企业级路由器

Web 配置指南

声明

前言

感谢选择腾达产品。开始使用本产品前，请先阅读本指南。

约定

本说明书适用于 Tenda 企业级路由器 G0-8G-PoE 产品。文中涉及的“路由器”、“企业级路由器”均指企业级路由器。如无特别说明。

文中使用的产品 Web 管理页面截图、IP 地址等数据信息均为举例说明，具体请以实际为准。

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
按钮	边框+底纹	点击 确定 。
窗口	【】	在【添加】窗口。

本文可能用到的标识说明如下。

标识	含义
	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
	表示对配置操作进行补充与说明。

相关资料获取方式

访问 Tenda 官方网站 www.tenda.com.cn，搜索对应产品型号，可获取最新的产品资料。

产品资料一览表

文档名称	描述
产品彩页	帮助您了解路由器的基本参数。包括产品概述、产品卖点、产品规格等。
快速安装指南	帮助您快速设置路由器联网。包括路由器的上网设置指导、指示灯/接口/按钮说明、常见问题解答、保修条款等。
Web 配置指南	帮助您了解路由器的更多功能配置。包括路由器 Web 界面上的所有功能介绍。

技术支持

如需了解更多信息，请通过以下方式与我们联系。

腾达官方网站：www.tenda.com.cn

热线：400-6622-666

邮箱：tenda@tenda.com.cn

腾达微信公众号

腾达官方微博

修订记录

版本号	发布日期	修订内容
V1.0	2022-01-05	首次发行。

目录

1 登录 Web 管理界面

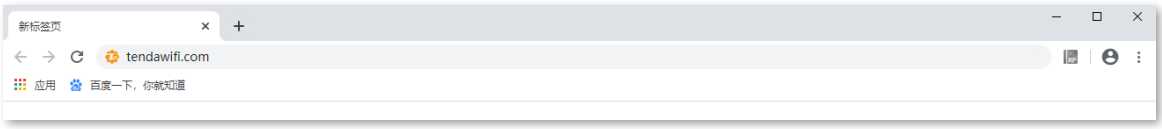
1.1 登录

如果您是首次使用路由器或已将路由器恢复出厂设置，请参考相应型号路由器的快速安装指南（前往 www.tenda.com.cn 可下载快速安装指南）。否则，请参考下文。

步骤 1 用网线将管理电脑接到路由器的任一内网接口（LAN 口）。

步骤 2 设置电脑的本地连接为“自动获得 IP 地址，自动获得 DNS 服务器地址”。

步骤 3 打开电脑上的浏览器（如 IE），访问路由器的管理地址“tendawifi.com”，进入路由器的登录页面。



步骤 4 输入登录密码，点击 登录 。

----完成

提示

- 用户首次设置路由器时，系统默认会将无线密码同步设置为登录密码。如果您无法确定是否设置过登录密码，请输入无线密码尝试登录。
- 如果还是不行，请将路由器恢复出厂设置后，重新尝试。注意，恢复出厂设置后需要重新路由器联网。恢复出厂设置方法：路由器 SYS 灯闪烁状态下，用尖状物按住机身前面板上的复位按钮（Reset）约 8 秒，待指示灯全亮时松开。当 SYS 灯重新闪烁时，路由器恢复出厂设置成功。

成功登录路由器管理页面。

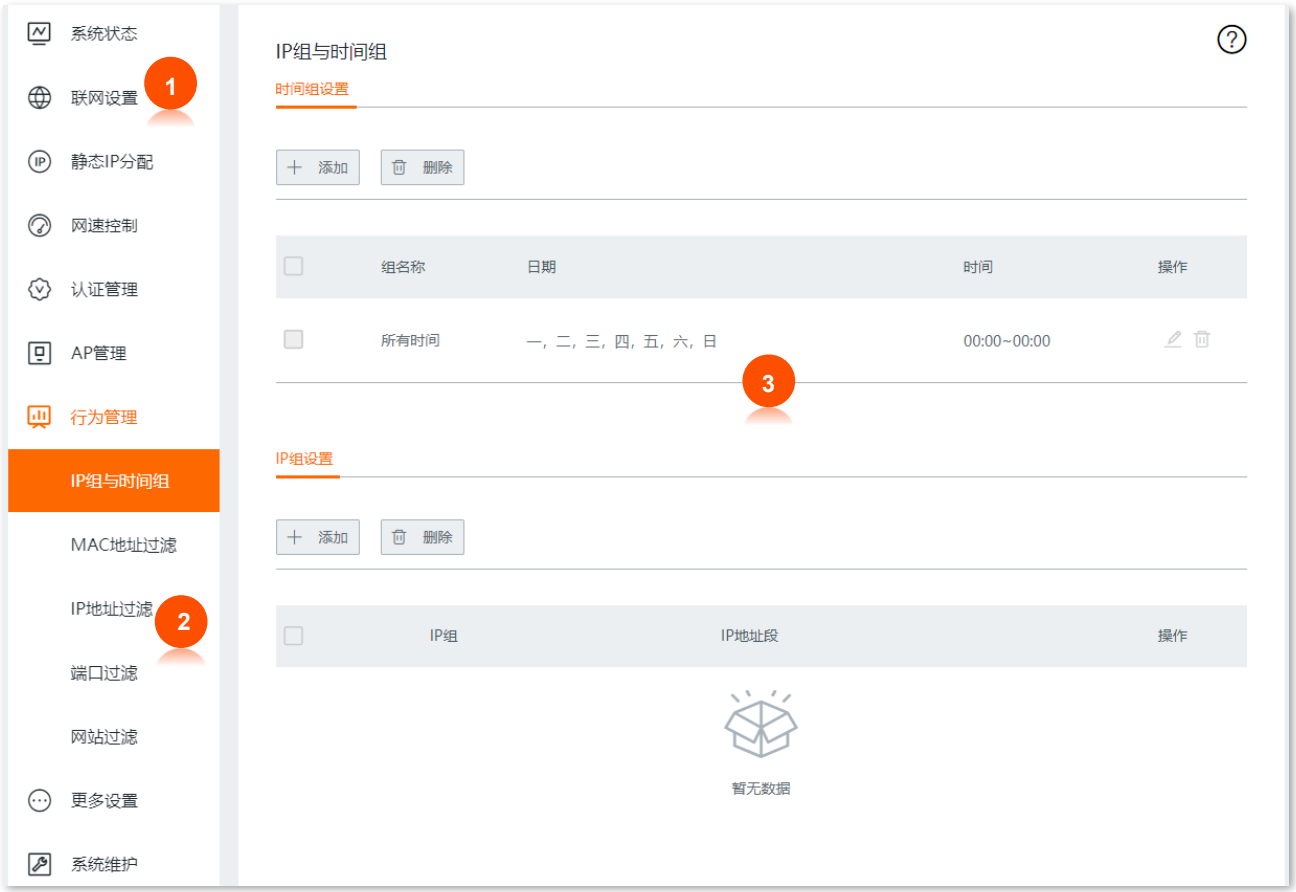
1.2 退出登录

您登录到路由器的管理页面后，如果在 20 分钟内没有任何操作，系统将自动退出登录。此外，在管理页面上，点击右上角的 退出 ，也可以安全地退出管理页面。

2 Web 界面简介

2.1 页面布局

路由器的管理页面共分为：一级导航栏、二级导航栏和配置区三部分。如下图所示。



提示

管理页面上显示为灰色的功能或参数，表示路由器不支持或在当前配置下不可修改。

序号	名称	说明
1	一级导航栏	以导航树的形式组织路由器的功能菜单。用户在导航栏中可以方便地选择功能菜单，选择结果显示在配置区。
2	二级导航栏	
3	配置区	用户进行配置或查看配置的区域。

2.2 常用元素

路由器管理页面中常用元素的功能介绍如下表。

常用元素	说明
保存	用于保存当前页面配置，并使配置生效。
取消	用于取消当前页面未保存的配置，并恢复到修改前的配置。
刷新	用于刷新当前的页面信息。
	用于查看当前页面设置的帮助信息。

3 系统状态

在路由器的「系统状态」模块，您可以：

- 查看连线状态及系统状态
- 查看流量统计
- 管理在线用户
- 添加/移出黑名单
- 管理在线 AP

3.1 查看连线状态及系统状态

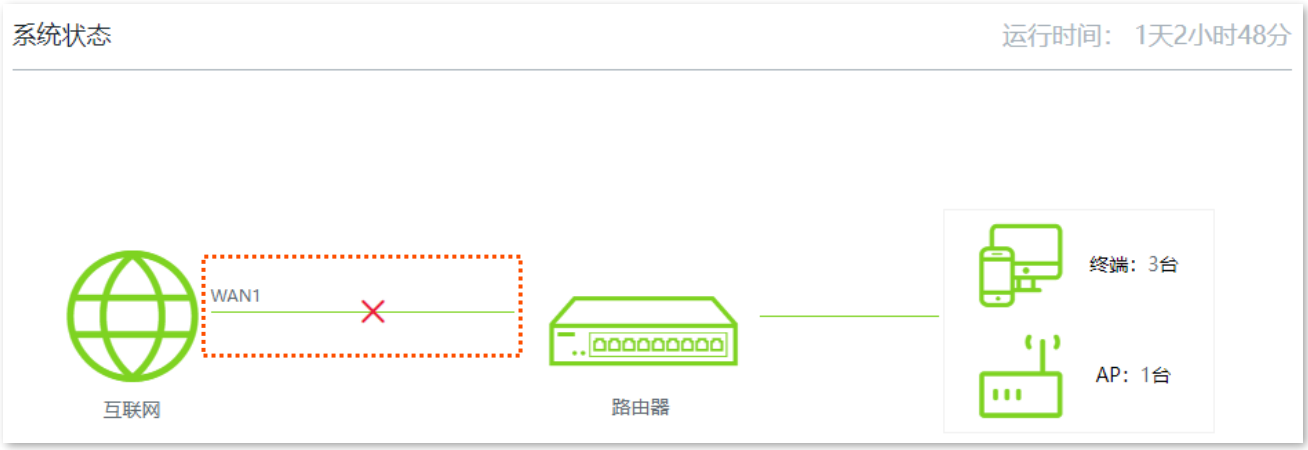
进入页面：点击「系统状态」。

在这里，您可以查看路由器的物理连线是否正常，也可以查看路由器系统状态。

3.1.1 查看连线状态

当“互联网”与“路由器”之间线路正常，如下图示，则表示对应 WAN 口网线连接正常。

当“互联网”与“路由器”之间线路打叉，如下图示，则表示对应 WAN 口网线连接异常，请检查并接好该 WAN 口网线。



3.1.2 查看系统状态

点击“系统状态”页面的路由器图标可以查看路由器的运行状态、LAN 口状态和 WAN 口联网信息。

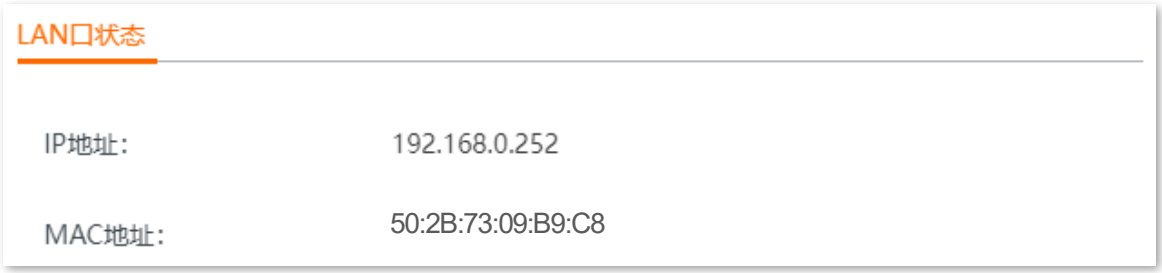
在“运行状态”模块，您可以查看路由器的系统时间、运行时间、软件版本等信息。

参数说明

标题项	说明
系统时间	路由器当前的系统时间。

标题项	说明
运行时间	路由器最近一次启动后连续运行的时长。
软件版本	路由器系统软件的版本号。
设备名称	路由器的名称。
CPU 使用率	路由器当前的 CPU 使用率。
内存使用率	路由器当前的内存使用率。

在“LAN 口状态”模块，您可以查看路由器的 LAN 口 IP 地址和 MAC 地址。



在“WAN 口联网信息”模块，您可以查看路由器当前所有 WAN 口的联网方式、接口连接状态、IP 地址等信息。

参数说明

标题项	说明
联网方式	对应 WAN 口的联网方式。
状态	对应 WAN 口的网线连接状态。
IP 地址	对应 WAN 口的 IP 地址。
子网掩码	对应 WAN 口的子网掩码。
默认网关	对应 WAN 口的网关地址。
首选 DNS	对应 WAN 口的首选/备用 DNS 服务器地址。
备用 DNS	
上传速率	对应 WAN 口的上传/下载速率。
下载速率	

3.2 查看流量统计

进入页面：点击「系统状态」，然后点击“更多统计”。

在这里，您可以查看路由器 WAN 口的上传和下载流量动态图，也可以了解局域网某个用户的基本信息，如上传/下载速率，在线时长等。

参数说明

标题项	说明
主机名称	用户设备的基本信息，包括用户设备上报的设备名称、连接到路由器的方式、IP 地址和 MAC 地址。
并发连接数	用户的并发连接数。
上传速率	用户当前的上传/下载速率。
下载速率	
下载总流量	用户下载数据的总量。
在线时长	用户的在线时长。

3.3 管理在线用户

进入页面：点击「系统状态」。

在这里，您可以查看或管理局域网内网速最高的 5 台终端，也可以点击“终端”查看或管理所有的在线终端。

管理所有在线用户时，您可以在搜索栏基于主机名称、IP 地址、MAC 地址、频段快速筛选相关用户信息。

3.4 添加/移出黑名单

进入页面：点击「系统状态」。

在这里，您可以添加/移出黑名单。

3.4.1 添加黑名单

加入黑名单的设备，不能通过路由器上网。

将网速排在前五的设备加入黑名单：

步骤 1 在“系统状态”页面找到要加入黑名单的设备。

步骤 2 点击 禁止上网 。

----完成

在“系统状态”页面点击，然后点击**黑名单**，进入“黑名单”列表，可以查看黑名单设备。

将其它在线设备加入黑名单：

步骤 1 在“系统状态”页面点击，进入“网速控制与黑名单”页面。

步骤 2 在“在线设备”列表中找到要加入黑名单的设备，点击 禁止上网 。

----完成

在“系统状态”页面点击，然后点击**黑名单**，进入“黑名单”列表，可以查看黑名单设备。

3.4.2 移出黑名单

如果需要将设备从黑名单中移出，可在“黑名单”页面设置。

设置步骤：

步骤 1 在“系统状态”页面点击，进入“网速控制与黑名单”页面。

步骤 2 点击**黑名单**，进入“黑名单”列表。

步骤 3 找到要移出黑名单的设备，点击 移出 。

----完成

3.5 管理在线 AP

进入页面：点击「系统状态」。

在这里，您可以查看或管理网络中的在线 AP。

如果路由器关闭了 AP 管理功能，您需要先启用 AP 管理功能，才能在此处查看或管理网络中的在线 AP。

查看或管理网络中的在线 AP：

步骤 1 在“系统状态”页面点击 AP 图标。

步骤 2 根据需要查看或管理在线 AP。

界面元素说明

界面元素	说明
跳转到 AP 管理	点击可转到路由器的“AP 管理”页面，对 AP 进行管理，详情请参考 AP 管理。
	点击可跳转到 AP 的管理页面。例如：AP 的型号为 i21V1.0，点击，即可跳转到 i21V1.0 的管理页面。

