TP-LINK®

主要功能配置实例

R系列企业级路由器

声明

目录

第1章 前言

本手册旨在帮助您正确使用 R 系列企业级路由器。内容包含配置路由器各种功能的的实例和详细说明。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-R473G	3.0
TL-R483G	4.0
TL-R483G 工业级	1.0
TL-R476G	2.0
TL-R476G+	2.0
TL-R478G	2.0
TL-R478G+	4.0
TL-R479G+	2.0
TL-R470GP-AC	3.0、4.0
TL-R473GP-AC	3.0、4.0
TL-R479GP-AC	3.0、4.0
TL-R479GPE-AC	3.0、4.0
TL-R488GPM-AC（路由模块）	2.0
TL-R489GP-AC	2.0
TL-R498GPM-AC（路由模块）	2.0、3.0
TL-R499GPM-AC（路由模块）	1.0
TL-R479P-AC	3.0

第2章 基础联网设置

2.1 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-R488GPM-AC 为例介绍 R 系列企业路由器的基本设置。

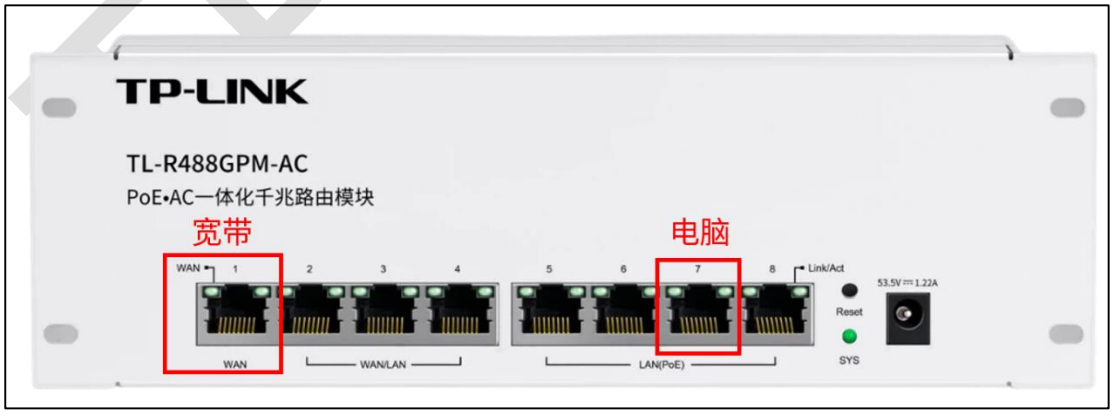
2.1.2 需求介绍

路由器接入网络，电脑连接路由器能够正常上网。

2.1.3 设置方法

第一步、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。



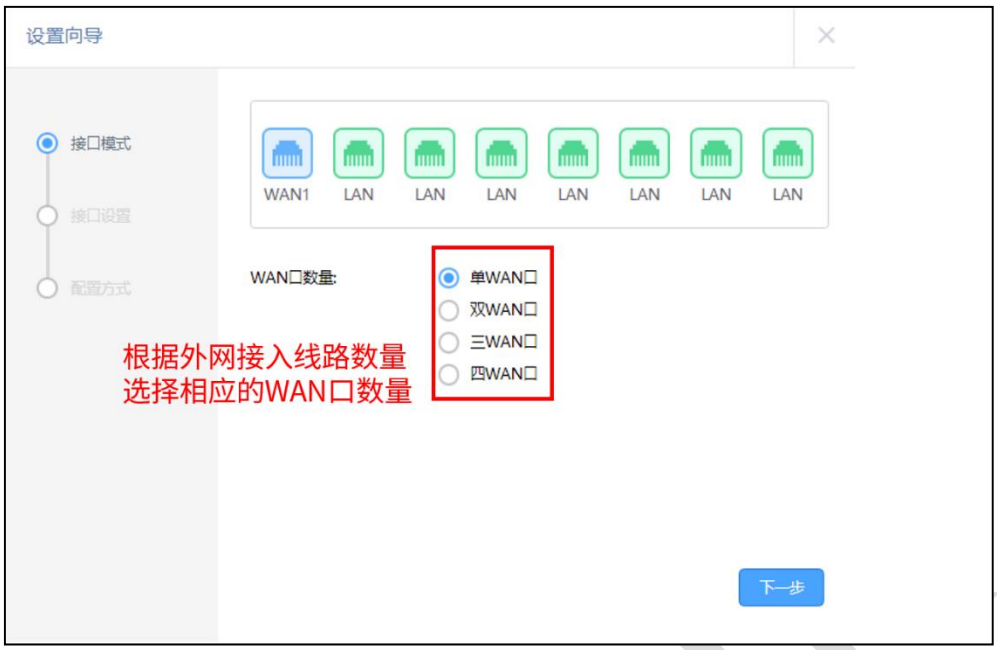
第二步、登录路由器管理界面

打开浏览器，清空地址栏并输入路由器的底部管理地址 tplogin.cn（部分型号路由器可能无法通过域名登陆，请以路由器底部标贴的登陆地址为准），在弹出的设置管理密码界面中，设置管理密码，点击<确定>，登录路由器管理界面。

注意：请记住设置好的管理密码，用于后续管理路由器。

第三步、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。

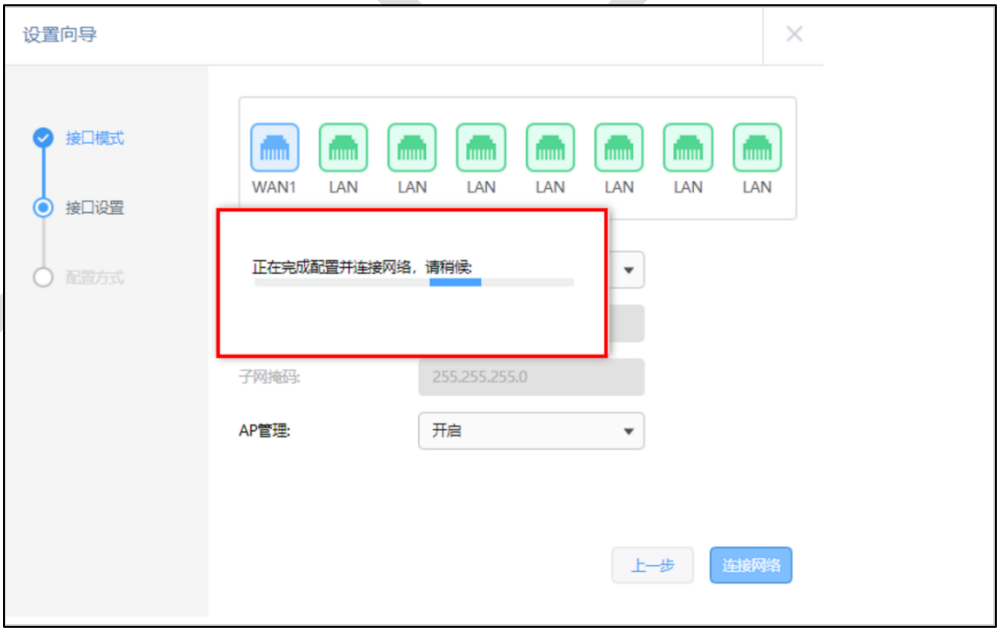


第四步、选择 WAN 口上网方式

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>。

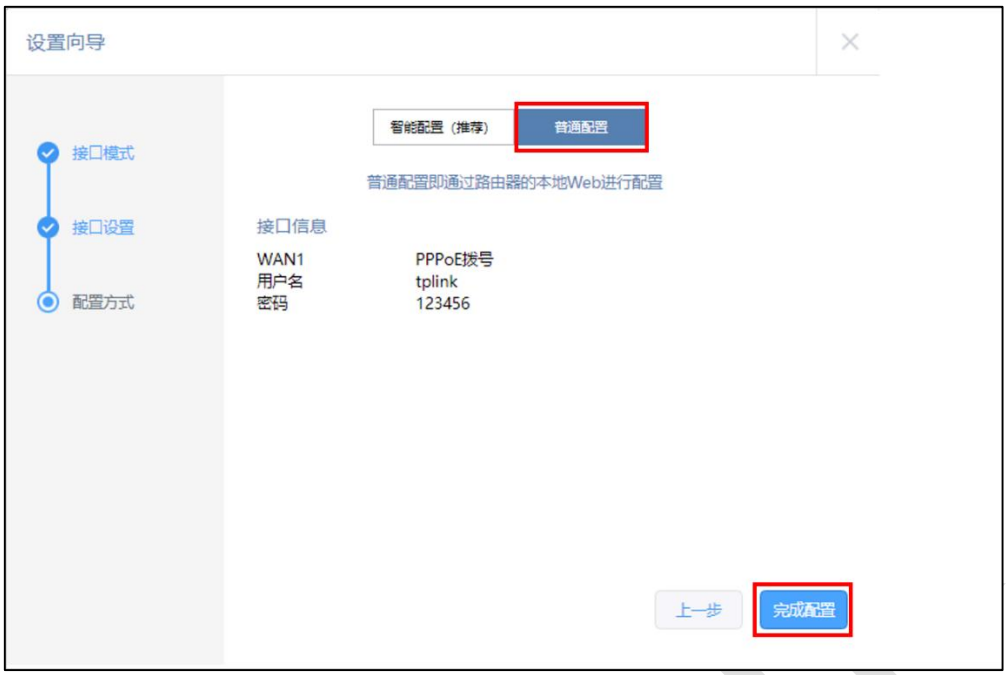
第五步、设置 LAN 口 IP

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。



第六步、选择配置方式

配置方式可选择智能配置和普通配置，这里选择普通配置，则点击完成配置即可。



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。

2.1.4 注意事项

- 请务必牢记设置好的管理密码，用于后续管理路由器。

2.2 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-R479GP-AC 为例介绍 R 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

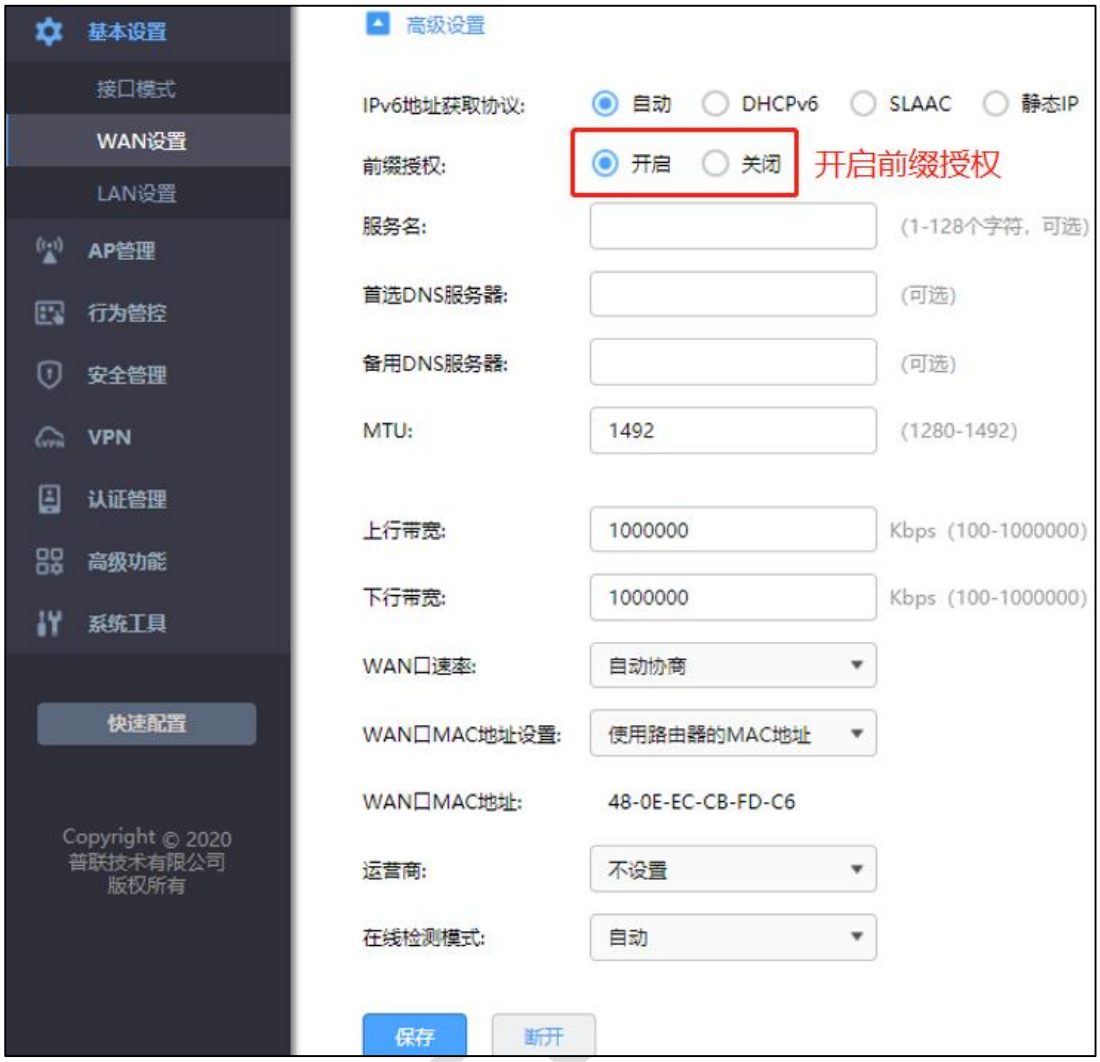
本节将根据前端运营商线路是否支持前缀授权分别进行介绍：

一、支持前缀授权的 IPv6 线路上网设置方法

第一步、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，并在高级设置中开启前缀授权功能，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。


运行状态
基本设置
接口模式
WAN设置
LAN设置
AP管理
行为管控
安全管理
VPN
认证管理
高级功能
系统工具
快速配置
WAN设置
流量均衡
ISP选路
接口设置
连接方式:
PPPoE拨号
IP协议类型:
IPv4
IPv6
选择IPv6
状态:
启用
禁用
复用IPv4拨号链路:
启用，并复用IPv4链路
用户名:
密码:
连接状态:
已连接
IP地址:
240e:fa:f8:546:4a0e:ec05:75cb:fdc6
DNS服务器:
240e:1f:1::1 , 240e:1f:1::33
在线时长:
0天0小时44分钟47秒



第二步、LAN 口参数设置

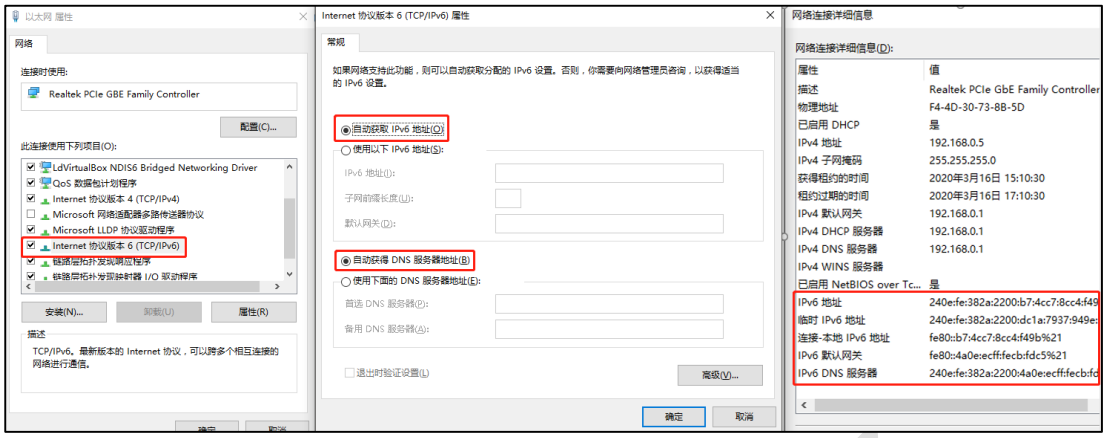
IP 协议类型选择 IPv6，并点击启用，地址配置方式选择 EUI-64，前缀授权接口选择刚才设置好的 WAN 口（EUI-64 表示自动获取 64 位 IPv6 的前缀地址）。

第三步、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。

第四步、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。



二、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 R 系列企业路由器支持 IPv6 桥模式，具体配置方法如下：

第一步、开启 IPv6 桥模式

在基本设置->接口模式中启用 IPv6 桥模式，点击保存。

第二步、开启桥模式后 WAN 口和 LAN 口的 IPv6 参数均不可设置


运行状态
基本设置
接口模式
WAN设置
LAN设置
AP管理
行为管控
安全管理
VPN
认证管理
高级功能
系统工具
快速配置
Copyright © 2020
普联技术有限公司
版权所有
WAN设置
流量均衡
ISP选路
接口设置
连接方式:
PPPoE拨号
IP协议类型:
IPv4
IPv6
状态:
启用
禁用
复用IPv4拨号链路:
用户名:
密码:
连接状态:
未连接
IP地址:
::
DNS服务器:
::
在线时长:
0天0小时12分钟33秒
高级设置
桥模式下WAN不能启用IPv6功能


运行状态
基本设置
接口模式
WAN设置
LAN设置
AP管理
行为管控
安全管理
VPN
认证管理
高级功能
系统工具
快速配置
Copyright © 2020
普联技术有限公司
版权所有
LAN设置
DHCP服务
客户端列表
静态地址分配
DHCPv6服务
接口设置
IP协议类型:
IPv4
IPv6
状态:
启用
禁用
地址配置方式:
EUI-64
手动
前缀授权接口:

IPv6地址前缀:
IP地址:
MAC地址:
48-0E-EC-CB-FD-C5
设置
注意:
在您使用IPv6的EUI-64地址配置方式时，当开启前缀授权接口并保存配置后，网络可能会短暂中断。
桥模式下LAN不能启用IPv6功能

2.2.4 疑问解答

Q1：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。

Q2：怎么判断 IPv6 线路是否支持前缀授权?

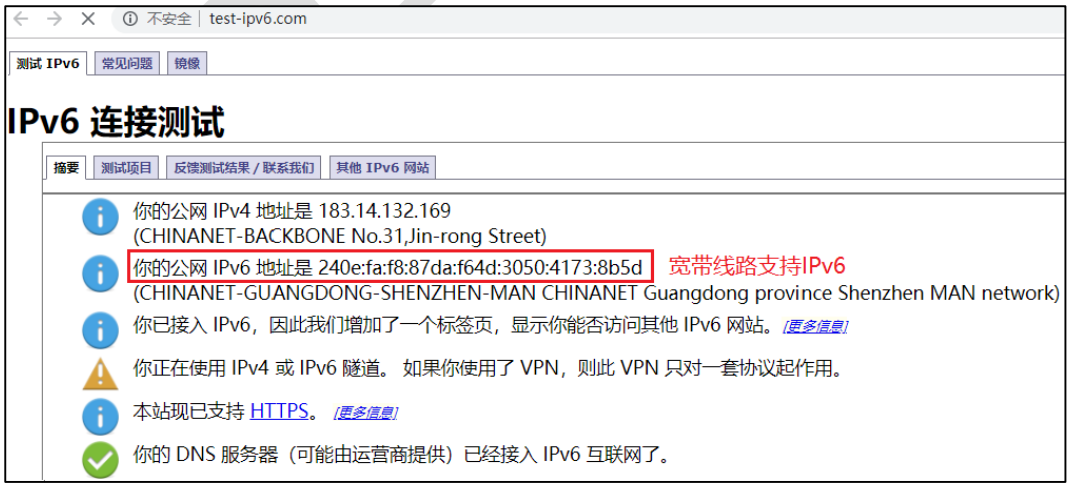
请致电宽带运营商确认。

Q3：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。

Q4：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。



Q5：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。

Q6：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。

Q7：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。

Q8：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。

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。

3.1.2 需求介绍

路由器接入网络后，管理员可以在外网管理或控制路由器。

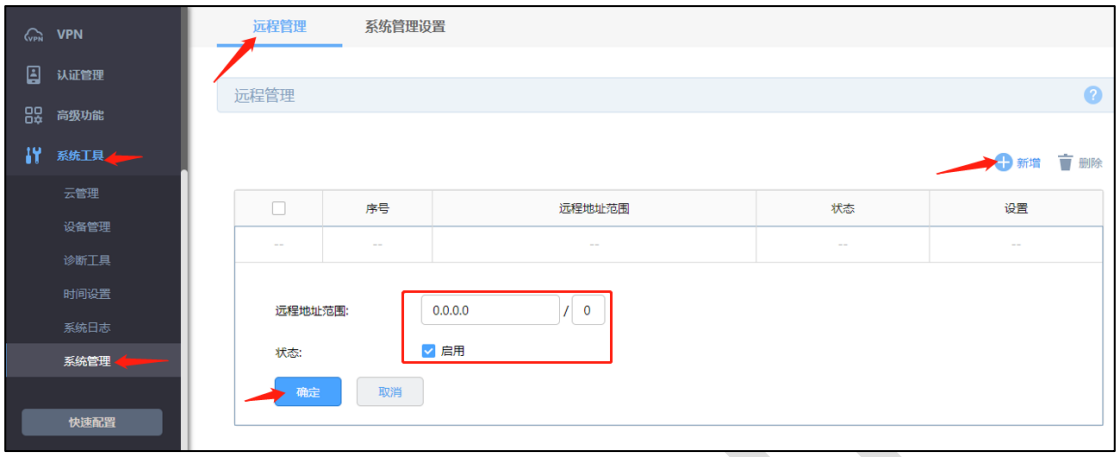
3.1.3 设置方法

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。

一、远程 WEB 管理

设置方法

登录路由器界面，在"系统工具 >> 系统管理 >> 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 >> 系统管理设置"中设置 WEB 服务端口，如下。

访问方法

在运行状态中，查看到 WAN 口 IP 地址。

注：通过 WAN 口 IP 在外网远程管理路由器需要 WAN 口 IP 为公网 IP，此处仅作演示。

外网电脑在浏览器地址栏输入 http://WAN 口 IP:端口来访问。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。

二、商云管理

第一步、开启云管理功能

登录本地 Web 管理界面，进入"系统工具 >> 云管理"，点击"开启云管理"，点击<保存>。

注：在开启云管理之前，先备份配置文件。

第二步、登录云平台

打开浏览器，访问 TP-LINK 商用网络云平台（smbcloud.tp-link.com.cn），在设备列表中点击<添加设备>，添加完成后在设备信息中找到对应路由器，点击条目后方"远程管理"，即可实现在外网远程管理路由器。

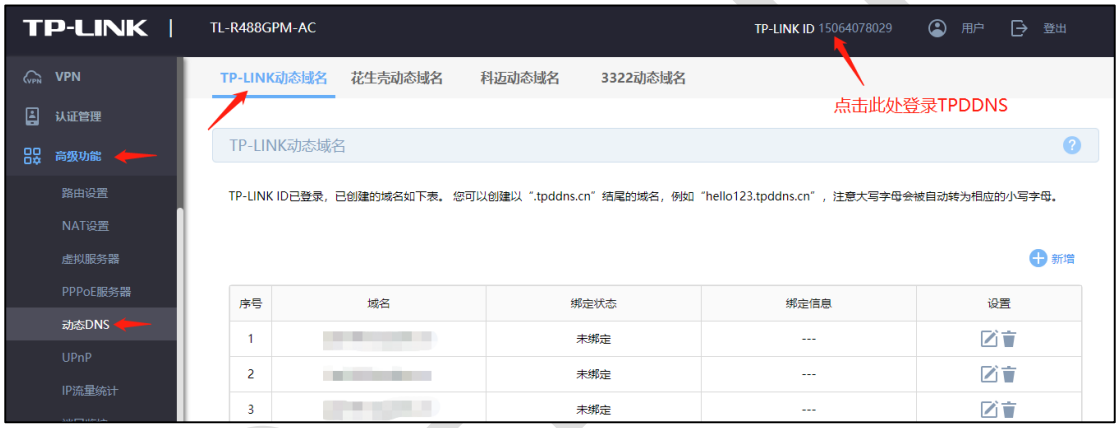
3.1.4 注意事项

- 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。
- 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。
- 部分企业路由器界面有保存配置的提示，请务必保存配置。
- 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)。

3.1.5 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。以 TP-LINK 动态域名为例，在下图所示位置点击后，登陆页面输入 TP-LINK ID 及密码登录 TPDDNS 后，即可在"高级功能 >> 动态 DNS >> TP-LINK 动态域名"中创建和绑定 WAN 口。



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。

3.2 如何设置自动重启?

3.2.1 应用介绍

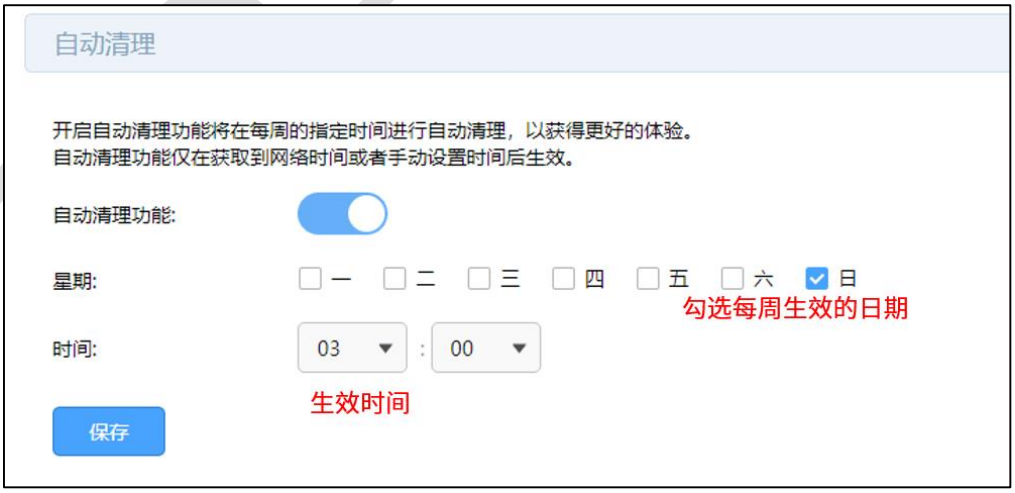
路由器长时间工作时，可能会出现路由器系统开销过大从而引起网络异常，就像电脑一样，长时间一直在工作可能会出现系统响应越来越慢，此时重启一下就好了。但由于路由器放置或其它因素，不方便手动重启。此时通过企业路由器的"自动清理"功能实现在指定时间段内让路由器自动重启。

3.2.2 需求介绍

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"，设置开启自动清理，设置自动重启的时间，点击<保存>，添加规则如下：



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。

3.2.4 注意事项

- 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。

第4章 负载均衡

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

进入路由器，点击“基本设置 >> WAN 设置 >> 流量均衡”，根据实际情况选择连接均衡或者宽带均衡并保存即可。如果设置带宽均衡，需提前在各 WAN 口中设置对应的上下行带宽为各 WAN 口实际的带宽值。

至此，负载均衡功能设置完成， 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

某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线路。

5.1.2 需求介绍

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 Internet，无法访问企业内部专网；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

第一步、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。

第二步、设置策略路由

登录到路由器界面，点击“高级功能 >> 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：

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。

5.1.4 疑问解答

Q1：什么情况下才需要设置策略路由呢?

简单讲，策略路由就是给流量找正确的出路。多条宽带的线路中，如果某条宽带连接的是公司专网，该网络和 Internet 之间不可以互通，所以上网数据从该网络转发出去会导致访问失败。设置策略路由需要同时满足两个条件：一是多个出接口（包括 VPN 等虚拟出接口）；二是不同接口连接的网络类型不同（部分为 Internet、部分为内网）。

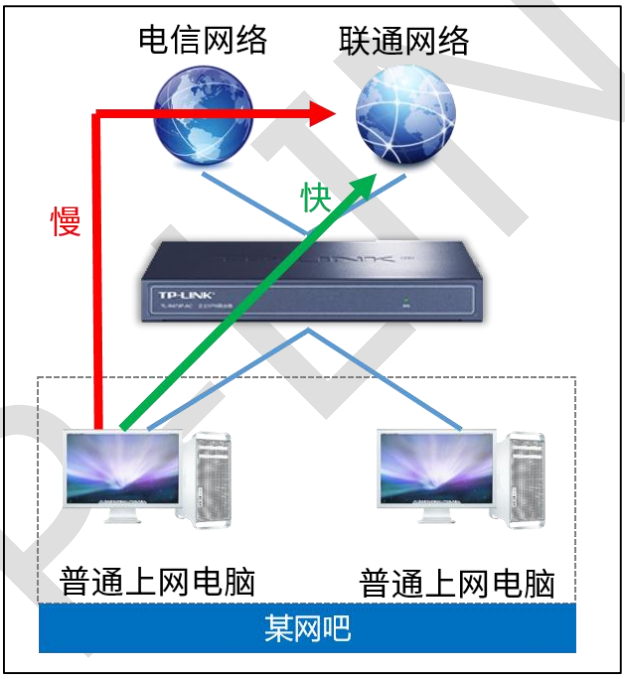
Q2：设置策略路由后，访问专网或上网还是有问题，怎么办?

