategy Settings) section contains a table with columns: 口 (checkbox), 序号 (Index), 策略名称 (Policy Name), 免认证方式 (Authentication Exemption Method), 源IP地址范围 (Source IP Address Range), 目的IP地址范围 (Destination IP Address Range), 源端口 (Source Port), 目的端口 (Destination Port), 服务协议 (Service Protocol), 状态 (Status), and 设置 (Settings). A new row is being edited, with fields: 策略名称: "打印机" (Printer), 免认证方式: "五元组方式" (Five-tuple Method), 源IP地址范围: "/ (可选)" (Optional), 源MAC地址: "7C-B5-9B-5B-DF-BB" (填写打印机MAC地址), 目的IP地址范围: "/ (可选)", 目的端口范围: "/ (可选)", 服务协议: "UDP" (选择协议类型), 备注: "", and 状态: "启用" (Enabled). Buttons at the bottom include "确定" (Confirm) and "取消" (Cancel). Below the table, a note says "激活 Windows 转到“设置”以激活 Windows." (Activate Windows by going to "Settings").

由于终端上网可能即需要使用 UDP 协议又需要使用 TCP 协议，所以一个终端设备需要建立两条免认证策略服务协议分别选择 UDP 和 TCP。

以上设置可以实现固定设备无需认证就可以上网。

2、无需认证即可访问到指定的外网服务器

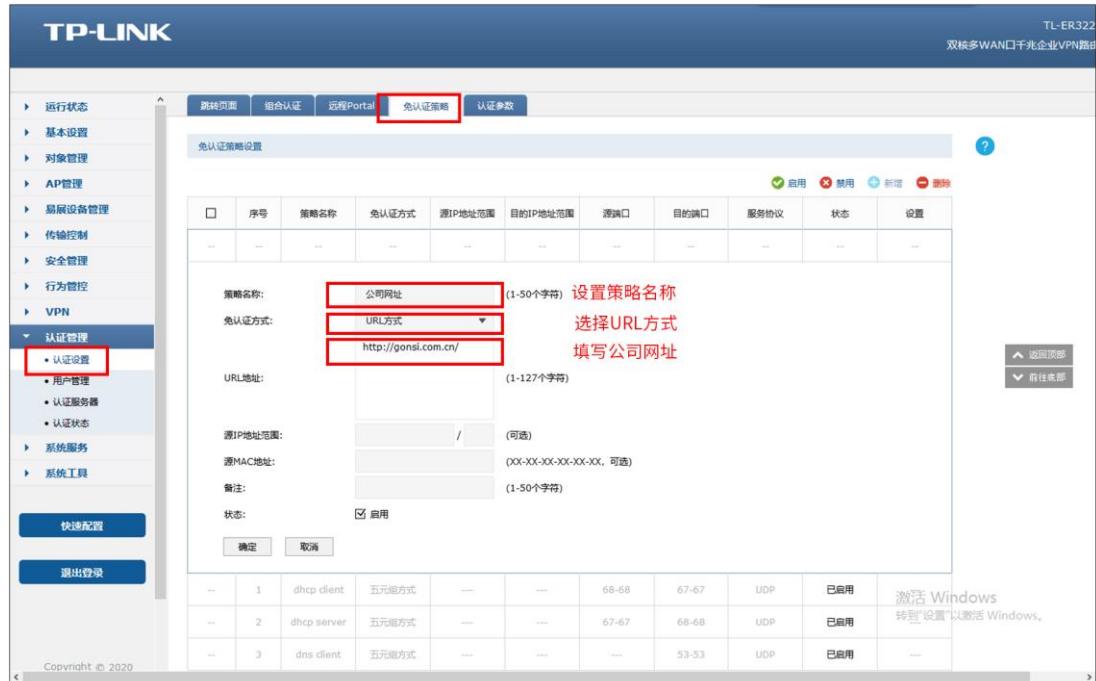
进入路由器界面，点击“认证管理>认证设置>免认证策略”，添加免认证策略，如下图：



以上设置可以实现局域网的所有电脑，无需认证即可访问 121.202.33.100 的外网服务器。

3、无需认证即可访问到指定的网站

进入路由器界面，点击“认证管理>认证设置>免认证策略”，添加免认证策略，如下图：



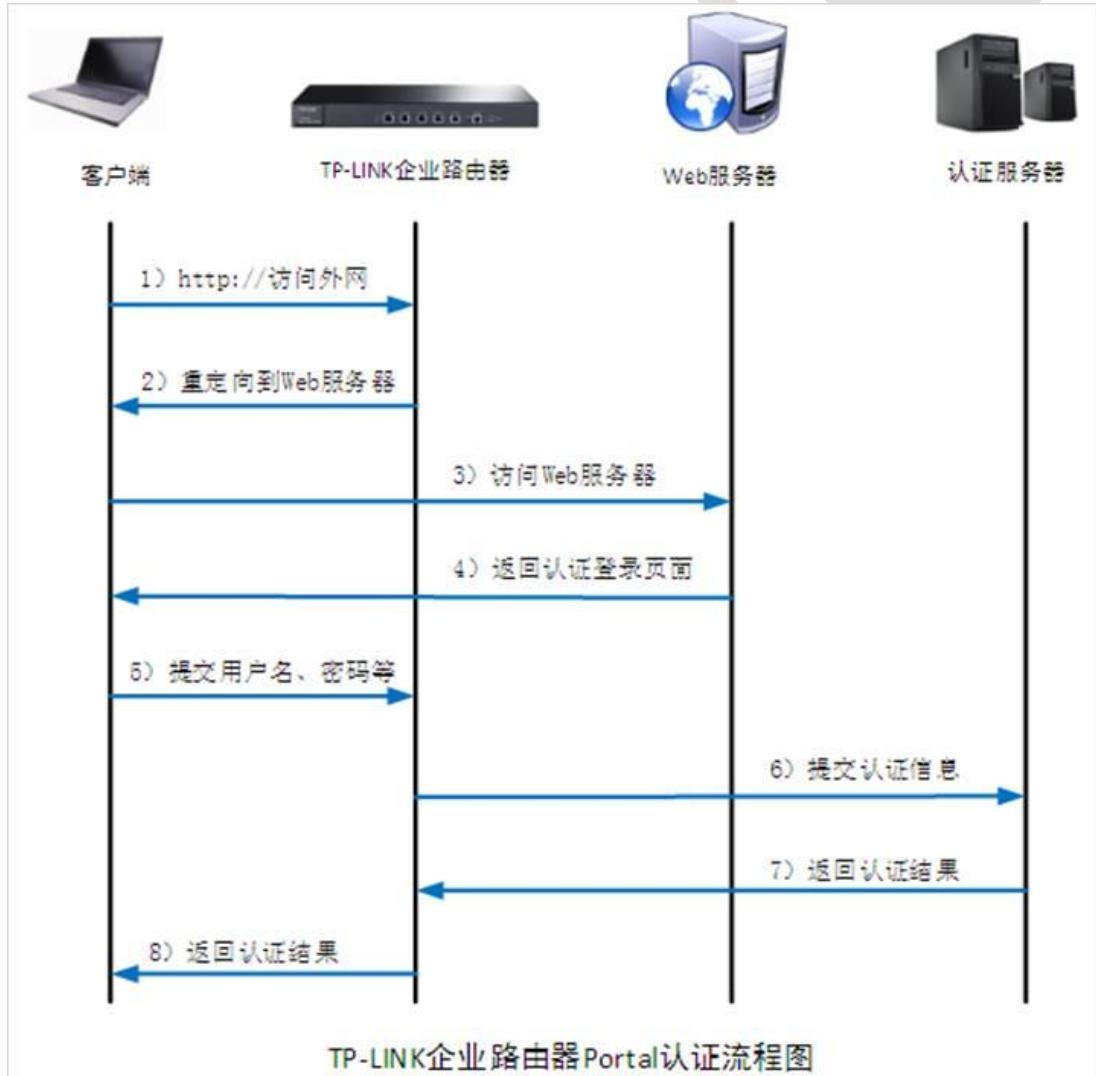
以上设置可以实现局域网的所有电脑，无需认证即可访问公司网站。

10.8 Portal 认证中外部 WEB 服务器建立规范

10.8.1 应用介绍

为了满足广告推送、微信认证等需求，商场、酒店等使用企业路由器中的 Portal 认证功能时需配合第三方认证系统，包括提供 Portal 认证页面的 WEB 服务器、认证服务器等系列设备。本文介绍外部 WEB 服务器与企业路由器认证接口对接的相关规范要求。