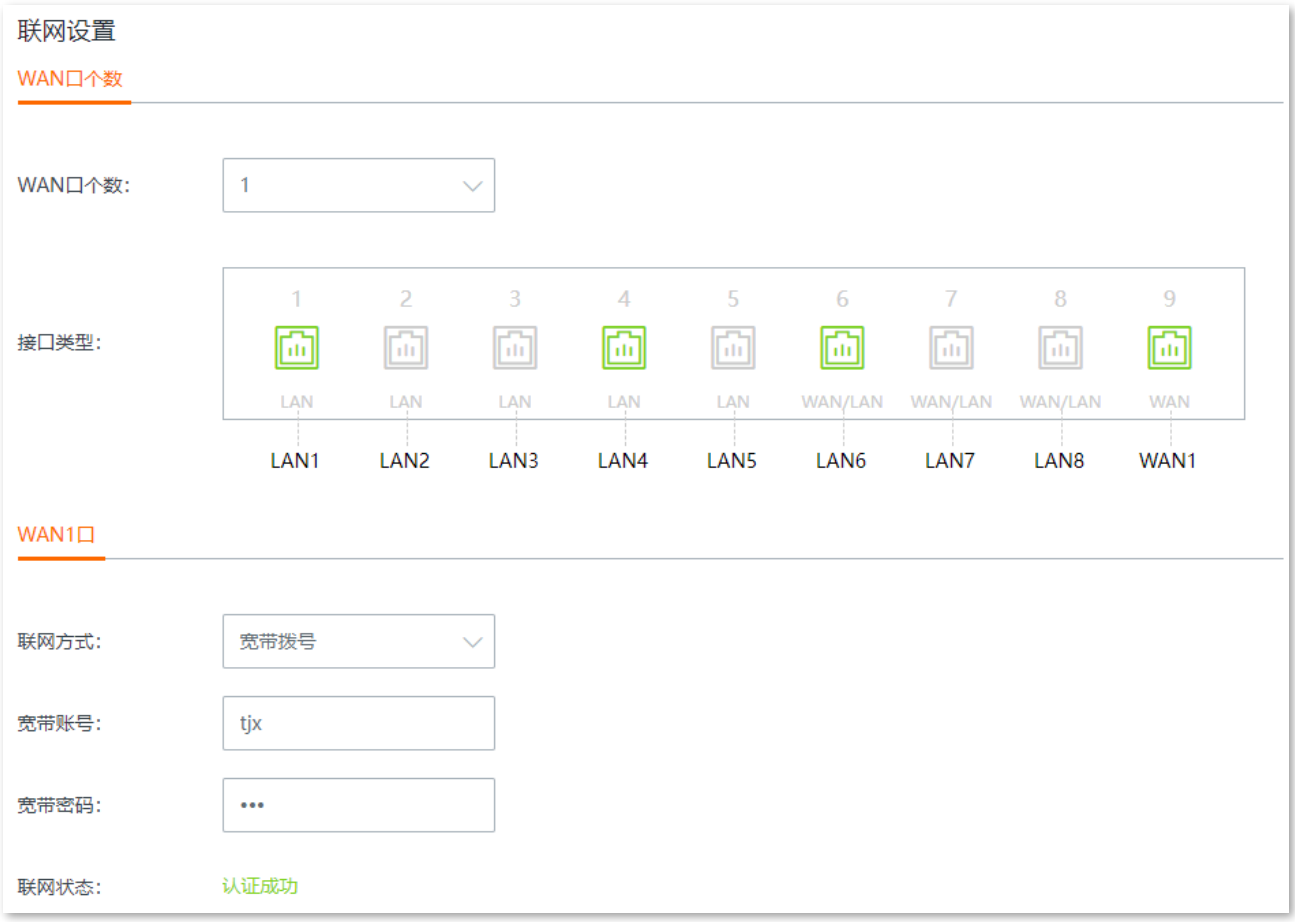
4 联网设置

4.1 概述

通过联网设置，可以实现局域网内的多台设备共享您办理的宽带服务上网。

首次使用路由器或将路由器恢复出厂设置后，请根据设置向导完成联网设置。之后，如果要修改或设置更多联网参数，可在本模块设置。

进入页面：点击「联网设置」。



参数说明

标题项	说明
WAN 口个数	路由器 WAN 口的个数，默认的 WAN 口个数为 1。可以根据需要修改 WAN 口个数。
接口类型	路由器接口的类型。  ：表示接口连接正常。：表示接口未连接设备或连接异常。
联网方式	路由器的联网方式，支持宽带拨号、静态 IP、动态 IP。 - 宽带拨号：路由器使用 ISP（互联网服务提供商）提供的宽带账号和密码拨号上网。 - 静态 IP：路由器使用 ISP 提供的固定 IP 地址、子网掩码、默认网关、DNS 服务器信息上网。 - 动态 IP：路由器使用 ISP 动态分配的 IP 地址信息上网。
宽带账号 宽带密码	联网方式为“宽带拨号”时，输入 ISP 提供的宽带账号和密码。
IP 地址 子网掩码 默认网关 首选 DNS 备用 DNS	联网方式为“静态 IP”时，在对应栏输入 ISP 提供的固定 IP 地址信息。 提示 如果 ISP 只提供一个 DNS 地址，“备用 DNS”可以不填。
联网状态	显示路由器 WAN 口的连接状态。 - 已联网：路由器 WAN 口已插网线，并已经获得 IP 地址信息。 - 认证成功：路由器拨号成功，并已经获得 IP 地址信息。 - 连接中...：路由器正在连接到上级网络设备。 - 未连接：未连接或连接失败，请检查网线连接状态、联网信息设置或咨询相应的 ISP。 如果显示其他状态信息，请根据联网状态提示信息采取相应措施。

4.2 设置联网

提示

- 路由器默认提供 1 个 WAN 口，即 WAN1。下文以 WAN1 设置为例，其他 WAN 口的设置与 WAN1 方法类似。
- 各上网参数均由 ISP 提供，如不清楚，请咨询您的 ISP。

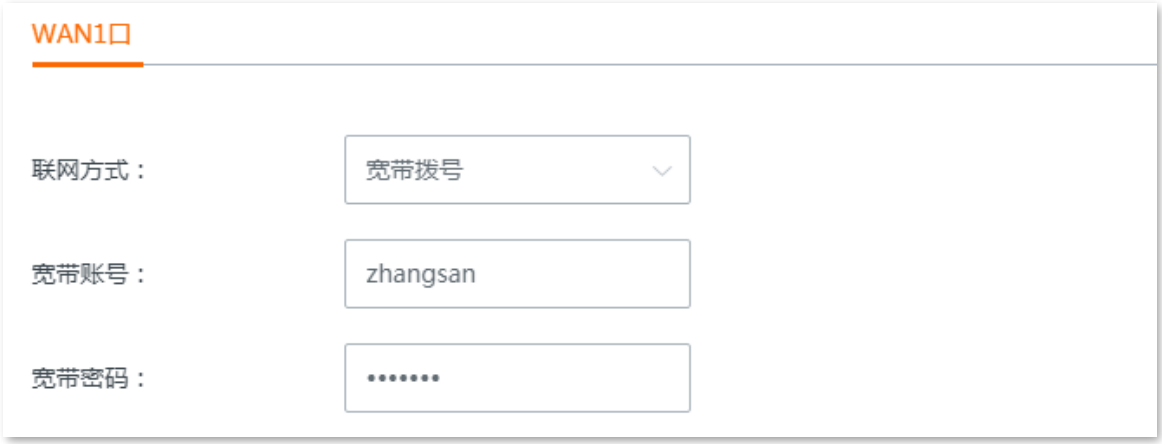
4.2.1 宽带拨号

步骤 1 点击「联网设置」。

步骤 2 选择“联网方式”为“宽带拨号”。

步骤 3 输入 ISP 提供的“宽带账号”和“宽带密码”。

步骤 4 点击页面底端的 保存 。



----完成

稍等片刻，当联网状态显示“认证成功”时，您可以尝试上网了。

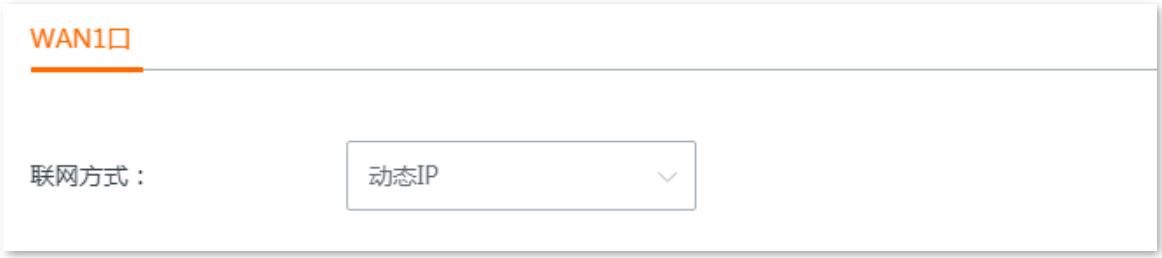
如果您不能上网，可以进入「更多设置」>「WAN 口参数」页面，尝试修改 WAN 口参数解决问题。

4.2.2 动态 IP

步骤 1 点击「联网设置」。

步骤 2 选择“联网方式”为“动态 IP”。

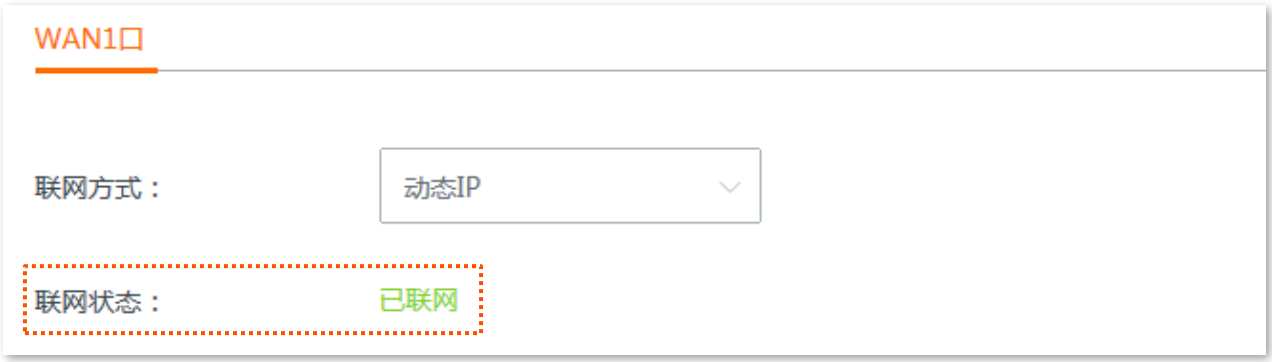
步骤 3 点击页面底端的 保存 。



----完成

稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。

如果您不能上网，可以进入「更多设置」>「WAN 口参数」页面，尝试修改 WAN 口参数解决问题。



4.2.3 静态 IP

步骤 1 点击「联网设置」。

步骤 2 选择“联网方式”为“静态 IP”。

步骤 3 输入 ISP 提供的“IP 地址”、“子网掩码”、“默认网关”和“首选/备用 DNS”。

步骤 4 点击页面底端的 保存 。

----完成

稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。

如果您不能上网，可以进入「更多设置」>「WAN 口参数」页面，尝试修改 WAN 口参数解决问题。

5 静态 IP 分配

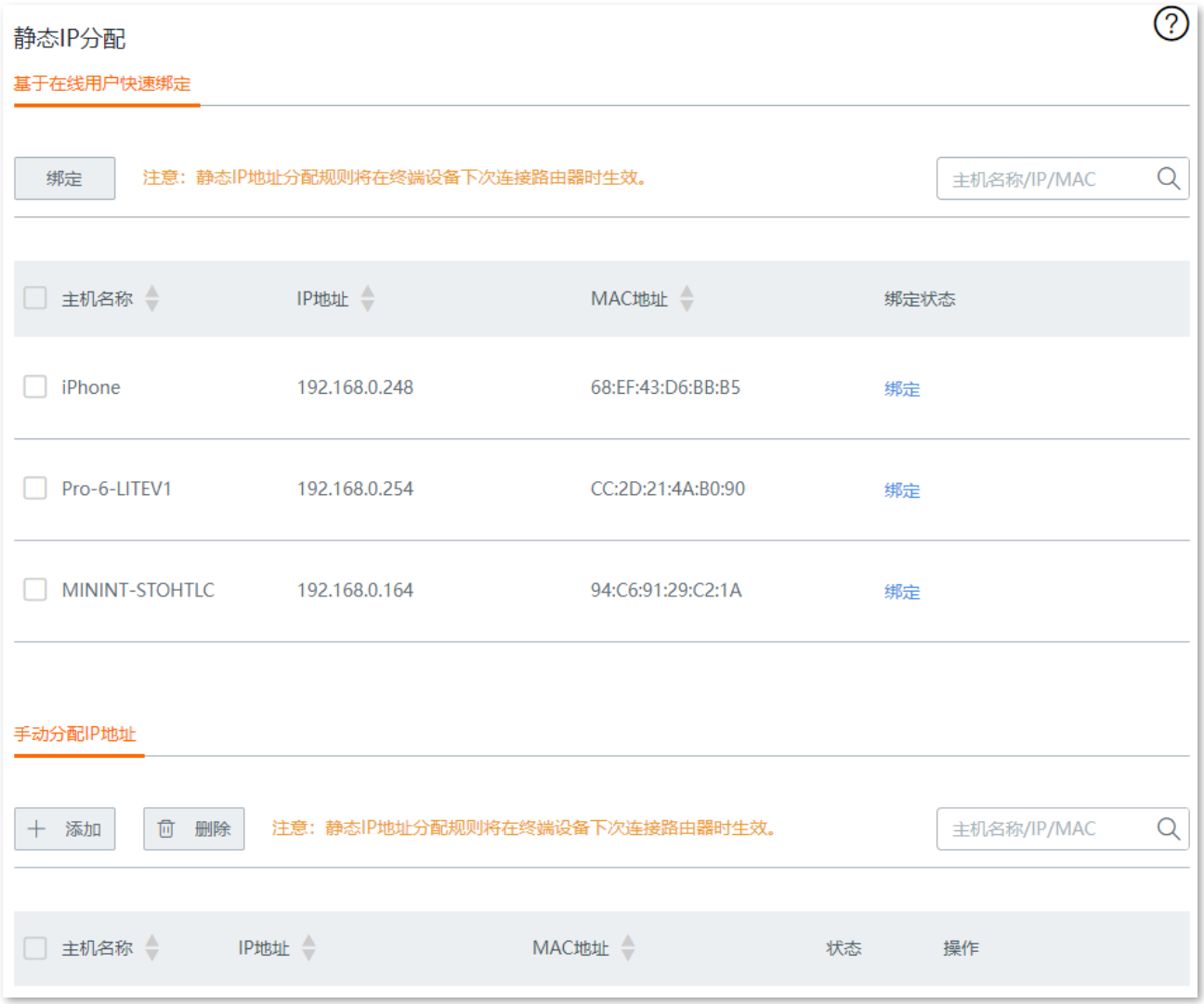
5.1 概述

通过静态 IP 分配功能，您可以让指定客户端始终获得预设的 IP 地址，避免“行为管理”、“网速控制”、“端口映射”等基于 IP 地址生效的功能因客户端 IP 地址变化而失效。

本功能仅在路由器“DHCP 服务器”功能开启时生效。路由器支持以下两种静态 IP 地址分配方式：

- 基于在线用户快速绑定：可以查看从路由器 DHCP 服务器自动获取 IP 地址的客户端信息，并一键绑定客户端，使 DHCP 服务器始终给同一客户端分配固定的 IP 地址。
- 手动分配 IP 地址：可以手动绑定客户端，使 DHCP 服务器始终给同一客户端分配固定的 IP 地址。

进入页面：点击「静态 IP 分配」。



参数说明

标题项		说明
基于在线用户快速绑定	绑定	将选中的客户端都进行 IP 地址、MAC 地址绑定。
	主机名称	客户端的名称。
	IP 地址	客户端的 IP 地址。
	MAC 地址	客户端的 MAC 地址。
	绑定状态	点击绑定即可一键绑定客户端 IP 地址、MAC 地址，使客户端始终获取规则对应的 IP 地址。绑定成功后将显示“已绑定”。
手动分配 IP 地址	主机名称	客户端的名称或静态 IP 分配规则的备注信息。
	IP 地址	为对应 MAC 地址的客户端预留的 IP 地址。
	MAC 地址	客户端的 MAC 地址。
	状态	规则的状态，可根据需要开启或关闭。
	操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
	导出静态 IP 地址分配表	可将静态 IP 地址分配表备份到本地电脑。
	导入静态 IP 地址分配表	可将之前备份的静态 IP 地址分配表文件导入到路由器。