遇到该问题，需要检查确认以下三点：路由器单独连接该网络的时候，确认局域网可以正常访问该网络；确认规则设置正确 (比如生效接口、目的地址等)，WAN 口状态均显示在线。

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。



5.2.2 需求介绍

某企业使用 R 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

第一步、设置 WAN 口

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。

第二步、设置 ISP 选路

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。 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。

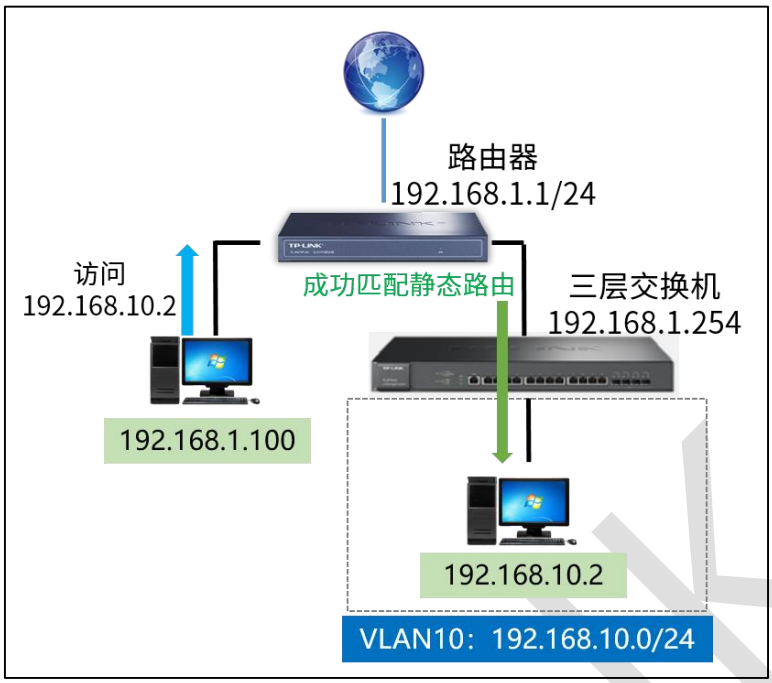
5.3 静态路由设置指南

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。

5.3.2 需求介绍

某企业使用 R 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 网段的终端进行互访。



5.3.3 设置方法

登录到路由器界面，点击“高级功能 >> 路由设置 >> 静态路由”，点击<新增>，进行设置。

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 网段的终端进行互访了。

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。

5.4.2 需求介绍

某企业接了两条外网线路，WAN1 口接运营商专线，WAN2 口接运营商普通宽带。需要实现当专线正常时所有数据都走专线线路，当专线故障时数据才走普通宽带线路。

5.4.3 设置方法

R 系列路由器没有单独的线路备份功能，不过可以通过设置策略路由的方式实现相同的效果。

在路由器界面，点击“高级功能 >> 路由设置 >> 策略路由”。

（1）设置规则：访问所有外网数据都从 WAN1 口转发，且当 WAN1 口不在线时，规则不生效，如下图：

(2) 再设置一条规则，用于第一条规则不生效时，访问外网的数据从 WAN2 口转发，如下图:

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。

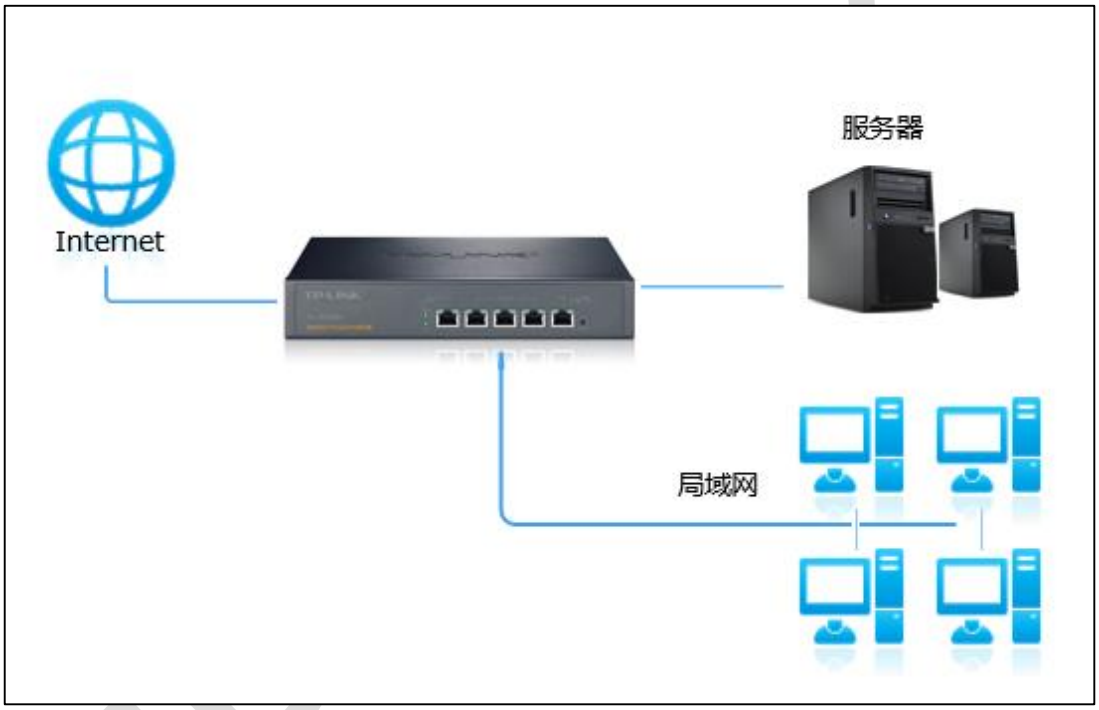
5.4.4 注意事项

- 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。
- 大多数应用程序和服务器建立的是一对一的连接，如果主线路故障，连接就会断开。然后需要重新在备用线路建立连接。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。



5.5.2 需求介绍

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

外部端口是指外网用户访问服务器使用的端口，内部端口是指内部服务器开放的服务端口。

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

第一步、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

第二步、添加虚拟服务器规则

登录路由器的管理界面，点击“高级功能 >> 虚拟服务器”，点击<新增>，添加如下映射规则，并点击<确定>。

说明：

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。

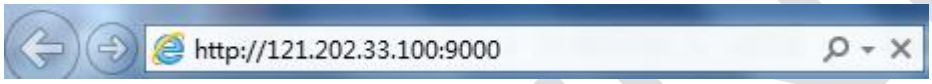
添加之后的条目如下：

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	WEB服务器	WAN1	9000	80	192.168.1.10	ALL	已启用	

至此，虚拟服务器规则设置完成。

第三步、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：



注意：具体的访问形式以实际服务器要求为准。

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。

5.5.4 疑问解答

Q1：设置虚拟服务器后外网无法访问怎么办？

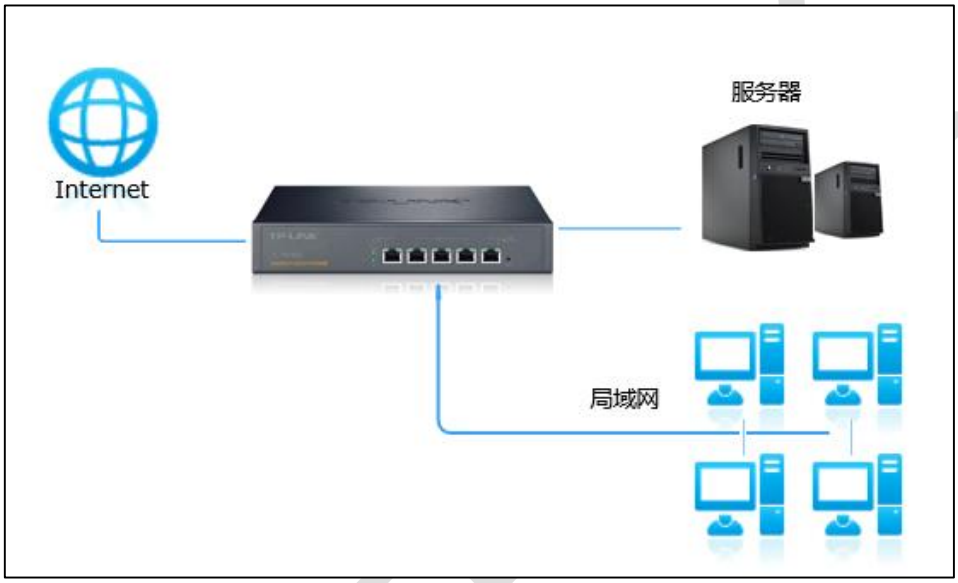
检查路由器映射条目设置正确，但是外网 telnet 服务器端口不通时，可以尝试关闭电脑所有的防火墙和杀毒软件后，再测试能否访问服务器。

如果电脑需要开启杀毒软件，需要在防火墙或者杀毒软件中开放相应的端口。例如卡巴斯基软件：在反黑客/包过滤规则--添加本地 IP 端口即可访问成功。

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。



5.6.2 需求介绍

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

第一步、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

第二步、添加 NAT-DMZ 规则

登录路由器的管理界面，点击“高级功能 >> 虚拟服务器 >> NAT-DMZ”，点击<新增>，添加如下规则，并点击<确定>。

说明：

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。

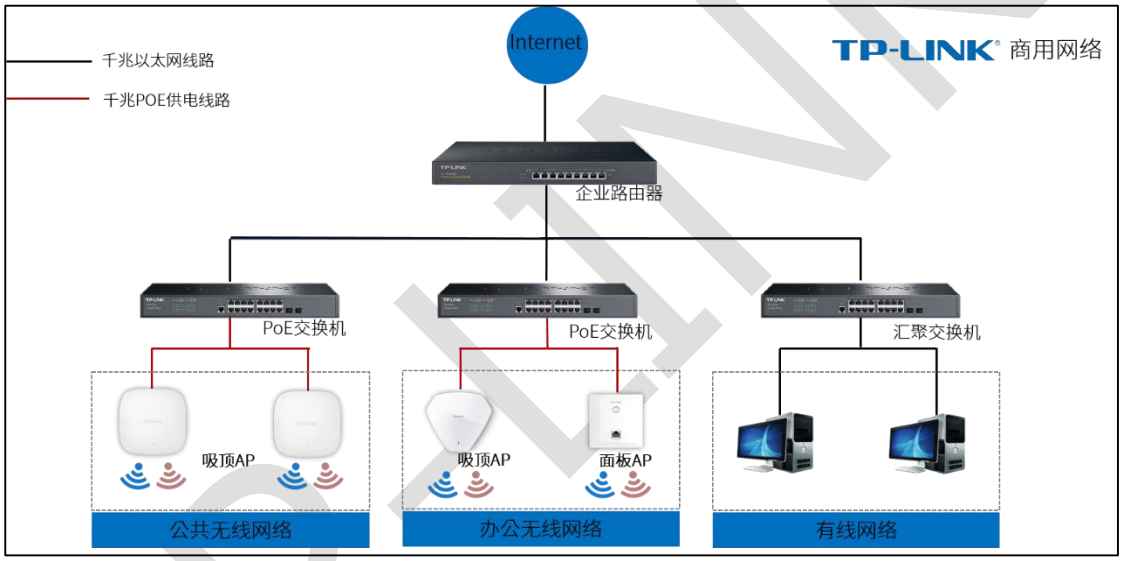
至此，NAT-DMZ 设置完成，终端在内外网都可以使用协议默认的端口进行访问。

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

R 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 R 系列新平台路由器 AP 管理功能的配置方法。



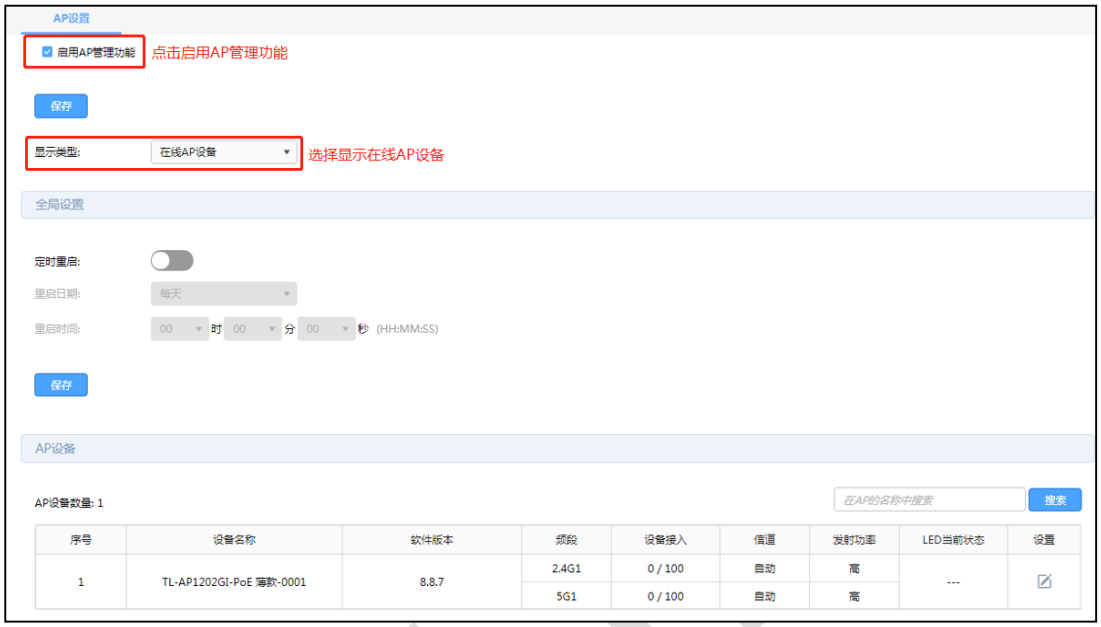
6.1.2 需求介绍

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

第一步、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”，显示类型选择为“在线 AP 设备”，列表中将会显示当前在线的 AP，确认路由器已经发现 AP，并可以对 AP 进行管理。



说明：

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。

第二步、设置 AP 的无线网络

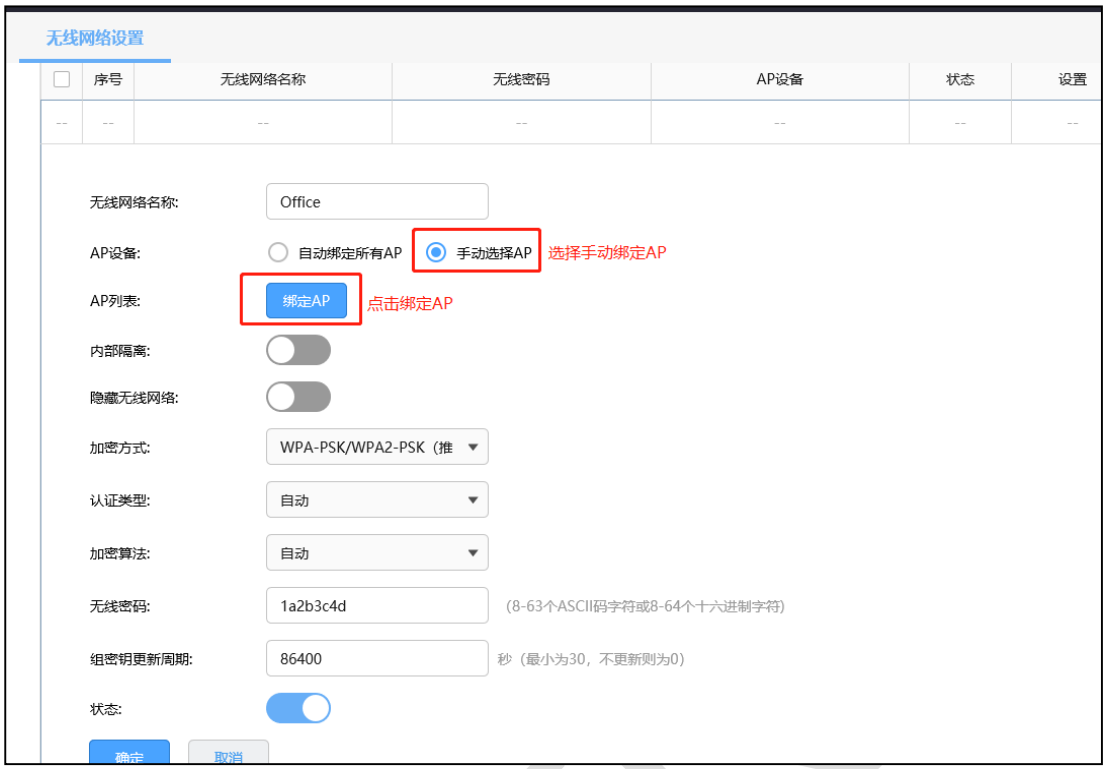
点击“AP 管理 >> 无线网络设置”，点击<新增>，设置员工无线网络，如下图：

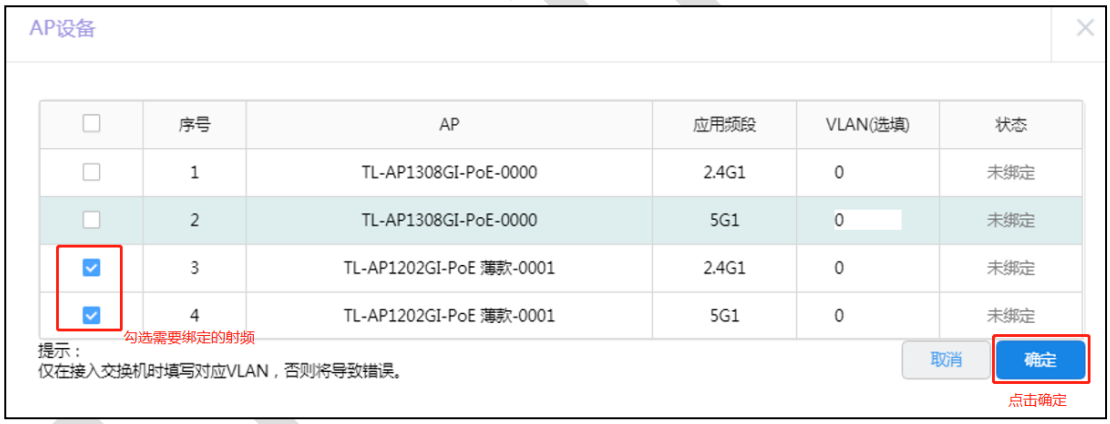
说明：

如果您新建的无线网络名称是绑定需要绑定到所有 AP，请选择“自动绑定所有 AP”的选项，则接入的所有 AP 都将自动绑定该无线网络，也就不需要进行下面第三步的操作；如果您新建的无线网络名称是只绑定部分 AP，请选择“手动选择 AP”的选项，并进行下面的第三步的 AP 绑定操作。如果您的无线网络中无线连接的客户端设备之间没有通过局域网互相访问的需求，建议开启“内部隔离”选项，可以提高无线网络稳定性；如果有互相访问的需求，建议关闭“内部隔离”选项。

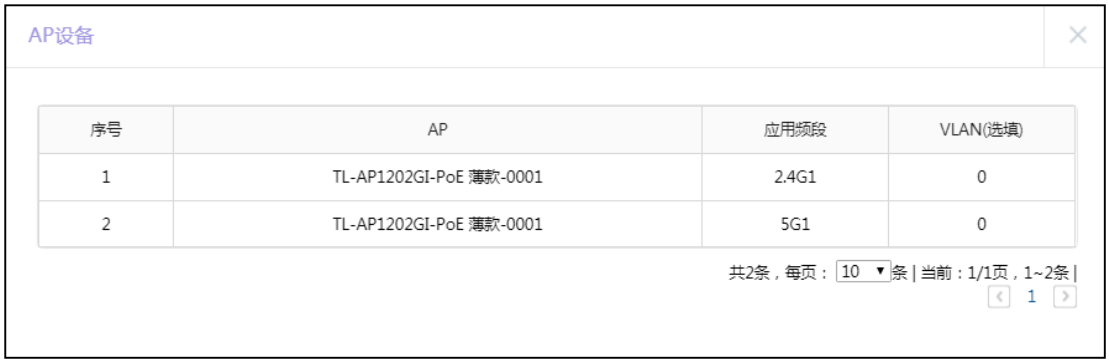
第三步、射频绑定

如果设置无线服务为<手动选择 AP>，可点击<绑定 AP>，然后勾选需要绑定的 AP 以及射频即可，如下图：





勾选需要绑定的 AP 和射频，点击<确定>即可。绑定完成后，点击"显示全部"可看到所有已绑定的 AP。



第四步、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 >> 射频调优”，进行 AP 频段带宽和信道调整，点击<立即调优>即可：

可选择启用功率调优和定时调优功能，参数可根据实际情况进行调整；

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

至此，R 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 需求介绍

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。

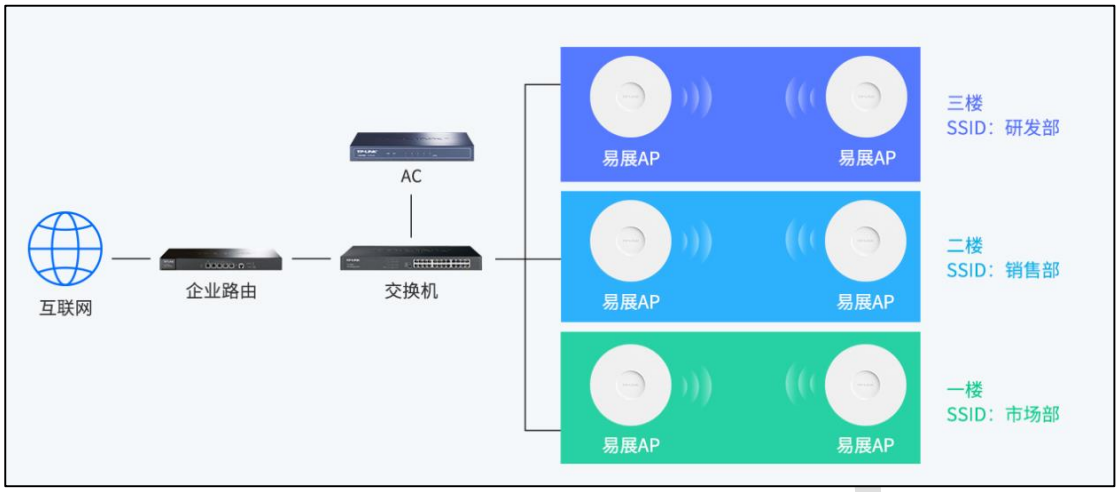
组网特点：

（1）不方便布线；

（2）不想破坏办公环境；

（3）有临时增加网络位点的需求；

（4）需要对设备统一管理，方便维护。



6.2.3 设置方法

第一步、配对方法介绍

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 R 系列路由器，易展 AP 将自动识别并工作在 FIT 模式；同时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。

说明：

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

第二步、易展 AP 的 FIT 模式使用方法介绍

（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”。

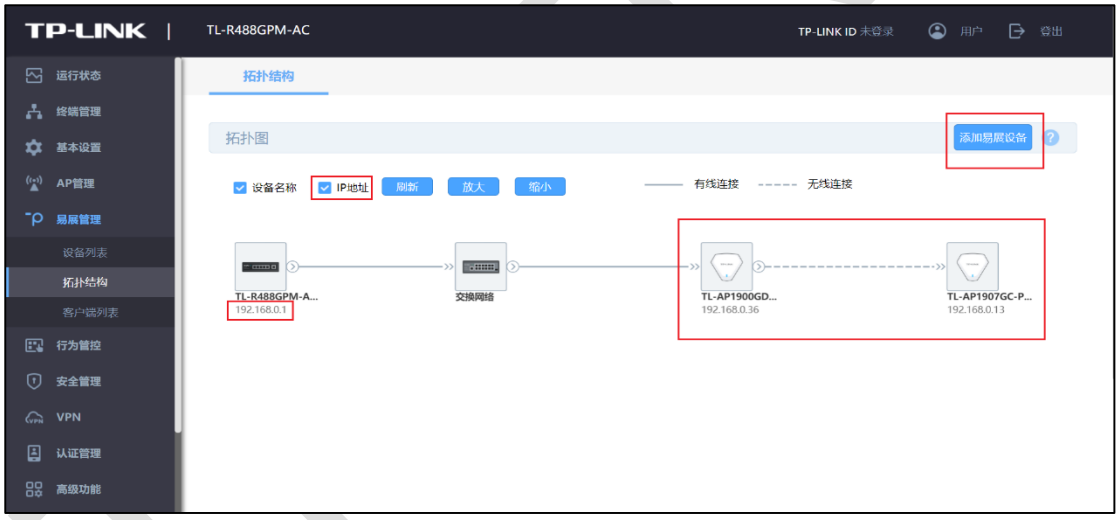
首先是主子 AP 的列表页面，可以在此页面对主子设备做相应的操作。

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。

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。

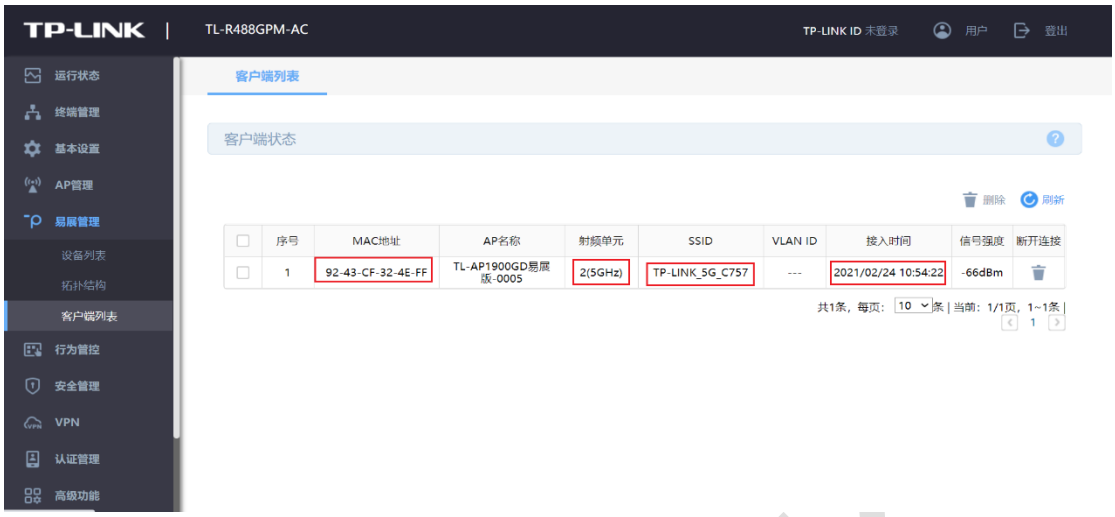
（2）拓扑结构

能够显示设备的网络拓扑，型号（名称）、IP 地址等参数。



（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，信号强度等信息。



以上就是易展 AP 的 FIT 模式使用方法及配置方式。

6.2.4 注意事项

- 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 需求介绍

某公司网关路由器使用 R 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“行为管控 >> 连接数限制”， 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 访问控制设置指南

7.2.1 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。

7.2.2 需求介绍

某企业使用 R 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：

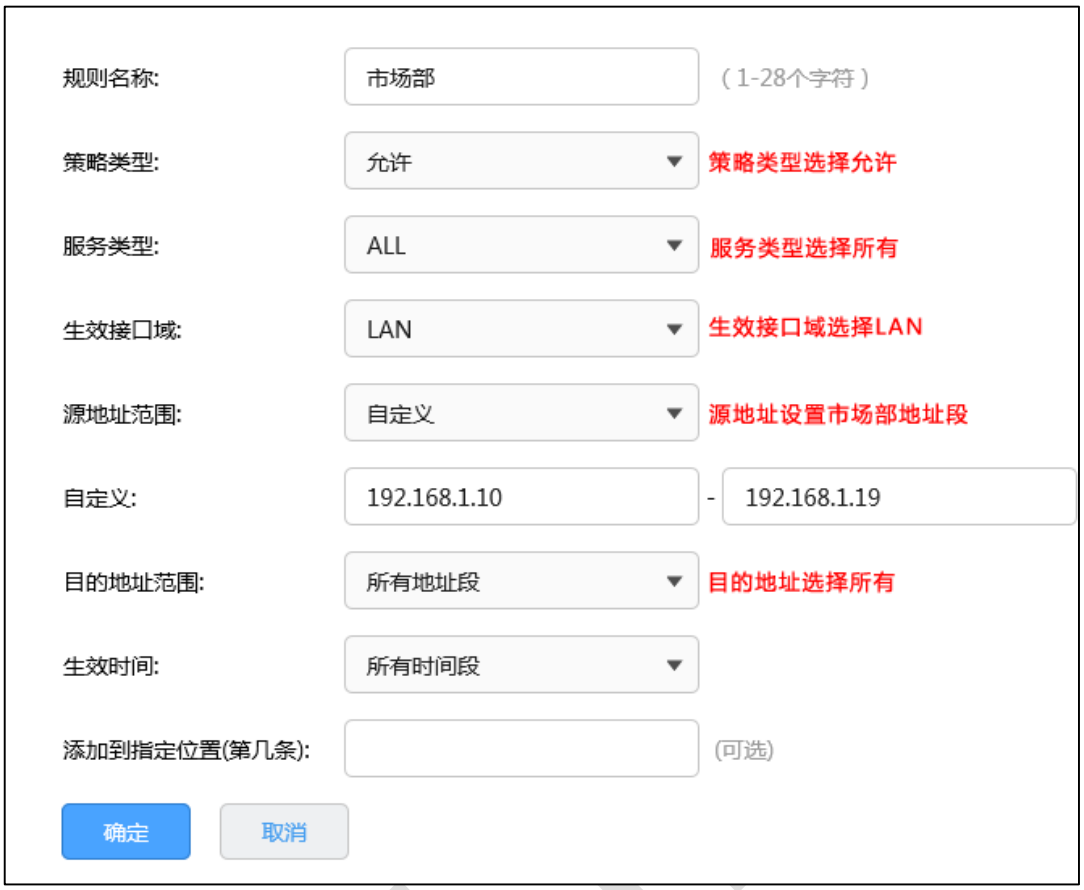
部门	允许的上网行为
市场部	所有网络应用
其它部门	浏览网页

注意：上述参数仅供参考，具体以实际应用为准。

7.2.3 设置方法

第一步、设置市场部的访问控制规则

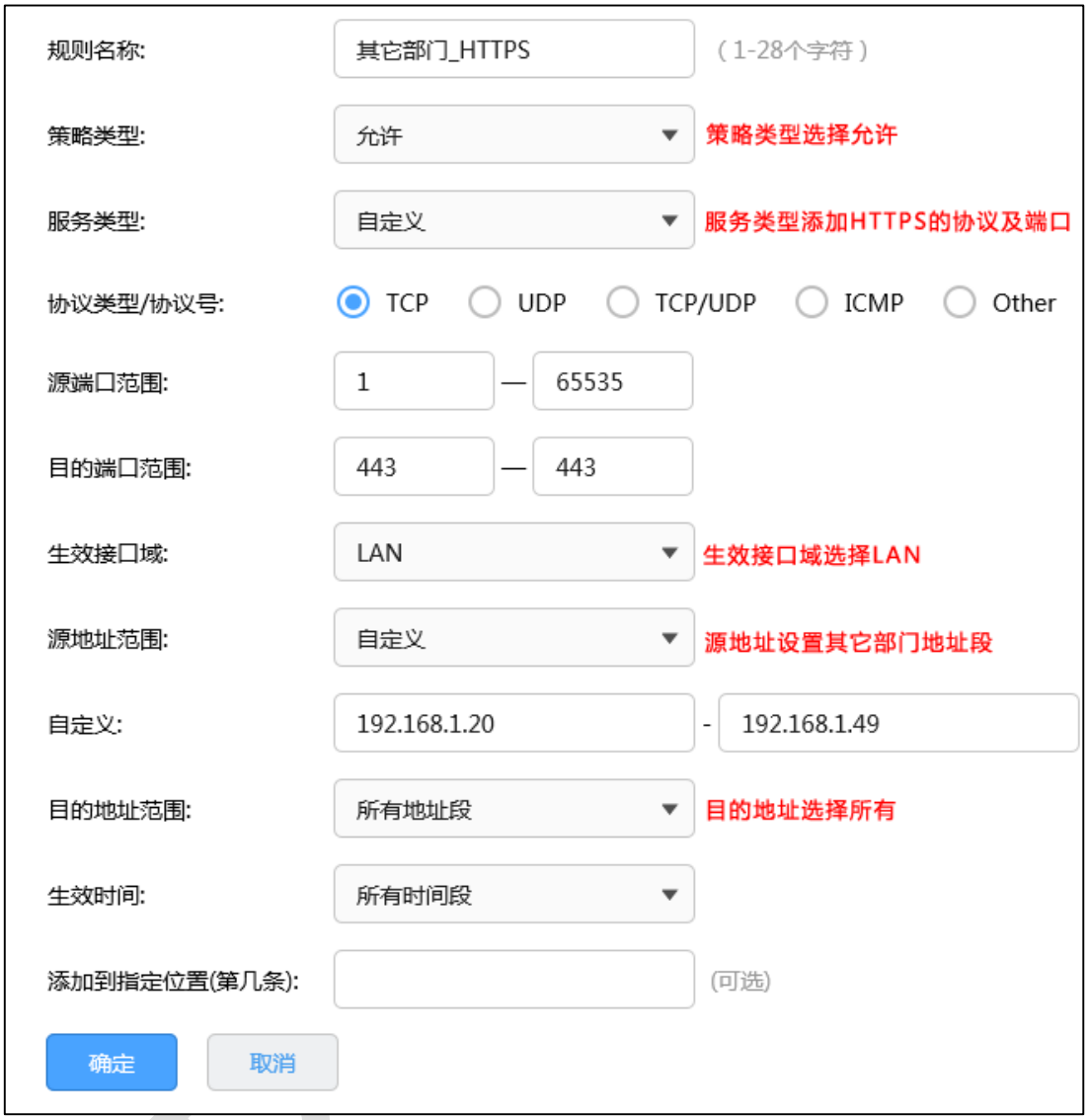
点击“行为管控 >> 访问控制”，点击<新增>，添加策略规则：允许市场部访问所有网络应用，如下图所示：