10.8.2 流程规范



10.8.3 实现流程

第一步：客户端连接 DUT 的网络，访问任意 http 外网网页

客户端连接上网络后，打开浏览器访问任意 http 外网网页，触发 portal 认证。

第二步：DUT 拦截无线客户端访问外网的 GET 数据包，并重定向到 WEB 服务器

没有通过认证的客户端发往外网的 GET 数据包会被 DUT 拦截，并且 TL-ER6520G 会向客户端返回一条重定向条目及若干指定参数（假设 WEB 服务器域名为 www.abc.com），重定向条目为：

http://www.abc.com/?interface_mode=true&pagetype=xx&stalp=xx&staMac=xx&url=xx

(接口模式)

http://www.abc.com/ssid_mode=true&pagetype=xx&stalp=xx&staMac=xx&apMac=xxx&aplp=xx&url=xx (SSID 模式)

其中重定向连接之后附加的参数在后续提交用户名密码请求时一并加上。

注意：该 WEB 服务器的 URL 地址需要在 DUT 设置免认证策略，若 WEB 服务器端口为非 80 端口，还需要将 WEB 服务器的端口设置免认证策略。

第三步：客户端访问 WEB 服务器

客户端根据第二步返回的重定向条目与 WEB 服务器建立连接。

第四步：WEB 服务器向客户端返回认证页面

WEB 服务器向无线终端返回认证登录页面，针对该认证登录页面，需满足以下规范：

(1) 认证页面必须有一个 Form：

接口模式：

```
action=http://LAN_IP:Port/portal/auth/?interface_mode=true&pagetype=xx  
&authtype=5&stalp=xx&staMac=xx&username=xx&password=xx
```

SSID 模式：

```
action=http://LAN_IP:Port/portal/auth/?ssid_mode=true&pagetype=xx  
&authtype=5&stalp=xx&staMac=xx&apMac=xxx&apIp=xx&  
username=xx&password=xx
```



相关参数说明如下：

- 1) LAN_IP 为当前 DUT LAN 口的 IP 地址
- 2) Port 为 Portal 服务端口
- 3) authtype 为固定值 5 表示远程 Portal 认证
- 4) username 为用户输入的用户名
- 5) password 为用户输入的密码
- 6) 其余参数的值和之前的重定向页面传递的参数保持一致

(2) 认证登录页面以 Get 方式提交 Form 表单；

(3) 认证登录页面必须包含以下参数：

参数	说明
----	----

username	用户名
password	密码

第五步：客户端向 DUT 提交用户名和密码

无线终端在认证登录页面填写用户名和密码后点击 登录 按钮，就以 GET 的方式将 username、password 等参数提交给 DUT。

第六步： DUT 向认证服务器提交认证信息

DUT 在获取客户端提交的信息之后，确定需要进行认证的设备，然后把所有的参数提交给认证服务器进行认证。

第七步： 认证服务器向 DUT 返回认证结果

认证服务器根据 DUT 提交的信息判断用户是否通过认证，并且向 DUT 返回认证结果。

第八步： DUT 向客户端返回认证结果

DUT 根据认证服务器返回来的结果向无线终端返回相应的认证结果，若认证成功，DUT 则根据之前获取的参数信息对相应设备的上网数据给予放行，返回值 ErrorCode 的常用含义：

ErrorCode 参数	说明
0	初始化
1	刷新中
2	认证错误，需访问 failUrl
3	认证超时

4	认证黑名单
5	认证过期
6	非认证时段
7	超过上限
8	服务器错误
9	认证成功, 如果有 successUrl 则跳转至 successUrl
10	登出
11	MAC 地址冲突
12	认证模式错误

Demo 页面下载请点击此处:[Demo 页面](#)

第11章 工业级特性

11.1 如何使用工业级路由器？

11.1.1 应用介绍

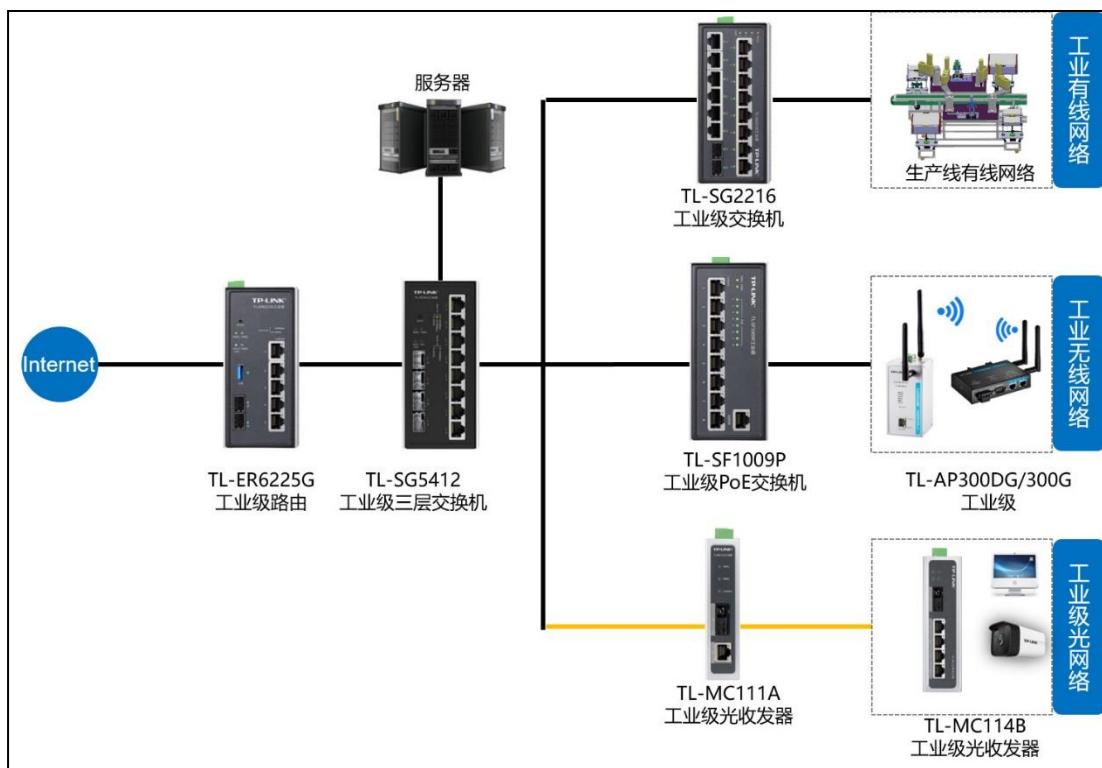
TP-LINK 新推出工业级路由器，其本质应用功能与普通 ER 系列路由器相同。主要区别是面向工业应用环境做出适应，主要包括：