5.2 分配静态 IP 地址

如果要给已连接到路由器的客户端分配 IP 地址，推荐在“基于在线用户快速绑定”模块进行设置。客户端未连接到路由器时，请在“手动分配 IP 地址”模块进行设置。

5.2.1 基于在线用户快速绑定

绑定单个客户端的 IP 地址

步骤 1 点击「静态 IP 分配」，找到“基于在线用户快速绑定”模块。

步骤 2 在“基于在线用户快速绑定”列表，找到要分配固定 IP 地址的客户端，点击绑定。

----完成

绑定成功后，您可以在「静态 IP 分配」的“手动分配 IP 地址”模块查看到已添加的规则。如下图示例。规则将在客户端下一次请求 IP 地址时生效。

同时绑定多个客户端的 IP 地址

步骤 1 点击「静态 IP 分配」，找到“基于在线用户快速绑定”模块。

步骤 2 在“基于在线用户快速绑定”列表，选择多个要分配固定 IP 地址的客户端。

步骤 3 点击 绑定 。

----完成

绑定成功后，您可以在「静态 IP 分配」的“手动分配 IP 地址”模块查看到已添加的规则。如下图示例。规则将在客户端下一次请求 IP 地址时生效。

5.2.2 手动分配 IP 地址

设置步骤：

步骤 1 点击「静态 IP 分配」，找到“手动分配 IP 地址”模块。

步骤 2 点击 +添加 。

步骤 3 在【添加】窗口配置各项参数，然后点击 保存 。

提示

点击 + 可以新增一条规则；点击 − 可以删除未保存的规则。

----完成

规则添加成功后，您可以在「静态 IP 分配」的“手动分配 IP 地址”模块查看到已添加的规则。如下图示例。规则将在客户端下一次请求 IP 地址时生效。

6 网速控制

6.1 概述

通过网速控制功能，网络管理员可以对用户的网速进行限制，使有限的带宽资源得到合理分配。

进入页面：点击「网速控制」。

参数说明

标题项		说明
WAN 口带宽	上传速率 下载速率	需填入所办理的宽带的带宽值。不清楚时，可以咨询您的 ISP。
限速方式	不限速	不对局域网用户的上传/下载速率进行限制。
	自定义限速	网络管理员根据实际环境需要，为连接到路由器的用户单独设置最大上传/下载速率，或统一设置最大上传/下载速率。 相较于分组限速来说，自定义限速设置更加灵活。
	自动分配网速	路由器根据「网速控制」页面设置的 WAN 口上传/下载速率，平均地给局域网用户分配带宽。
	分组限速	网络管理员根据实际环境需要，通过分组进行网速控制。控制指定 IP 组内的用户在指定时间组内共享或独享所设置的上传/下载速率，并设置单台设备并发连接数。

6.2 自定义限速

假设要为连接到路由器的用户单独设置最大上传/下载速率。

设置步骤：

步骤 1 点击「网速控制」。

步骤 2 选择“限速方式”为“自定义限速”。

步骤 3 根据需要选择“在线设备”或“离线设备”。

步骤 4 设置对应主机的最大上传/下载速率。

步骤 5 点击页面底端的 保存 。

----完成

参数说明

标题项	说明
主机名称	用户设备名称，可根据需要修改。
下载总流量	该用户下载数据的总量。
离线时间	该用户的离线时间。
上传速率	该用户的实时上传/下载速率。
下载速率	

标题项	说明
最大上传速率	限定该用户使用的最大上传/下载速率。
最大下载速率	

假设要为局域网所有在线用户或离线用户统一设置最大上传/下载速率。

设置步骤：

步骤 1 点击「网速控制」。

步骤 2 选择“限速方式”为“自定义限速”。

步骤 3 根据需要选择“在线设备”或“离线设备”，图示以在线设备为例进行说明。

步骤 4 点击 全部限速 。

步骤 5 为局域网所有的在线用户或离线用户设置最大上传速率和下载速率，图示以在线设备为例进行说明，然后点击 保存 。

----完成

6.3 自动分配网速

为连接到路由器的在线用户平均分配网速。

设置步骤：

步骤 1 点击「网速控制」。

步骤 2 根据 ISP 提供的带宽，设置对应 WAN 口的上传速率和下载速率。

步骤 3 选择“限速方式”为“自动分配网速”。

步骤 4 点击页面底端的 保存 。

----完成

6.4 分组限速

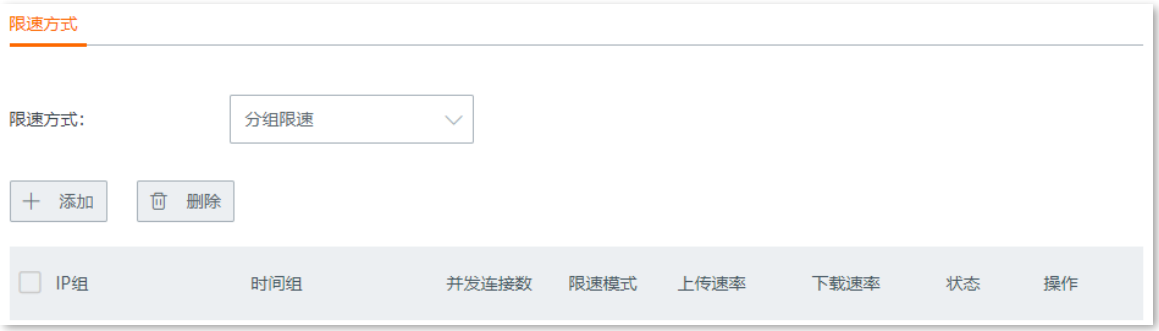
通过分组限速功能，使 IP 组内的用户在一段时间内共享或独享所设置的上传/下载速率。

> 提示
>
> 配置分组限速规则前，请先配置好相应的 IP 组和时间组。

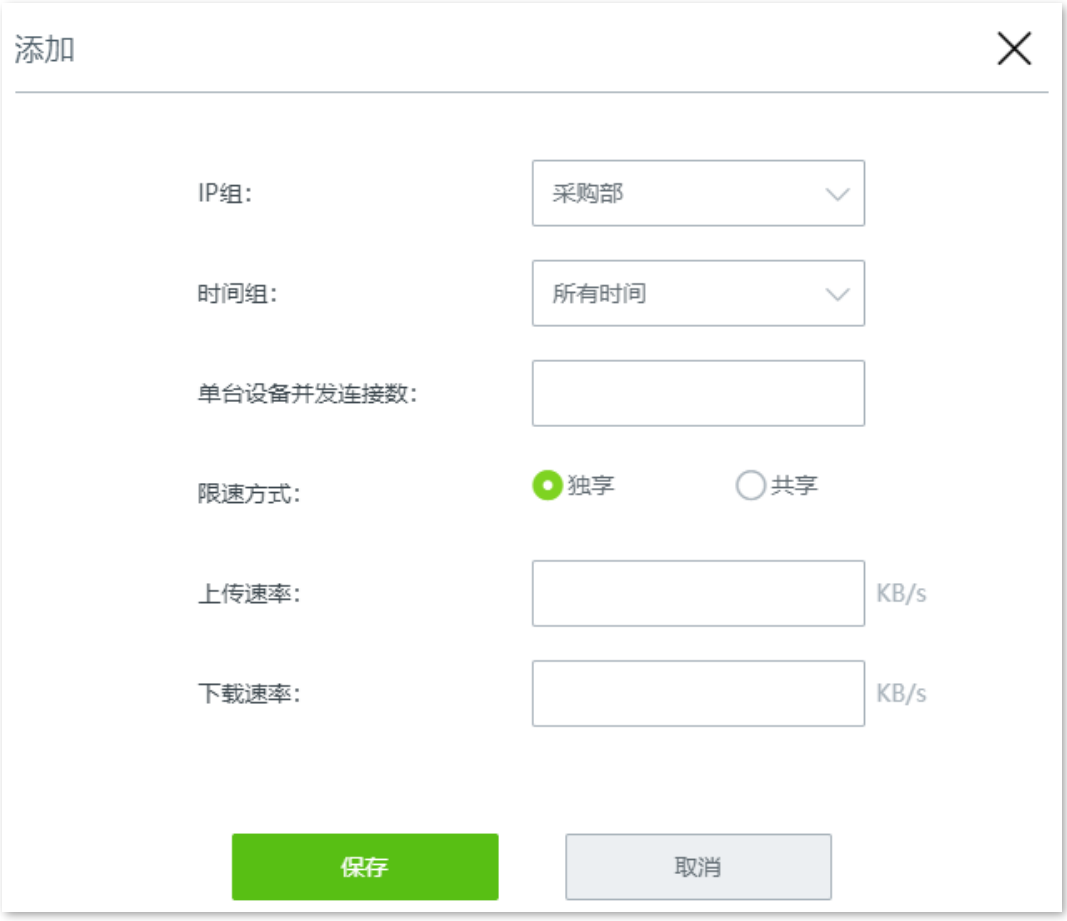
步骤 1 点击「网速控制」。

步骤 2 选择“限速方式”为“分组限速”。

步骤 3 点击 +添加 。



步骤 4 在【添加】窗口配置各项参数，然后点击 保存 。



----完成

成功添加“分组限速”规则后，可以在「网速控制」页面查看到已添加的规则。如下图示例。

参数说明

标题项	说明
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。
时间组	选择引用的时间组，以指定规则的生效时间。时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。
并发连接数（单台设备并发连接数）	受控 IP 地址范围中，每台用户设备所能使用的最大连接数。若无特殊需求，建议设置为 600。
限速模式（限速方式）	设置网速控制的模式。 - 独享：受控 IP 地址范围内的每个用户独享所设置的上传/下载速率。此模式下，每个受控用户所获得的带宽都是一样的。 - 共享：受控 IP 地址范围内的所有用户共享所设置的上传/下载速率。此模式下，每个受控用户所获得的带宽可能不一样。
上传速率 下载速率	限定的最大上传/下载速率。
状态	规则的状态，可根据需要开启或关闭。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。

6.5 分组限速配置举例

组网需求

某企业使用企业级路由器进行网络搭建。

要求：局域网中采购部（IP 地址范围：192.168.0.2~192.168.0.250）的每位员工在星期一到星期五的上班时间（8:00~18:00）都能使用 1Mbps（1Mbps=128KB/s）的固定上下行带宽上网。对于局域网其他设备，不限制带宽。

可以使用路由器网速控制功能中的“分组限速”功能实现上述需求。假设每台用户设备的并发连接数为 600。

配置步骤

配置流程图：

步骤 1 配置时间组。

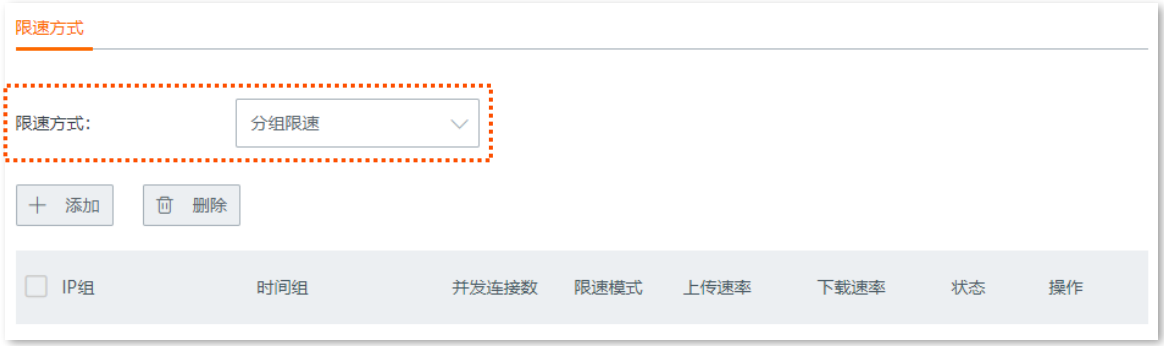
进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

步骤 2 配置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

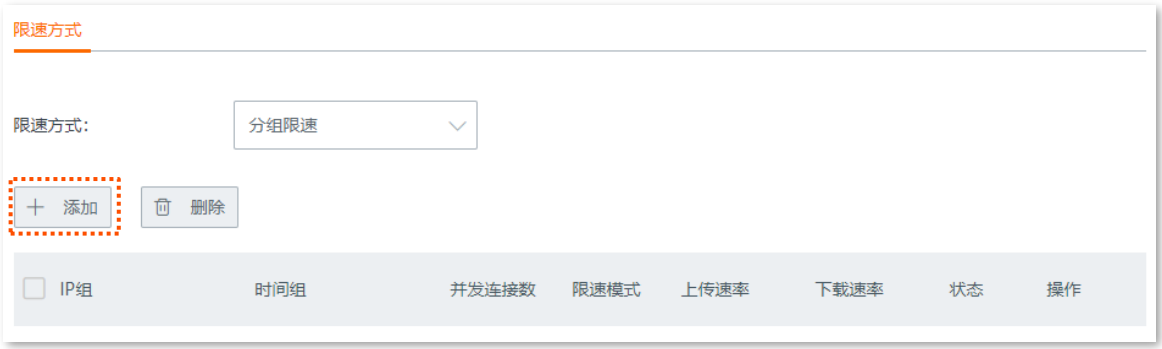
步骤 3 开启分组限速功能。

进入「网速控制」页面，在“限速方式”模块选择“分组限速”，然后点击页面底端的 保存 。



步骤 4 添加分组限速规则。

1. 进入“网速控制”页面，点击 +添加 。



2. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 点击下拉框，选择规则应用的 IP 组，本例为“采购部”。

(2) 点击下拉框，选择规则应用的时间组，本例为“上班时间”。

(3) 设置单个客户端并发连接数，本例为“600”。

(4) 选择限速方式，本例为“独享”。

(5) 设置客户端的最大上传速率和下载速率，本例均为“128KB/s”。

----完成

验证配置

IP 地址在 192.168.0.2~192.168.0.250 范围内的用户，在星期一到星期五的 8:00~18:00 的最大上传速率为 128KB/s，最大下载速率为 128KB/s。

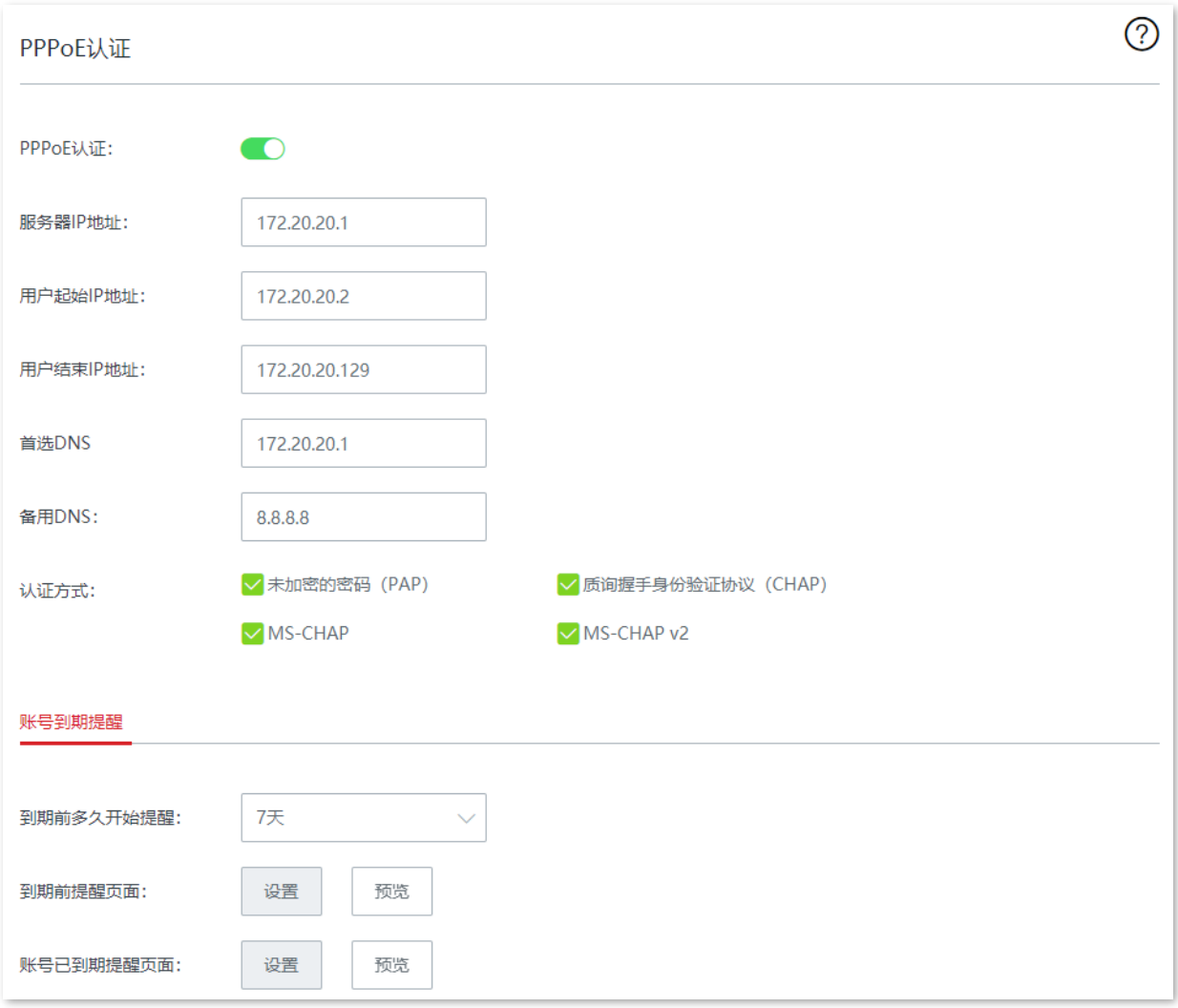
7 认证管理

7.1 PPPoE 认证

默认情况下，路由器接入互联网后，路由器的局域网用户就可以访问互联网了；然而某些商用场景网络（例如：出租房网络、网吧）统一管理需求，需要对上网用户进行认证和计费。本路由器集成了 PPPoE 服务器和计费功能，您可以配置基于 VLAN 接口生效的 PPPoE 认证策略，来对用户的上网行为进行计费和限制。