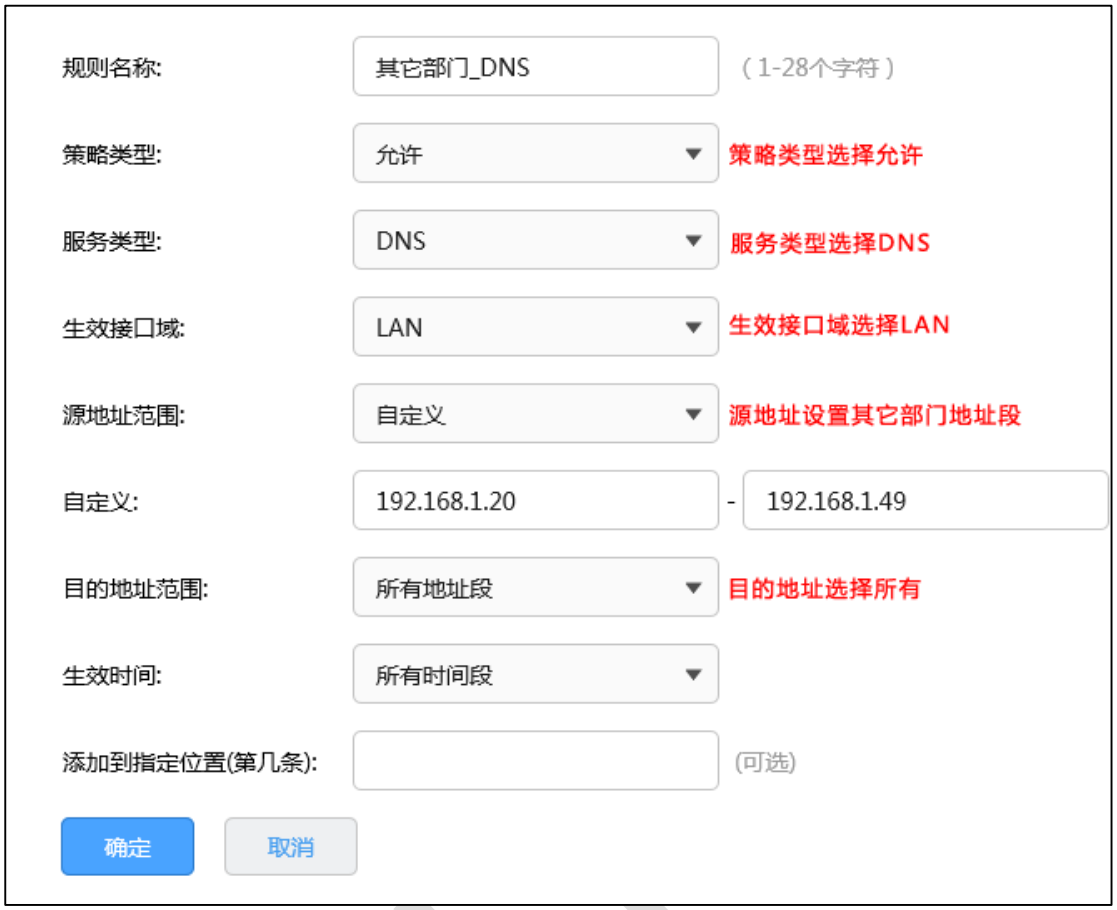


第二步、设置其它部门的访问控制规则

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：


规则名称:
其它部门_HTTP
(1-28个字符)
策略类型:
允许
策略类型选择允许
服务类型:
HTTP
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:
自定义
源地址设置其它部门地址段
自定义:
192.168.1.20
-
192.168.1.49
目的地址范围:
所有地址段
目的地址选择所有
生效时间:
所有时间段
添加到指定位置(第几条):
(可选)
确定
取消

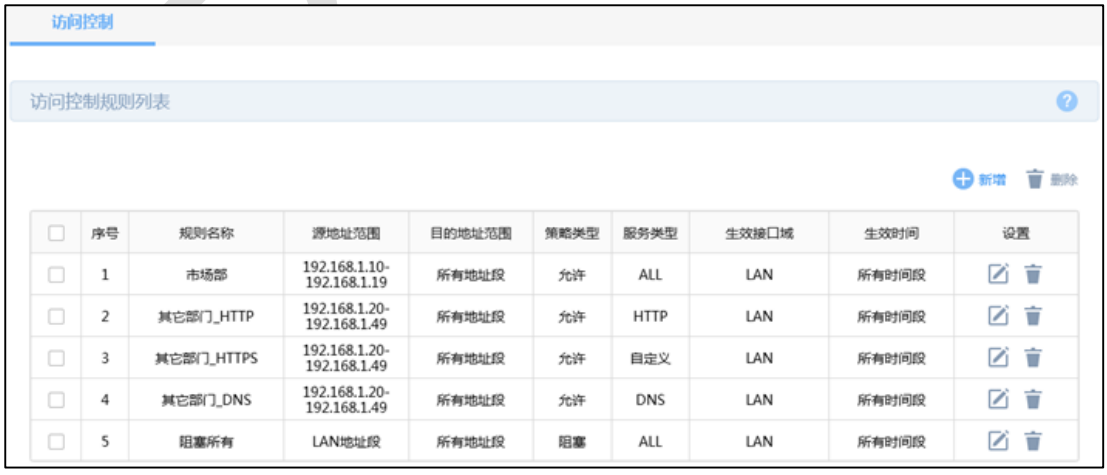

规则名称:
其它部门_HTTPS
（1-28个字符）
策略类型:
允许
策略类型选择允许
服务类型:
自定义
服务类型添加HTTPS的协议及端口
协议类型/协议号:
TCP
UDP
TCP/UDP
ICMP
Other
源端口范围:
1
—
65535
目的端口范围:
443
—
443
生效接口域:
LAN
生效接口域选择LAN
源地址范围:
自定义
源地址设置其它部门地址段
自定义:
192.168.1.20
-
192.168.1.49
目的地址范围:
所有地址段
目的地址选择所有
生效时间:
所有时间段
添加到指定位置(第几条):
(可选)
确定
取消



第三步、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：

添加完成后，规则列表如下：



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。

7.2.4 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。

Q2：如何在服务类型中添加新的服务？

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“服务类型”的下拉窗口中选择“自定义”，并进行相关设置。如下图：

7.3 应用限制设置指南

7.3.1 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。

7.3.2 需求介绍

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）；

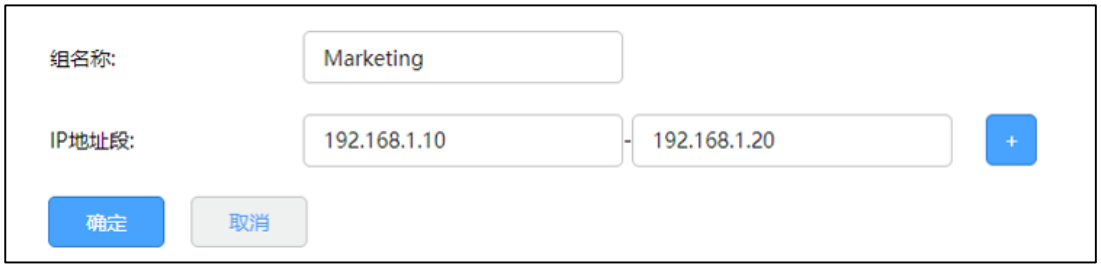
2、允许市场部员工登录 12345678，987654321 这两个 QQ 号码；

3、其它部门不做限制。

7.3.3 设置方法

第一步、添加市场部地址组

为了方便灵活管理 IP 地址，可以先建立地址组。在路由器界面，点击“对象管理 >> 地址管理 >> 地址”，点击<新增>，添加市场部地址组。

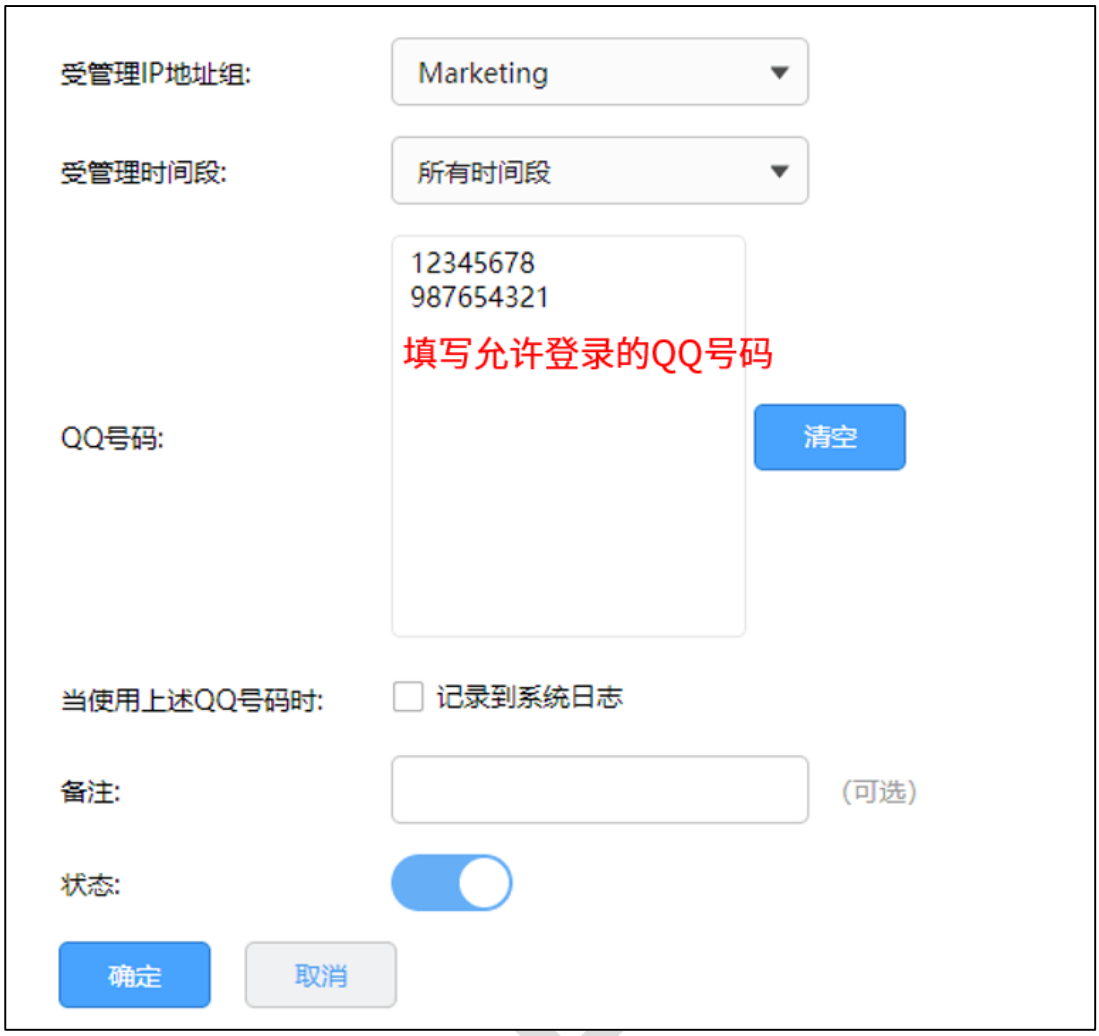


第二步、设置应用控制规则

点击“行为管控 >> 应用控制”，点击<新增>，为市场部设置如下规则：

第三步、设置 QQ 白名单

点击“行为管控 >> 应用控制 >> QQ 白名单”，点击<新增>，设置允许市场部登录如下 QQ。



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。

7.4 网址过滤设置指南

7.4.1 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。企业路由器的网址过滤功能可以实现对不同地址组的网页访问权限设置，从而实现合理管控网络权限。

7.4.2 需求介绍

某企业需要限制公司不同部门的网络权限，需求如下：

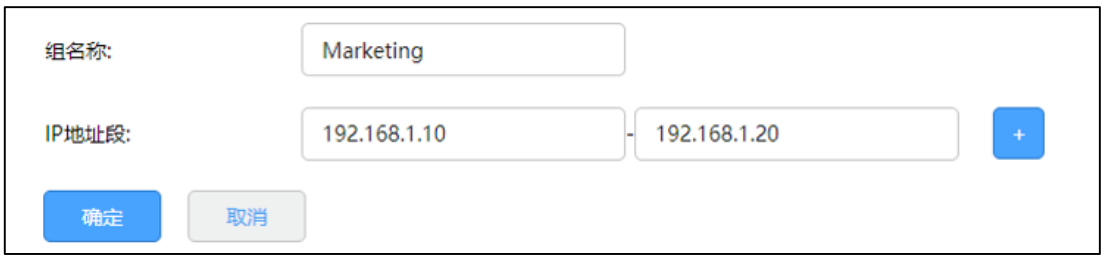
部门	网络权限
市场部	禁止访问视频、游戏、购物类网站
其他部门	仅允许访问公司网站及百度

注意：上述参数仅供参考，具体以实际应用为准。

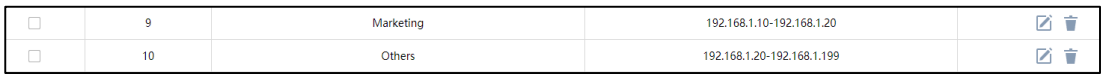
7.4.3 设置方法

第一步、添加地址组

添加市场部和其他部门的地址组，方便后续的控制规则针对地址组进行控制。在路由器界面，点击“行为管控 >> 地址管理”，点击<新增>，添加市场部地址组。



同样的方法添加其他部门的地址组，添加完成的地址组如下：



第二步、添加网站分组

点击“行为管控 >> 网站访问 >> 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：

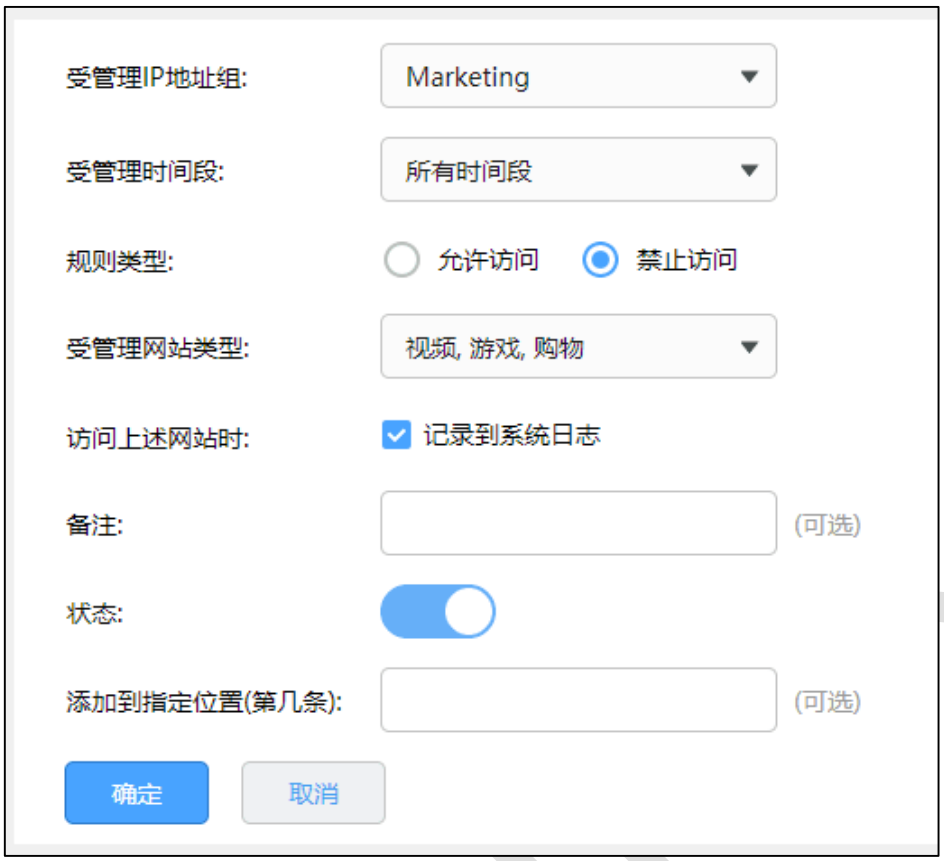
说明：

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。

第三步、设置网站访问规则

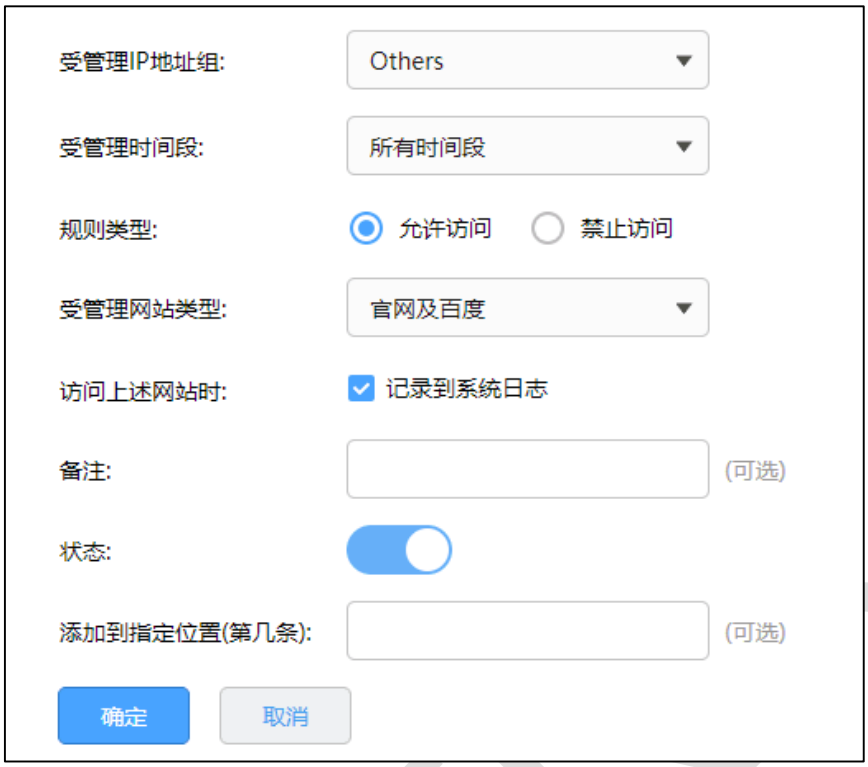
添加市场部规则

在“行为管控 >> 网站访问 >> 网站访问”，点击<新增>，添加市场部的过滤规则，即禁止市场部访问视频、游戏、购物类的网站，如下图：



添加其他部门的规则

在“行为管控 >> 网站访问 >> 网站访问”，点击<新增>，添加允许其他部门访问官网及百度，如下图：



再点击<新增>，添加禁止其他部门访问所有网站，如下图：

设置完成，可以查看到网站访问的列表如下：

序号	受管理IP地址组	规则类型	受管理网站类型	受管理时间段	状态	备注	设置
1	Marketing	禁止访问	视频,游戏,购物	所有时间段	已启用	---	
2	Others	允许访问	官网及百度	所有时间段	已启用	---	
3	Others	禁止访问	所有网站	所有时间段	已启用	---	

至此，网站访问功能设置完成，企业所有部门员工将按照设置的规则来上网。

7.4.4 疑问解答

Q1：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。

Q2：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 或 sohu，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。主流域名如嵌套如下：

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

7.5 网页安全设置指南

7.5.1 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。

7.5.2 需求介绍

某企业网络环境中，为了确保内部网络安全，需求如下：

1、禁止企业内部人员对网页内容的上传和网站、论坛等用户名密码的登录；

2、禁止企业内部人员从网页上下载 exe，rar 后缀的文件。

7.5.3 设置方法

登录路由器的管理界面，点击“行为管控 >> 网页安全”，选择相应的地址组，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：

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

备注：网页安全功能目前仅对采用 HTTP 协议的上传和下载生效。

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。

8.1.2 需求介绍

某企业希望通过路由器的设置来防范内网发生 ARP 欺骗问题而导致终端无法上网，影响企业正常办公。

8.1.3 设置方法

第一步、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	192.168.1.100	50-E5-49-1E-91-F3	办公
.....	..	..	..

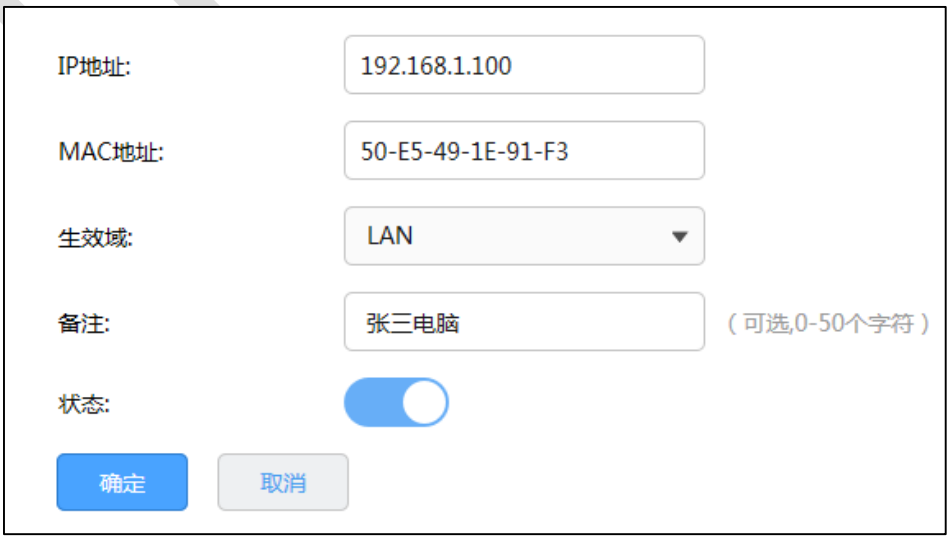
注意：以上表格仅供参考，具体信息请根据实际需要记录。

第二步、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：

手动添加方法介绍：

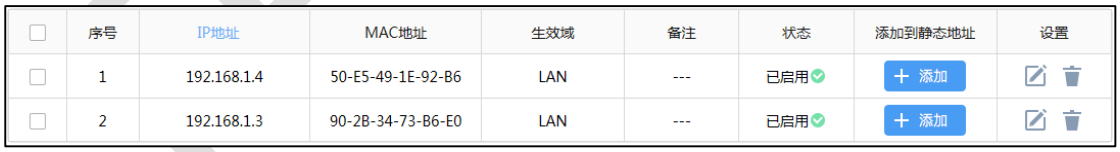
手动添加操作复杂，但是安全性高。在网络中已经存在 ARP 欺骗或者不确定网络中是否存在 ARP 欺骗的情况下，建议使用手动添加的方式。手工进行添加，先点击<新增>，填写需要绑定的电脑的 IP 和 MAC 地址，选择生效域，填写备注信息，并点击<确定>。如下图所示：



扫描添加方法介绍：

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：

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。



说明：

- 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）。
- 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。

第三步、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 >> ARP 防护”中，确认已勾选“启用 ARP 防欺骗功能”，点击<保存>。如下图所示：

说明：

如果勾选“禁止非 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，防止 ARP 欺骗设置完成。

第四步、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：

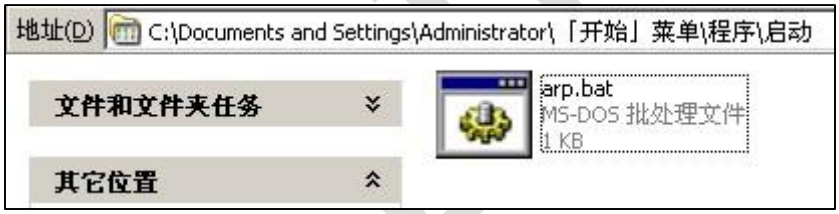
Windows XP 系统：

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：

说明：

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）。

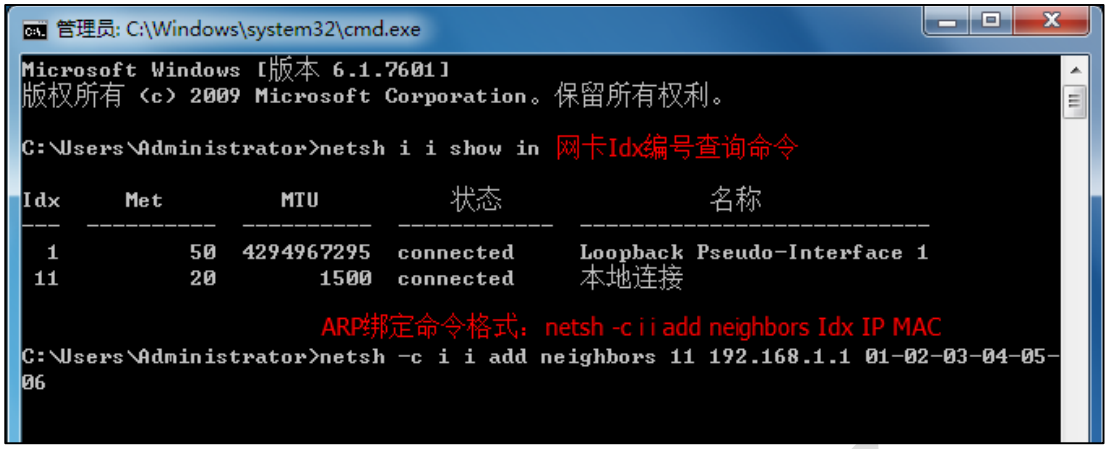
保存之后将该文件修改为.bat 后缀的批处理文件，比如“arp.bat”。然后将其放入系统启动项中，以后系统每次开机时都会执行该绑定命令。如下图所示：



Windows 7/ Windows 8/ Windows 10 系统：

（1）打开命令提示符，使用命令：“netsh i i show in”查看网卡 idx 编号；

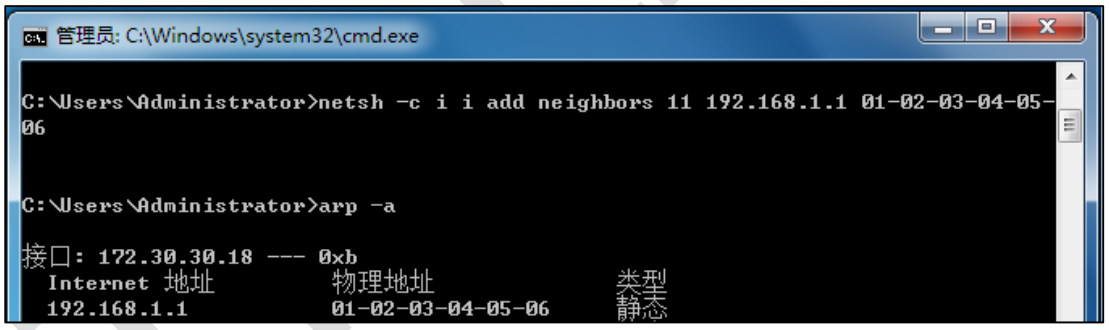
（2）查询到网卡 idx 编号后，再使用命令“ netsh –c i i add neighbors idx ip mac”进行 ARP 绑定，如下图所示：