- 支持工业环境的导轨和壁挂安装方式；
- 支持宽电压 9.6-60VDC 三路电源输入，三电源冗余；
- 支持 DIP 拨码开关，方便管理和维护；
- 更强的环境适应能力，包括更宽的上下限工作温度、一定的防尘防腐能力、IP30 防护等级以及增强的电磁兼容性。

11.1.2 需求分析

某工厂利用我司工业级路由器组网，要实现工厂环境的设备可以稳定上网。

11.1.3 应用拓扑



11.1.4 设置方法

下面以 TL-ER6225G 工业级为例，讲解一下如何快速设置上网和报警功能。

1、基本上网配置

电脑配置和路由器同网段的 IP 地址，如：192.168.1.100，网线接到路由器的 5 口，打开浏览器输入路由器的管理 IP，192.168.1.1，在显示的界面输入默认用户名和密码“admin”。

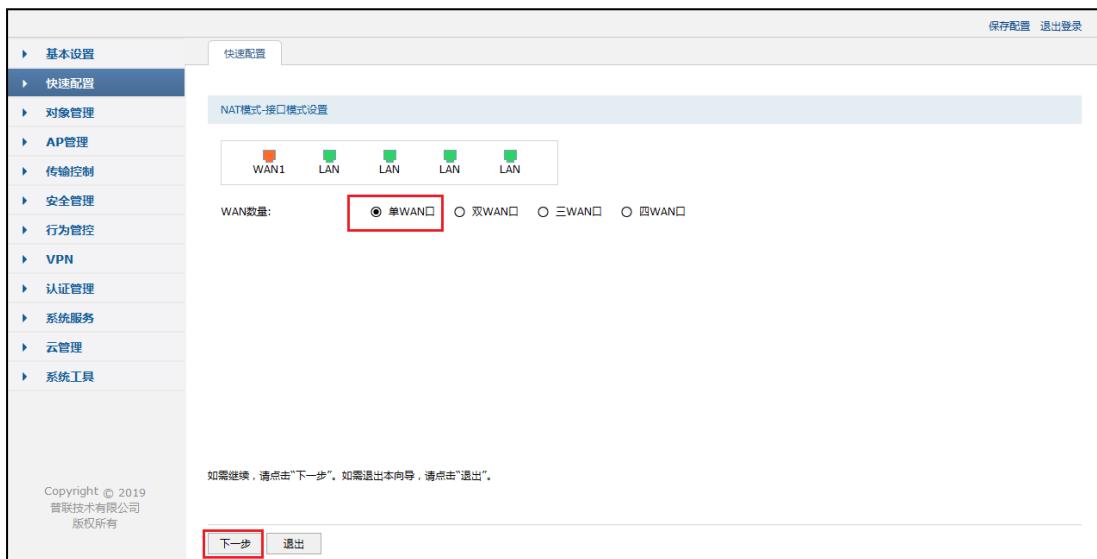


注意：路由器出厂默认的管理端口为 5 口。

进入到路由器的配置界面，点击“快速配置”，点击下一步；



选择 WAN 口模式，本例选择单 WAN 口模式；



选择 WAN 口上网方式，可以根据自己实际需求选择，本例选择“动态 IP”方式上网；

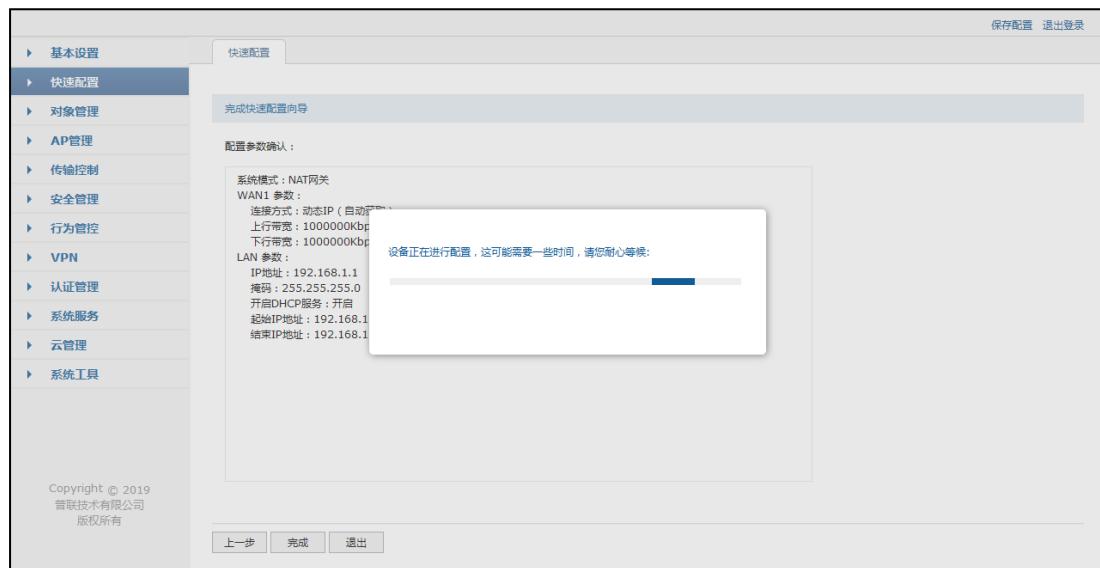


配置 LAN 网段的 IP 地址和 DHCP 服务器。



快速设置配置已经完成，界面点击“完成”按钮，设备将会自动配置，等待一段时间后配置完成，路由器便可上网。





至此，通过快速设置，下面连接路由器的终端便可以通过路由器上网。

2、报警功能配置

端口中断报警功能可以在路由器设备上拨动拨码开关来设置，也可以在路由器 Web 界面配置开启或者关闭报警功能。

路由器 Web 界面点击“系统工具”——“告警器”，可以配置报警相关信息。





相关参数说明如下：

- 1) 电源告警：通过设置来决定电源告警器是否开启。开启该告警功能时，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。
- 2) DI 告警：你可以通过设置来决定 DI 告警器是否开启。
- 3) DI 高状态：当 DI 接口监测的电压值为 13V-30V 时，告警器告警，其余电压值不确定是否告警。
- 4) DI 低状态：当 DI 接口监测的电压值为 -30V-3V 时，告警器告警，其余电压值不确定是否告警。

配置完成之后，记得点击界面右上角“保存配置”按钮。

The screenshot shows the configuration interface for the ER series router. On the left is a navigation sidebar with various management options like Basic Settings, Quick Configuration, Object Management, AP Management, etc. The 'System Tools' section is expanded, and 'Alarms' is selected. The main panel displays the 'Alarms Configuration' settings. It includes three sections: 'Power Alarm' (radio buttons for 'On' or 'Off'), 'DI Alarm' (radio buttons for 'On' or 'Off'), and 'DI Status' (radio buttons for 'High State Alarm' or 'Low State Alarm'). Below these settings is a 'Save' button. At the top right of the main panel, there are status indicators ('Configuration Not Saved', 'Save Configuration', 'Logout') and a note 'Click Save Configuration after configuration is completed'.