进入页面：点击「认证管理」>「PPPoE 认证」。

默认情况下，路由器关闭了 PPPoE 认证，开启后，页面显示如下。



参数说明

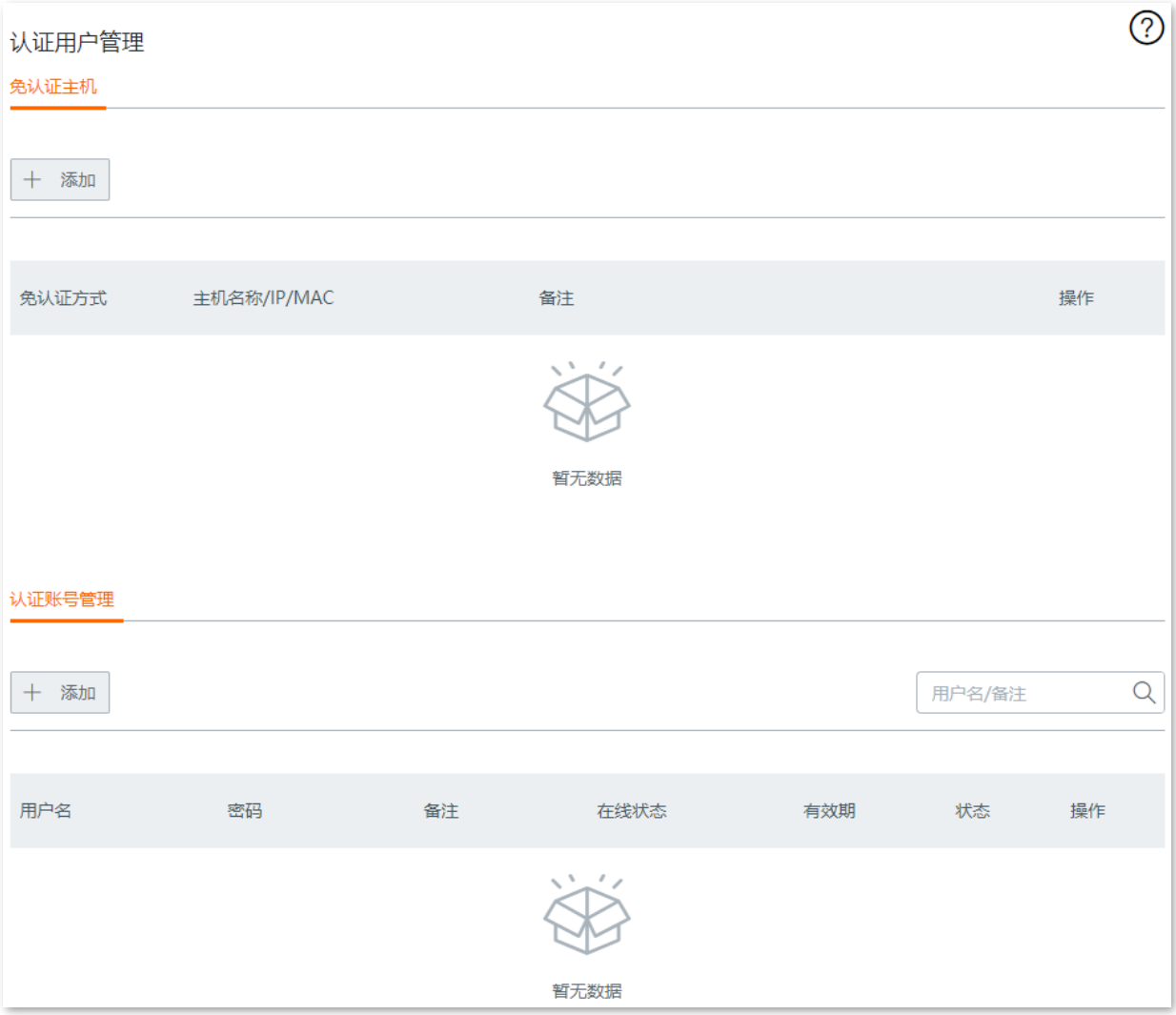
标题项		说明
PPPoE 认证	PPPoE 认证	PPPoE 认证功能开关。表示关闭，  表示开启。
	服务器 IP 地址	PPPoE 服务器的 IP 地址，也是认证客户端的网关地址，不能与路由器的 LAN 口、WAN 口在同一个网段。
	用户起始 IP 地址	认证客户端的地址池，PPPoE 认证服务器可分配给认证客户端的 IP 地址范围。
	用户结束 IP 地址	
	首选 DNS	PPPoE 服务器分配给 PPPoE 客户端的首选/备用 DNS 服务器 IP 地址。
	备用 DNS	 为了使 PPPoE 客户端能够正常上网，请务必确保修改的首选 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。
	认证方式	PPPoE 认证时支持的身份验证方式。 - 未加密的密码（PAP）：客户端以明文的方式传递用户名和密码到 PPPoE 服务器进行身份验证。 - 质询握手身份验证协议（CHAP）：PPPoE 服务器向客户端发送挑战消息，客户端使用密码和挑战信息计算出请求值再次发送给服务器。服务器将请求消息和本地计算出的字符串进行对比，验证客户端的身份。 - MS-CHAP：Microsoft 版本的质询握手身份验证协议（CHAP），支持 Microsoft 点对点加密（MPPE）方式来加密数据。 - MS-CHAP v2：MS-CHAP 的升级版本，要求双向认证，不仅服务器需要验证客户端的身份，客户端也需要验证服务器的身份。  如果网络中存在 Windows NT 或 Windows 98 系统的认证客户端，需勾选 MS-CHAP 和 MS-CHAP v2。
账号到期提醒	到期前多久开始提醒	PPPoE 账号到期提醒时间。
	到期前提醒页面	账号到期前提醒用户的页面。
	账号已到期提醒页面	账号到期时提醒用户的页面。

7.2 认证用户管理

7.2.1 概述

进入页面：点击「认证管理」>「认证用户管理」。

在这里，可以添加免于认证的主机，还可以添加用户进行 PPPoE 认证上网时使用的用户名和密码，以及导出或导入认证账号信息。



参数说明

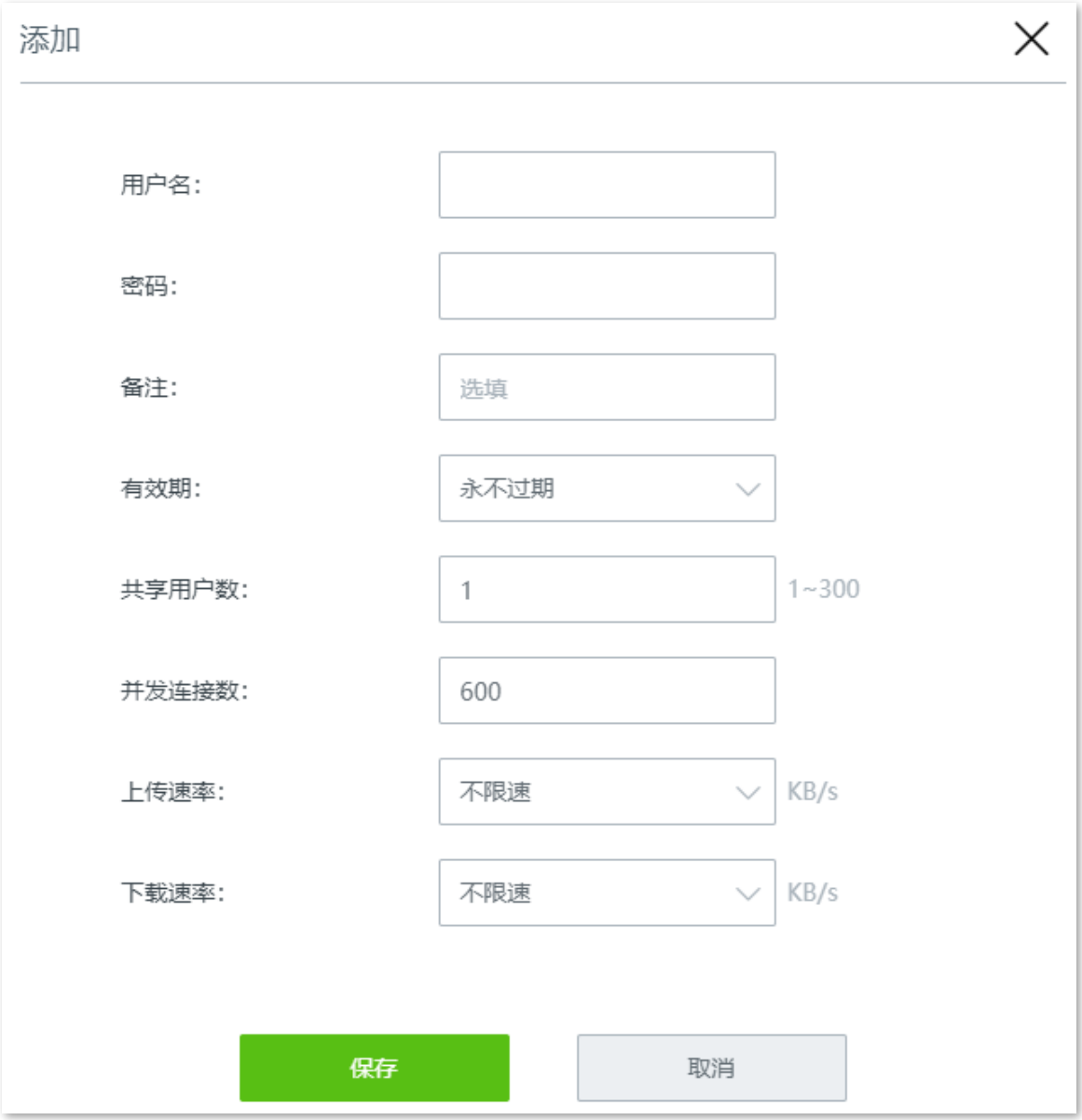
标题项		说明
免认证主机	免认证方式	以何种形式指定免认证主机，本路由器支持主机名称、IP 地址、MAC 地址。
	主机名称/IP/MAC	不需要进行认证的主机信息。 - 当“免认证方式”选择为“主机名称”时，输入不需要进行认证的设备的主机名称。请将「系统状态」页面的主机名称填到此处。如果修改了主机名称，需同步修改此处的主机名称。 - 当“免认证方式”选择为“IP 地址”时，输入不需要进行认证上网的设备的 IP 地址。此时建议到「静态 IP 分配」页面为该设备绑定此 IP 地址，以避免 IP 地址变化导致功能失效。 - 当“免认证方式”选择为“MAC 地址”时，输入不需要进行认证上网的设备的 MAC 地址。
	备注	免于认证的上网设备的描述。
	操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
认证账号管理	用户名	用户认证上网使用的用户名、密码。 开启账号认证功能后，用户上网前，需要先使用此用户名/密码在浏览器页面进行认证。
	密码	
	备注	账号的描述信息。
	在线状态	账号的使用状态。
	有效期	该账号的有效使用时间。过了有效期后，用户不能使用该账号认证上网。
	状态	规则的状态，可根据需要开启或关闭。
	操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
	导出用户账户	将已配置好的认证用户账号数据导出到本地电脑保存。
	导入用户账户	导入之前导出的认证用户账号数据到路由器。

7.2.2 新增认证账号

步骤 1 点击「认证管理」>「认证用户管理」。

步骤 2 在“认证账号管理”模块点击 +添加 。

步骤 3 在【添加】窗口配置各项参数，然后点击 保存 。



----完成

部分参数说明

标题项	说明
共享用户数	允许同时使用该账号认证上网的用户数量。
并发连接数	单台设备的最大并发连接数。
上传速率	该账号的最大上传/下载速率。
下载速率	

7.3 PPPoE 认证配置举例

组网需求

某企业使用企业级路由器进行网络搭建。

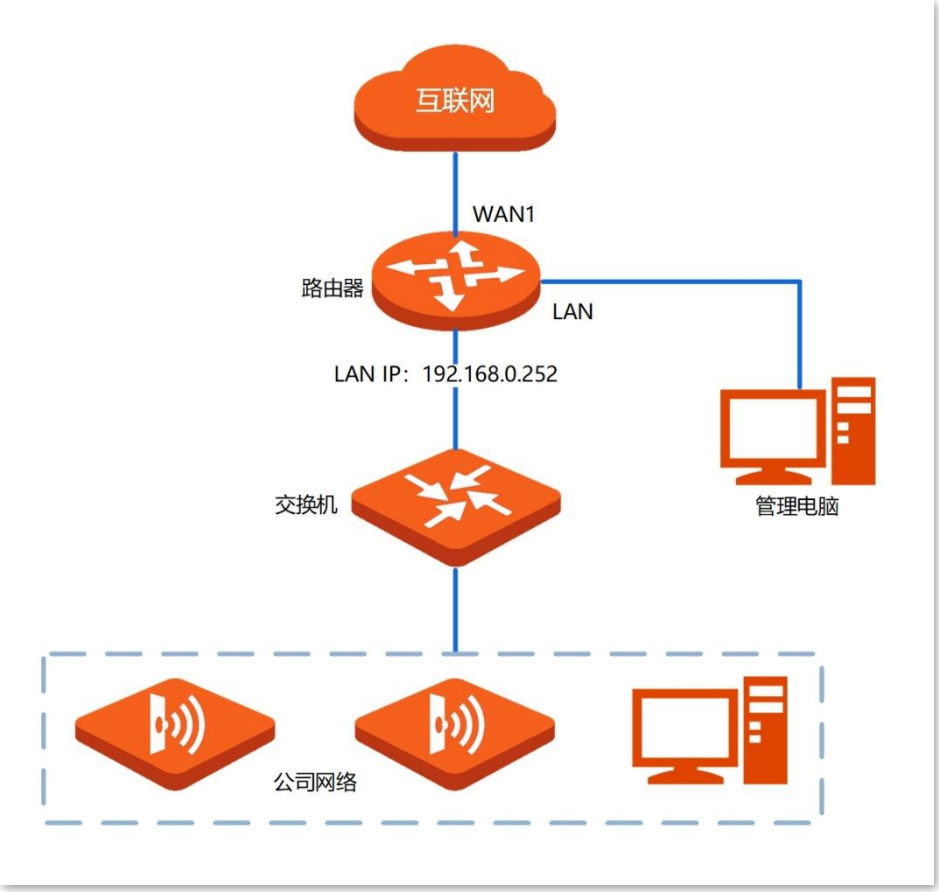
为了规范网络使用，要求：

- 连接路由器 LAN 口的员工访问互联网时需要认证。
- 网络管理员访问互联网时不需要认证。

方案设计

可以通过 PPPoE 认证功能实现上述需求。假设：

- 网络管理员电脑的物理地址为 44:37:E6:12:34:56。
- PPPoE 服务器的 IP 地址为 172.20.20.1。



配置步骤

配置流程图：

进行 PPPoE 认证设置 > 添加免认证主机

步骤 1 配置 PPPoE 认证服务器。

1. 点击「认证管理」>「PPPoE 认证」。
2. 点击滑块至 。
3. 配置 PPPoE 认证基本参数，然后点击 保存 。
   (1) 设置服务器 IP 地址为“172.20.20.1”。
   (2) 设置客户端起始 IP 地址，如“172.20.20.2”。
   (3) 设置客户端结束 IP 地址，如“172.20.20.129”。
   (4) 设置首选 DNS，如“172.20.20.1”。
   (5) 设置备用 DNS，如“8.8.8.8”。
   (6) 勾选相应的认证方式。