说明：

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。

（3）使用 arp –a 的命令可以查询到绑定是否生效，如下图所示：



设置完成后，电脑重启，ARP 绑定条目也不会失效。

说明：

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。

8.1.4 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。

8.2.2 需求介绍

某企业希望通过路由器的设置来实现仅允许某些电脑接入网络，防止不被允许的电脑接入企业的网络进行通信。

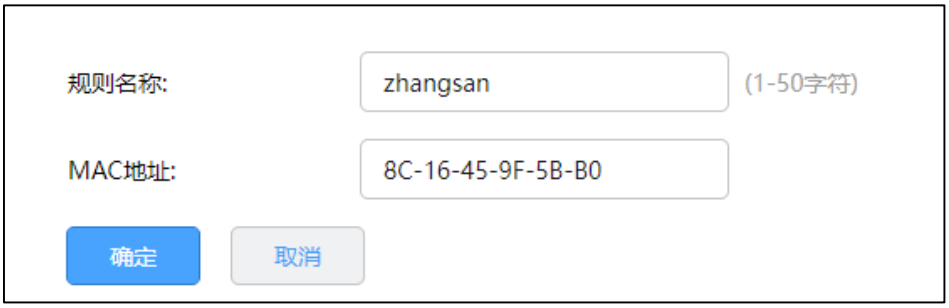
8.2.3 设置方法

第一步、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，此处选择"白名单"，表示仅允许规则列表中的设备访问外网，点击<保存>。

第二步、添加 MAC 地址

在第一步的界面中，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。

说明：

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。那么需要将第一步中的规则类型选择为“黑名单（不允许设备访问外网）”。

第9章 VPN 模块

9.1 IPSec VPN 设置指南

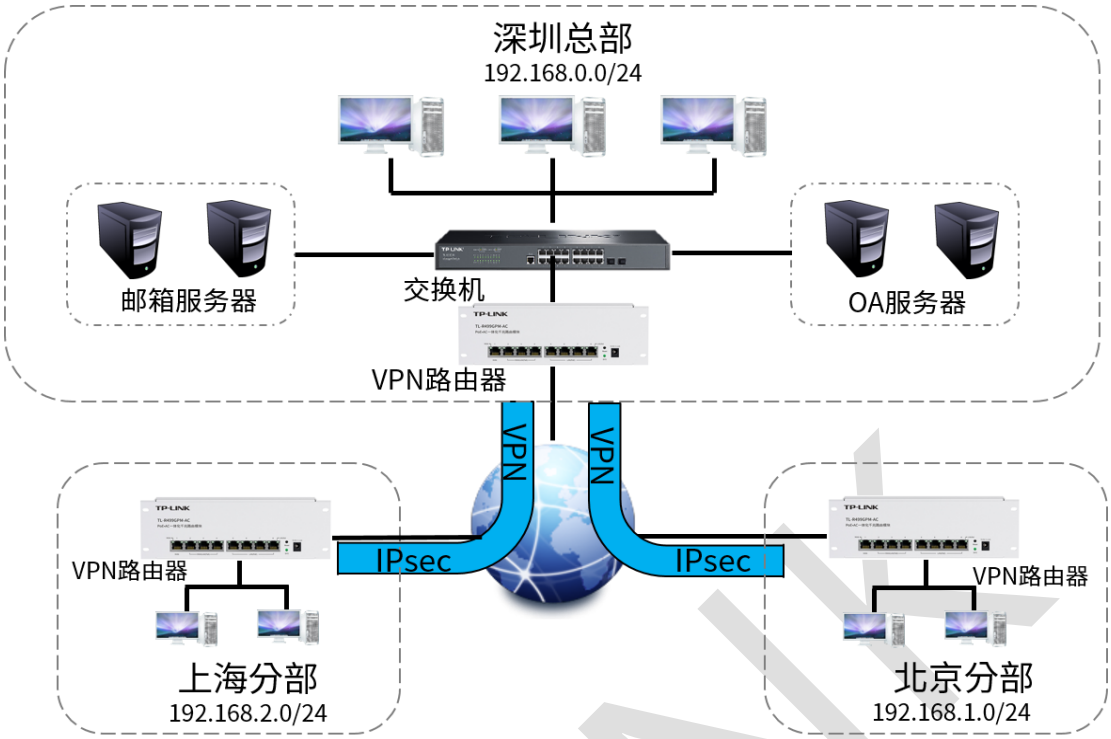
9.1.1 应用介绍

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。

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-R499GPM-AC 与 TL-R488GPM-AC 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

本节将分别介绍深圳总部 TL-R499GPM-AC 设置步骤和上海、北京分公司 TL-R488GPM-AC VPN 配置方法。

一、深圳总部 TL-R499GPM-AC 设置步骤

第一步、基本设置

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-R499GPM-AC：

（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。

说明：

- 策略名称：设置 IPSec 安全策略名称。
- 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-R488GPM-AC WAN 口 IP 地址“183.15.15.30”。
- 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。
- 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”。
- 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”。

- 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。
- 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。一般地，用户不需要配置高级设置，采用默认值即可。

说明:

阶段 1 设置：设定 IKEv1 的第一阶段的相关参数。

- 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。
- 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。
- 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。
- 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。
- 生存时间 ：用于 IKE 协商方式下 IPSec 会话密钥的生存时间。
- 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

- 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。
- 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。
- 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。

- 生存时间：用于 IKE 协商方式下 IPSec 会话密钥的生存时间。

二、上海、北京分公司 TL-R488GPM-AC VPN 配置方法

第一步、基本设置

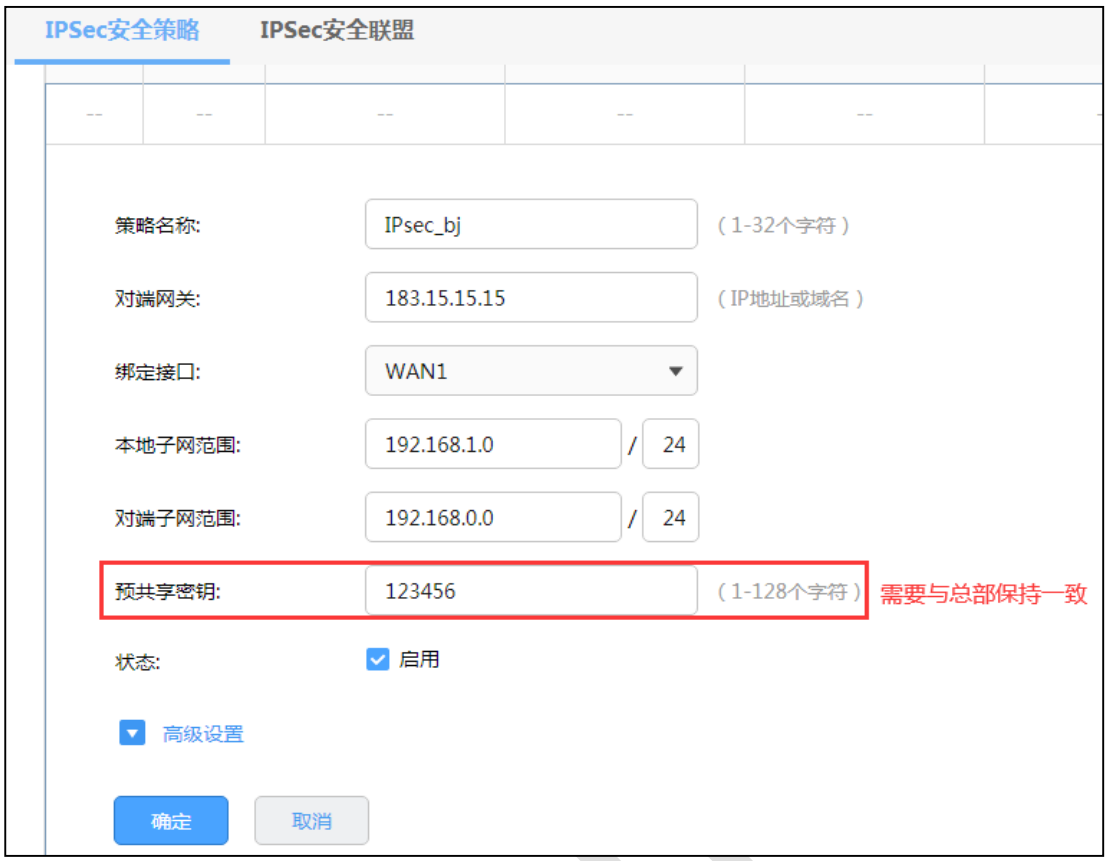
设置路由器的 WAN 口模式：网络参数 >> WAN 口设置，根据需求设置 WAN 口连接类型，此处我们设置为静态 IP：183.15.15.30。

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-R499GPM-AC，再进行配置分部 TL-R488GPM-AC：

（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-R499GPM-AC 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。

9.2 L2TP VPN 设置指南

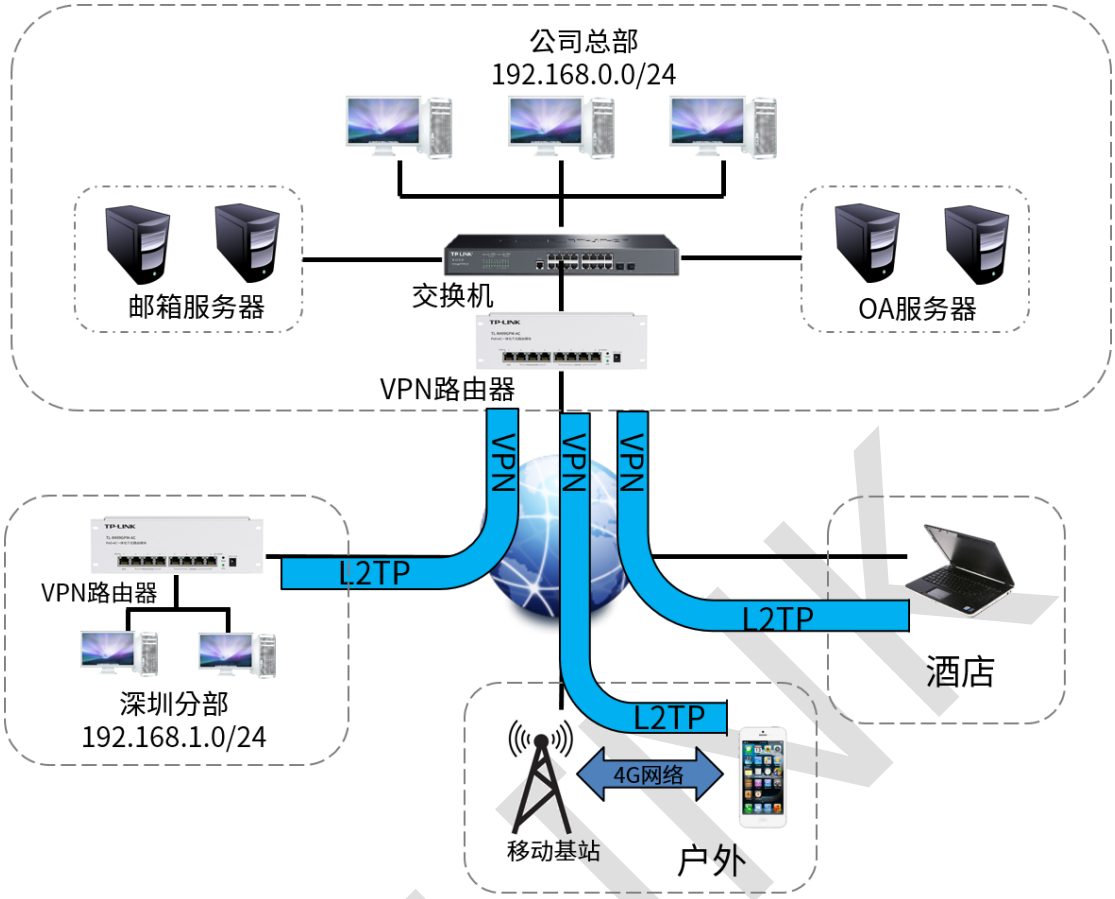
9.2.1 应用介绍

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 。

9.2.2 需求介绍

某公司的总部与分部均使用 R 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 设置方法

本节将分别介绍 L2TP VPN 站点到站点设置方法和 L2TP VPN PC 到站点设置方法。

一、L2TP 站点到站点设置方法

第一步、服务器端的设置 (以 TL-R499GPM-AC 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

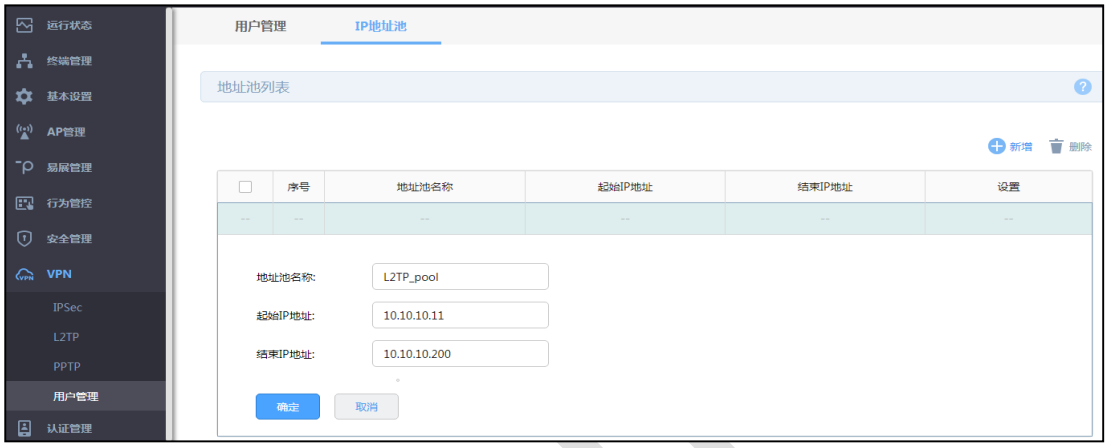
（2）WAN 口设置

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。

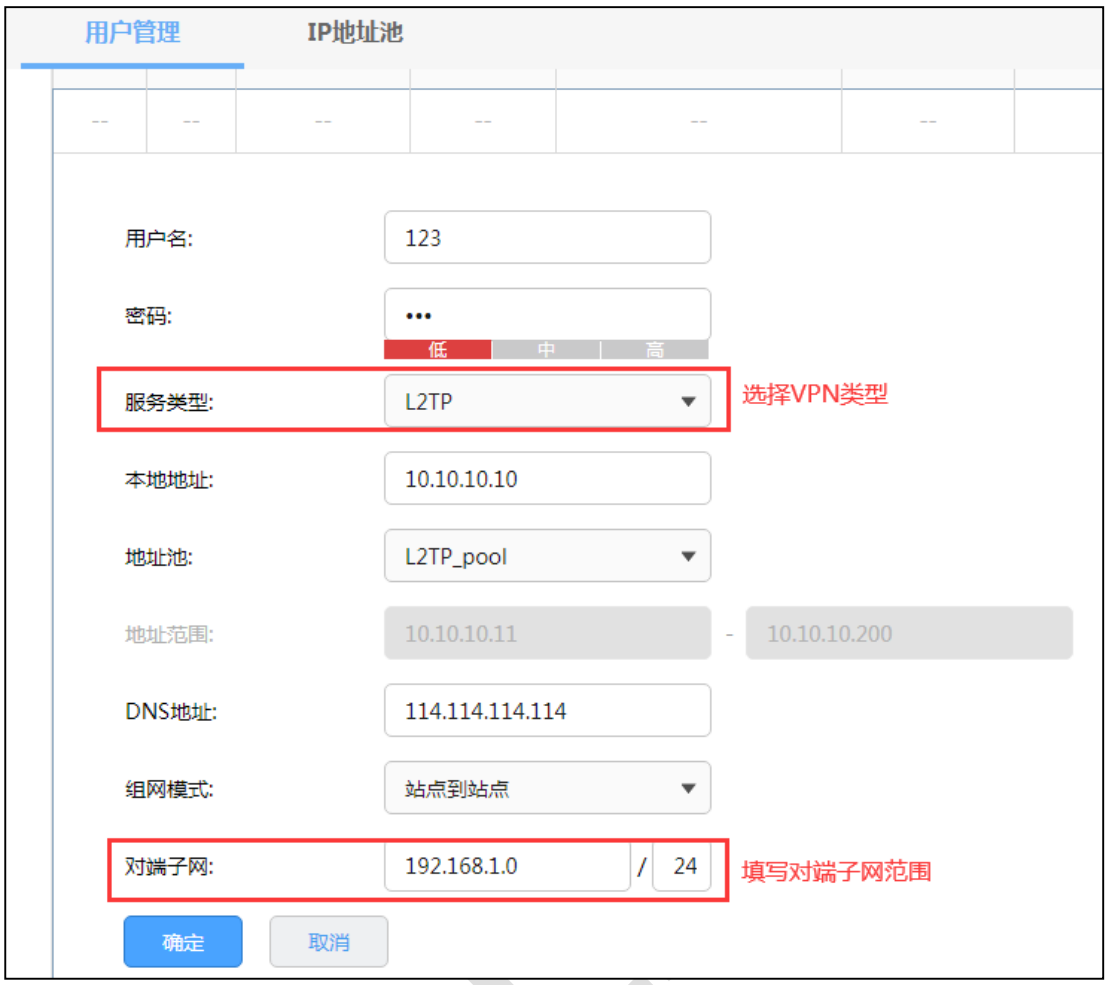
注：服务器端 WAN 口 IP 推荐为公网 IP，若非公网 IP，需要在前端设备做映射。

（3）L2TP 服务器的设置

1）打开“VPN >> 用户管理 >> 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)：



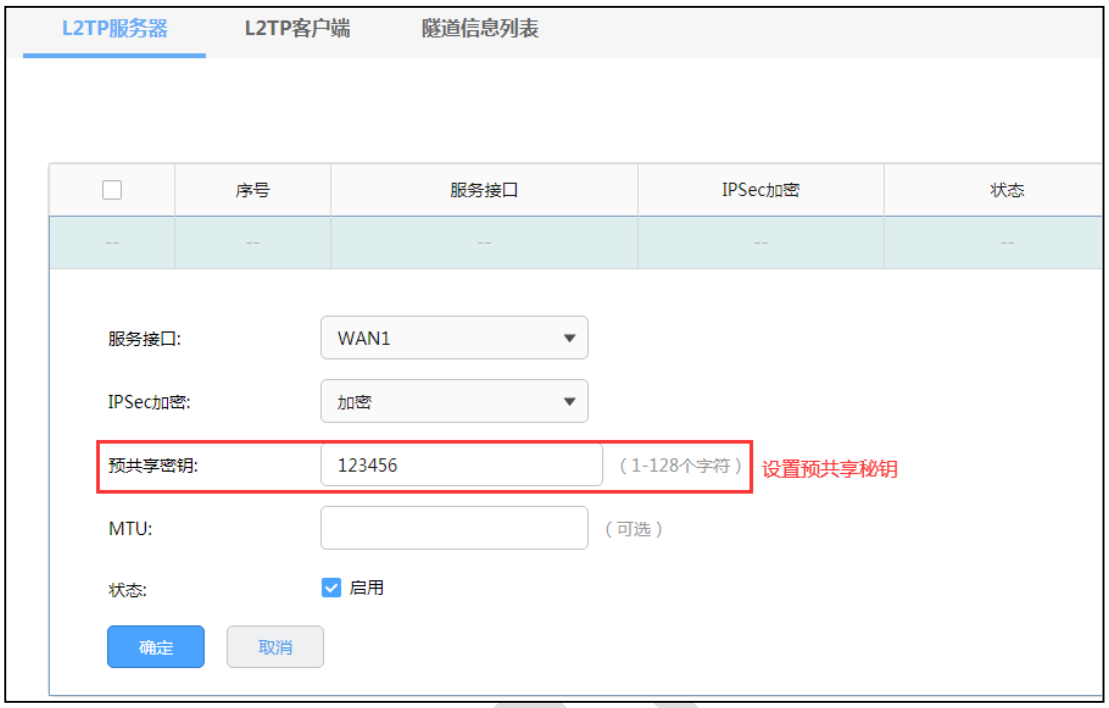
2）打开“VPN >> 用户管理”页面，进行用户管理配置，点击<新增>。



说明：

- 用户名：客户端与服务器端建立连接的用户名。
- 密码：客户端与服务器端建立连接的密码。
- 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。
- 本地地址：VPN 隧道的本地虚拟 IP 地址。
- 地址池：就是 A 步骤建立的隧道地址池，选择即可。
- 组网模式：可选择站点到站点或 PC 到站点。
- 对端子网范围：客户端 LAN 口的网段（服务器端和客户端 LAN 口地址不能在同一个网段）。
- 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）。

3）打开 “VPN >> L2TP”页面，设置 L2TP VPN 服务器:



说明：

- 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。
- IPSec 加密：是否对隧道进行加密，可选择加密、不加密、可选加密。
- 预共享秘钥：设置 IPSec 加密时的预共享密钥，VPN 两端需要保持一致。
- 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。

第二步、客户端的设置（以 TL-R488GPM-AC 为例）

（1）进入管理界面

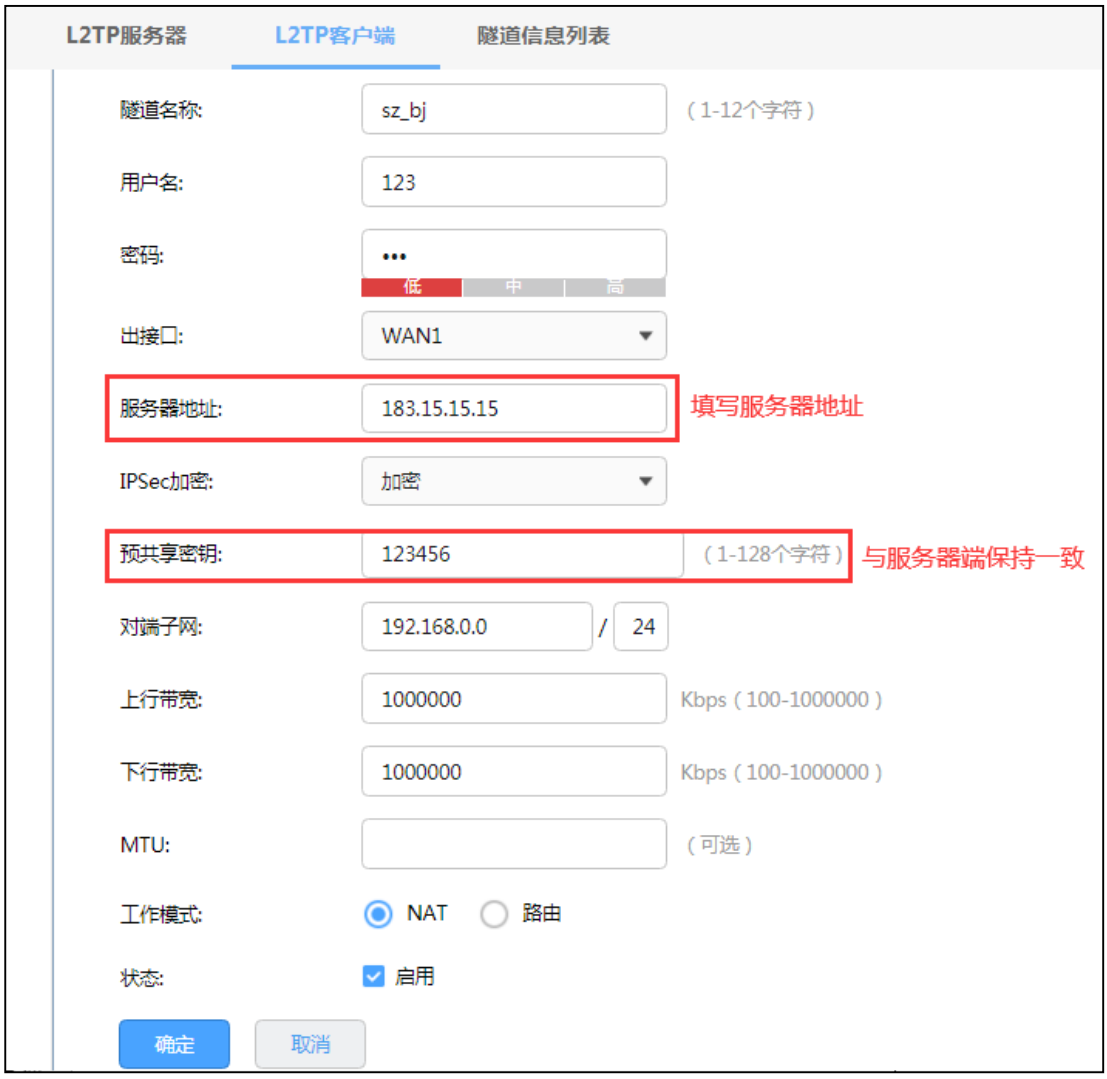
设置 LAN 口网段（与服务器端不在同一个网段），本例为 192.168.1.0/24

（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，点击<新增>，填写客户端配置信息。



说明：

- 用户名：服务器端设置的用户名。
- 密码：服务器端设置的密码。
- 出接口：选择已经设置上网的 WAN 口。

- 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）。
- IPSec 加密：选择是否加密，与服务器端设置一致。
- 预共享秘钥：选择加密时需要填写预共享秘钥，与服务器端保持一致。
- 对端子网范围：服务器端 LAN 口的网段（与本地 LAN 不同网段）。
- 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。

第三步、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/L2TP 隧道信息中将有条目：

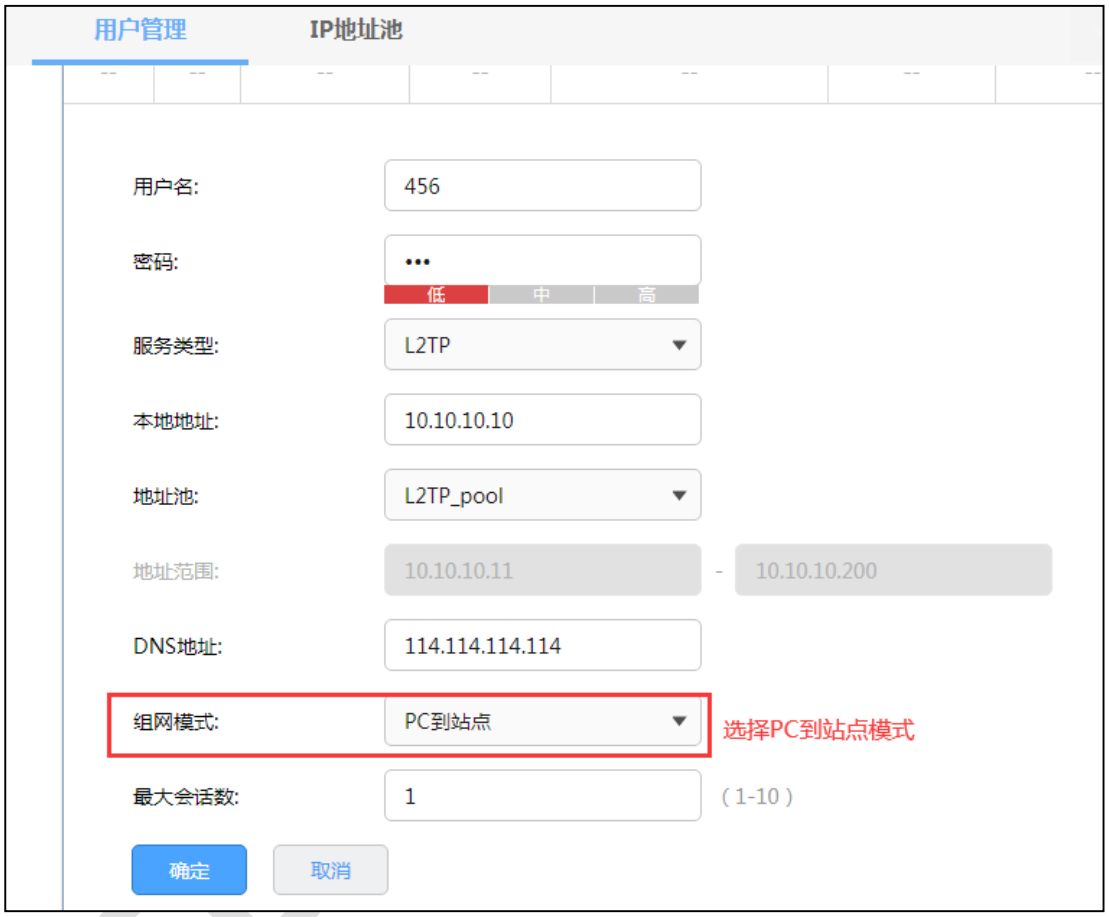
（1）服务器隧道条目：

（2）客户端条目：

二、L2TP PC 到站点设置方法

第一步、服务器端的设置（以 TL-R499GPM-AC 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：