至此，工业级路由器的报警功能就设置完了。

第12章 其他功能

12.1 地址组的设置与管理

12.1.1 应用介绍

ER 系列路由器的应用控制、网站访问、网页安全、带宽控制、访问控制等行为管控功能均是基于地址组的，将需要进行同一管控策略的一个或多个 IP 添加到同一地址组，就可以针对该地址组内的所有 IP 来进行上网行为的管控。本文详细介绍地址组的设置与管理。

12.1.2 需求分析

某公司办公网络包含市场、人事等部门，需要进行上网行为管控，以下为各部门的网段：

部门	IP 地址段
人事部 (10 人)	192.168.1.100-192.168.1.109
市场部 (30 人)	192.168.1.120-192.168.1.149

注意：该分组方式仅供举例，具体以实际需求进行划分。

12.1.3 设置方法

1、地址的添加与管理

在路由器管理界面，点击“对象管理 >> 地址管理 >> 地址”，点击“新增”，填写地址名称和包含的地址，其中地址有两种类型：IP 段、IP/MASK，此处选择相对更加灵活的 IP 段的类型，还可根据需求填写备注，点击确定即可完成添加。



按照需求中的要求，新增的两个地址组如下图所示，还可点击对应条目后的编辑或删除按钮对已添加地址组进行管理，勾选对应条目点击页面上方删除按钮也可对多个条目进行删除。

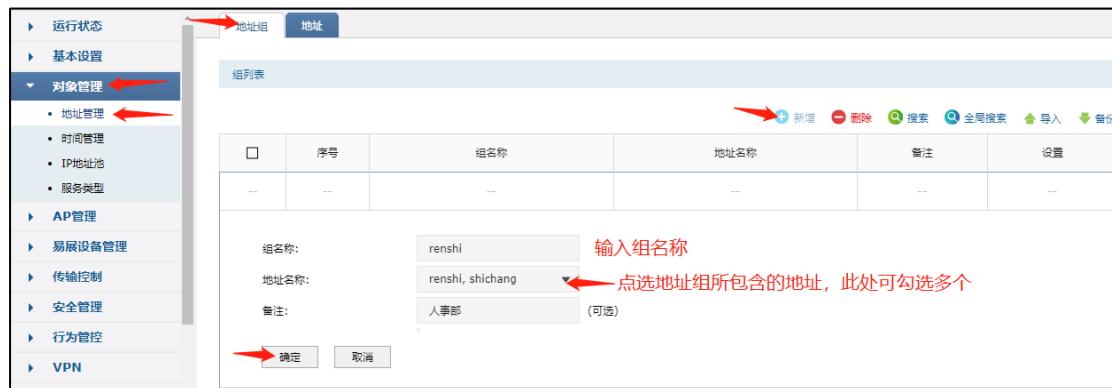


当地址条目较多不好寻找自己想找到的条目时，此处还提供了搜索和全局搜索两种条目搜索方式，可基于地址名称、IP 段、备注进行条目搜索，包括在所有条目中/结果中搜索。

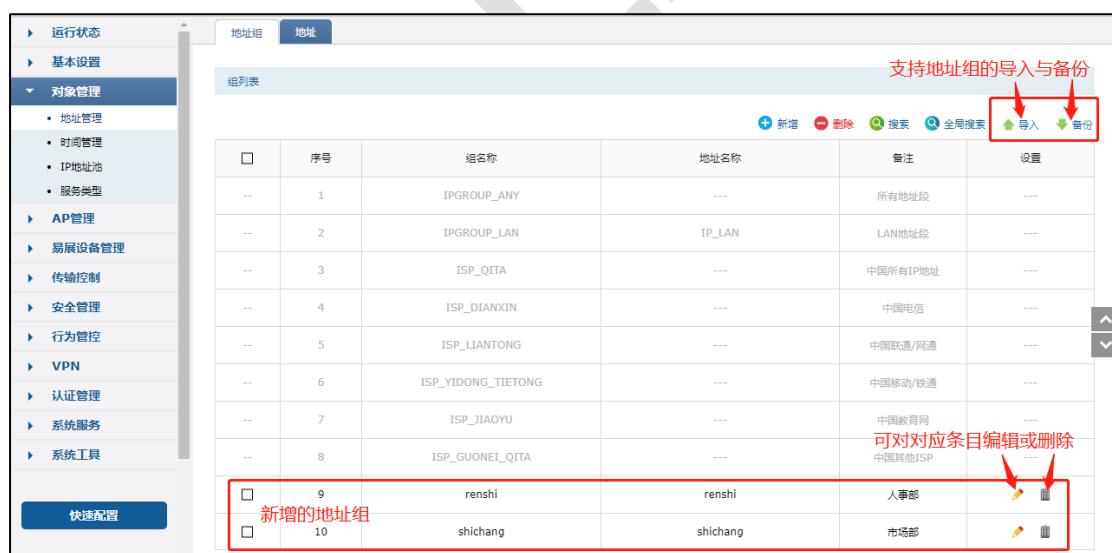


2、地址组的添加与管理

在路由器管理界面，点击“对象管理 >> 地址管理 >> 地址组”，点击“新增”，填写地址名称，勾选地址组包含的地址（此处可勾选多个地址），还可根据需求填写备注，点击确定即可完成添加。



除了第一步中介绍的地址管理相同的删除、编辑、搜索功能之外，该页面还提供了地址组的备份和导入功能，可以通过备份功能获取符合规则的 CSV 文件，以查看文件的正确格式，备份文件也可直接通过导入功能重新添加到地址组列表和地址列表中。



3、地址组的使用

在行为管控相关功能的用户组或源、目的地址范围处选择已添加的地址组即可对此地址组内的 IP 进行对应行为管控，以应用控制为例，如下图所示，点击“行为管控 >> 应用控制 >> 应

用控制”，点击“新增”，点击用户组的下拉选项框，点选第二步中已添加的对应地址组，即可对此地址组进行对应上网行为的管控。



至此，地址组的设置与管理就完成了，可以根据实际需求进行设置。

12.1.4 疑问解答

Q1 如何进行分组比较合理？

分组是针对上网行为管控的需求进行的准备，比如带宽控制中需要为不同部门分配不同的带宽，那么就需要将各个部门分为不同的组。如果需要对人事、市场部门的管理人员开放网络权限，那么可以将这些特定的电脑分为一个组，针对该组进行权限控制。合理的分组基于对需求的考虑全面。

Q2 不同地址组包含的 IP 地址段能否有交集？

可以，在新增地址时地址段的设置与已有地址存在交集，新增地址组时也可以选择被已有地址组引用的地址。

Q3 地址组已经被设置规则引用，是否可以在已被引用的地址组继续添加地址呢？

可以，新加入的 IP 地址也会与所在地址组一样一起被管控。

12.2 带宽控制设置指南

12.2.1 应用介绍

网络的带宽资源是有限的，而且宽带使用时经常会出现“20%的主机占用了 80%的资源”的问题，导致网络的应用出现“上网慢、网络卡”等现象。ER 系列路由器提供了基于 IP 地址的带宽控制功能，可以有效防止少部分主机占用大多数的资源，为整个网络带宽资源的合理利用提供保证。