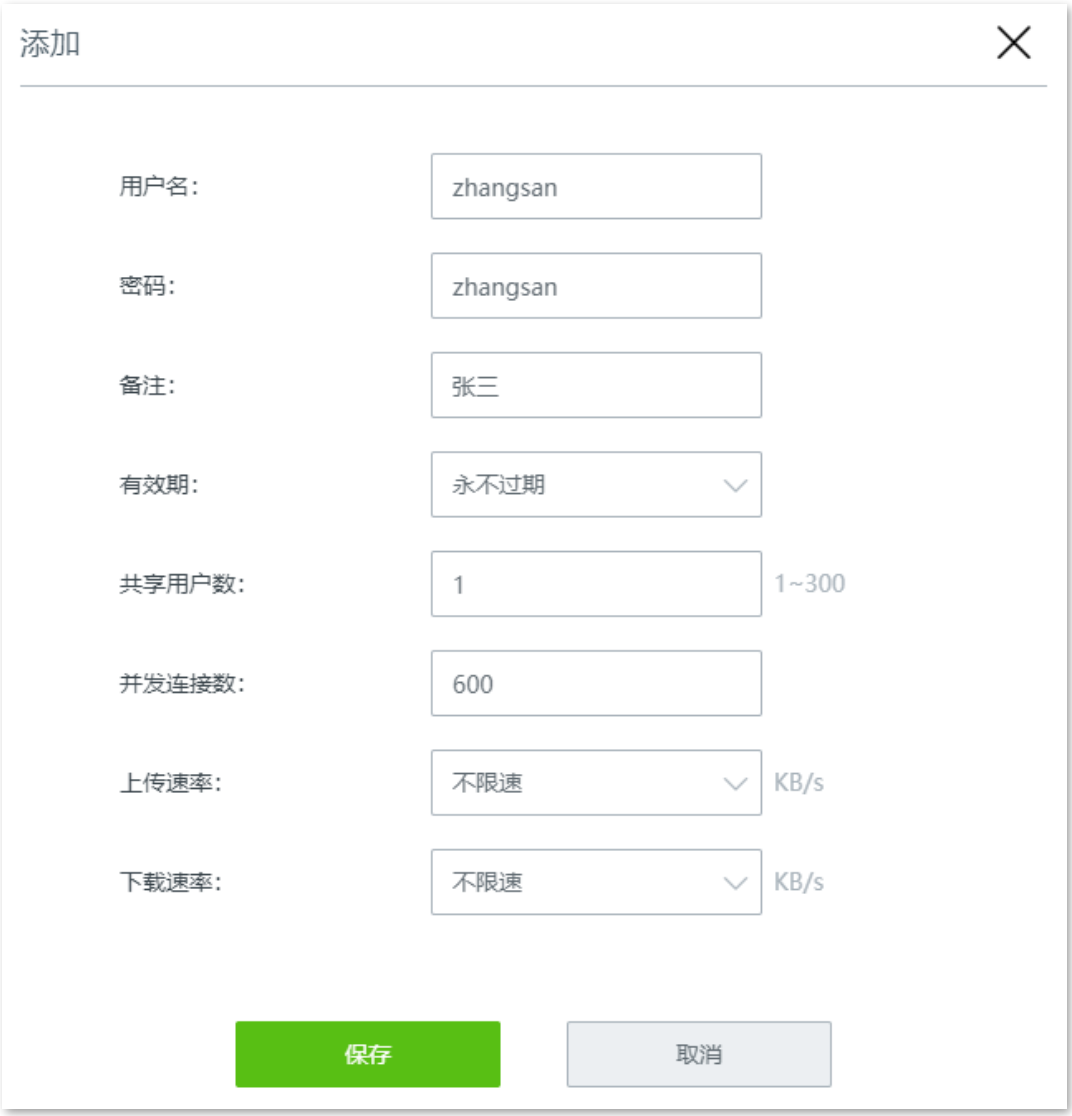
步骤 2 配置 PPPoE 认证账号。

1. 点击「认证管理」>「认证用户管理」。
2. 在“认证账号管理”模块点击 +添加 。
3. 在【添加】窗口配置各项参数，然后点击 保存 。
   (1) 设置用户名，如“zhangsan”。

(2) 设置密码，如“zhangsan”。

(3) 设置账号的备注，如“张三”。

(4) 其他参数保持默认。



步骤 3 添加免认证主机。

1. 点击「认证管理」>「认证用户管理」。
2. 在“免认证主机”模块点击 +添加 。
3. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 选择以何种形式指定免认证主机，本例为“MAC 地址”。

(2) 输入该客户端的 MAC 地址，本例为“44:37:E6:12:34:56”。

(3) （可选）设置该用户的备注，本例为“网络管理员”。


添加
免认证方式:
MAC地址
MAC地址:
44:37:E6:12:34:56
备注:
网络管理员
保存
取消

----完成

添加成功，如下图示。


免认证主机
添加
免认证方式
主机名称/IP/MAC
备注
操作
MAC地址
44:37:E6:12:34:56
网络管理员

验证配置

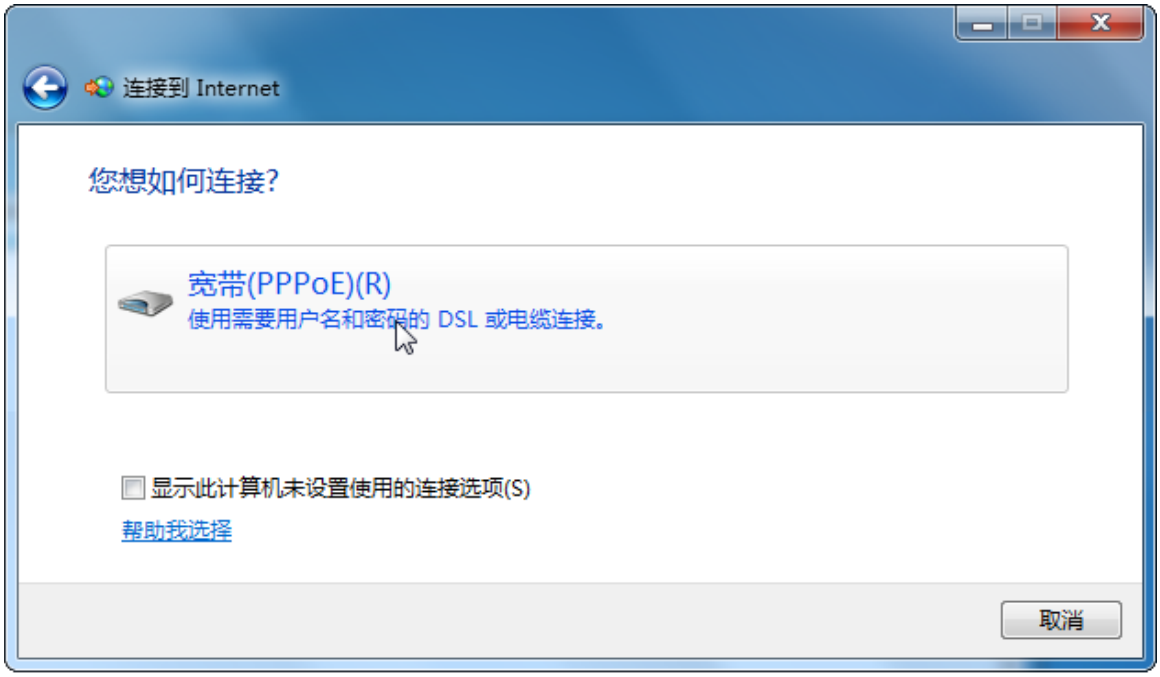
网络管理员访问网络时无需进行认证。其他员工访问网络时，需要先在电脑上进行宽带连接，步骤如下（以Window 7 为例说明）。

步骤 1 点击桌面左下角的开始图标。

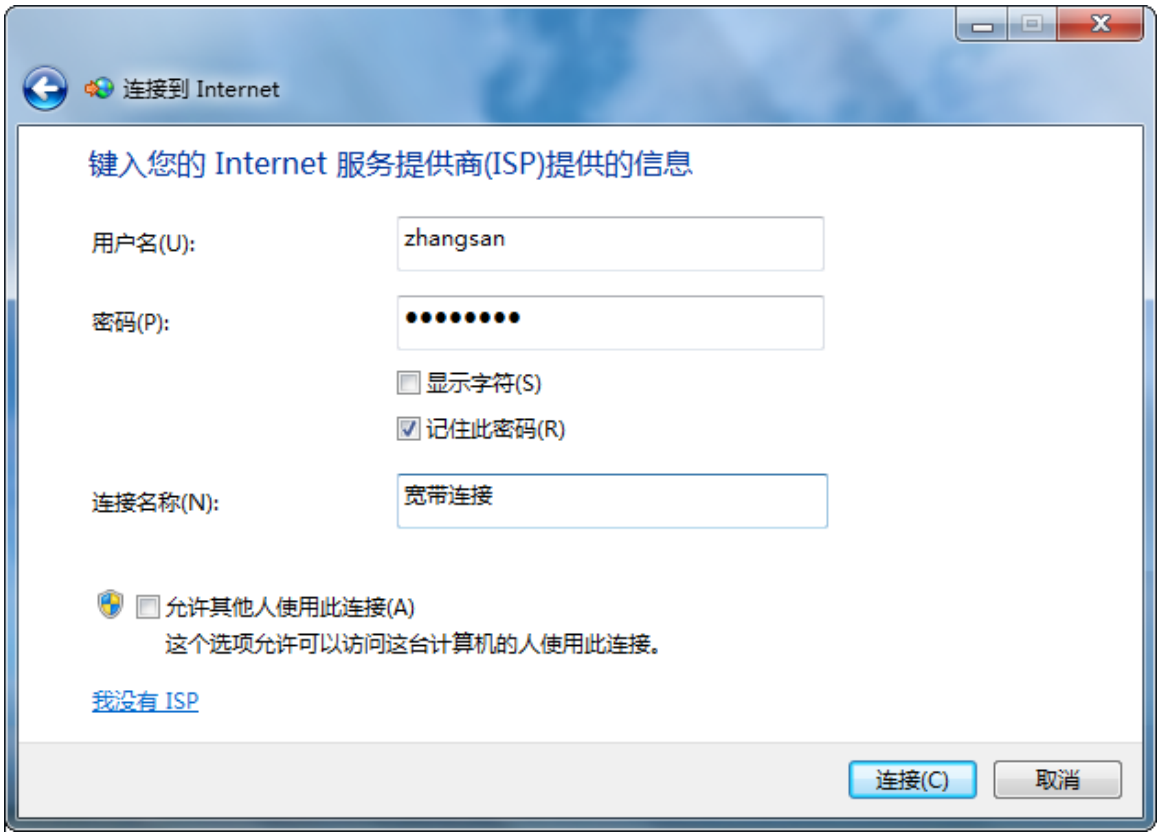
步骤 2 点击**控制面板>网络和 Internet>网络和共享中心>设置新的连接或网络**。

步骤 3 选择**连接到 Internet**，然后点击 下一步 ；

步骤 4 点击**宽带（PPPoE）（R）**；



步骤 5 填写 **PPPoE 认证用户名和密码**，本例中用户名为 zhangsan，密码为 zhangsan，勾选**记住此密码（R）**，点击 连接 。

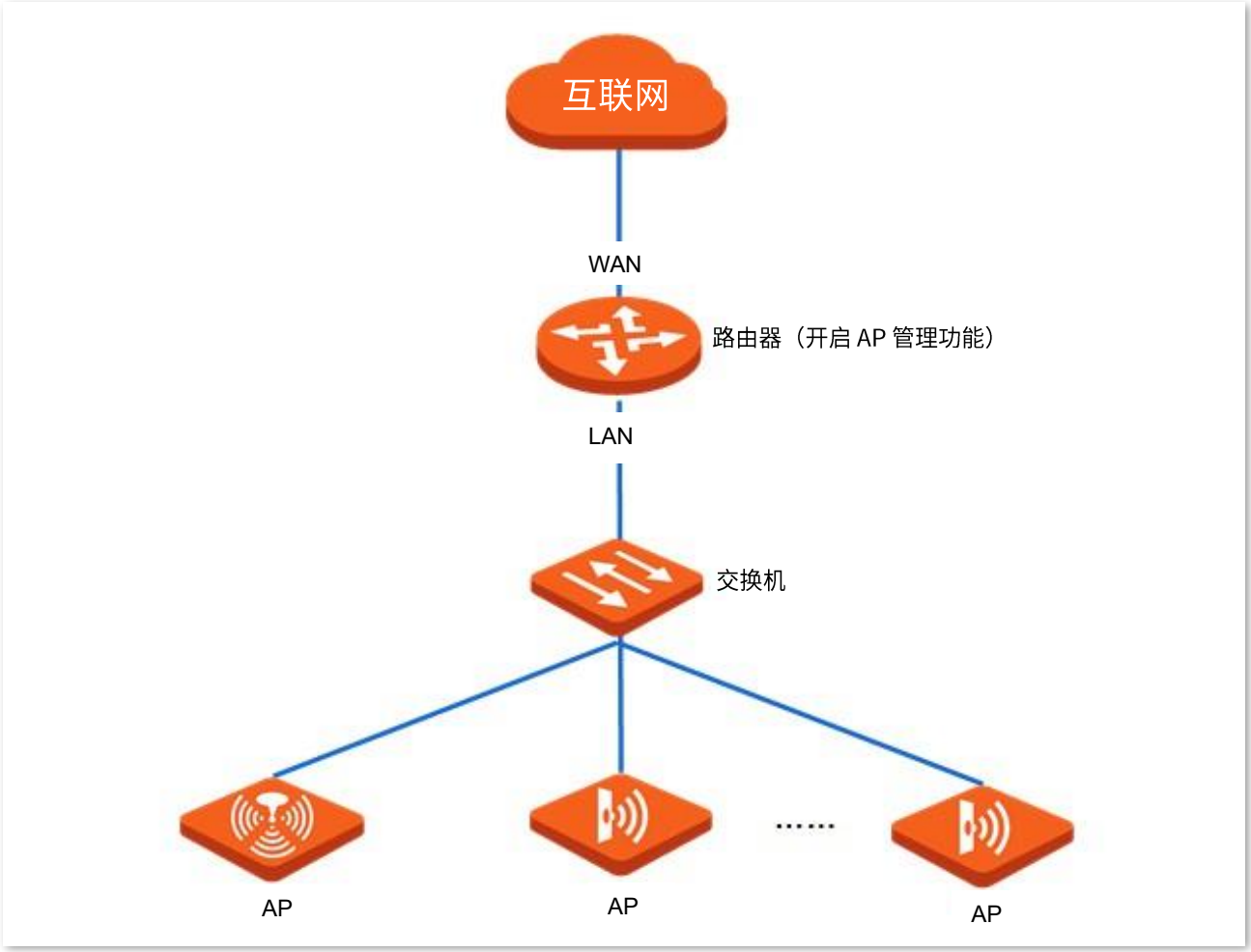


稍等片刻，拨号成功，可以上网了。

以后每次开机后，点击电脑桌面右下角的网络图标，然后点击宽带连接，拨号成功后即可正常上网。

8 AP 管理

路由器集成了无线控制器的功能，可以管理 Tenda 公司 AP。网络应用拓扑图如下。

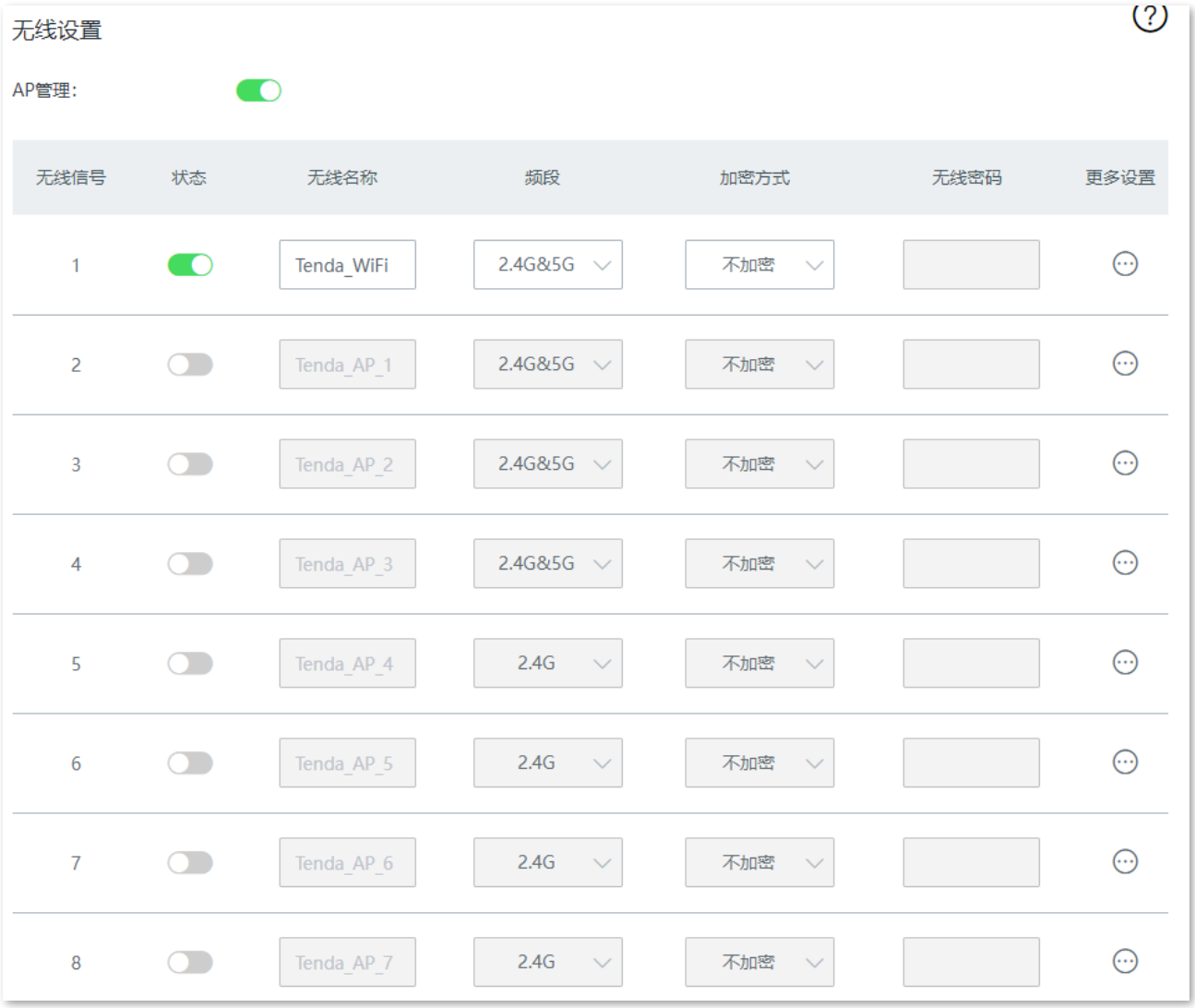


8.1 基本配置

8.1.1 概述

进入页面：点击「AP 管理」>「基本配置」。

在这里，您可以开启/关闭路由器的 AP 管理功能。开启后，可以集中配置局域网中 AP 的无线网络相关参数，如无线名称、无线网络启用状态、频段、无线密码等。这些配置在 Tenda AP 连接到路由器后自动生效。