第二步、L2TP PC 到站点客户端拨号设置

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。

第三步、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：

9.3 PPTP VPN 设置指南

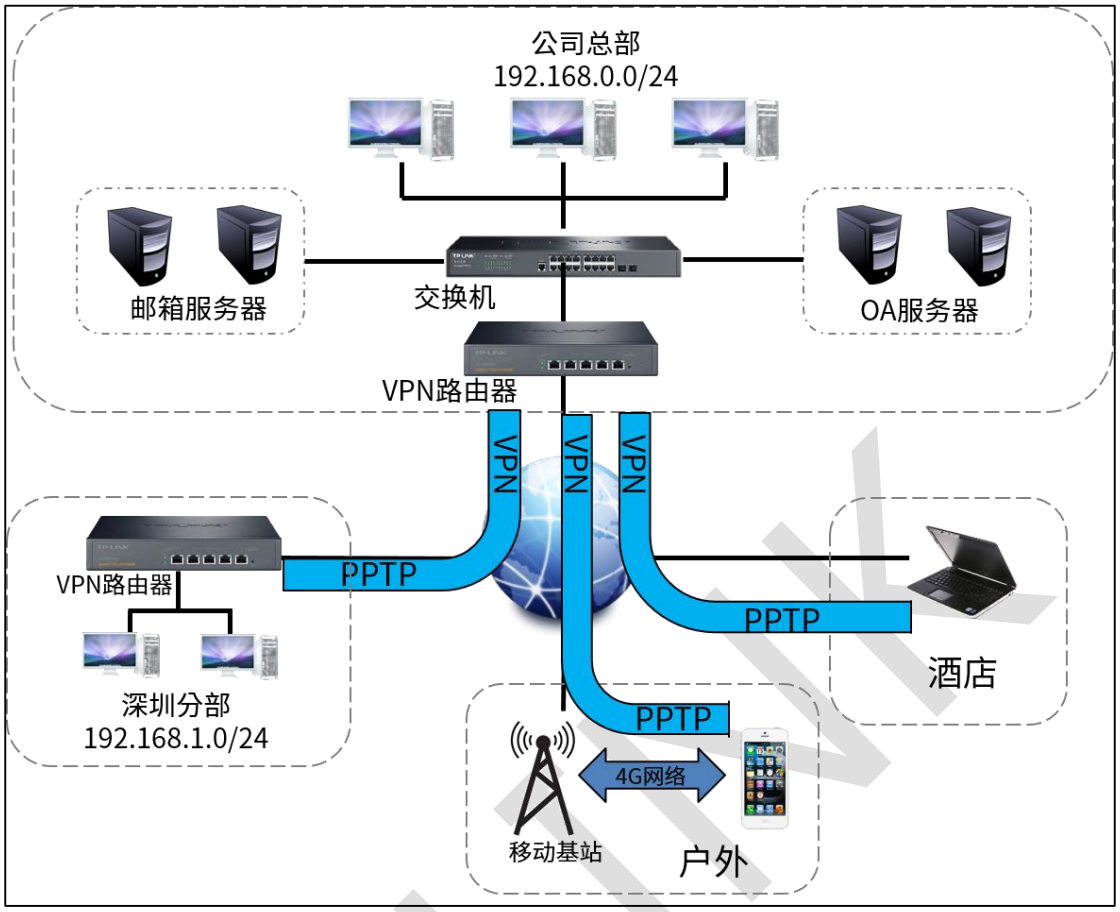
9.3.1 应用介绍

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 。

9.3.2 需求介绍

某公司的总部与分部均使用 R 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 设置方法

本节将分别介绍 PPTP VPN 站点到站点设置方法和 PPTP VPN PC 到站点设置方法。

一、PPTP 站点到站点设置方法

第一步、服务器端的设置 （以 TL-R499GPM-AC 为例）

（1）进入管理界面

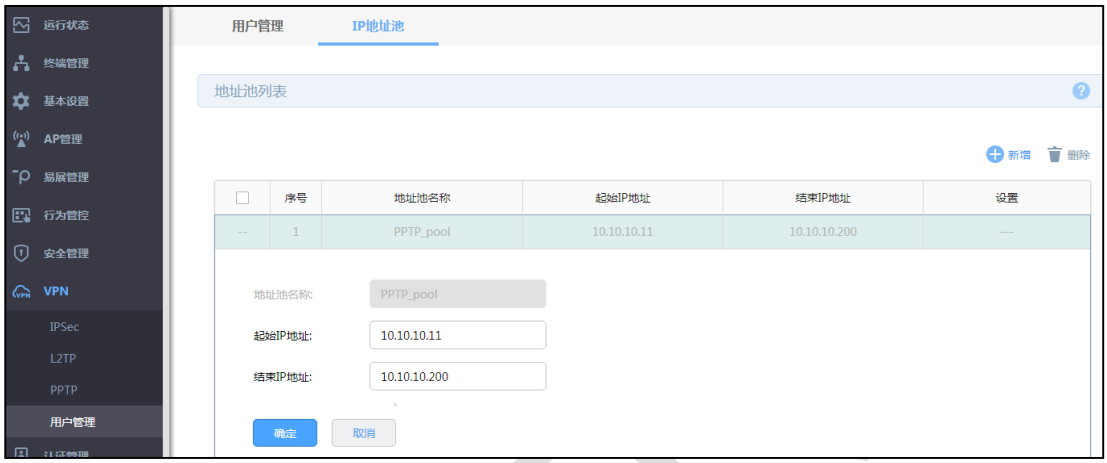
设置 LAN 口网段（与客户端不在同一个网段）,本例中将 LAN 网段设置为 192.168.0.0/24

（2）WAN 口设置

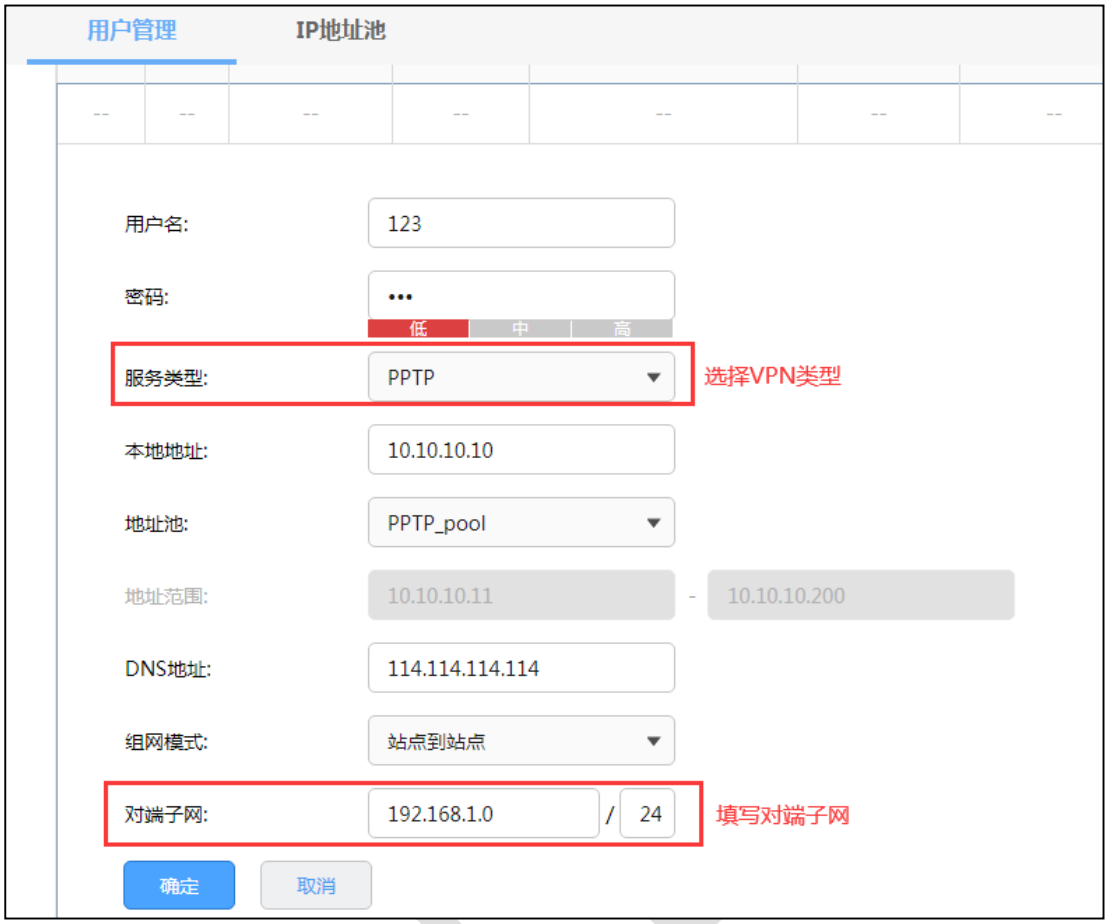
静态 ip 方式上网或者 PPPoE 方式上网（如果使用的是 PPPoE 上网，由于获取的 IP 地址会变化，此时建议使用动态域名 DDNS），本例使用静态 IP：183.15.15.15。

（3）PPTP 服务器的设置

1）打开"VPN >> 用户管理 >> 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)：



2)打开"VPN >> 用户管理"页面，进行用户管理配置，点击<新增>。



说明：

- 用户名：客户端与服务器端建立连接的用户名。
- 密码：客户端与服务器端建立连接的密码。
- 服务类型：L2TP：本用户只用于 L2TP；PPTP：本用户只用于 PPTP；自动：本用户既可用于 L2TP 也可用于 PPTP。
- 本地地址：VPN 隧道的本地虚拟 IP 地址。
- 地址池：就是 A 步骤建立的隧道地址池，选择即可。
- 组网模式：可选择站点到站点或 PC 到站点。
- 对端子网范围：客户端 LAN 口的网段（服务器端和客户端 LAN 口地址不能在同一个网段）。
- 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）。

3）打开“VPN >> PPTP”页面，设置 PPTP VPN 服务器:

说明：

- 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。
- 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。
- 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。

第二步、客户端的设置（以 TL-R488PM-AC 为例）

（1）进入管理界面

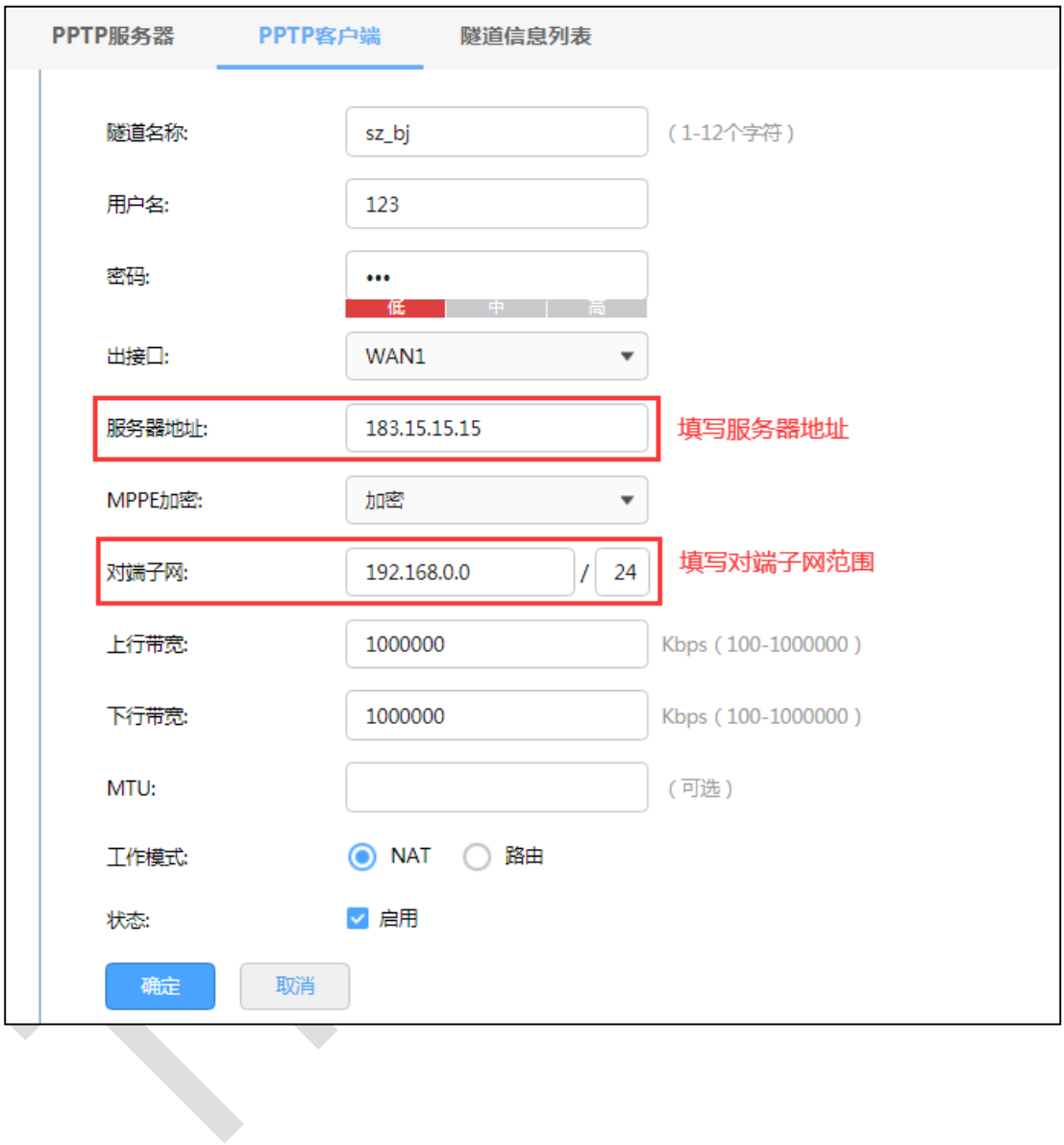
设置 LAN 口网段（与服务器端不在同一个网段），本例为 192.168.1.0/24

（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，点击<新增>，填写客户端配置信息。



说明：

- 用户名：服务器端设置的用户名。
- 密码：服务器端设置的密码。
- 出接口：选择已经设置上网的 WAN 口。
- 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）。

- MPPE 加密：与服务器端设置一致。
- 对端子网范围：服务器端 LAN 口的网段（与本地 LAN 不同网段）。
- 工作模式： NAT：对经过此 PPTP 隧道的数据包进行 NAT 转换（数据包的源 IP 替换为 PPTP 隧道的本地虚拟 IP）。路由：对经过此 PPTP 隧道的数据包进行路由转发。

第三步、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 隧道信息中将有条目：

（1）服务器隧道条目：

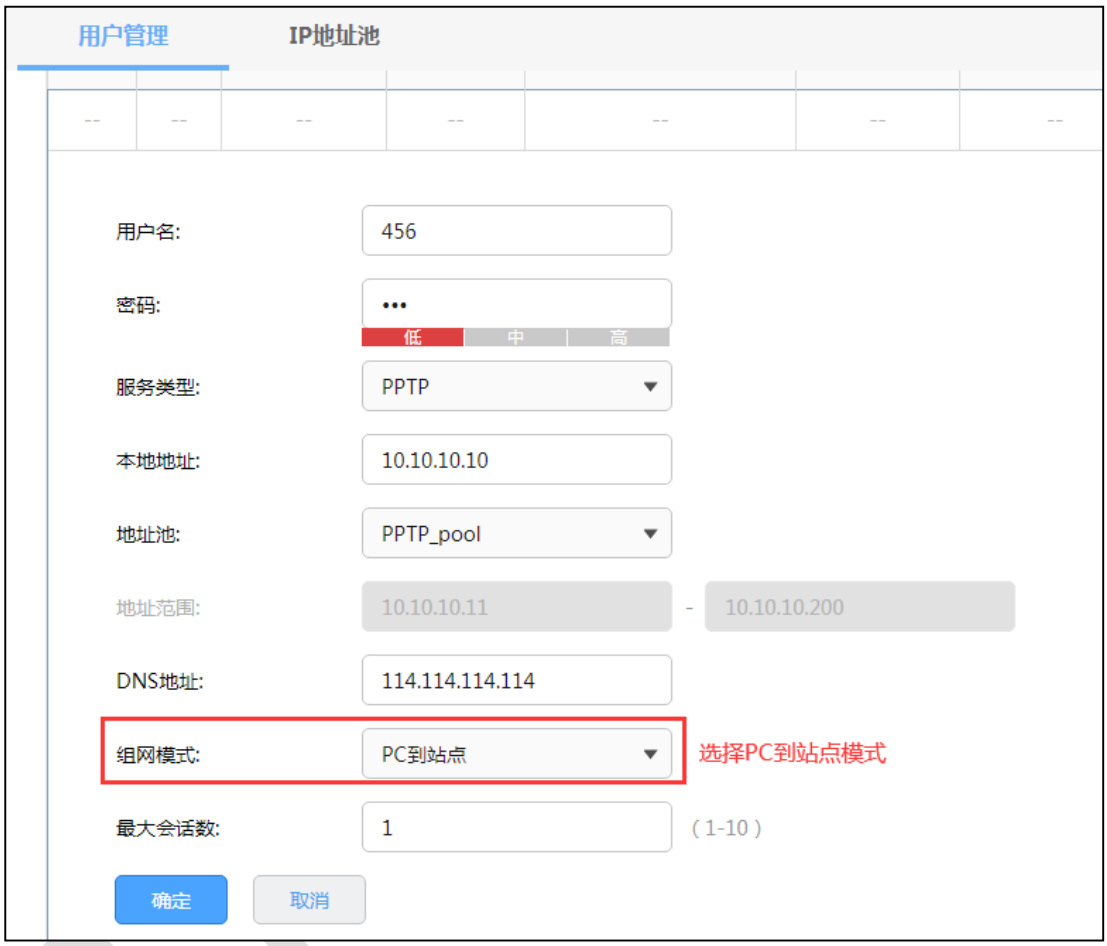
（2）客户端条目：

二、PPTP PC 到站点设置方法

第一步、服务器端的设置（以 TL-R499GPM-AC 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。



第二步、PPTP 拨号客户端的设置

电脑、手机或不同操作系统的客户端 PPTP 播放方式有所差异，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。

第三步、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：

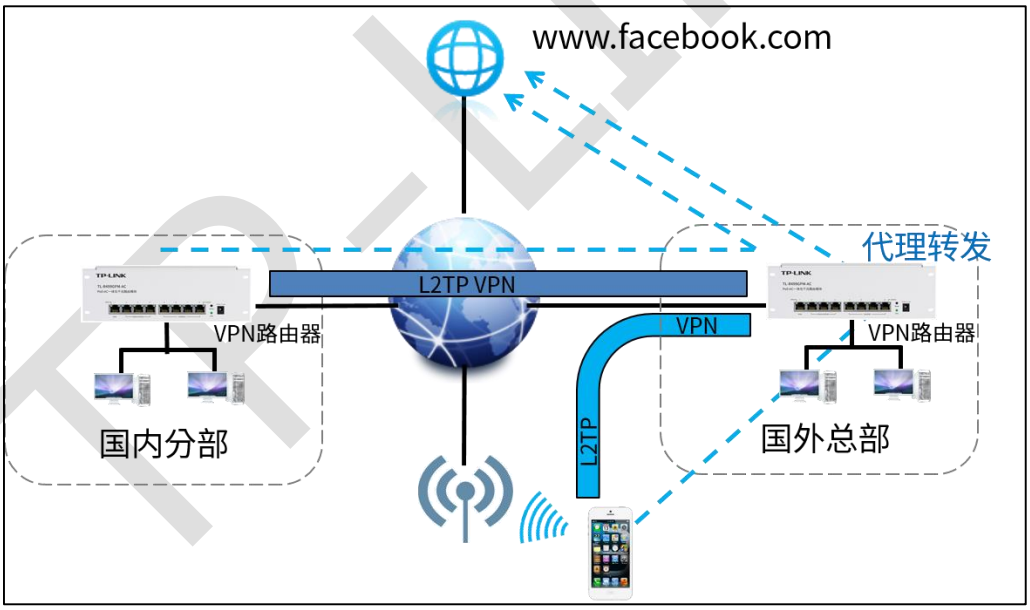
9.4 L2TP VPN 代理上网设置指南

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 R 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。

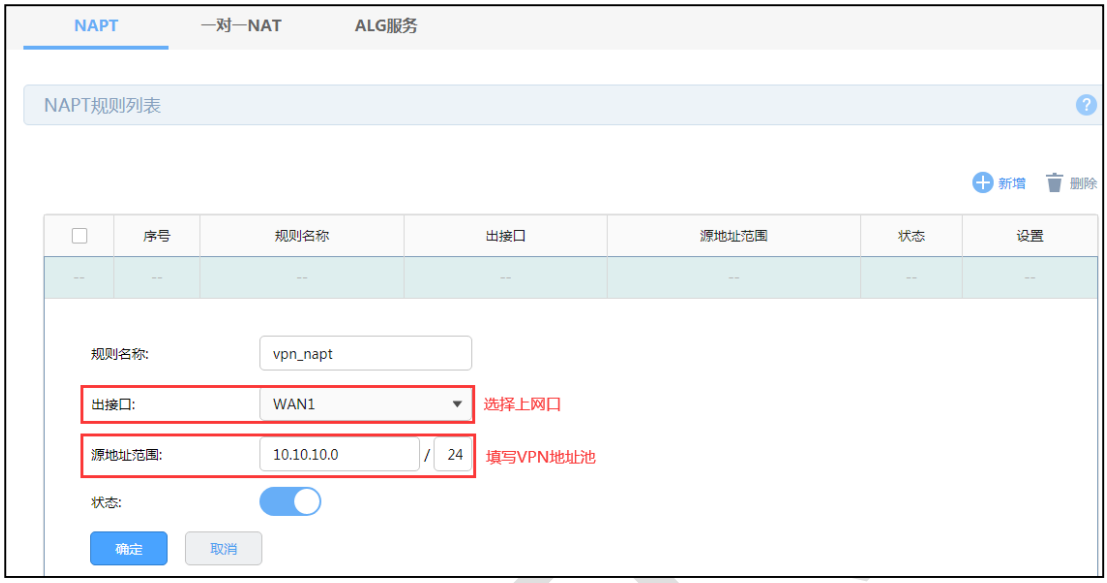


9.4.3 设置方法

【准备工作】已搭建好 L2TP VPN 隧道。设置方法请点击：9.2 L2TP VPN 设置指南。

第一步、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：

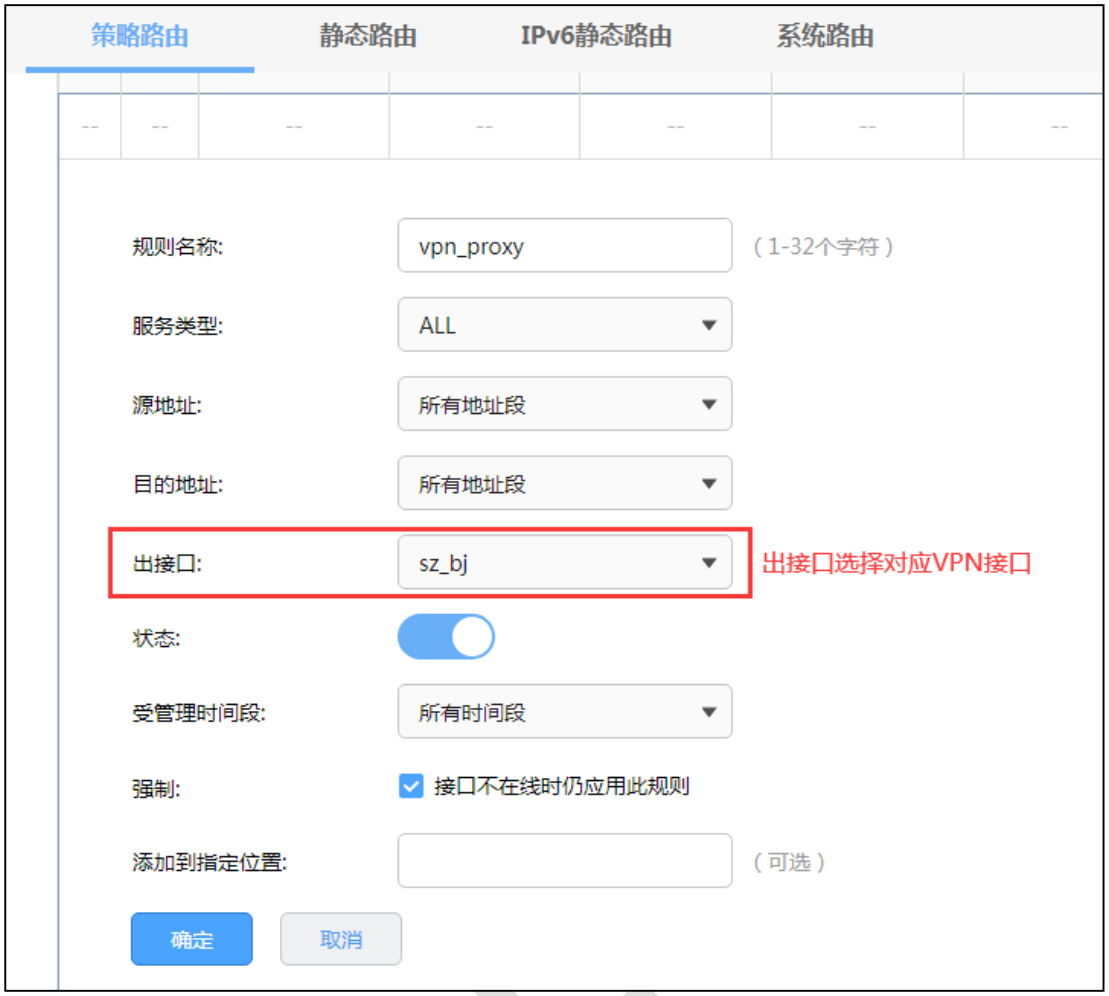


第二步、VPN 客户端设置

（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。

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：



（2）PC 到站点客户端设置

PC 到站点拨号方法见链接：

[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

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：

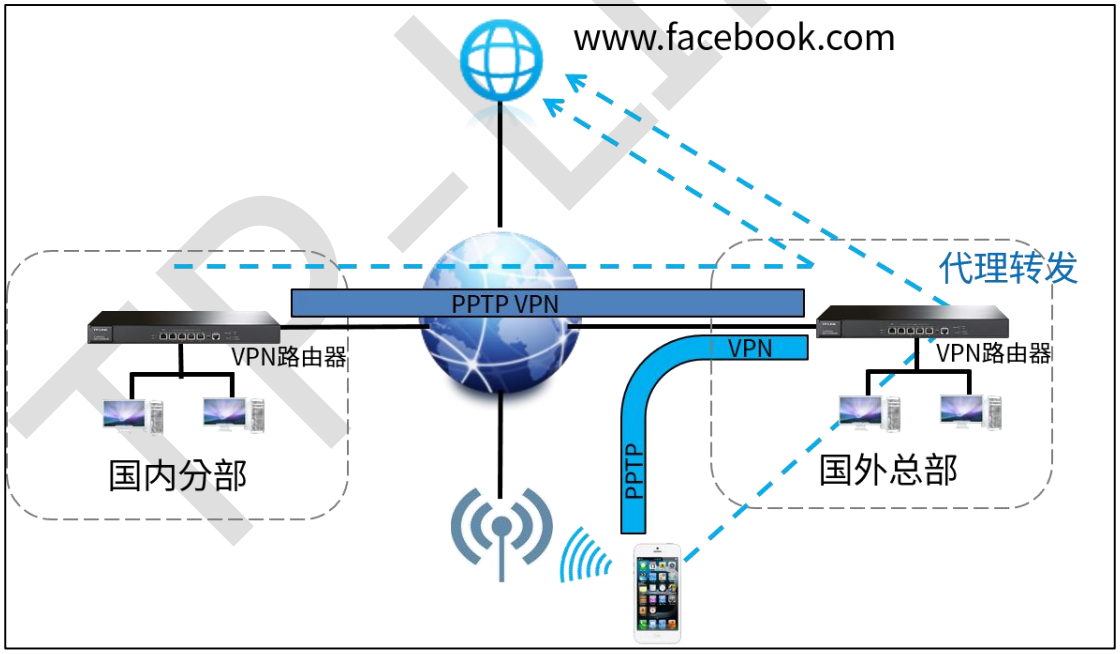
9.5 PPTP VPN 代理上网设置指南

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 R 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。