本文以 TL-ER5120G 为例，介绍 ER 系列路由器带宽控制的设置方法。

12.2.2 需求分析

某企业 20M 光纤宽带接入，内网电脑 IP 地址设置为手动指定，根据需求，指定以下需求表格：

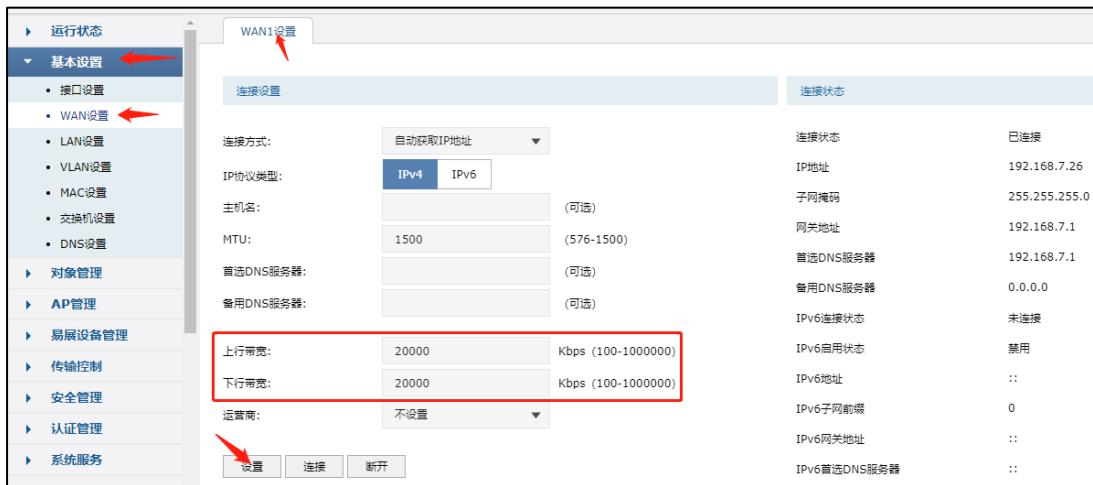
部门	带宽需求	IP 地址段	最大带宽分配
市场部 (10 人)	浏览网页、下载内容、需要较大的带宽	192.168.1.10-19	每人 3Mbps
其他部门 (30 人)	浏览网页、收发邮件满足一般上网应用	192.168.1.20-49	每人 1Mbps

注意：上述表格数据仅供参考，具体以实际环境为准。

12.2.3 设置方法

1、设置接口带宽

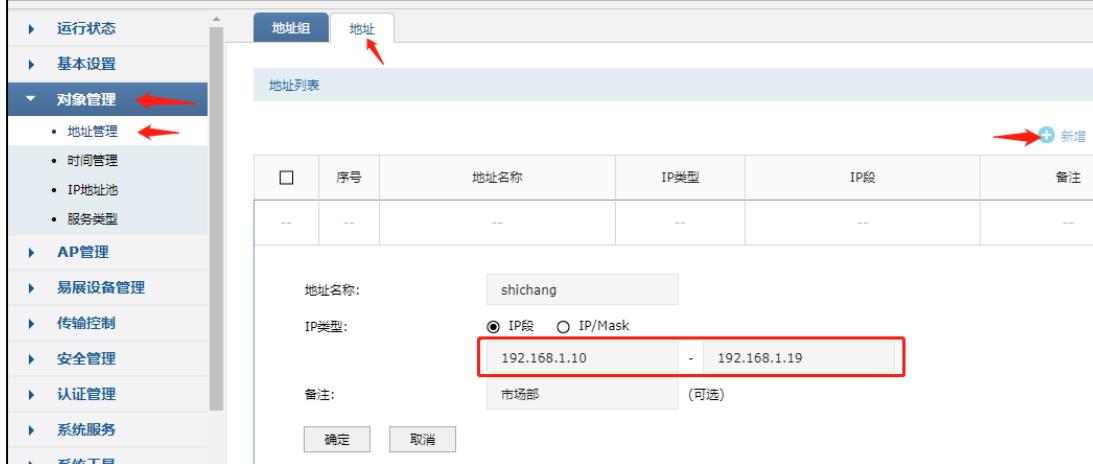
在路由器界面，点击“基本设置>WAN 设置”，选择连接外网的 WAN 口，填写宽带线路真实的上行、下行带宽（本例中上下行带宽均为 20Mbps），并点击“设置”。（本文以自动获取 IP 地址上网为例）



注意：1Mbps=1024Kbps，为了便于计算，文档以1Mbps=1000Kbps为例。

2、添加地址组

添加市场部和其他部门的地址组，后续的宽带控制规则中针对地址组进行控制。点击“对象管理>地址管理>地址”，点击“新增”，添加如下地址，点击“确定”。



同一页面，选择“地址组”，点击“新增”，选择之前添加的地址，点击“确定”。



其他部门地址组的添加，也是相同操作。

3、设置带宽控制规则

点击“传输控制>带宽限制”，点击“新增”，为市场部设置如下的带宽控制规则：



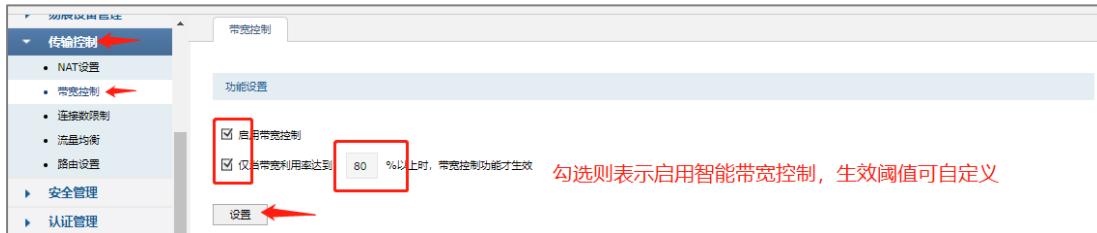
注意：共享表示地址组中的所有电脑共用设定的上下行带宽。本例中选择独立，表示每个IP单独限制。

同样的方法，新增其他部门的带宽控制规则。

4、智能带宽控制

设置好带宽控制规则后，需要勾选“启用带宽控制”并点击“设置”后，带宽控制规则才会生效；

智能带宽控制表示仅当前带宽利用率超过设置的百分比时，带宽控制功能才开始生效。具体计算公式为：第一步中填写的线路实际下行带宽×设置的百分比。



至此，带宽控制设置完成，企业员工的电脑将按照带宽控制规则中的设置来使用网络。

12.2.4 疑问解答

Q1、带宽控制最大限制多少才合适呢？

限制带宽取决于两个方面：一是业务需求，不同部门、电脑的工作需求决定对网络带宽的需求，该需求决定占用总带宽的比例；二是接口带宽，企业总带宽的大小决定给各个业务主机分配的具体值。例如公司总带宽为 10M 光纤，A 部门 10 台电脑需要下载、上传、收发邮件，那么每台主机建议限制上下行最大值为 1500~2000Kbps。

Q2、设置好带宽控制后不生效，怎么办？

需要分别检查以下三点：电脑的 IP 地址是否固定、受控电脑的 IP 地址是否属于受控地址组、控制带宽值设置是否合理，检查并排查以上问题即可。

Q3、设置好带宽控制后，受控地址组是否可以继续加入 IP？

可以。直接在“地址管理”中编辑对应的地址组，并填写要加入的 IP 地址段，最后点击“确定”。

12.3 PPPoE 服务器应用设置指南

12.3.1 应用介绍

PPPoE 即 PPP over Ethernet，是指在以太网中传输 PPP 的技术。目前国内大多数宽带服务商使用 PPPoE 作为宽带接入技术，通过给用户分配宽带账号密码，结合认证、计费服务器实现宽带运营服务。终端用户通过在电脑或家庭网关（路由器）上进行宽带拨号，实现连接到网络上网。

PPPoE 拨号可以避免局域网 ARP 欺骗、隔离用户间的访问，一定程度上保证网络安全稳定，

如下图：



12.3.2 需求分析

某小区宽带服务商使用 TL-ER5120G 作为接口路由器，接入宽带为 500M 光纤，小区有 80 家宽带用户。该宽带服务商需要为用户分配宽带账号密码，让有账号的用户通过拨号上网，