参数说明

标题项	说明
无线信号	无线策略的序号。 - 1~4：用于修改 AP 2.4GHz 或 5GHz 频段的第 1~4 个 SSID 的相关参数。 - 5~8：用于修改 AP 2.4GHz 频段的第 5~8 个 SSID 的相关参数。

标题项	说明
状态	无线策略的状态，也是 AP 对应 SSID 的启用/禁用状态。默认启用第一条无线策略，禁用其他无线策略。
无线名称	无线网络名称，可根据需要自定义。
频段	无线策略的应用频段，即，该无线策略要下发到 AP 的哪个频段。 - 2.4G：无线策略下发到 AP 的 2.4GHz 频段。 - 5G：无线策略下发到 AP 的 5GHz 频段。 - 2.4G&5G：无线策略同时下发到 AP 的 2.4GHz 频段和 5GHz 频段。 注意 第 1 条无线策略的频段为单频，如 2.4G（或 5G），则点击 保存 后，AP 将关闭对应 SSID 另一频段如 5G（或 2.4G）的无线功能。
加密方式	无线网络的加密方式。 - 不加密：不加密无线网络，用户连接无线网络时，无需输入密码即可接入。为保障网络安全，不建议选择此项。 - WPA-PSK：无线网络采用 WPA-PSK 认证方式（AES 加密规则），此加密方式的兼容性比 WPA2-PSK 好。 - WPA2-PSK：无线网络采用 WPA2-PSK 认证方式（AES 加密规则），此加密方式的安全等级比 WPA-PSK 高。 - WPA3-SAE：无线网络使用 WPA3-SAE 认证方式（AES 加密规则），此加密方式采用对等实体同时验证（SAE），支持管理帧保护（PMF），可以抵御字典暴破攻击，防止信息泄露，用户无需再设置复杂而难记的密码。 提示 WPA3-SAE 加密方式是 WPA2-PSK 的升级版，如果无线客户端不支持 WPA3-SAE 加密方式，或者 WiFi 使用体验不好，建议将无线网络的加密方式设置为“WPA2-PSK”。
无线密码	WPA-PSK、WPA2-PSK 或 WPA3-SAE 的预共享密码，也是用户连接无线网络时需要输入的无线密码。
更多设置	点击可进行高级参数设置，包括：客户端隔离、隐藏无线网络、最大用户数、VLAN ID。 - 客户端隔离：启用后，连接到该无线网络下的设备之间不能互相通信，可增强无线网络的安全性。 - 隐藏无线网络：启用后，其他无线设备不能扫描到该 SSID。 - 最大用户数：无线网络最多允许接入的无线设备数量。默认为 48。 - VLAN ID：此版本暂不支持。

8.1.2 下发无线策略到 AP

注意

下发无线策略时，如果部分功能 AP 不支持，那么配置可以下发成功，但不会生效。例如：通过 AP 管理功能下发 5G 的配置，若网络中有 AP 不支持 5G，虽然配置可以下发成功，但该 AP 不会生效。

步骤 1 点击「AP 管理」>「基本配置」。

步骤 2 修改无线网络参数。

步骤 3 点击页面底端的 保存 。

----完成

稍等片刻，局域网中 AP 的相关无线设置会变为与无线策略一致。

8.2 AP 配置

8.2.1 概述

进入页面：点击「AP 管理」>「AP 配置」。

在这里，您可以批量升级/复位/重启在线 AP，批量删除离线 AP 信息，单独修改某一 AP 的配置信息、查看/导出“管理 AP”信息等。

8.2.2 升级

使用升级功能，可以同时升级多个 AP 的软件版本。

> 注意
> AP 升级过程中，为了避免损坏 AP 导致其无法使用，请切勿关闭路由器和 AP 的电源。

设置步骤：

步骤 1 访问 Tenda 官网 www.tenda.com.cn，下载对应型号的 AP 软件到本地电脑并解压。

步骤 2 登录路由器管理页面，点击「AP 管理」>「AP 配置」。

步骤 3 选择需要进行软件升级的 AP。

步骤 4 点击 升级 ，之后按页面提示操作。

----完成

8.2.3 复位

使用复位功能，可以同时将多个 AP 恢复出厂设置。

设置步骤：

步骤 1 点击「AP 管理」>「AP 配置」。

步骤 2 选择需要恢复出厂设置的 AP。

步骤 3 点击 复位 ，之后按页面提示操作。

----完成

8.2.4 重启

使用重启功能，可以同时将多个 AP 重新启动。

设置步骤：

步骤 1 点击「AP 管理」>「AP 配置」。

步骤 2 选择需要重新启动的 AP。

步骤 3 点击 重启 ，之后按页面提示操作。

----完成

重启时，AP 将离线一段时间，重启完成后，AP 将自动上线。AP 从离线到重新上线的过程可能需要 1~2 分钟，请耐心等待。您可以点击 刷新 查看。

8.2.5 删除

使用删除功能，可以同时删除多个处于离线状态的 AP。

设置步骤：

步骤 1 点击「AP 管理」>「AP 配置」。

步骤 2 选择需要删除的离线 AP。

步骤 3 点击 删除 ，之后按页面提示操作。

----完成

8.2.6 刷新

如果要更新页面显示的 AP 信息，请点击 刷新 。

8.2.7 导出

使用导出功能，可以将 AP 列表信息以 Excel 的格式导出并保存到本地电脑。

设置步骤：

步骤 1 点击「AP 管理」>「AP 配置」。

步骤 2 点击 导出列表 ，之后按页面提示操作。

----完成

8.2.8 更多设置

使用更多设置功能，可以单独修改某一 AP 的配置信息，如无线开关、国家或地区、信道、发射功率等参数。

设置步骤：

步骤 1 点击「AP 管理」>「AP 配置」。

步骤 2 找到需要修改配置的 AP，然后点击对应操作栏的。

步骤 3 根据需要修改 AP 的配置，然后点击页面底端的 保存 。

----完成

8.3 高级设置

8.3.1 概述

进入页面：点击「AP 管理」>「高级设置」。

在这里，可以集中配置局域网中 AP 的高级参数。

2.4GHz/5GHz 高级设置

在“2.4GHz/5GHz 高级设置”模块，可以集中配置局域网中 AP 的网络模式、信道、发射功率等参数。

2.4GHz/5GHz 高级设置参数说明

标题项	说明
国家或地区	AP 当前所在的国家或地区。
网络模式	AP 的无线网络模式。 您可以参考以下说明选择 2.4GHz 无线网络下的网络模式。 - 11b：路由器工作在 802.11b 无线网络模式下。 - 11g：路由器工作在 802.11g 无线网络模式下。 - 11b/g：路由器工作在 802.11b/g 无线网络模式下。 - 11b/g/n：路由器工作在 802.11 b/g/n 无线网络模式下。 - 11b/g/n/ax：路由器工作在 802.11 b/g/n/ax 无线网络模式下。 您可以参考以下说明选择 5GHz 无线网络下的网络模式。 - 11a：路由器工作在 802.11a 无线网络模式下。 - 11ac：路由器工作在 802.11ac 无线网络模式下。 - 11a/n：路由器工作在 802.11 a/n 无线网络模式下。 - 11a/n/ac/ax：路由器工作在 802.11 a/n/ac/ax 无线网络模式下。
信道带宽	AP 的无线信道带宽。 - 20MHz：AP 使用 20MHz 的信道带宽。 - 40MHz：AP 使用 40MHz 的信道带宽。 - 80MHz：仅适用 5GHz，AP 使用 80MHz 的信道带宽。 - 160MHz：仅适用于 5GHz，AP 使用 160MHz 的信道带宽。 - 自动配置：在 2.4GHz 下，AP 根据周围环境，自动调整信道带宽为 20MHz 或 40MHz；在 5GHz 下，AP 根据周围环境，自动调整信道带宽为 20MHz、40MHz、80MHz 或 160MHz。
信道	AP 的无线工作信道。 信道的可选择范围由当前选择的“国家或地区”和“频段”（2.4GHz 或 5GHz）决定。
发射功率	AP 的发射功率。 若 AP 不支持设置的功率，则配置下发后，以 AP 支持的最大范围为准生效。即，当功率超过 AP 的上限功率时，只使用 AP 的最大功率；当功率小于 AP 的下限功率时，只使用 AP 的最小功率。
接入信号强度限制	AP 相关射频可接受的无线客户端信号强度。如果无线客户端信号强度比此阈值小，AP 将主动断开无线客户端。

标题项	说明
客户端老化时间	客户端连接到 AP 的 WiFi 后，如果在该时间段内与 AP 没有数据通信，AP 将主动断开该客户端；如果在该时间段内与 AP 有数据通信，则停止老化计时。
5GHz 优先	仅“5GHz 高级设置”支持。开启后，当 AP 的 2.4GHz 和 5GHz 的无线名称（SSID）和无线密码都相同，且无线客户端支持双频 WiFi 时，客户端将会优先选择 5GHz 频段的 SSID 进行连接。 生效前提：无线网络加密方式为 WPA/WPA2-PSK，并且 SSID 不能包含中文字符。
空口调度	开启/关闭空口调度功能。 空口调度可以保证每个客户端的数据传输时间相等，如果低速率终端在单位时间内没有传输完数据，也要等到下次继续传输。解决了某些低速率客户端占用无线空口太多资源问题，提升 AP 的整体效率，有效保障了带机量和吞吐量。
与其他无线网络隔离	开启/关闭 AP 的无线网络隔离功能。 开启后，连接到该无线网络的用户与连接到 AP 对应频段其他无线网络的用户之间不能互相通信，可增强无线网络的安全性。
WMM	开启/关闭 WMM 功能。WMM，即“无线多媒体”。 开启 WMM 后，音视频数据优先转发。如果要提高 AP 对于无线多媒体数据（如观看在线视频）的传输性能，建议开启。
APSD	开启/关闭 APSD 功能。APSD，即“自动省电模式”，是 WiFi 联盟的 WMM 省电认证协议。 开启“APSD”能降低 AP 的电能消耗。默认关闭。
部署模式	仅“2.4GHz 高级设置”支持。请根据实际应用场景，选择“部署模式”特性。 - 强覆盖：常用于 AP 部署密度较低的场景，此模式可以尽可能地确保客户端成功接入 AP。 - 高密度：常用于 AP 部署密度较高的场景，此模式可以确保客户端连接到信号好的 AP。 - 默认：介于“强覆盖”和“高密度”之间。

全局设置

在“全局设置”模块，可以集中配置局域网 AP 的端口驱动模式、指示灯状态、定时重启相关参数。

参数说明

标题项	说明
端口驱动模式	AP 的以太网口驱动距离。 - 标准：速率高，驱动距离一般。正常情况下，建议选择此模式。 - 增强：驱动距离远，但速率较低，一般协商为 10Mbps。 连接 AP 以太网口与对端设备的网线超过 100 米时，才建议尝试改为“增强”来提高网线驱动距离。此时，必须确保对端端口工作模式为自协商，否则可能导致 AP 以太网口无法正常收发数据。
指示灯	开启/关闭 AP 的指示灯显示功能。 开启后，AP 的所有指示灯正常指示，可根据指示灯判断 AP 的工作状态。默认为“开启”。
重启	AP 自动重启，可以预防长时间地运行 AP 导致 WLAN 出现性能降低、不稳定等现象。但重启过程中，会断开所有连接，因此建议将“维护时间”设置在无线业务相对空闲的时间。 - 关闭：不开启 AP 自动重启功能。 - 定时重启：AP 在指定日期的指定时间点自动重启一次。 - 按间隔时间段重启：AP 每隔一个“间隔时间”就会自动重启一次。

点击显示更多设置>，可以配置 AP 的 VLAN 相关参数。

参数说明

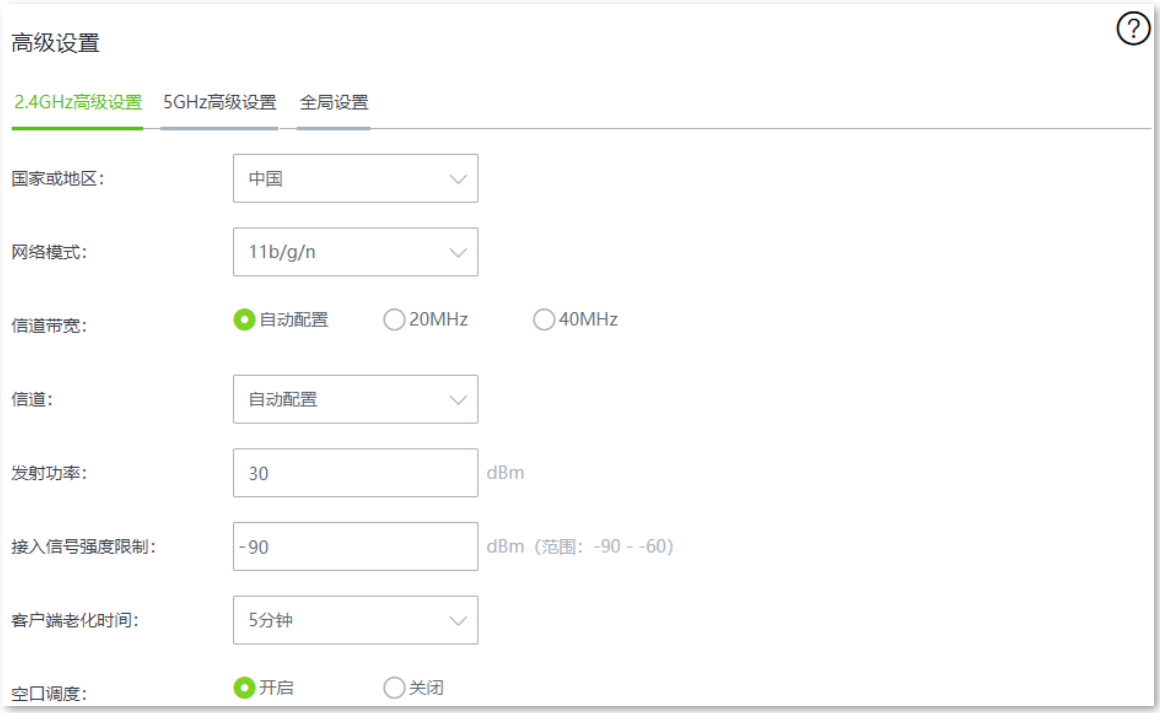
标题项	说明
VLAN	开启/关闭 AP 的 802.1Q VLAN 功能。
管理 VLAN ID	AP 的管理 VLAN ID。 更改管理 VLAN 后，管理电脑或无线控制器需要重新连接到新的管理 VLAN，才能管理 AP。
PVID	AP Trunk 口默认所属的 VLAN 的 ID。
Trunk 口	开启 VLAN 功能后，AP 的 LAN 口至少有一个为 Trunk 口。Trunk 口允许所有 VLAN 通过。

8.3.2 下发 2.4GHz/5GHz 网络配置到 AP

步骤 1 点击「AP 管理」>「高级设置」。

步骤 2 在“高级设置”模块修改相关参数。

步骤 3 点击页面底端的 保存 。



----完成

稍等片刻，局域网中 AP 的相关网络配置会变为与此处下发的策略一致。

8.3.3 下发端口驱动模式等其他配置到 AP

步骤 1 点击「AP 管理」>「高级设置」。

步骤 2 在“全局设置”模块修改相关参数。

步骤 3 点击页面底端的 保存 。

----完成

稍等片刻，局域网中 AP 的相关配置会变为与此处下发的策略一致。

8.4 IPTV

8.4.1 概述

IPTV，Internet Protocol Television，交互式网络电视。它是集互联网、多媒体、电信等多种技术于一体的技术，通过互联网宽带线路向家庭用户提供包括数字电视在内的互动服务。