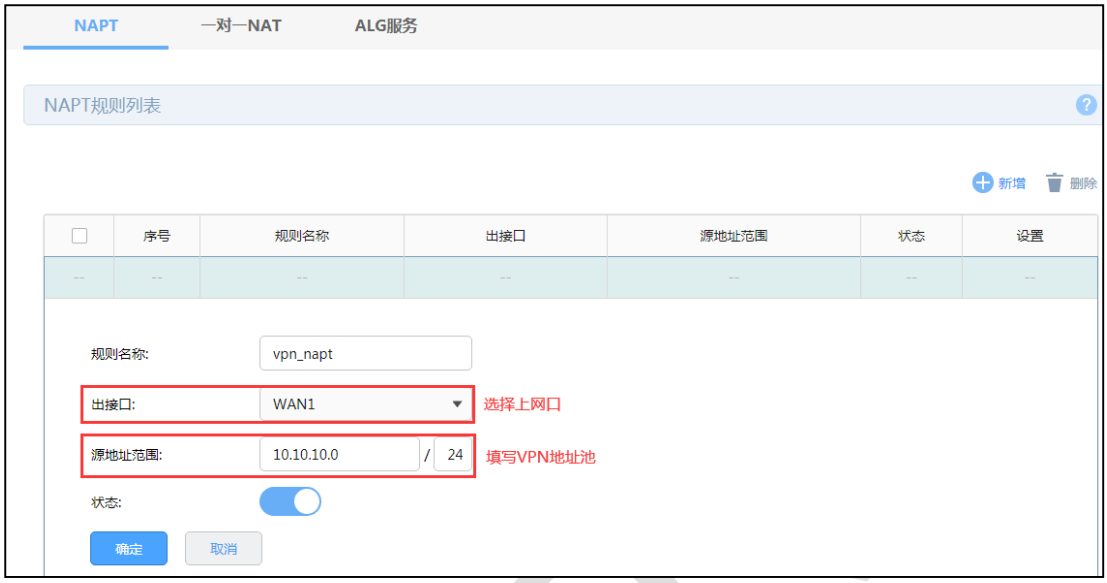


9.5.3 设置方法

【准备工作】已搭建好 PPTP VPN 隧道。设置方法请点击：9.3 PPTP VPN 设置指南。

第一步、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：

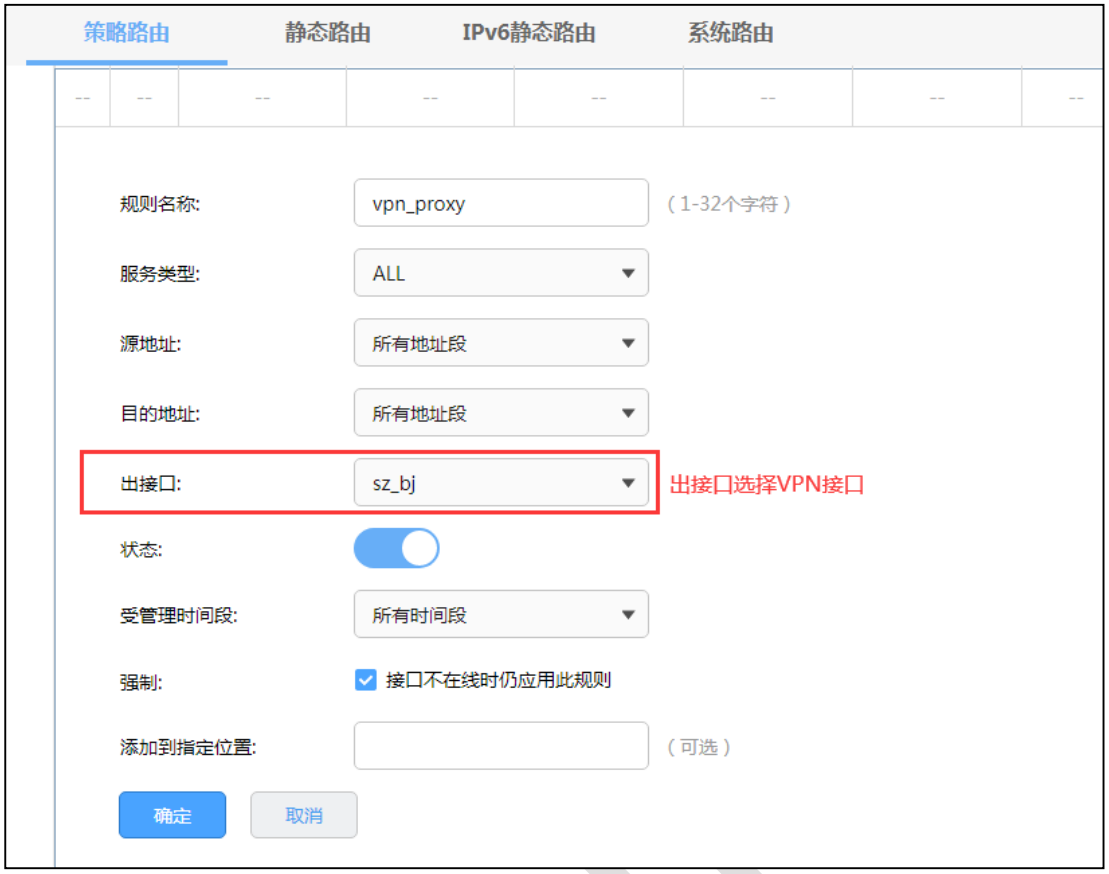


第二步、VPN 客户端设置

（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。

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：



（2）PC 到站点客户端设置

PC 到站点拨号方法见链接：

[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

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：

第10章 认证管理

10.1 一键上网设置指南

10.1.1 应用介绍

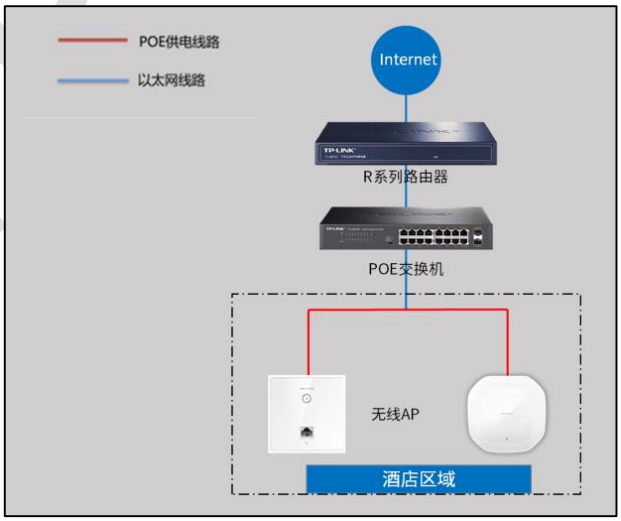
目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客接入网络的方式有很多，一键认证就是其中的一种。商户可以通过一键认证推送广告，而访客无需账号密码，一键免费上网。本文通过典型应用实例介绍 R 系列路由器一键上网的应用与配置。

10.1.2 需求介绍

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。

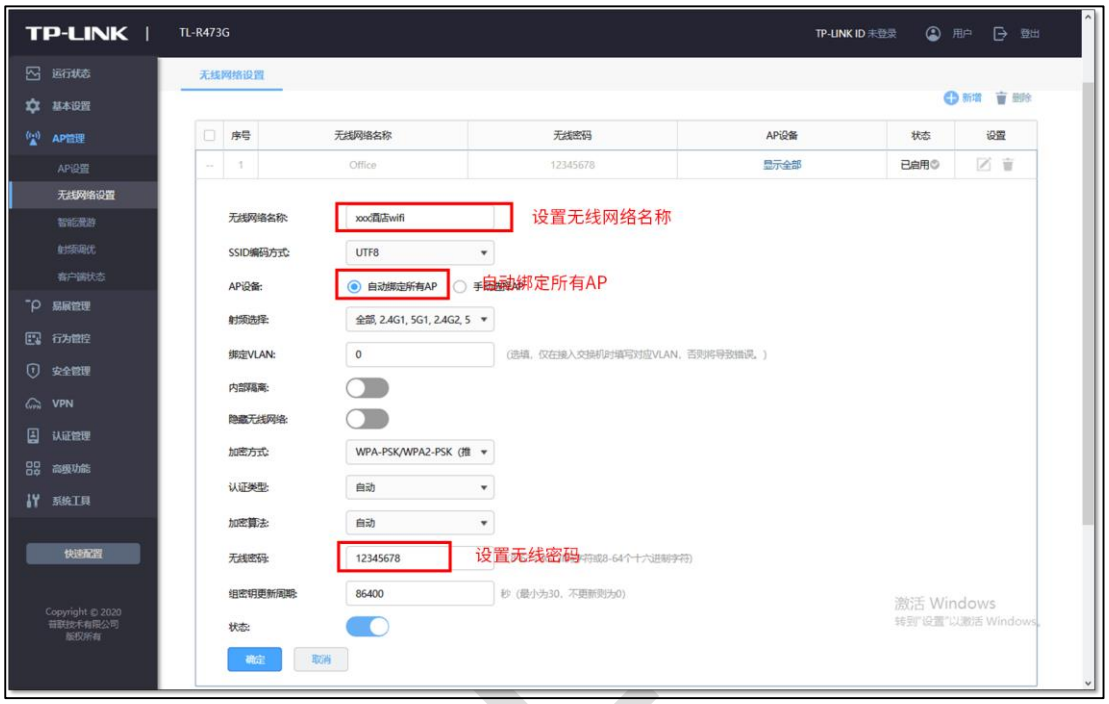
根据用户需求，路由器和 AP 连接参考拓扑如下：



10.1.3 设置方法

第一步、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：



第二步、认证参数设置

点击“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式，如下图：

说明：

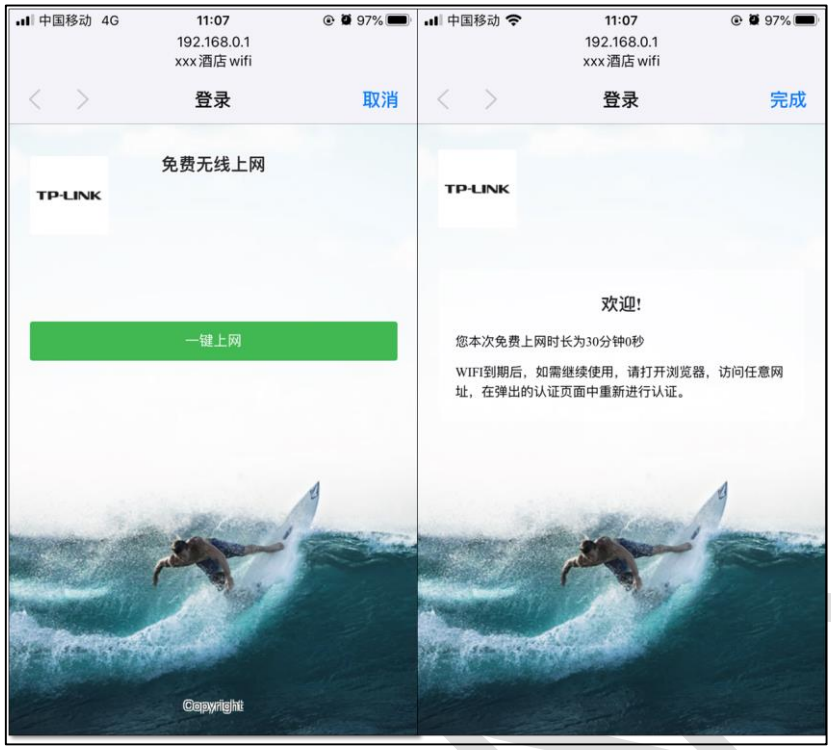
- 认证老化时间：当已认证客户端断开连接后，对应认证条目的老化时间。客户端在老化时间内重新连接，则不需要重新认证，超过老化时间后接入的客户端需要重新认证。
- Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 认证模式：设置 Portal 认证的认证模式，支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示连接到这个接口中的终端都需要认证才能上网。

第三步、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，R 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：


中国移动 4G
11:07
97%
192.168.0.1
xxx 酒店 wifi
登录
取消
免费无线上网
TP-LINK
一键上网
Copyright
中国移动
11:07
97%
192.168.0.1
xxx 酒店 wifi
登录
完成
TP-LINK
欢迎!
您本次免费上网时长为30分钟0秒
WIFI到期后，如需继续使用，请打开浏览器，访问任意网址，在弹出的认证页面中重新进行认证。

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 R 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 R 系列路由器短信认证的应用与配置。

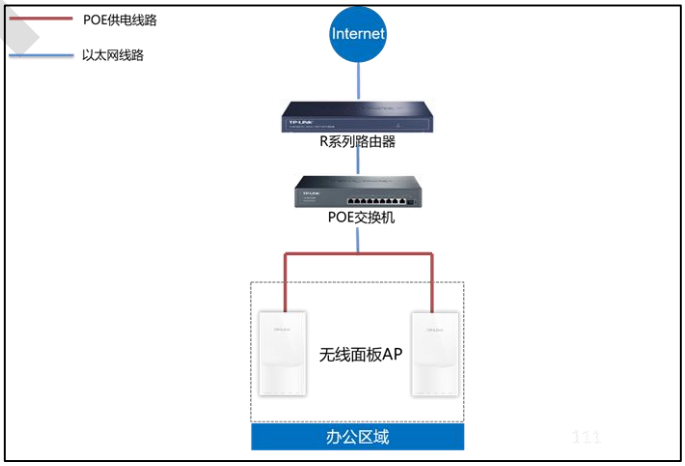
注意：使用短信认证时，短信服务平台会收取通信服务费，具体收费标准请参考云平台。

10.2.2 需求介绍

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 页面中输入手机号进行短信认证，认证通过之后才能上网。

根据用户需求，路由器和 AP 连接参考拓扑如下：



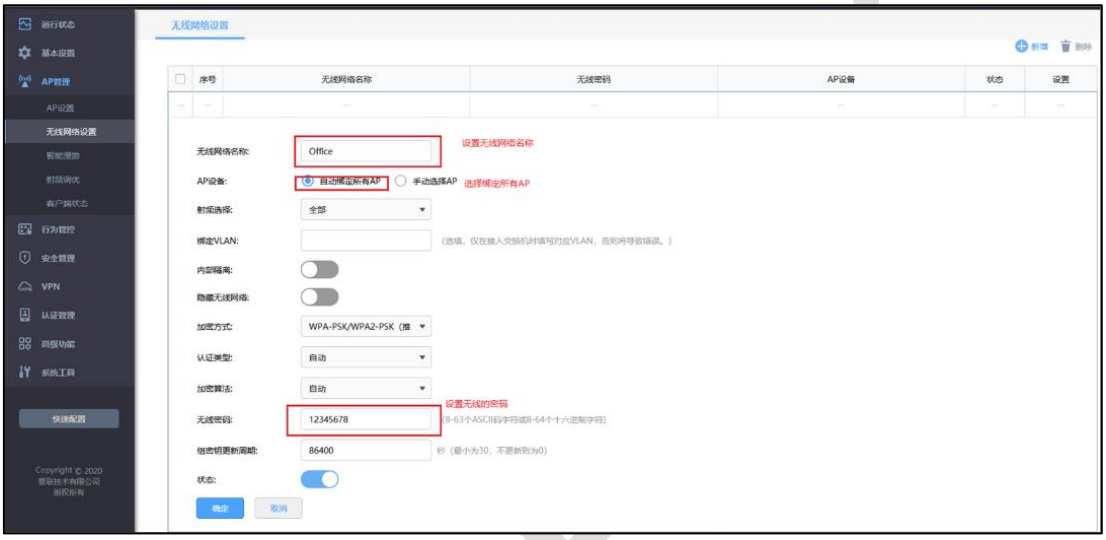
10.2.3 设置方法

第一步、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

第二步、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 >> 全局参数”，配置认证老化时间和认证模式，如下图：

说明：

- 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，则不需要重新认证，超过老化时间后接入的客户端需要重新认证。
- Portal 认证端口：用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
- 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。

第四步、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>，下面将逐一进行介绍：

1）阿里云

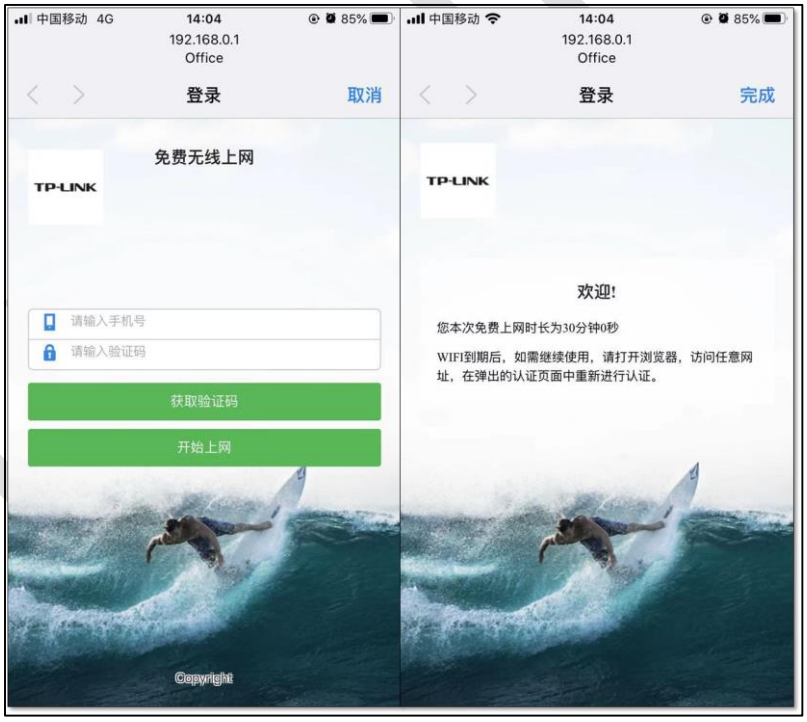
2）腾讯云

3）百度云

4）网易云信

5）HTTP 协议

以上内容配置完毕，R 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

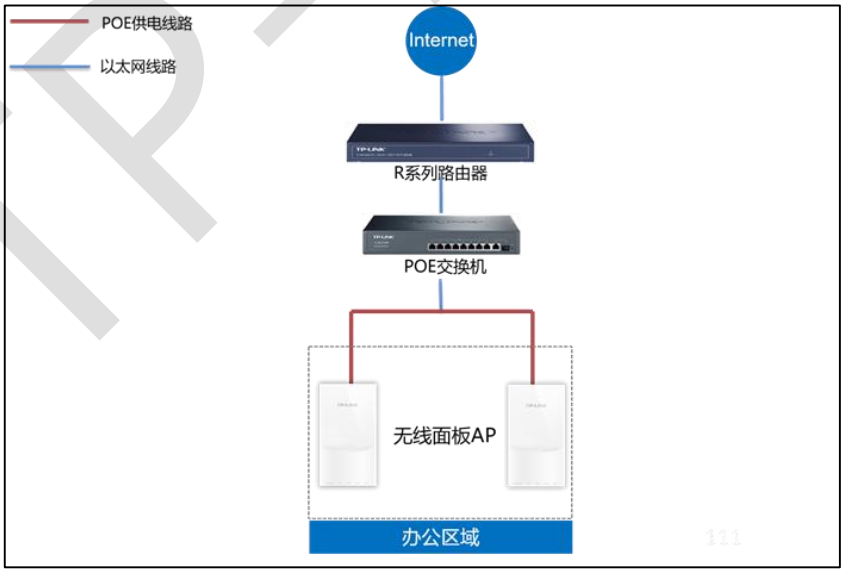
随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。R 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 R 系列路由器 Portal 认证功能的应用与配置。

10.3.2 需求介绍

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。

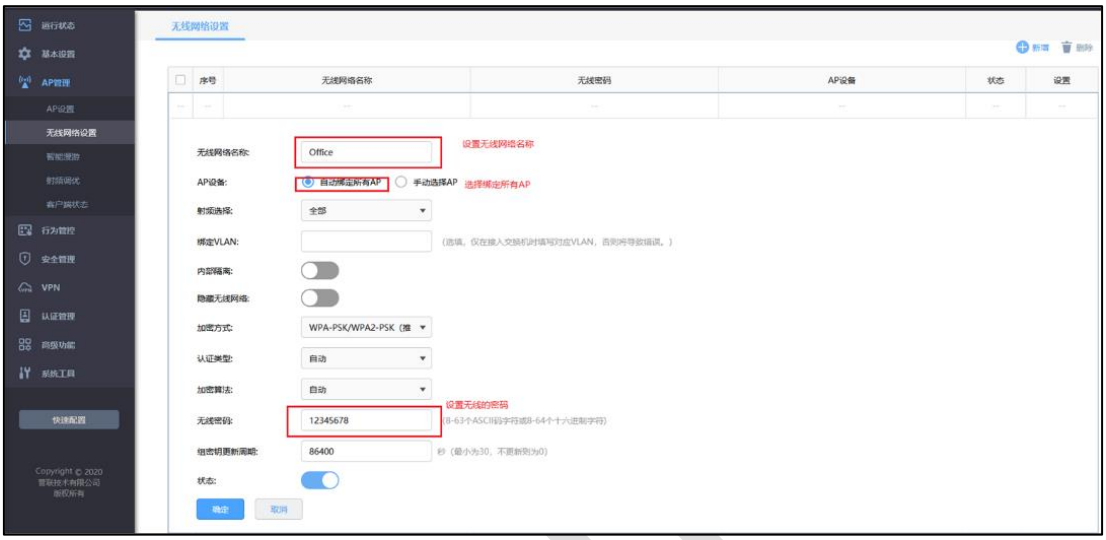
根据用户需求，路由器和 AP 连接参考拓扑如下：



10.3.3 设置方法

第一步、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：



第二步、认证参数设置

点击“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式，如下图：

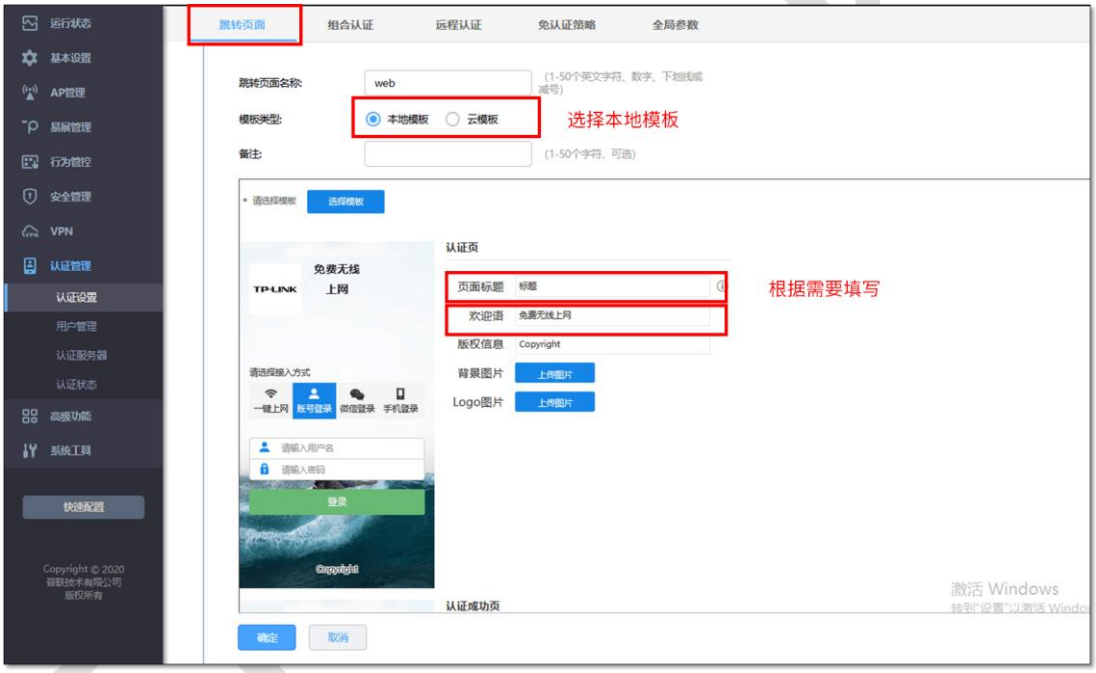
说明：

- 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。

- 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。
- 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。

第三步、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：

第四步、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，R 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

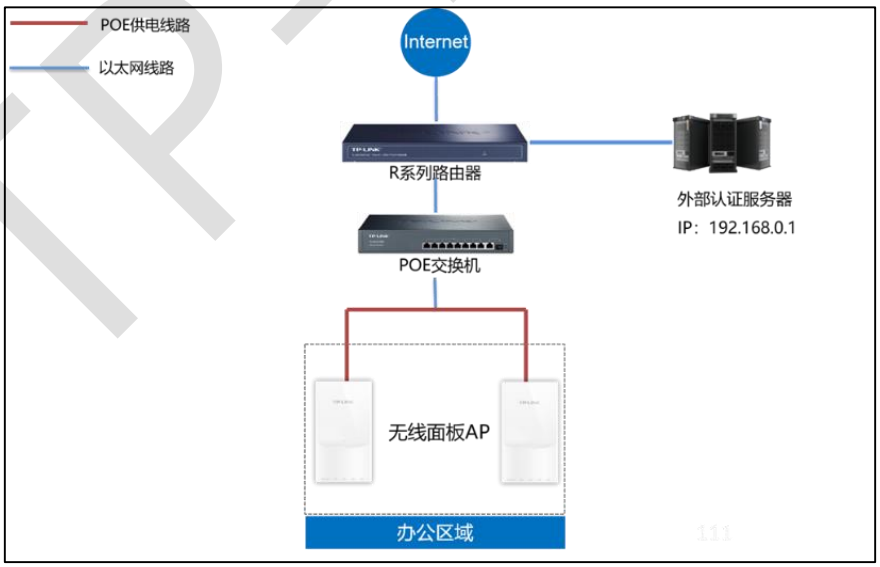
随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。R 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 R 系列路由器 Portal 认证功能的应用与配置。

10.4.2 需求介绍

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。

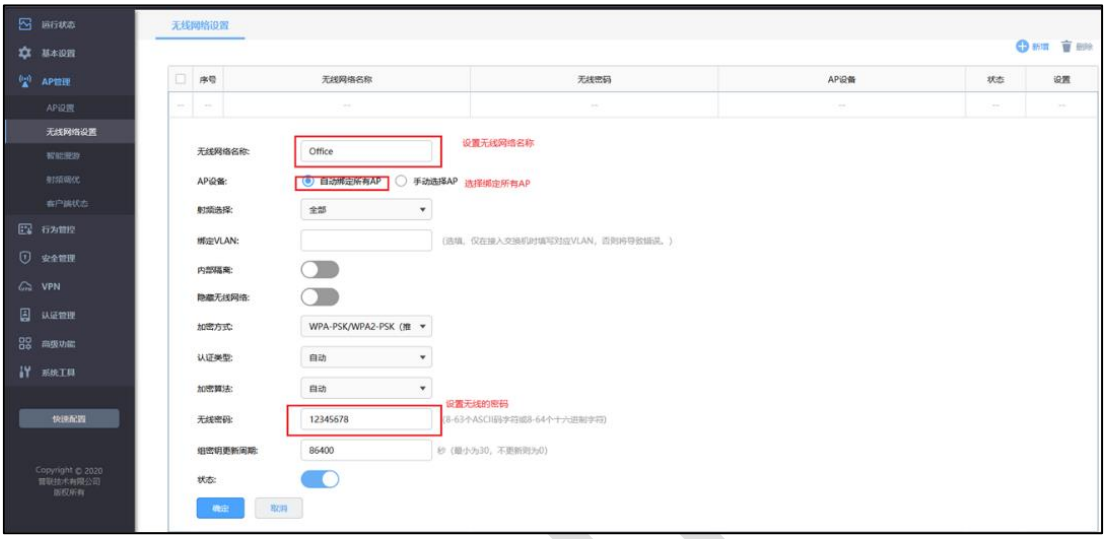
根据用户需求，路由器和 AP 以及服务器连接参考拓扑如下：



10.4.3 设置方法

第一步、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：



第二步、认证参数设置

点击“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式，如下图：

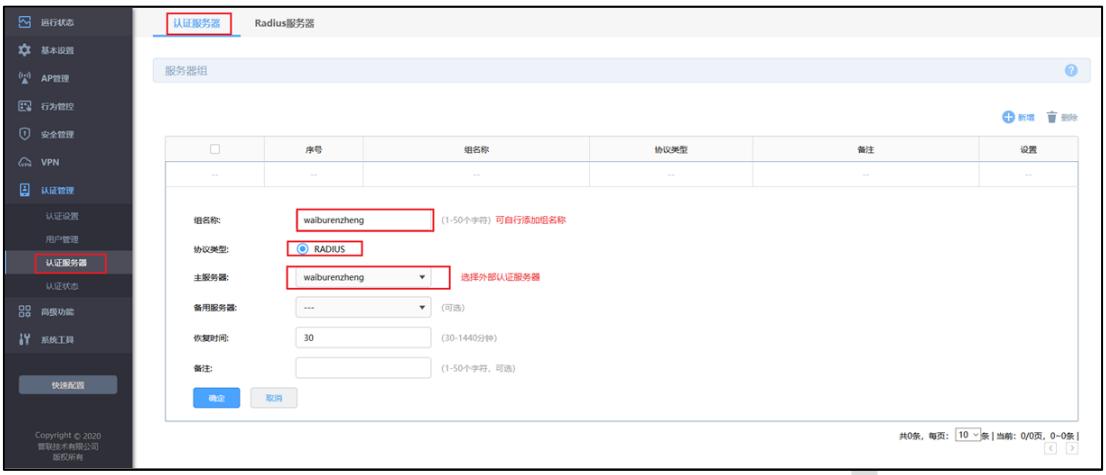
说明：

- 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。
- 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。
- 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。

第三步、配置外部认证服务器并添加服务器组

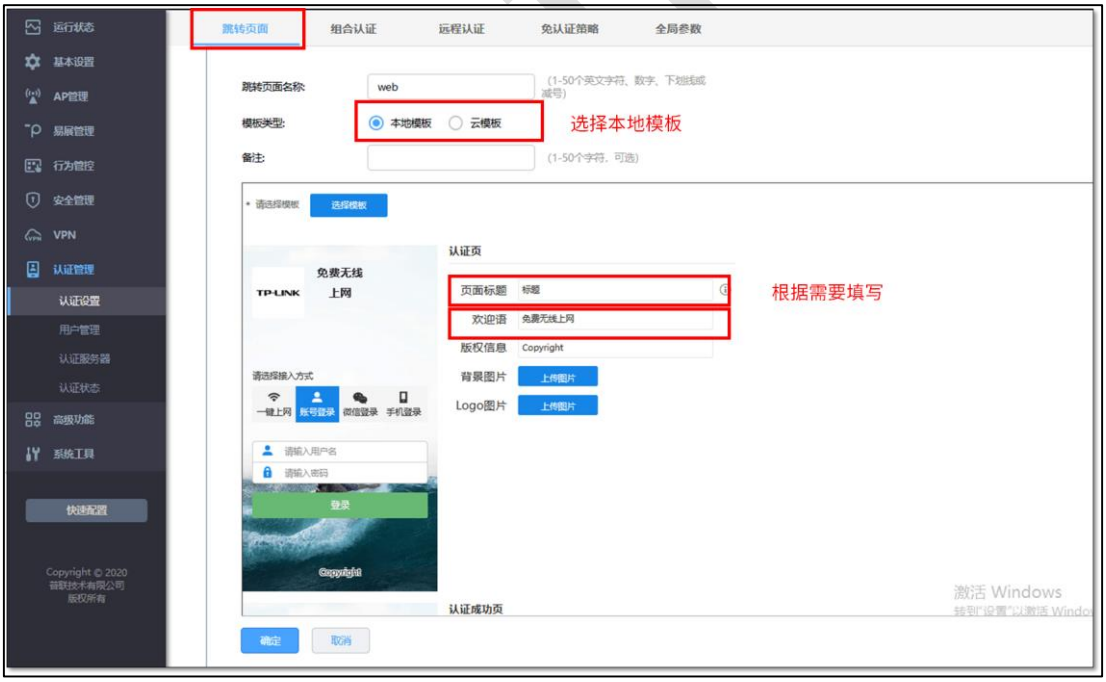
（1）点击“认证服务器 >> Radius 服务器”，根据自己设置的外部认证服务器在路由器添加条目。

（2）添加外部服务器组



第四步、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，R 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