没有账号的用户无法上网，同时宽带服务商的管理主机（192.168.1.2-12）无需拨号即可上网。

注意：PPPoE 服务器功能丰富，具体配置需结合实际需求，以上仅供本文举例。

12.3.3 设置方法

1、设置 IP 地址池

登录路由器管理界面，点击“对象管理 >> IP 地址池”，点击“新增”，自定义设置地址池名称、地址池的起始 IP 地址和结束 IP 地址，点击“确定”，如下图：



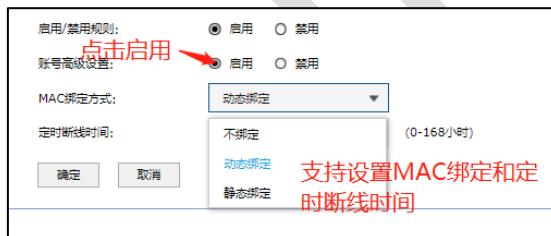
注意：地址池范围不能与 LAN 或 VLAN 网段相同。

2、设置账号

点击“系统服务>> PPPoE 服务器 >> 账号管理”，点击“新增”，添加用于拨号上网的账号、密码，选择第一步中设置的 IP 地址池，设置最大会话数（表示设定数量的用户可同时使用该账号拨号）和账号到期时间，设置账号带宽控制模式：其中共享表示账号的所有用户共用的带宽；独立表示账号的所有用户独占设置的带宽，选择启用账号后点击“确定”，设置如下图：



“启用”账号高级设置，支持设置 MAC 绑定和定时断线时间（当定时断线时间为 0 时表示不会定时断线），如下图：



MAC绑定方式说明：

- 1) 不绑定：不进行用户和 MAC 的绑定。
- 2) 静态绑定：选择静态绑定时，需要设置一个 MAC 地址，该账号只能在该 MAC 的主机上登录。
- 3) 动态绑定：路由器记录第一次登录该账号的 MAC 地址，以后必须是该 MAC 的主机才能登录该账号。

3、设置例外 IP 管理

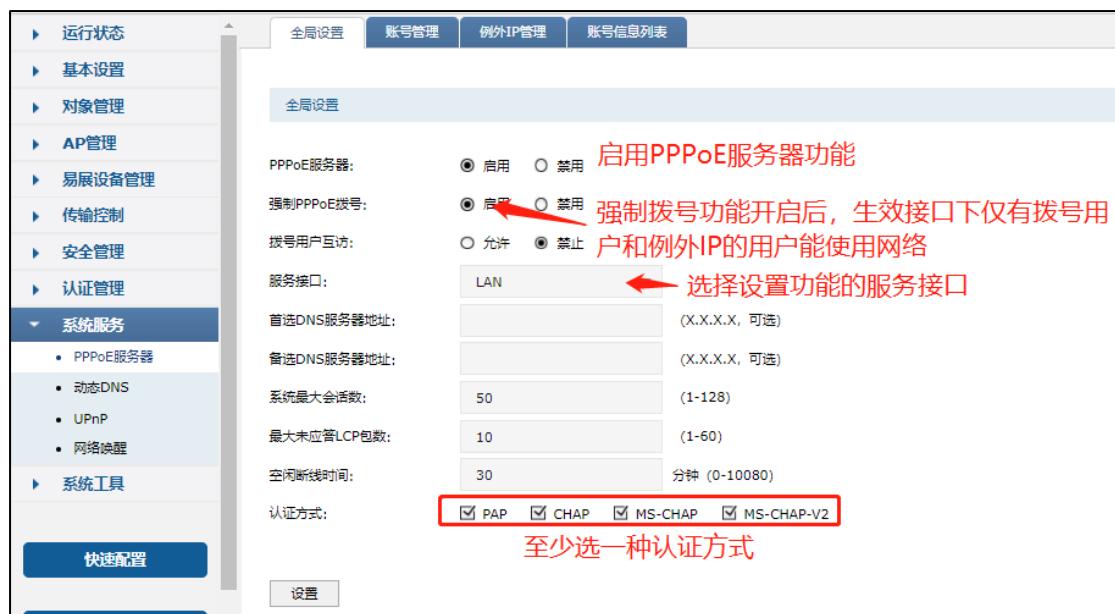
例外 IP 的用户无需拨号即可上网（即使设置为强制拨号）。点击“系统服务>> PPPoE 服务器 >> 例外 IP 管理”，点击“新增”，根据需求，设置规则如下，点击“确定”：



注意：例外 IP 中的地址是局域网电脑的本地连接地址。

4、设置全局设置

点击“系统服务>> PPPoE 服务器 >> 全局设置”，启用 PPPoE 服务器和强制 PPPoE 拨号，在首选 DNS 及备用 DNS 服务地址的位置输入当地宽带线路的 DNS，其它参数可保持默认，点击“设置”，如下图：



至此，PPPoE 服务器设置完成，局域网中的宽带用户均需要使用分配的账号密码拨号才可以上网，管理员主机无需拨号即可上网，没有账号或账号过期的用户，不可以上网。

在“系统服务>> PPPoE 服务器 >> 账号信息列表”页面可以查看到 PPPoE 拨号用户的连接信息，也可对已连接用户进行断开连接操作，如下图：



12.3.4 疑问解答

Q1 设置好 PPPoE 服务器，如何控制拨号用户的带宽和上网行为？

PPPoE 服务器完成，宽带用户拨号后会获取到 IP 地址，将对应 IP 地址添加到用户组中，实现带宽控制和上网行为管控。

Q2 是否可以级联路由器，使用路由器拨号？

可以。连接网线到二级路由器的 WAN 口，在二级路由器上设置 PPPoE 拨号。并可以实现二级路由器下面的电脑和手机等设备不需拨号即可共享上网。



12.4 网络唤醒功能的使用指南

12.4.1 应用介绍

许多用户朋友为了方便网络管理，需要远程唤醒内网已经关机的 PC/NAS/Server 等设备，对网络唤醒功能有着强烈的需求。但之前为了完成网络唤醒，需要进行复杂的步骤：在路由器 WAN 口地址是公网地址的前提下，还需要设置 IP 静态地址分配、arp 绑定、虚拟服务器、动态 DDNS 且还需要下载专门的远程唤醒工具才能实现，远程唤醒十分不方便。现在此功能添加到企业路由器中，方便大家使用。

12.4.2 需求分析

某企业使用 TL-ER3220G，内网有台 Server 设备平时是关闭的，只有需要时才会打开，且不想专门跑到设备旁边开机，需要远程唤醒此设备，已知该设备支持并开启了远程唤醒，设备的 MAC 地址是 94-DE-80-57-9D-5A。

12.4.3 设置方法

1、开启网络唤醒

在“系统服务 >> 网络唤醒”，点击“新增”，自定义主机名称，输入需要远程唤醒的设备的 MAC 地址，选择此主机所在内网网段的接口，此处被唤醒设备在默认的 LAN 网段，因此是选择 LAN 口，点击“确定”。