通过 IPTV 功能，您可以在路由器与 AP 之间建立 IPTV 数据透传通道，改善因 IPTV 机顶盒与光猫距离较远而产生的不易连接问题。

如果您办理的宽带含有 IPTV 业务，则可以启用路由器的 IPTV 功能，使您在通过路由器上网的同时，也可以通过网络机顶盒和电视机观看丰富的 IPTV 节目。

> 提示
>
> 此功能需配合支持 IPTV 功能的 Tenda AP 使用。

进入页面：点击「AP 管理」>「IPTV」。

IPTV 功能默认关闭，开启后，页面显示如下。

参数说明

标题项		说明
IPTV 设置	IPTV 端口	指定路由器的一个 LAN 口作为 IPTV 口，用于连接光猫的 IPTV 口。LAN 端口号参考路由器机身接口标识。
	IPTV 功能	开启或关闭路由器的 IPTV 功能。
AP 列表	AP 型号	AP 的产品型号。仅支持 IPTV 功能的 AP 才会显示在 AP 列表中。

标题项		说明
	MAC 地址	AP 的 MAC 地址。
	指定网口	在 AP 上指定一个有线网口与路由器建立 IPTV 数据透传通道，指定网口用于连接到 IPTV 机顶盒。  该网口固定指定网口 1。

8.4.2 观看 IPTV 节目

场景一

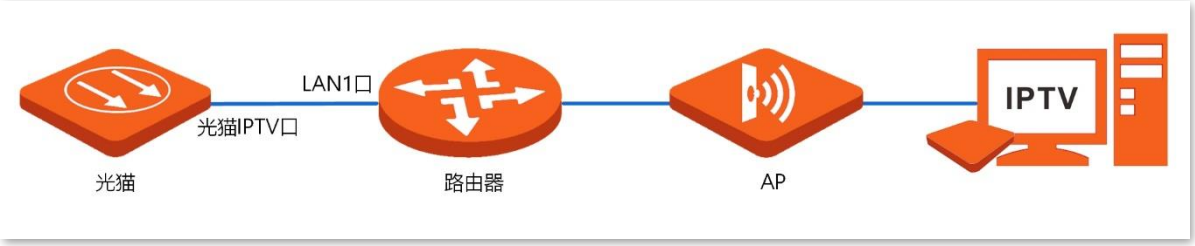
组网需求

您的宽带业务中包含 IPTV 业务。ISP 提供了 IPTV 账号和密码，未提供 IPTV 业务的 VLAN ID。

需求：能够观看 IPTV 节目。

方案设计

可以通过配置路由器的 IPTV 功能实现上述需求。



配置步骤

步骤 1 配置路由器

1. 开启路由器 IPTV 功能与指定 IPTV 端口。

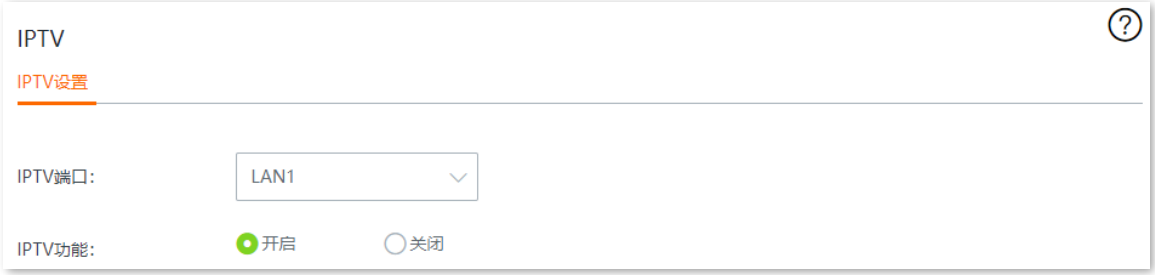
   (1) 在已连接到路由器的手机或电脑上，打开浏览器访问 ipcwifi.com 或者 192.158.0.252，进入路由器管理页面。

   (2) 点击「AP 管理」>「IPTV」。

   (3) 选择“IPTV 功能”为“开启”。

   (4) 指定“LAN1”作为 IPTV 端口。

   (5) 点击页面底端的 保存 。



2. 指定 AP 的有线网口。

   (1) 在 AP 列表，找到待连接 IPTV 机顶盒的 AP，点击 。

   (2) 在弹出的窗口中，勾选指定网口后，点击页面底端的 保存 。

此时，AP 列表中显示 AP 所指定网口对应的物理接口。

步骤 2 光猫下来的 IPTV 网线接到路由器的 IPTV 端口。

步骤 3 IPTV 机顶盒连接至指定的 AP 有线网口。

步骤 4 设置您的 IPTV 机顶盒。

使用 ISP 提供的 IPTV 账号和密码在 IPTV 机顶盒进行网络设置。

----完成

验证配置

完成配置后，您可以在您的电视上观看 IPTV 节目。

场景二

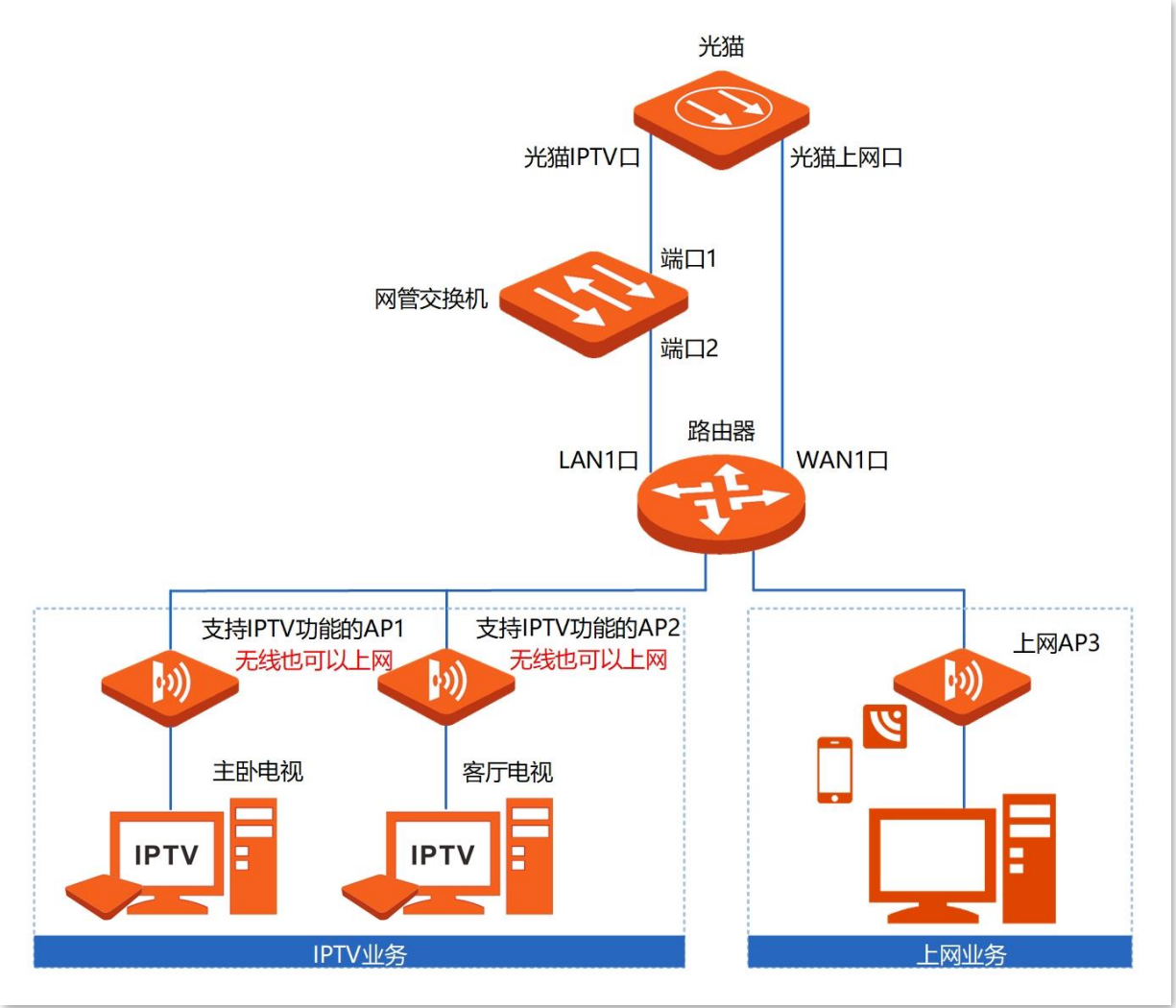
组网需求

您的宽带业务中包含 IPTV 业务。ISP 提供了 IPTV 账号和密码，且提供了 IPTV 业务的 VLAN ID（此处以 VLAN ID 为 2 为例）。

需求：能够同时观看 IPTV 节目和上网。

方案设计

可以通过配置路由器的 IPTV 和上网功能，以及配置网管交换机的 VLAN 功能，来实现上述需求。



配置步骤

配置 IPTV 业务

步骤 1 配置交换机（此处以 Tenda 二层网管型交换机 TEG3328FV1.0 为例）。

1. 添加 VLAN。

   (1) 点击「常用功能」>「VLAN 划分」>「802.1Q VLAN」。

(2) 点击 + 添加，在弹出的窗口中输入如下参数后点击 确认。

- “VLAN ID”为“2”。
- “VLAN 描述”为“IPTV”。

2. 配置端口成员。

(1) 点击「常用功能」>「VLAN 划分」>「端口成员」。

(2) 点击端口 1 后面的 按钮，设置“PVID”为“2”。

(3) 点击端口 2 后面的 按钮，设置“PVID”为“2”。

步骤 2 配置路由器

1. 开启路由器 IPTV 功能与指定 IPTV 端口。

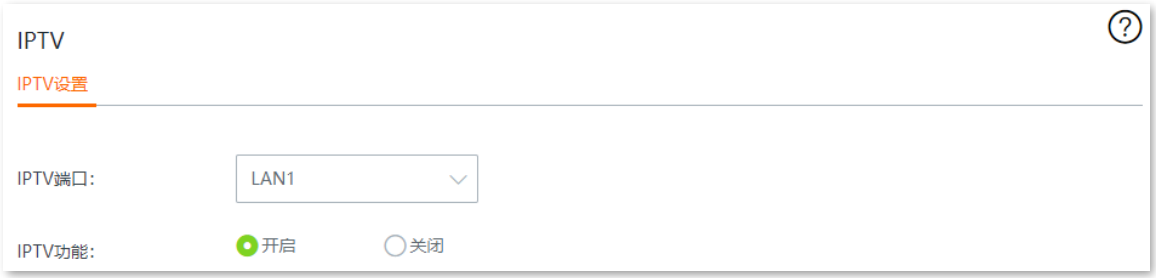
(1) 在已连接到路由器的手机或电脑上，打开浏览器访问 ipcwifi.com 或者 192.158.0.252，进入路由器管理页面。

(2) 点击「AP 管理」>「IPTV」。

(3) 选择“IPTV 功能”为“开启”。

(4) 指定“LAN1”作为 IPTV 端口。

(5) 点击 保存。



2. 指定 AP1（支持 IPTV 功能）的有线网口。

(1) 在 AP 列表，找到待连接 IPTV 机顶盒的 AP1，点击 。

(2) 在弹出的窗口中，勾选指定网口后，点击 保存。

此时，AP 列表中显示 AP 所指定网口对应的物理接口。

3. 重复步骤 2 的 2，指定其他 AP2（支持 IPTV 功能）的有线网口。

步骤 3 光猫下来的 IPTV 线接到交换机的端口 1。

步骤 4 用网线将交换机的端口 2 连接至路由器的 IPTV 口。

步骤 5 IPTV 机顶盒连接至指定的 AP 有线网口。

步骤 6 设置您的 IPTV 机顶盒。

使用 ISP 提供的 IPTV 账号和密码在 IPTV 机顶盒进行网络设置。

----完成

配置上网业务

步骤 1 光猫下来的上网线接到路由器的 WAN1 口。

步骤 2 用网线将路由器的 LAN 口连接至 AP3 的 LAN 口。

步骤 3 参考联网设置，设置路由器联网参数。

----完成

验证配置

完成配置后，您可以同时观看 IPTV 节目和上网。

9 行为管理

9.1 IP 组与时间组

9.1.1 概述

进入页面：点击「行为管理」>「IP 组与时间组」。

您在配置 MAC 地址过滤、IP 地址过滤、端口过滤、网站过滤、分组限速和自定义多 WAN 策略等基于 IP 组或时间组生效的功能时，需要先配置好相应的 IP 组和/或时间组。

路由器默认已添加 1 条时间组，如下图示。默认时间组不支持删除和编辑操作。

参数说明

标题项		说明
时间组设置	组名称	时间组的名称。组名称不能重复。
	日期	时间组所包含的日期。
	时间	时间组的开始~结束时间。00:00~00:00，表示全天。
	操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
IP 组设置	IP 组	IP 组的名称。组名称不能重复。
	IP 地址段	IP 组的开始~结束 IP 地址。
	操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。

9.1.2 新增时间组

步骤 1 点击「行为管理」>「IP 组与时间组」。

步骤 2 在“时间组设置”模块，点击 +添加 。

步骤 3 在【添加】窗口配置各项参数，然后点击 保存 。

----完成

9.1.3 新增 IP 组

步骤 1 点击「行为管理」>「IP 组与时间组」。

步骤 2 在“IP 组设置”模块，点击 +添加 。

步骤 3 在【添加】窗口配置各项参数，然后点击 保存 。

----完成

9.2 MAC 地址过滤

9.2.1 概述

通过 MAC 地址过滤功能，可以允许或禁止指定用户通过路由器上网。

进入页面：点击「行为管理」>「MAC 地址过滤」。

MAC 地址过滤功能默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
MAC 地址过滤	MAC 地址过滤功能开关。 表示关闭， 表示开启。
过滤模式	MAC 地址过滤模式。 - 白名单：即，允许访问互联网。使用此模式时，指定 MAC 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。 - 黑名单：即，禁止访问互联网。使用此模式时，指定 MAC 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。
MAC 地址	规则对应的用户设备的 MAC 地址。
时间组	规则引用的时间组，以指定规则的生效时间。

标题项	说明
	时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。
备注	规则的备注信息。
状态	规则的状态，可根据需要开启或关闭。 表示关闭， 表示开启。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
允许未启用规则中的主机和列表外的主机访问互联网	- 勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都可以访问互联网。 - 未勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都不能访问互联网。

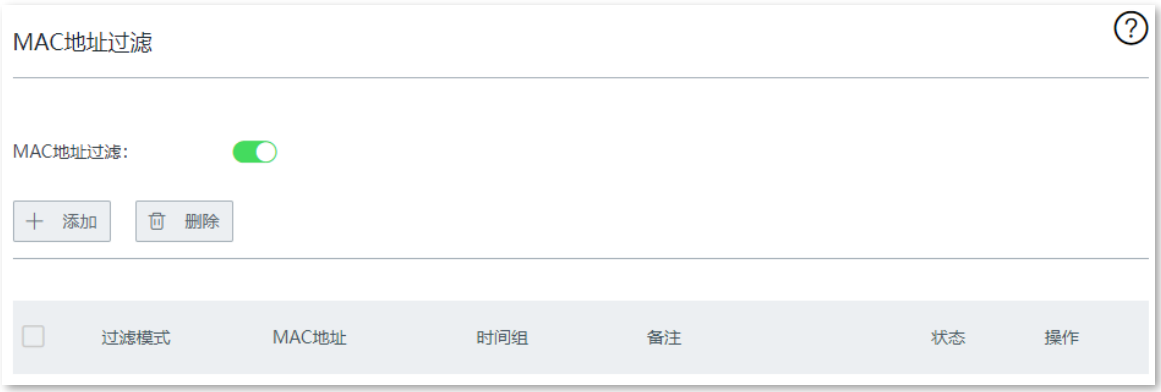
9.2.2 新增 MAC 地址过滤规则

提示

配置 MAC 地址过滤规则前，请先配置好相应的时间组。

步骤 1 开启 MAC 地址过滤功能。

1. 点击「行为管理」>「MAC 地址过滤」。
2. 点击滑块至 。
3. 点击页面底端的 保存 。



步骤 2 添加 MAC 地址过滤规则。

1. 点击 +添加 。

2. 在【添加】窗口配置各项参数，然后点击 保存 。

----完成

9.2.3 MAC 地址过滤配置举例

组网需求

某企业使用企业级路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），仅允许某一采购人员访问互联网，其他员工禁止访问互联网。