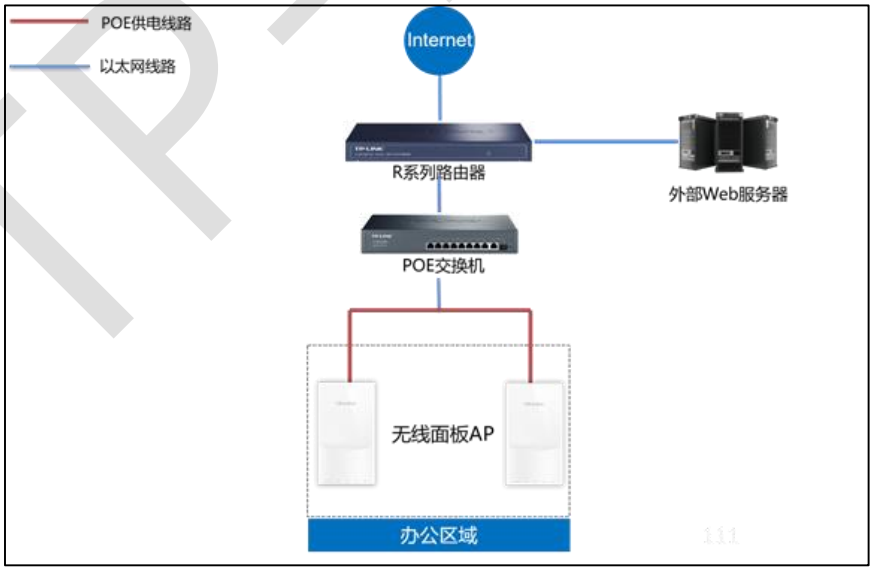
随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。R 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 R 系列路由器 Portal 认证功能的应用与配置。

10.5.2 需求介绍

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。

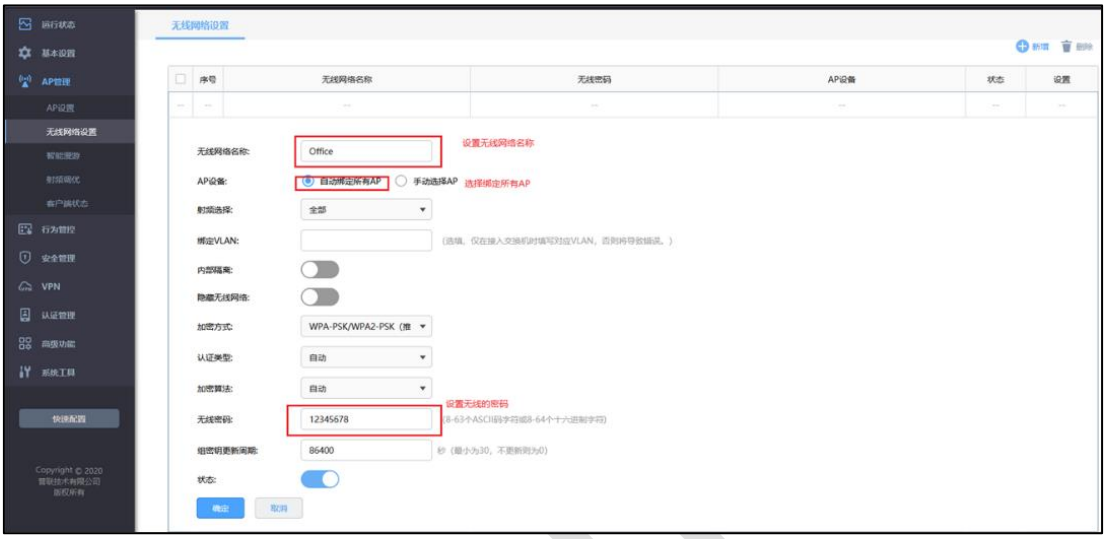
根据用户需求，路由器和 AP 以及服务器连接参考拓扑如下：



10.5.3 设置方法

第一步、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：



第二步、认证参数设置

点击“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式，如下图：

说明：

- 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。
- 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。
- 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。

第三步、配置外部 Web 服务器

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

第四步、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，R 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

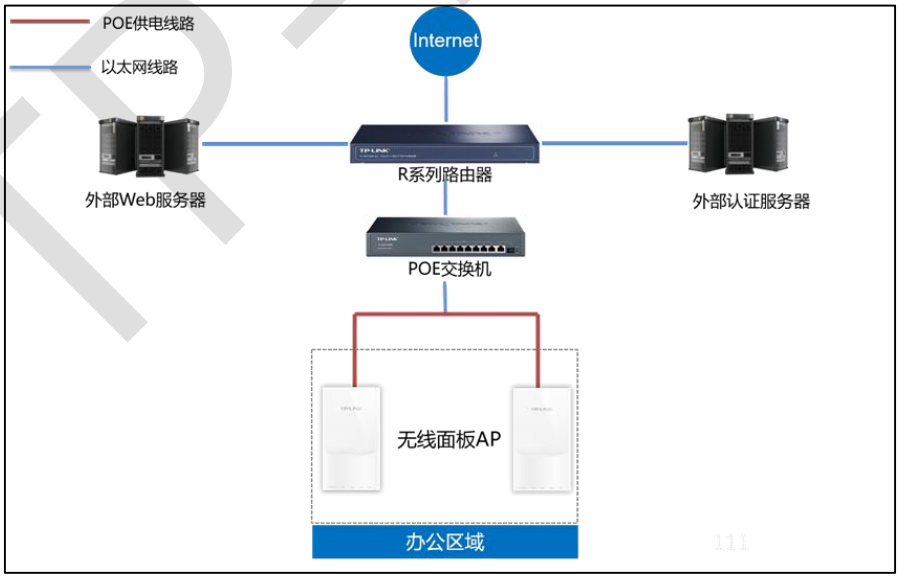
随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。R 系列路由器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 R 系列路由器 Portal 认证功能的应用与配置。

10.6.2 需求介绍

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。

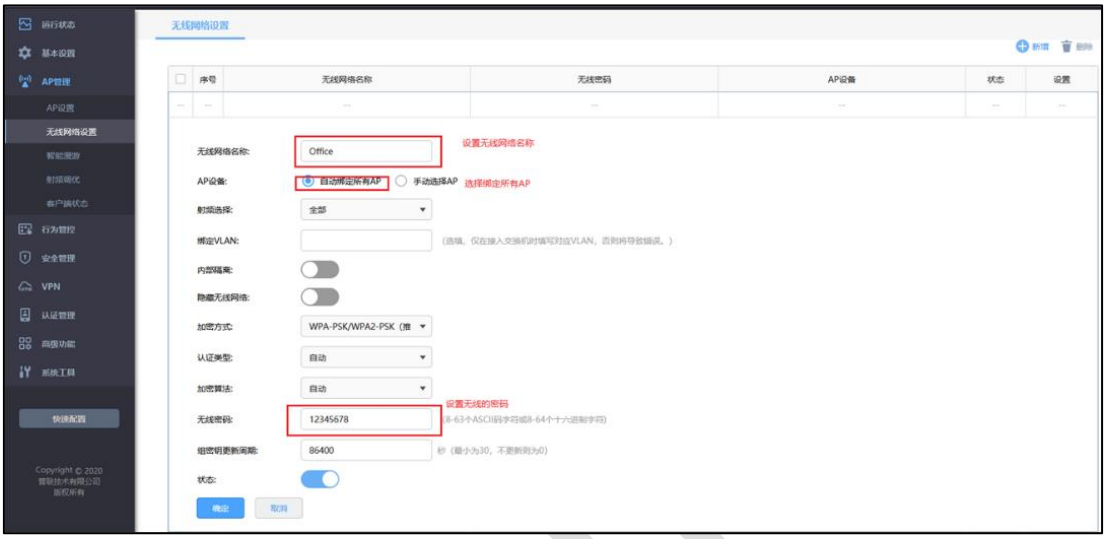
根据用户需求，路由器和 AP 以及服务器连接参考拓扑如下：



10.6.3 设置方法

第一步、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：



第二步、认证参数设置

点击“认证管理 >> 认证设置 >> 全局参数”，配置认证老化时间和认证模式，如下图：

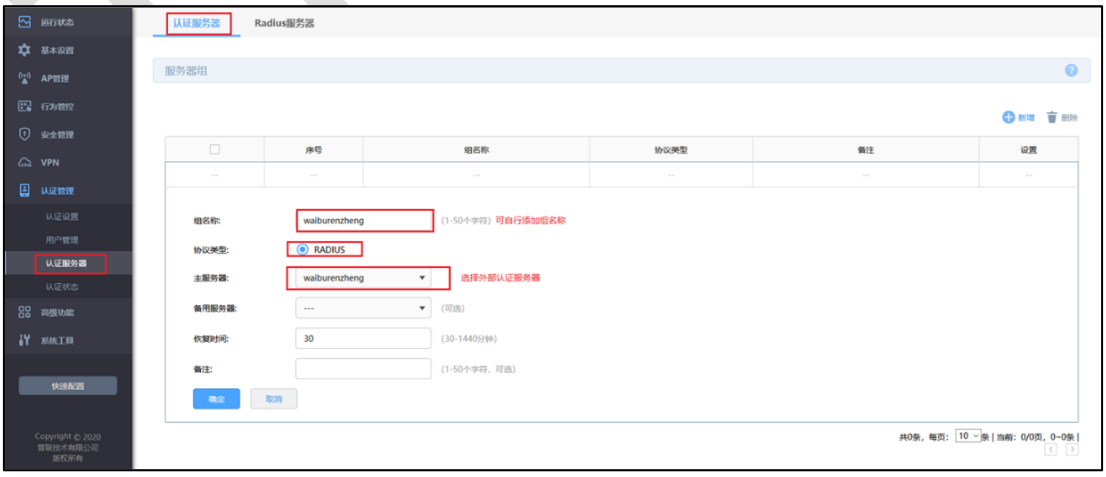
说明：

- 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。
- 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。
- 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。

第三步、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



第四步、配置外部 Web 服务器

点击“认证管理 >> 认证设置 >> 远程认证”，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，R 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 R 系列路由器免认证策略的应用与配置。

10.7.2 需求介绍

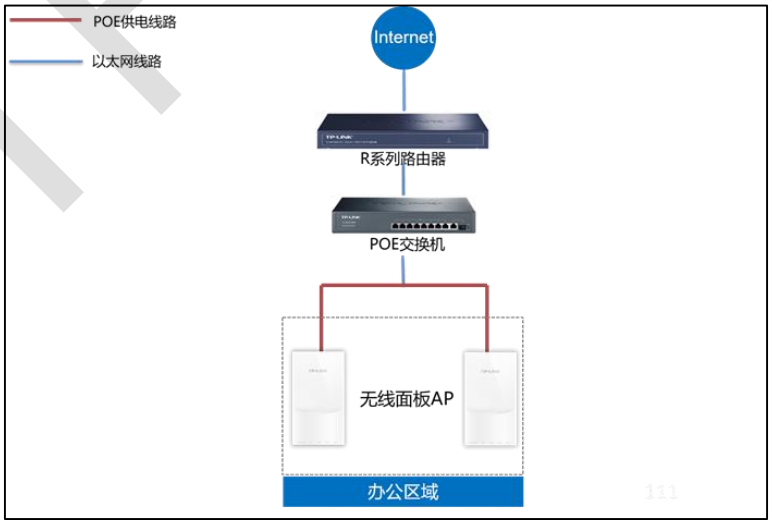
某办公室需要实现无线覆盖，员工需要通过认证后才能上网，有以下需求：

1. 特定终端如打印机不需要认证即可上网；

2. 员工无需认证也可以访问公司外网服务器；

3. 员工无需认证也可以访问公司网站；

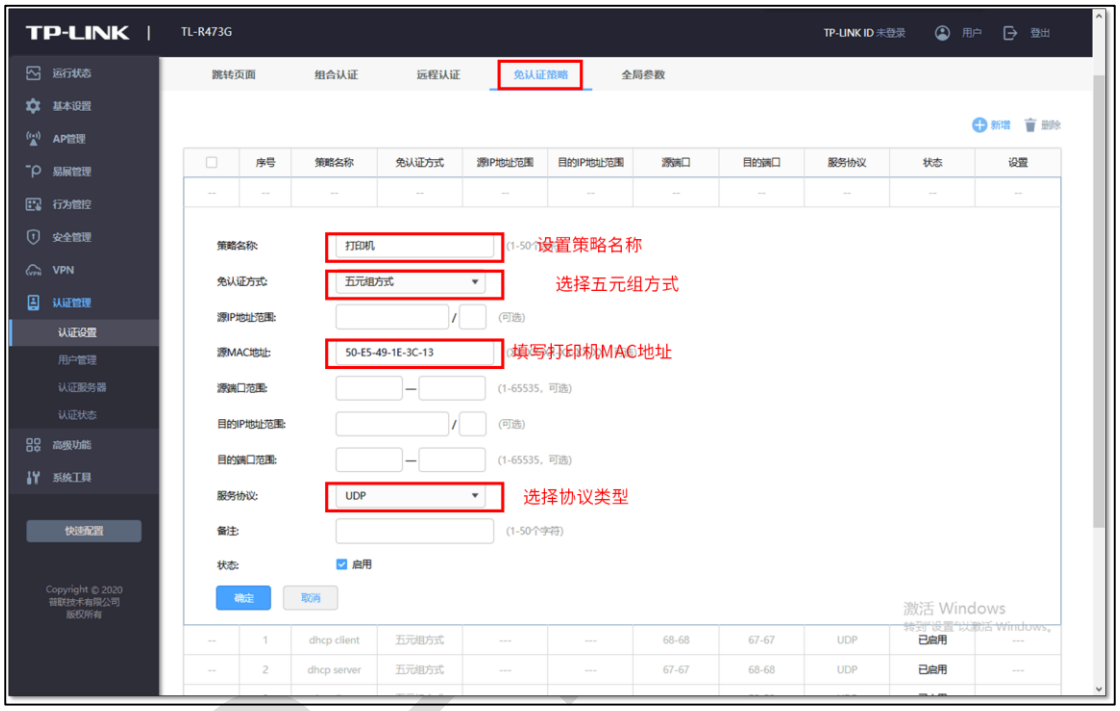
根据用户需求，路由器和 AP 连接参考拓扑如下：



10.7.3 设置方法

第一步、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：

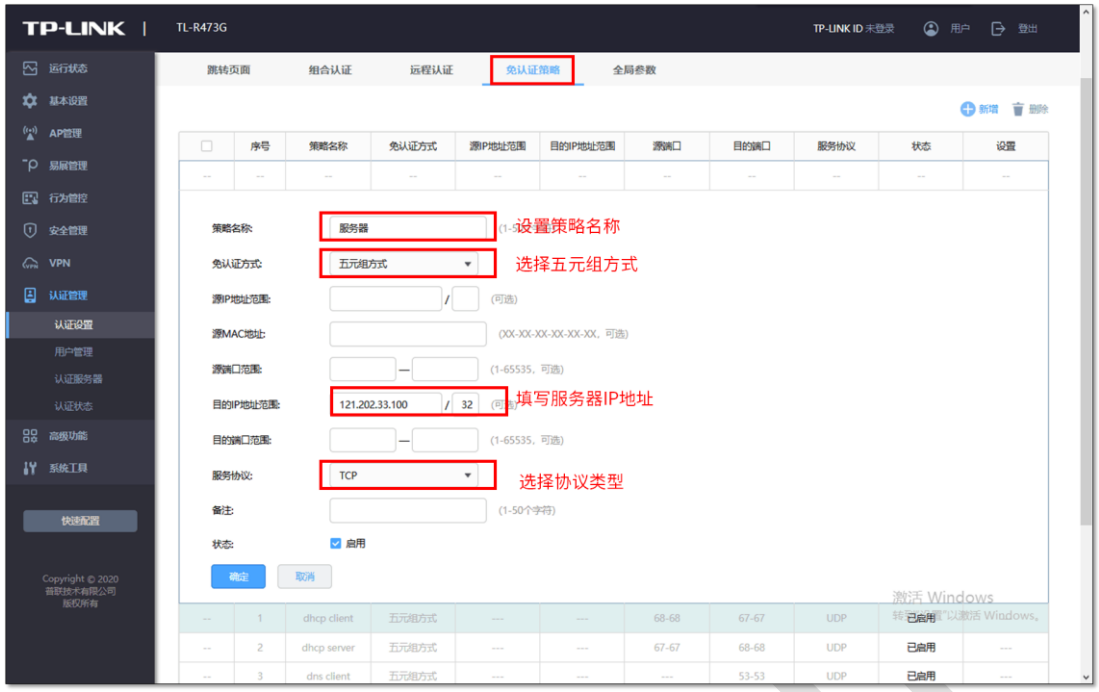


由于终端上网可能即需要使用 UDP 协议又需要使用 TCP 协议，所以一个终端设备需要建立两条免认证策略服务协议分别选择 UDP 和 TCP。

以上设置可以实现固定设备无需认证就可以上网。

第二步、无需认证即可访问到指定的外网服务器

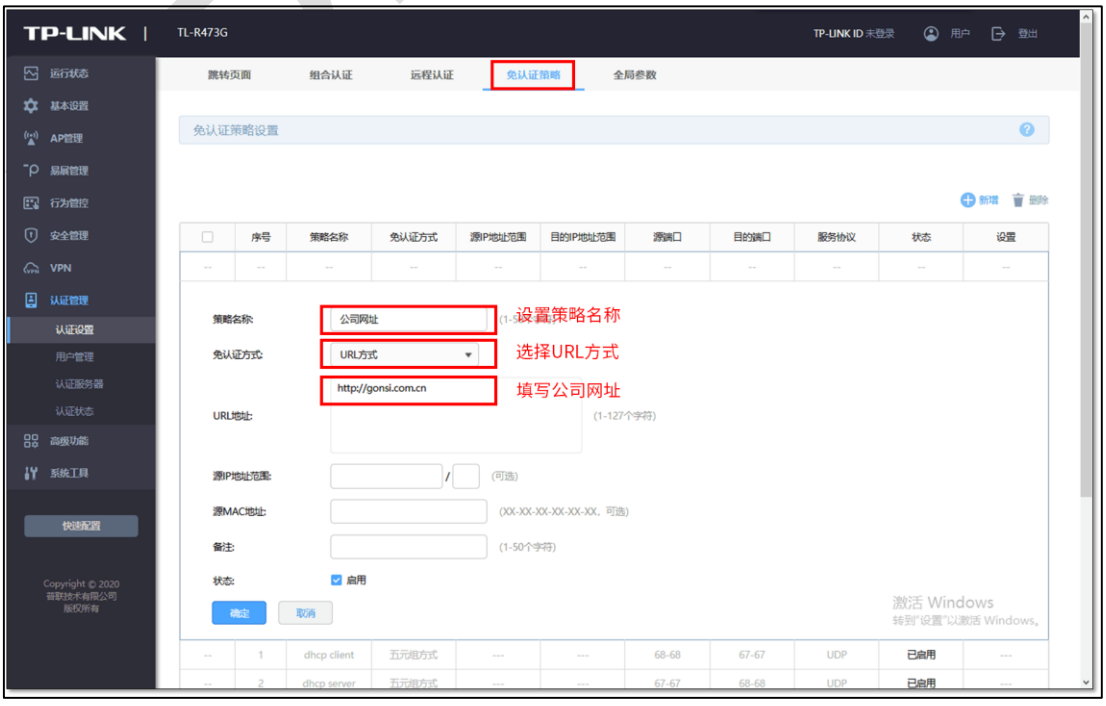
进入路由器界面，点击“认证管理 >> 认证设置 >> 免认证策略”，添加免认证策略，如下图：



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。

第三步、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。

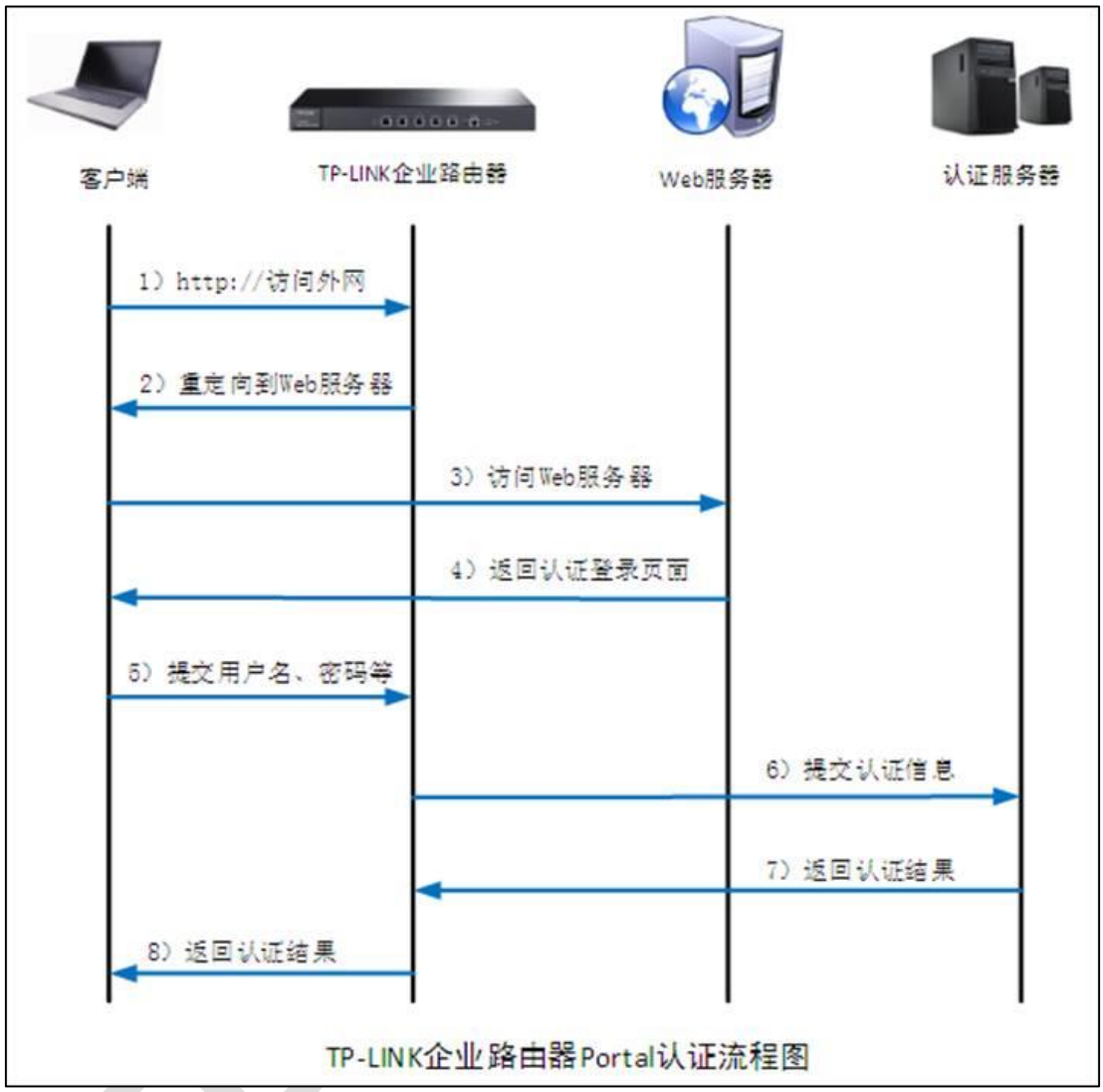
10.8 Portal 认证中，外部 WEB 服务器建立规范

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



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，并且路由器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&staIp=xx&staMac=xx&url=xx（接口模式）

http://www.abc.com/ssid_mode=true&pagetype=xx&staIp=xx&staMac=xx&apMac=xxx&apIp=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。

说明：

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：

action= http:// LAN_IP:Port/portal/auth/?interface_mode=true&pagetype=xx&authtype=5&staIp=xx&staMac=xx& username=xx&password=xx（接口模式）

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

username=xx&password=xx（SSID 模式）

其中 LAN_IP 为当前 DUT LAN 口的 IP 地址，Port 为 Portal 服务端口，authtype 为固定值 5 表示远程 Portal 认证，username 为用户输入的用户名，password 为用户输入的密码，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 ErroCode 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 产品介绍

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：

（1）支持工业环境的导轨和壁挂安装方式；

（2）支持宽电压 9.6-60VDC 三路电源输入，三电源冗余；

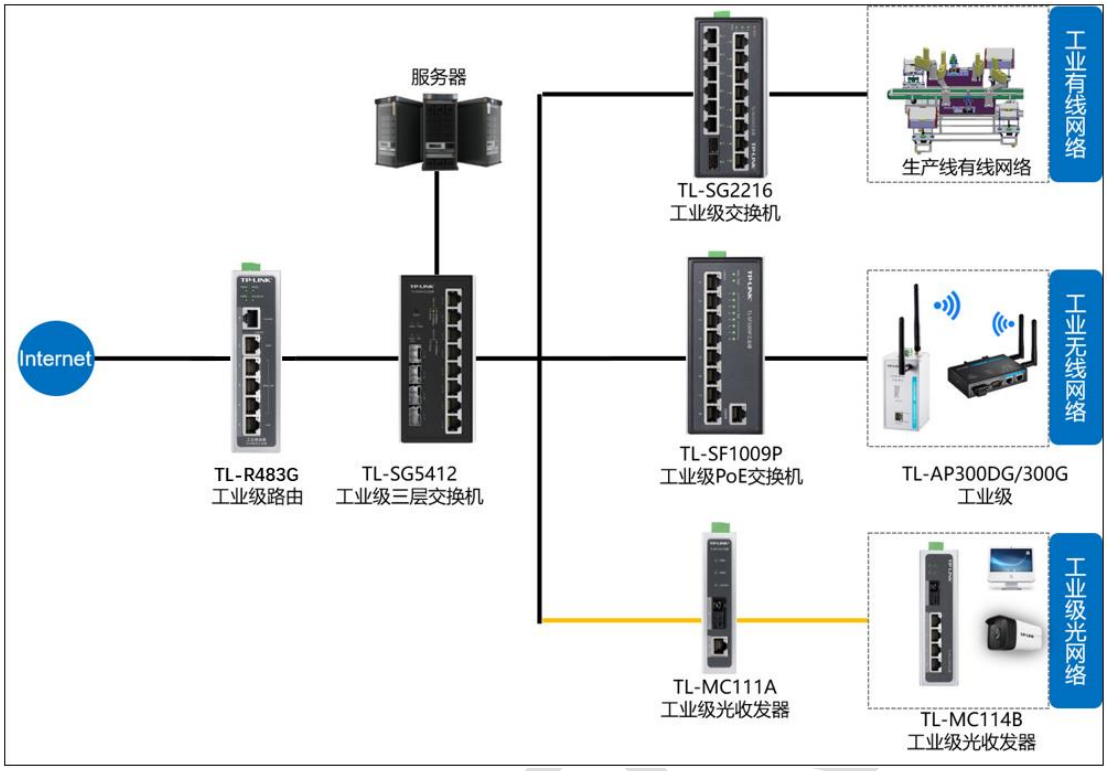
（3）支持 DIP 拨码开关，方便管理和维护；

（4）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 需求介绍

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。

工厂的应用拓扑：



11.1.3 设置方法

下面以 TL-R483G 工业级为例，讲解一下如何快速设置上网和报警功能。

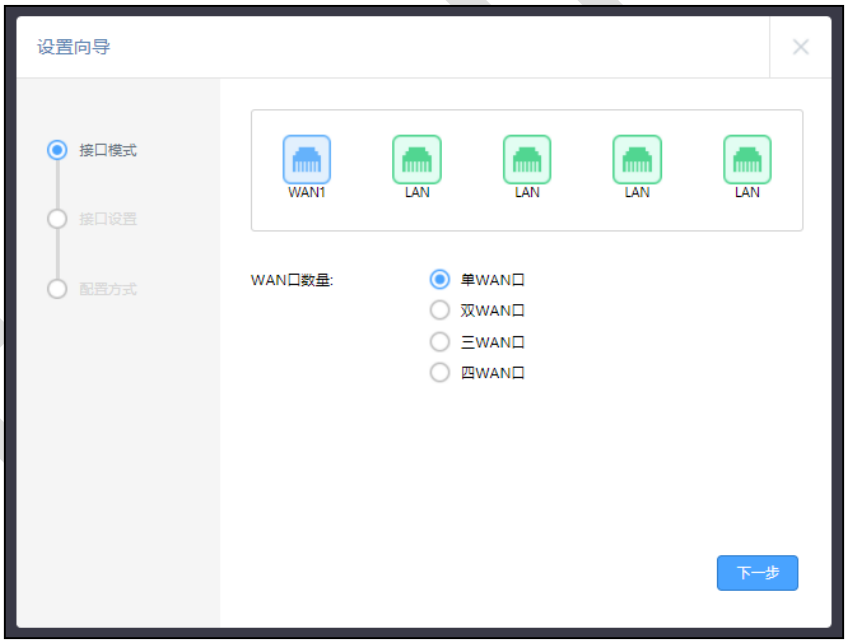
第一步、登录路由器管理界面

电脑设置为自动获取或者配置与路由器同网段的静态 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，在显示的界面设置用户名和密码（确认提交前请牢记管理员账户和密码）。