此时路由器端的配置已完成。

2、进行远程唤醒的两个途径

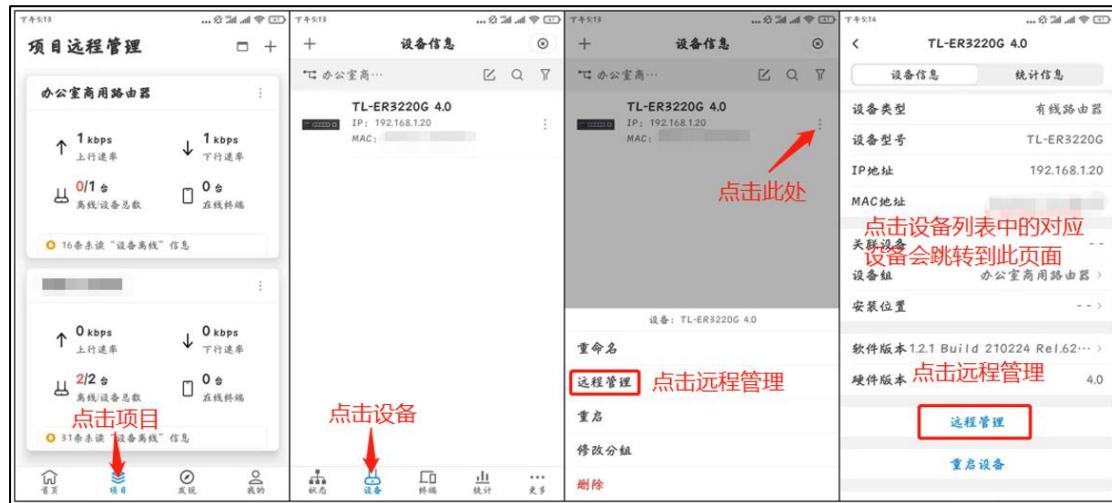
方法 1：远程登录到路由器的 WEB 界面，进行远程唤醒，此时路由器需要设置开启远程管理，同时需要 WAN 口为公网 IP。在“系统服务 >> 网络唤醒”的列表中，找到对应的设备，点击网络唤醒按钮，即可一键唤醒内网设备。



方法 2 (推荐使用)：将路由器添加至“商云”进行管理，电脑登陆 TP-LINK 商云管理平台，点击“设备列表”，找到对应设备的“远程管理”按钮，点击后即可实现远程管理，在“方法 1”所示界面，点击网络唤醒即可成功唤醒内网设备。



手机打开“TP-LINK 商云”APP，点击页面下方“项目”，选择对应路由器所在项目，点击页面下方的“设备”，找到路由器后点击如下图所示对应位置后，点击“远程管理”，或者点击设备列表中的相应路由器，页面下方也有“远程管理”按钮，点击即可进入路由器管理页面，在“方法 1”所示界面，点击网络唤醒即可成功唤醒内网设备。



12.5 诊断工具的使用指南

12.5.1 应用介绍

ER 系列路由器的诊断工具包括两种类型：PING 通信测试和路由跟踪检测，可分别用于测试外网的连通性和检测数据包访问目的 IP/域名所经过的路由节点及延迟。

以 TL-ER5120G 的配置界面为例，登陆路由器管理界面，选择“系统工具>诊断工具>诊断工具”，可以看到两种诊断工具：PING 通信检测、路由跟踪检测。



12.5.2 需求分析

某用户内网无法上外网，希望通过路由器诊断下问题原因所在。此时可以通过 PING 通信检测来判断 WAN 口与外网之间是否连通（出接口选择对应 WAN 口），或者可以检测路由器与内网主机之间是否连通（出接口选择对应 LAN/VLAN 口）；也可以通过路由跟踪检测来检测数据包访问目的 IP/域名所经过的路由节点及延迟。

12.5.3 设置方法

1、PING 通信检测

诊断工具类型选择“PING 通信检测”，目的 IP/域名选择常见 DNS 服务器如 114.114.114.114 或者门户网站如 www.qq.com，出接口则选择上网实际使用的 WAN 口，此处因为仅用 WAN1 口上网，所以选择“WAN1”，点击“开始”，测试结果如下图所示即为正常，也可以根据测试结果中的 time 判断延迟是否正常。



而当 WAN 口无法 Ping 通目的 IP 或域名，则不会显示 PING 回复时间，而是显示“Request timed out”，请求超时；或者无法解析域名时，显示“There is no response from DNS”，如下图所示。

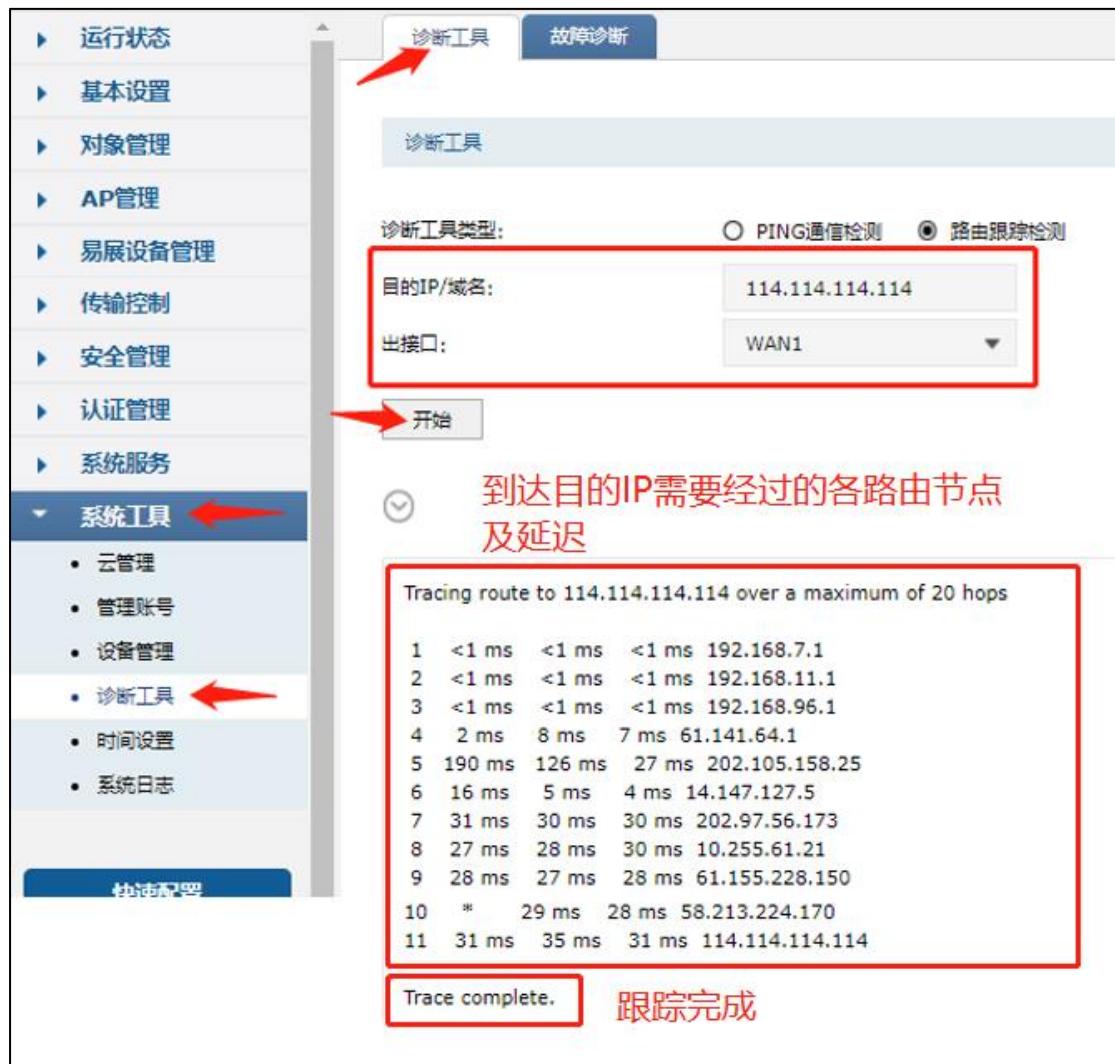


点击“开始”下方的圆形按钮，还可以自定义“PING 包次数”（1-50）和“PING 包大小”（4-1472 Bytes）。



2、路由跟踪检测

诊断工具类型选择“路由跟踪检测”，目的 IP/域名选择常见 DNS 服务器如 114.114.114.114 或者门户网站如 www.qq.com，出接口则选择实际使用的 WAN 口，此处因为仅用 WAN1 口上网，所以选择“WAN1”，测试结果如下图所示即为正常，可以看到访问目的 IP/域名所经过的路由节点及延迟。



点击“开始”下方的圆形按钮，还可以自定义“路由跟踪最大 TTL”（Time To Live，生存时间值），TTL 是 IP 数据包在计算机网络中可以转发的最大跳数，可设置值为 1-30。



12.6 DDNS 的使用指南

12.6.1 应用介绍

许多用户需要远程访问路由器或者远程访问内网服务器，但是又没有静态公网 IP 地址。这时候就可以通过 DDNS+变化的公网 IP 地址的方式达到相同的使用效果。DDNS 也称为动态 DNS，中文名称叫动态域名解析，指的是将变化的 IP 地址与固定的域名对应起来的服务。

宽带拨号上网时路由器 WAN 口 IP 是动态变化的，如果登录动态 DNS，那么只需要使用该域名即可访问到路由器或开放的服务器，无需理会动态变化的 IP 地址。本文介绍企业路由器动态 DNS 的设置方法。

12.6.2 需求分析

某企业使用 TL-ER3320G，内网有台服务器通过虚拟服务器映射端口到公网，需要在外网可以访问到该服务器。路由器是带宽拨号上网，获取的是动态 IP 地址，使用 IP+端口的方式需要经常变化 IP 地址，使用十分麻烦。

可以通过 DDNS，将 WAN 口 IP 绑定到某个域名上。通过域名+端口的形式访问内网服务器，域名会实时更新绑定当前 WAN 口 IP。

12.6.3 设置方法

TL-LINK 企业级路由器支持 TP-LINK 动态域名、花生壳动态域名、科迈动态域名和 3322 动态域名等多种动态域名，选择其中一种进行设置即可。下面分别介绍这几种动态域名的设置方法：

一、TP-LINK 动态域名

在“系统服务>动态 DNS”中选择“TP-LINK 动态域名”，使用 TP-LINK 动态域名需要先登录

TP-LINK ID，如果没有可以在路由器中免费注册一个。



登录账号之后，根据需要创建域名；

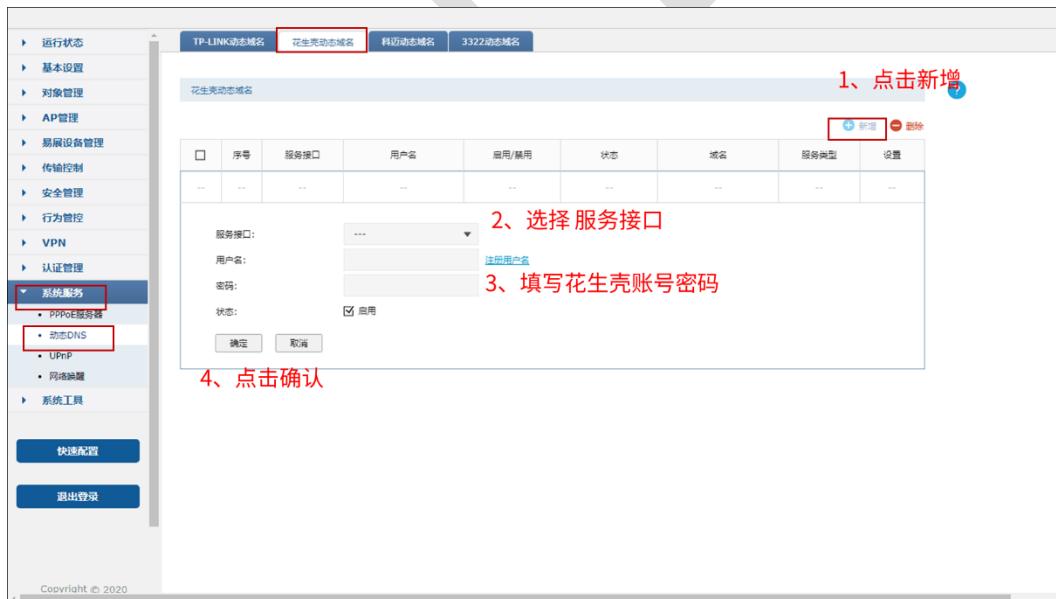


创建域名之后，绑定到对应接口即可；



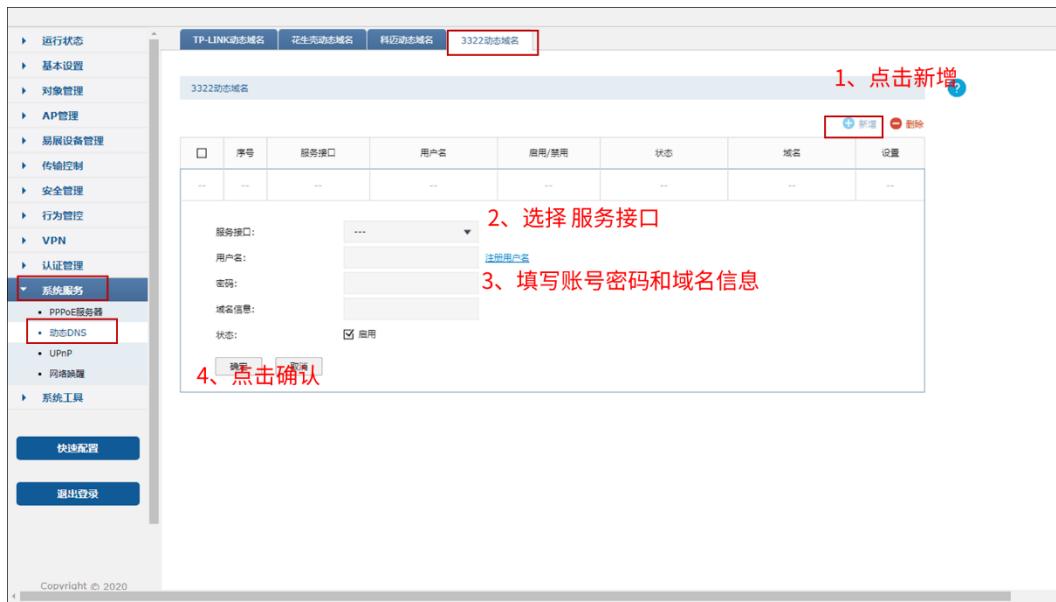
二、花生壳/科迈动态域名

选择使用花生壳动态域名或科迈动态域名只需要选择对应的服务接口并登录相应的账号密码即可。下图以使用花生壳动态域名为例：



三、3322 动态域名

选择使用 3322 动态域名配置过程与花生壳基本一致，只需要填写账号密码与域名信息然后绑定对应接口即可。



12.6.4 疑难解答

1、使用 DDNS 后，为什么在远端无法正常解析？

DDNS 会将域名与 WAN 口所在的公网 IP 地址绑定，可以尝试访问 IP138.com，确认 WAN 口的 IP 地址为公网 IP；

尝试更换 DNS 服务器地址，如 114.114.114.114，再次尝试解析。

2、无法登录 TPLINK ID 或其它动态域名账号怎么办？

查看 WAN 口是否正常联网，检查 WAN 口的 DNS 设置是否正确；

查看路由器下的电脑是否可以正常登录对应账号，判断是否为账号问题。