注意：路由器出厂默认的管理端口为 5 口。

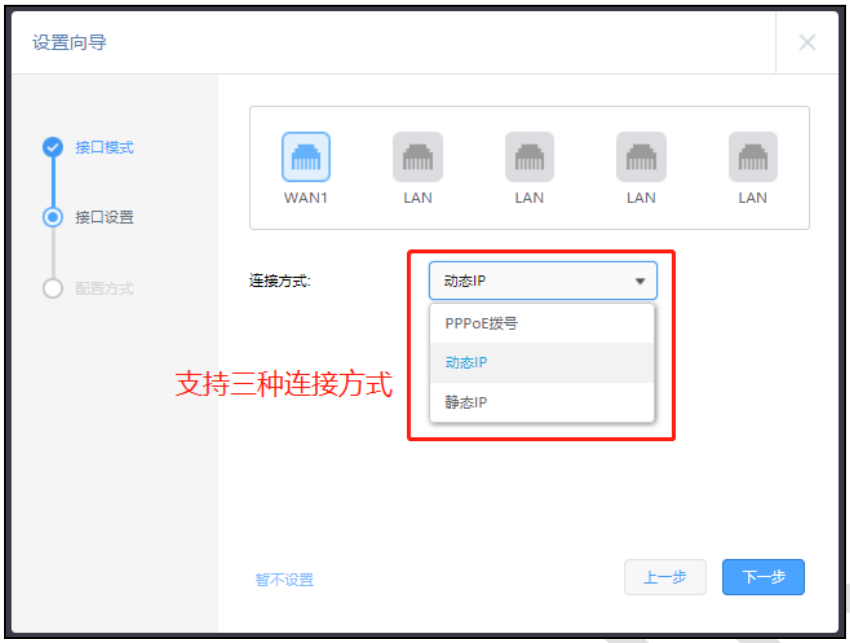
第二步、选择 WAN 口数量

选择 WAN 口数量，本例选择单 WAN 口模式；



第三步、选择 WAN 口上网方式

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；



第四步、设置 LAN 口 IP

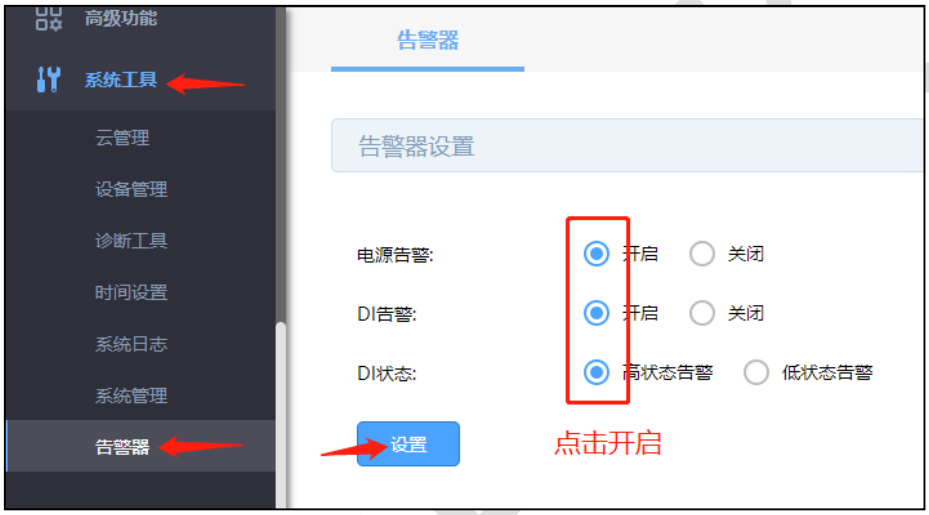
自动或手动配置 LAN 网段的 IP 地址和子网掩码，手动配置需要自定义 LAN 网段 IP 地址和子网掩码；设置是否开启 AP 管理，若内网有 FIT 模式的 AP 需要管理，则选择开启。界面点击<连接网络>按钮，设备将会自动配置，等待一段时间后配置完成，路由器便可上网。

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。

第五步、端口中断报警功能配置

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，点击<设置>。



说明：

- 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。
- DI 告警：你可以通过设置来决定 DI 告警器是否开启。
- DI 高状态：当 DI 接口监测的电压值为 13V-30V 时，告警器告警，其余电压值不确保是否告警。
- DI 低状态：当 DI 接口监测的电压值为-30V-3V 时，告警器告警，其余电压值不确保是否告警。

第12章 其它功能

12.1 地址组的设置与管理

12.1.1 应用介绍

R 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 需求介绍

某公司办公网络包含市场、人事等部门，需要对各部门进行上网行为管控，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

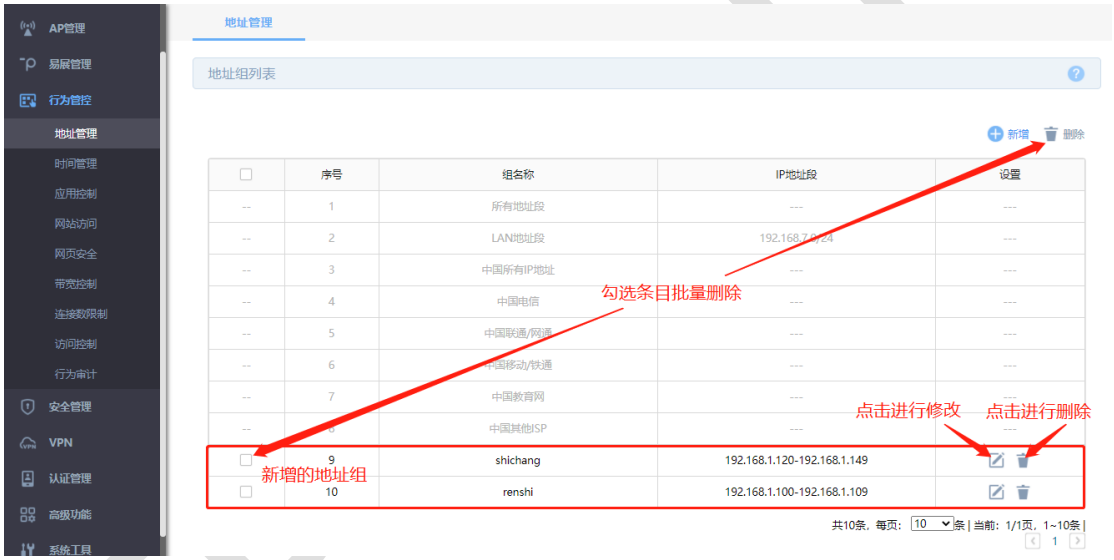
注意：该分组方式仅供举例，具体以实际需求进行划分。

12.1.3 设置方法

第一步、地址组的添加与管理

在路由器管理界面，点击“行为管控 >> 地址管理”，点击<新增>,填写组名称和对应地址组内包含的 IP 地址段，还可点击图中“+”按钮新增其他地址段，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，还可以勾选条目进行批量删除。



第二步、地址组的使用

在行为管控相关功能的“受管理 IP 地址组”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>，点击受管理 IP 地址组的下拉选项框，点选第一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。

也可以在"受管理 IP 地址组"的下拉选项框中选择"自定义"，即可以输入想要进行应用控制的 IP 地址段，但是此处仅可添加一个地址段且不能用于其他上网行为管控的设置，远不如第一步中介绍的灵活与便捷。

至此，地址组设置完成，在路由器上进行内网用户的上网行为管控的时候，可以直接针对地址组进行设置。

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。

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。R 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-R479GPE-AC 为例，介绍 R 系列路由器带宽控制的设置方法。

12.2.2 需求介绍

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:

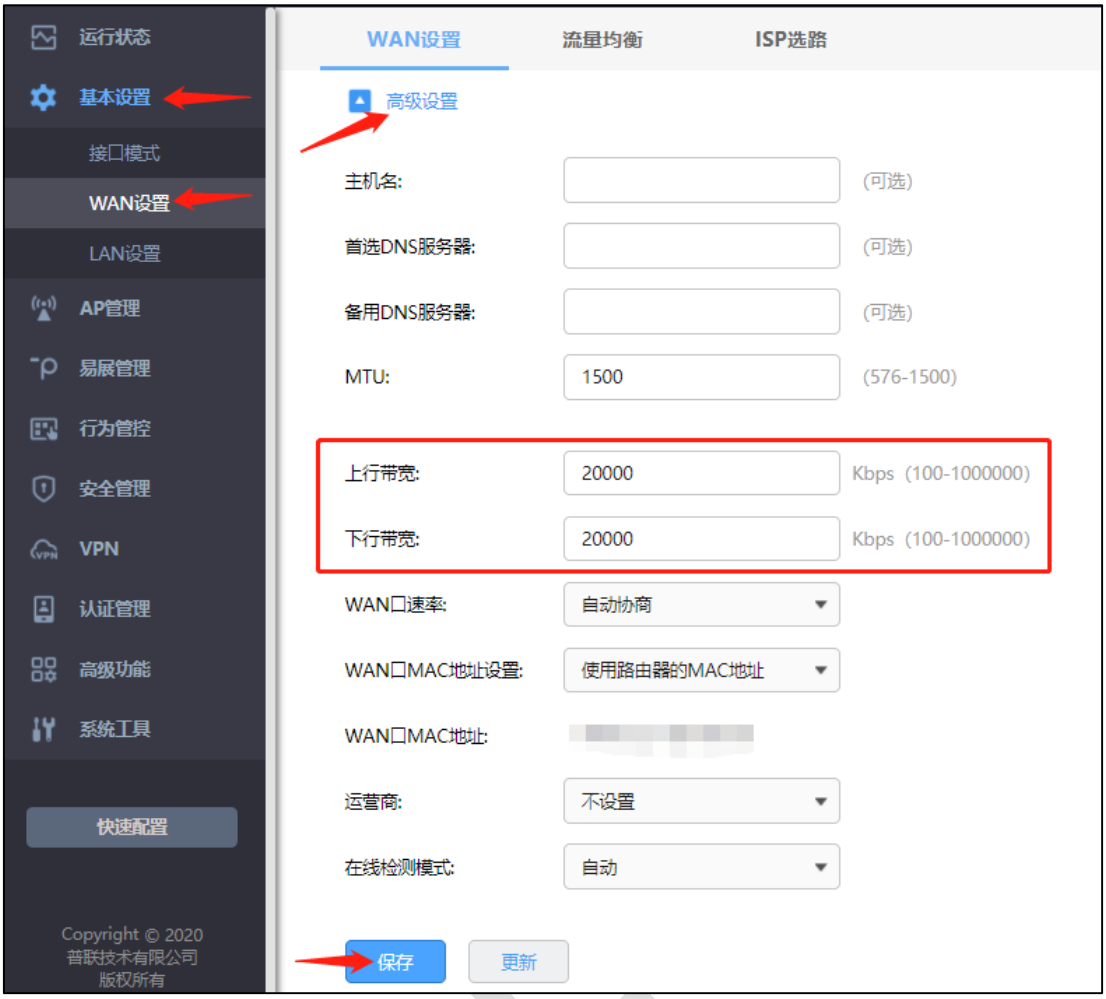
部门	带宽需求	IP 地址段	最大带宽分配
市场部（10 人）	浏览网页、下载内容、需要较大的带宽	192.168.1.10-19	每人 3000Kbps
其他部门（30 人）	浏览网页、收发邮件满足一般上网应用	192.168.1.20-49	每人 1000Kbps

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

第一步、设置接口带宽

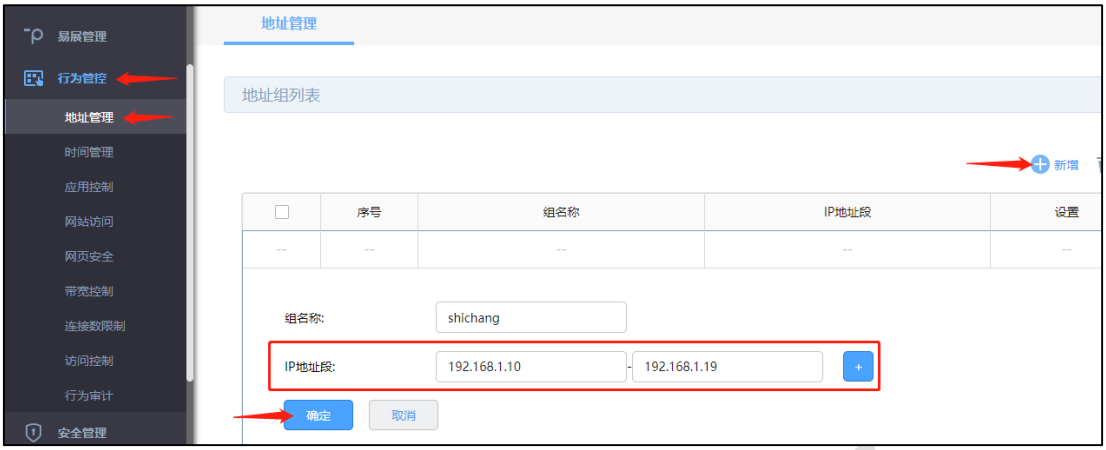
在路由器界面，点击"基本设置 >> WAN 设置"，选择连接外网的 WAN 口，点击<高级设置>，填写宽带线路真实的上行、下行带宽（本例中上下行带宽均为 20Mbps），并点击<保存>。



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

第二步、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"行为管控 >> 地址管理"，点击<新增>，添加如下地址，点击<确定>。



其他部门地址组的添加，也是相同操作。

第三步、设置带宽控制规则

点击“行为管控 >> 带宽限制”，点击<新增>，为市场部设置如下的带宽控制规则：

说明：

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。

第四步、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?

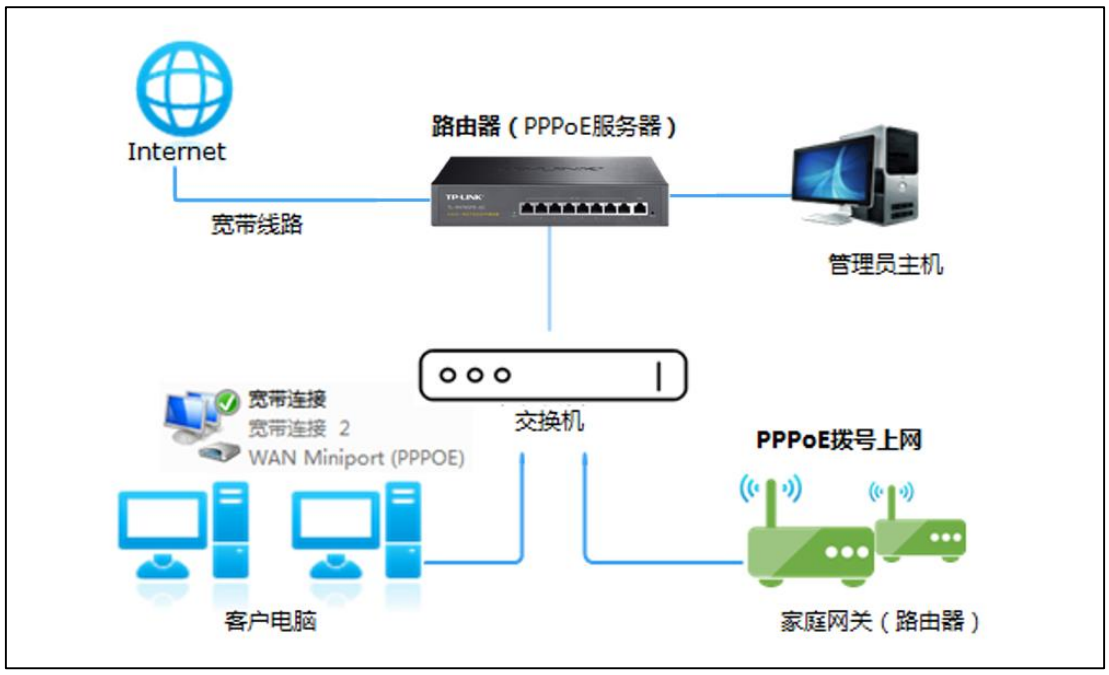
可以。直接在“地址管理”中编辑对应的地址组，并填写要加入的 IP 地址段，最后点击“确定”。

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 需求介绍

某小区宽带服务商使用 TL-R479GPE-AC 作为接口路由器，接入宽带为 500M 光纤，小区有 10 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

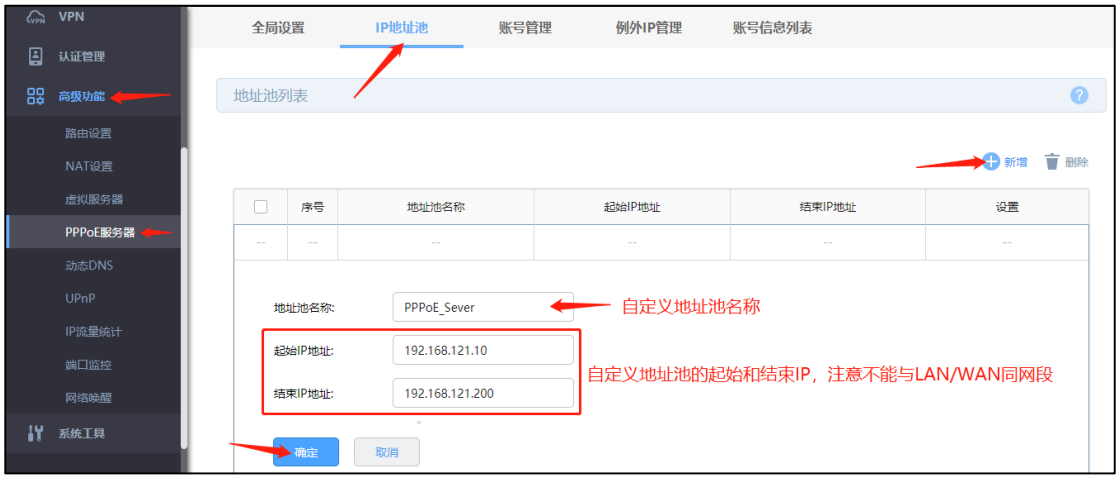
上网，没有账号的用户无法上网，同时宽带服务商的管理主机（192.168.1.2-12）无需拨号即可上网。

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

第一步、设置 IP 地址池

登录路由器管理界面，点击“高级功能 >> PPPoE 服务器 >> 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 WAN 网段相同。

第二步、设置账号

点击“高级功能 >> 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：

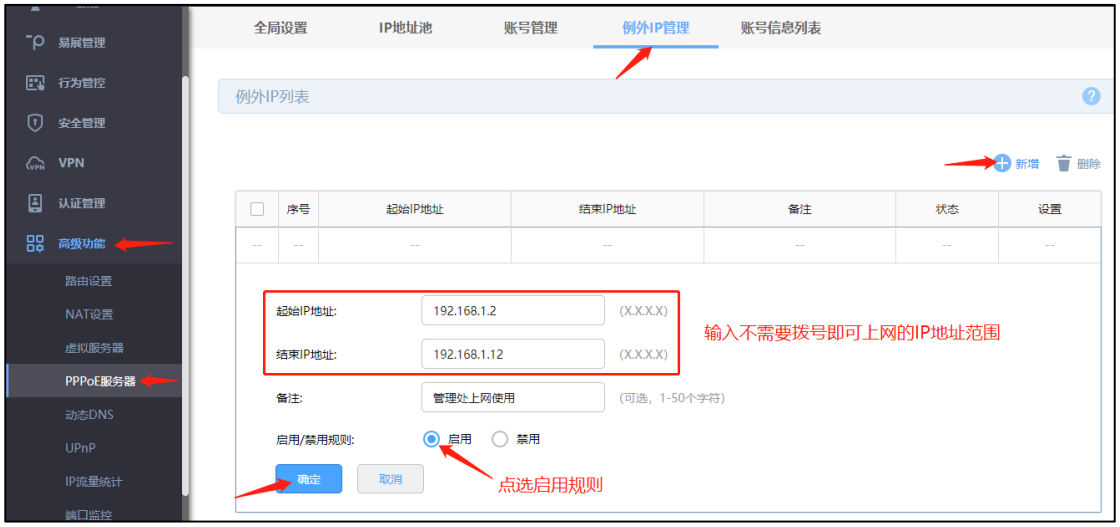
说明：

MAC 绑定方式有三种：

- 不绑定：不进行用户和 MAC 的绑定。
- 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。
- 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。

第三步、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“高级功能 >> 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。

第四步、设置全局设置

点击“高级功能 >> 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<保存>，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“高级功能 >> 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。

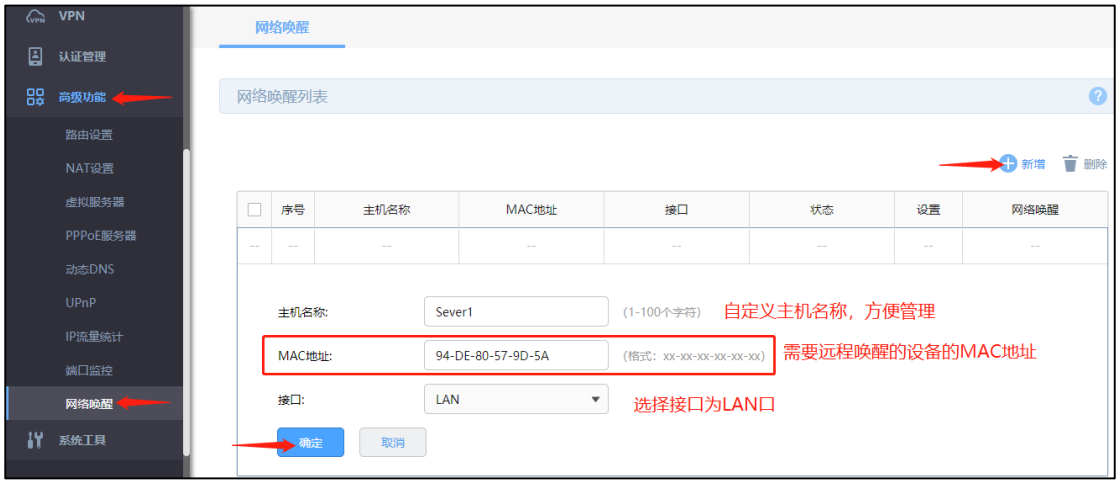
12.4.2 需求介绍

某企业使用 TL-R479GPE-AC，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

第一步、开启网络唤醒

在"高级功能 >> 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>。

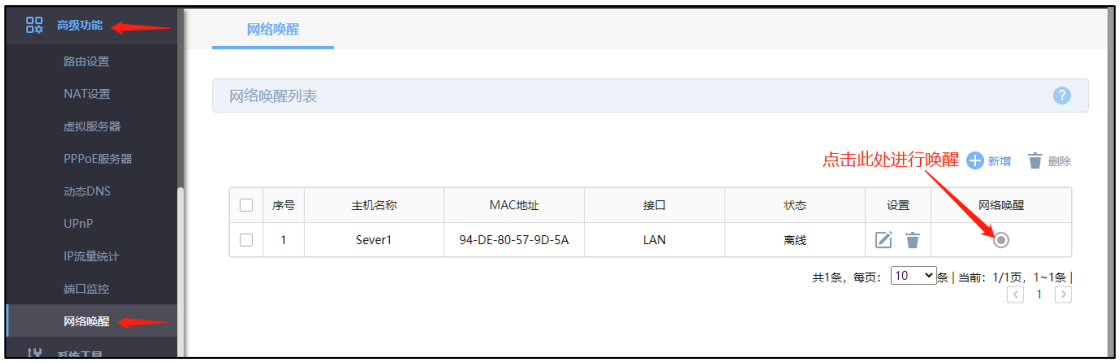


说明：

远程唤醒的是个同一局域网内才可生效的功能，只有 LAN 网段的设备才可以支持唤醒。

第二步、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“高级功能 >> 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 诊断工具使用指南

12.5.1 应用介绍

R 系列路由器的诊断工具包包括两种类型：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-R479GPE-AC 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。

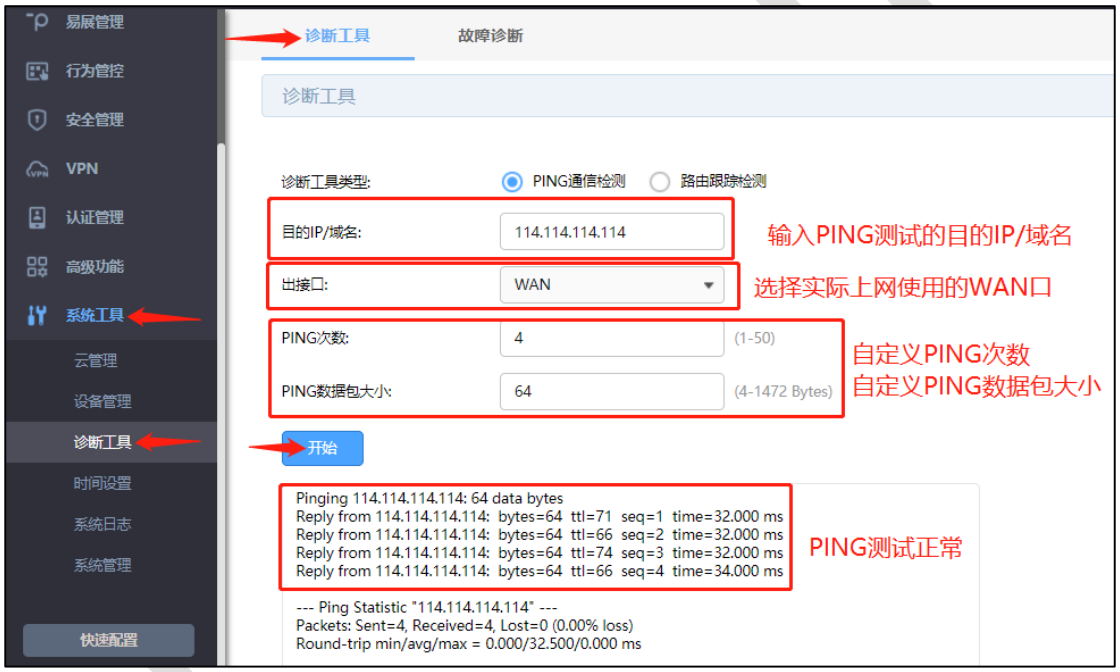
12.5.2 需求介绍

某用户内网无法上外网，希望可以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 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

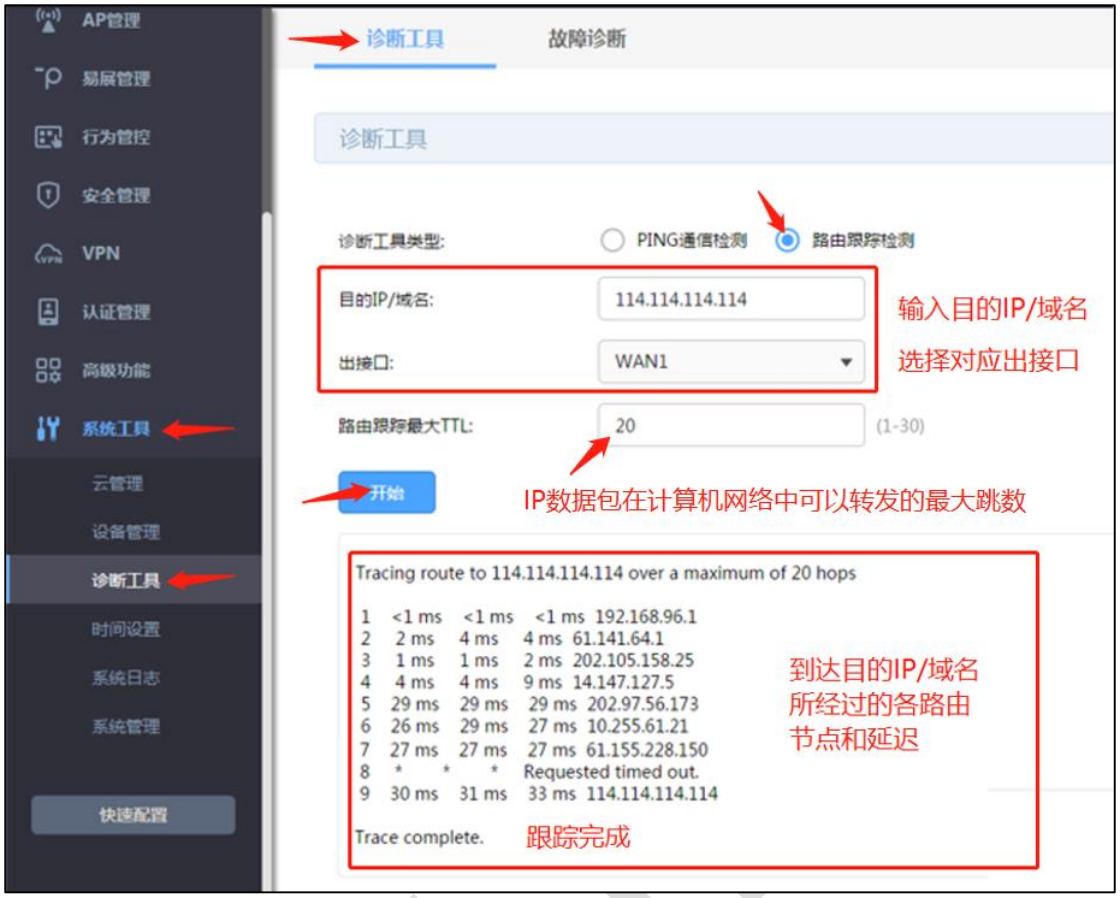
诊断工具类型选择“PING 通信检测”，目的 IP/域名选择常见 DNS 服务器如 114.114.114.114 或者门户网站如 www.qq.com，出接口则选择实际上网使用的 WAN 口，此处因为仅用 WAN1 口上网，所以选择“WAN1”，还可以自定义“PING 次数”（1-50）和“PING 包大小”（4-1472 Bytes），点击<开始>，测试结果如下图所示即为正常，也可以根据测试结果中的 time 判断延迟是否正常。



而当 WAN 口无法 Ping 通目的 IP 和域名，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。

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”，还可以自定义“路由跟踪最大 TTL”（Time To Live，生存时间值），点击<开始>。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。


AP管理
易展管理
行为管控
安全管理
VPN
认证管理
高级功能
系统工具
云管理
设备管理
诊断工具
时间设置
系统日志
系统管理
快速配置
诊断工具
故障诊断
诊断工具
诊断工具类型:
PING通信检测
路由跟踪检测
目的IP/域名:
114.114.114.114
输入目的IP/域名
出接口:
WAN1
选择对应出接口
路由跟踪最大TTL:
20
(1-30)
开始
IP数据包在计算机网络中可以转发的最大跳数
Tracing route to 114.114.114.114 over a maximum of 20 hops
1 <1 ms <1 ms <1 ms 192.168.96.1
2 2 ms 4 ms 4 ms 61.141.64.1
3 1 ms 1 ms 2 ms 202.105.158.25
4 4 ms 4 ms 9 ms 14.147.127.5
5 29 ms 29 ms 29 ms 202.97.56.173
6 26 ms 29 ms 27 ms 10.255.61.21
7 27 ms 27 ms 27 ms 61.155.228.150
8 * * * Requested timed out.
9 30 ms 31 ms 33 ms 114.114.114.114
Trace complete.
跟踪完成
到达目的IP/域名
所经过的各路由
节点和延迟