可以使用路由器的 MAC 地址过滤功能实现上述需求。假设该采购人员电脑的物理地址为 CC:3A:61:71:1B:6E。

配置步骤

配置流程图：

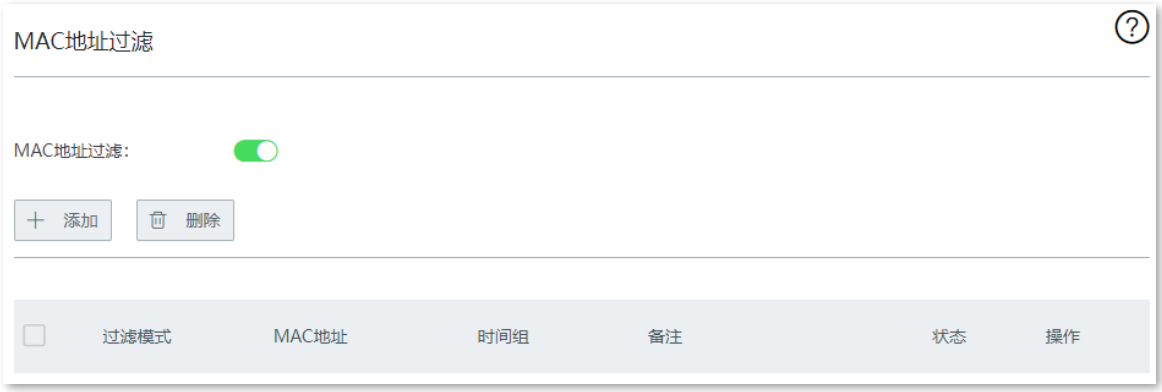
配置时间组 → 开启 MAC 地址过滤功能 → 添加 MAC 地址过滤规则

步骤 1 配置时间组。

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

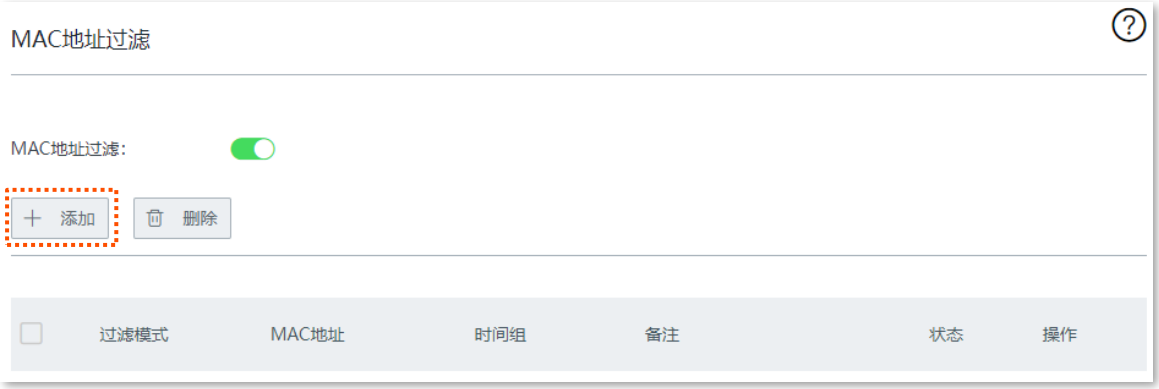
步骤 2 开启 MAC 地址过滤功能。

1. 点击「行为管理」>「MAC 地址过滤」。
2. 点击滑块至  。
3. 点击页面底端的 保存 。



步骤 3 添加 MAC 地址过滤规则。

1. 点击 +添加 。



2. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 选择“过滤模式”，本例为“白名单（允许访问互联网）”。

(2) 选择规则生效的时间组，本例为“上班时间”。

(3) 输入采购人员电脑的物理地址，本例为“CC:3A:61:71:1B:6E”。

(4) （可选）设置本规则的备注，如“允许上网”。

3. 禁止未启用规则中的主机和列表外的主机访问互联网。

(1) 取消勾选“允许未启用规则中的主机和列表外的主机访问互联网”。

(2) 点击页面底端的 保存 。

----完成

验证配置

星期一到星期五的 8:00~18:00，局域网中，只有使用 MAC 地址为 CC:3A:61:71:1B:6E 的电脑的采购人员才能访问互联网，使用其他员工的电脑不能访问互联网。

9.3 IP 地址过滤

9.3.1 概述

通过 IP 地址过滤功能，可以允许或禁止指定用户通过路由器上网。

进入页面：点击「行为管理」>「IP 地址过滤」。

IP 地址过滤功能默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
IP 地址过滤	IP 地址过滤功能开关。 表示关闭， 表示开启。
过滤模式	IP 地址过滤模式。 - 白名单：即，允许访问互联网。使用此模式时，指定 IP 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。 - 黑名单：即，禁止访问互联网。使用此模式时，指定 IP 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。
IP 组	规则引用的 IP 组，以指定规则对应的用户。 IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。

标题项	说明
时间组	规则引用的时间组，以指定规则的生效时间。 时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。
备注	规则的备注信息。
状态	规则的状态，可根据需要开启或关闭。 表示关闭， 表示开启。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
允许未启用规则中的主机和列表外的主机访问互联网	- 勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都可以访问互联网。 - 未勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都不能访问互联网。

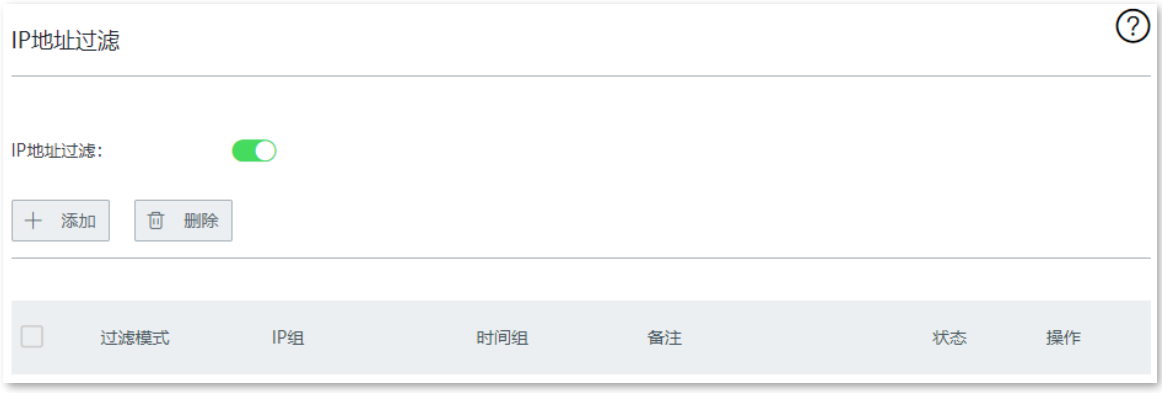
9.3.2 新增 IP 地址过滤规则

提示

配置 IP 地址过滤规则前，请先配置好相应的 IP 组和时间组。

步骤 1 开启 IP 地址过滤功能。

1. 点击「行为管理」>「IP 地址过滤」。
2. 点击滑块至 。
3. 点击页面底端的 保存 。



步骤 2 添加 IP 地址过滤规则。

1. 点击 +添加 。

2. 在【添加】窗口配置各项参数，然后点击 保存 。

----完成

9.3.3 IP 地址过滤配置举例

组网需求

某企业使用企业级路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），仅允许采购部门人员访问互联网，其他员工禁止访问互联网。

可以使用路由器的 IP 地址过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.10。

配置步骤

配置流程图：

配置时间组 → 配置 IP 组 → 开启 IP 地址过滤功能 → 添加 IP 地址过滤规则

步骤 1 配置时间组。

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

步骤 2 配置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

步骤 3 开启 IP 地址过滤功能。

1. 点击「行为管理」>「IP 地址过滤」。
2. 点击滑块至 。

3. 点击页面底端的 保存 。

步骤 4 添加 IP 地址过滤规则。

1. 点击 +添加 。

2. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 选择“过滤模式”，本例为“白名单（允许访问互联网）”。

(2) 选择规则生效的时间组，本例为“上班时间”。

(3) 选择规则生效的 IP 组，本例为“采购部”。

(4) （可选）设置本规则的备注，如“允许上网”。

3. 禁止未启用规则中的主机和列表外的主机访问互联网。

(1) 取消勾选“允许未启用规则中的主机和列表外的主机访问互联网”。

(2) 点击页面底端的 保存 。

----完成

验证配置

星期一到星期五的 8:00~18:00，局域网中，只有使用采购部门人员的电脑（IP 地址在 192.168.0.2~192.168.0.10 范围内）才能访问互联网，使用其他员工的电脑不能访问互联网。

9.4 端口过滤

9.4.1 概述

互联网上众多服务所涉及的应用协议都有特定的端口号，从 0 到 1023 是常用服务的端口号，这些端口号一般固定分配给特定的服务。

端口过滤通过禁止用户对互联网上指定端口的访问，以此来控制用户访问的互联网服务类型。

进入页面：点击「行为管理」>「端口过滤」。

端口过滤功能默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
端口过滤	端口过滤功能开关。 表示关闭， 表示开启。
IP 组	规则引用的 IP 组，以指定规则对应的用户。 IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。
时间组	规则引用的时间组，以指定规则的生效时间。 时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。
端口	禁止访问的服务使用的 TCP 或 UDP 端口号。

标题项	说明
协议	禁止访问的服务使用的协议。“全部”表示 TCP 和 UDP。
状态	规则的状态，可根据需要开启或关闭。 表示关闭， 表示开启。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。

9.4.2 新增端口过滤规则

提示

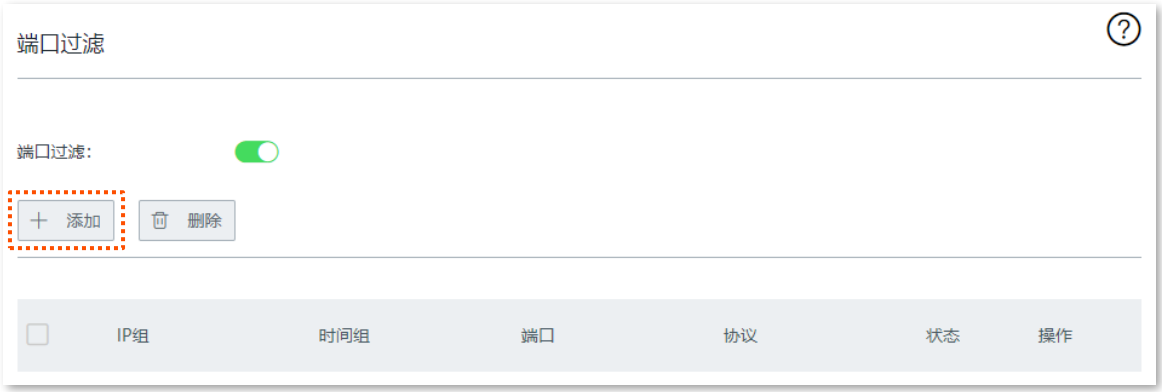
配置端口过滤规则前，请先配置好相应的 IP 组和时间组。

步骤 1 开启端口过滤功能。

1. 点击「行为管理」>「端口过滤」。
2. 点击滑块至 。
3. 点击页面底端的 保存 。

步骤 2 添加端口过滤规则。

1. 点击 +添加 。



2. 在【添加】窗口配置各项参数，然后点击 保存 。

----完成

9.4.3 端口过滤配置举例

组网需求

某企业使用企业级路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），禁止财务部门员工浏览网页（浏览网页服务默认的端口号是 80）。

可以使用路由器的端口过滤功能实现上述需求。假设财务部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.10。

配置步骤

配置流程图：

设置时间组 → 设置 IP 组 → 开启端口过滤功能 → 添加端口过滤规则

步骤 1 设置时间组。

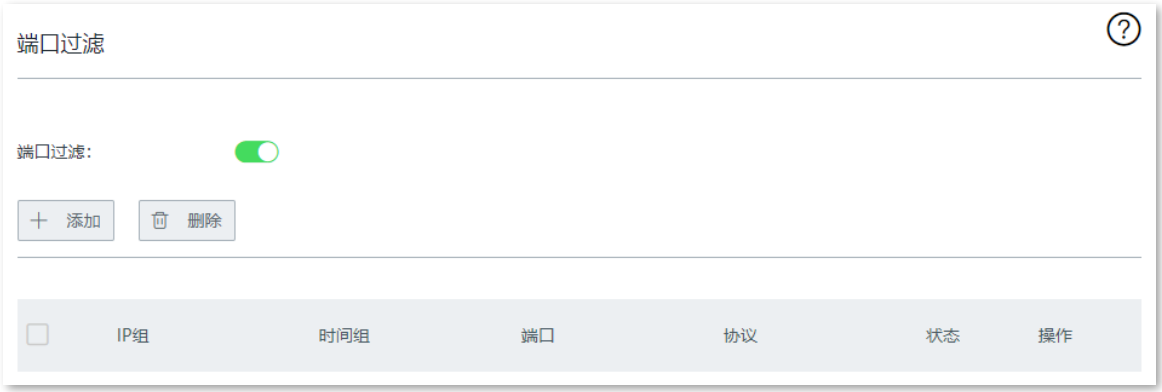
进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

步骤 2 设置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

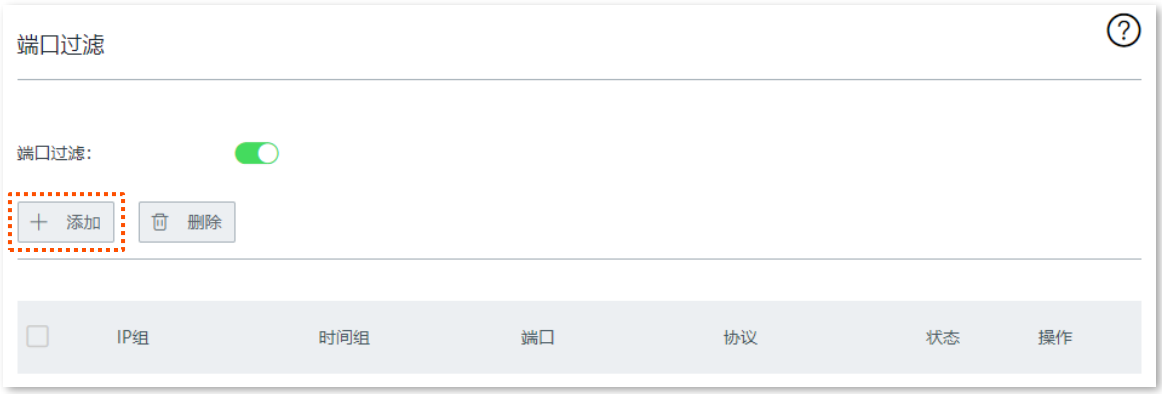
步骤 3 开启端口过滤功能。

1. 点击「行为管理」>「端口过滤」。
2. 点击滑块至 。
3. 点击页面底端的 保存 。



步骤 4 添加端口过滤规则。

1. 点击 +添加 。



2. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 选择规则生效的 IP 组，本例为“财务部”。

(2) 选择规则生效的时间组，本例为“上班时间”。

(3) 输入浏览网页服务使用的端口号“80”。

(4) 选择服务使用的协议，建议保持默认“全部”。

添加成功，如下图示。

----完成

验证配置

星期一到星期五的 8:00~18:00，局域网中，IP 地址在 192.168.0.2~192.168.0.10 范围内的电脑不能进行网页浏览服务。

9.5 网站过滤

9.5.1 概述

通过网站过滤，允许或禁止用户访问指定类别网址，以规范局域网用户上网行为。用户可根据实际情况自定义新增分类。

进入页面：点击「行为管理」>「网站过滤」。

网站过滤功能默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
网站过滤	网站过滤功能开关。 表示关闭， 表示开启。
过滤模式	网站过滤模式。 - 白名单：即，允许访问互联网。允许 IP 组内的用户在对应时间段内访问指定的网站，不能访问其他网站；在其他时间段内可以访问所有网站。 - 黑名单：即，禁止访问互联网。禁止 IP 组内的用户在对应时间段内访问指定的网站，可以访问其他网站；在其他时间段内可以访问所有网站。
IP 组	规则引用的 IP 组，以指定规则对应的用户。 IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。

标题项	说明
时间组	规则引用的时间组，以指定规则的生效时间。 时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。
网址	规则对应的网址分类。
状态	规则的状态，可根据需要开启或关闭。 表示关闭， 表示开启。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
网址管理	查看路由器预置的网址或自定义网址。 提示 如果路由器没有预置网址，且您需要快速添加网址，请参考特征库本地升级进行设置。

9.5.2 自定义网址组

步骤 1 开启网站过滤功能。

1. 点击「行为管理」>「网站过滤」。
2. 点击滑块至 。
3. 点击页面底端的 保存 。

步骤 2 添加网址组。

1. 点击 网址管理 。

2. 点击 新增分类 。

3. 在【添加】窗口配置各项参数，然后点击 保存 。

----完成

9.5.3 新增网站过滤规则

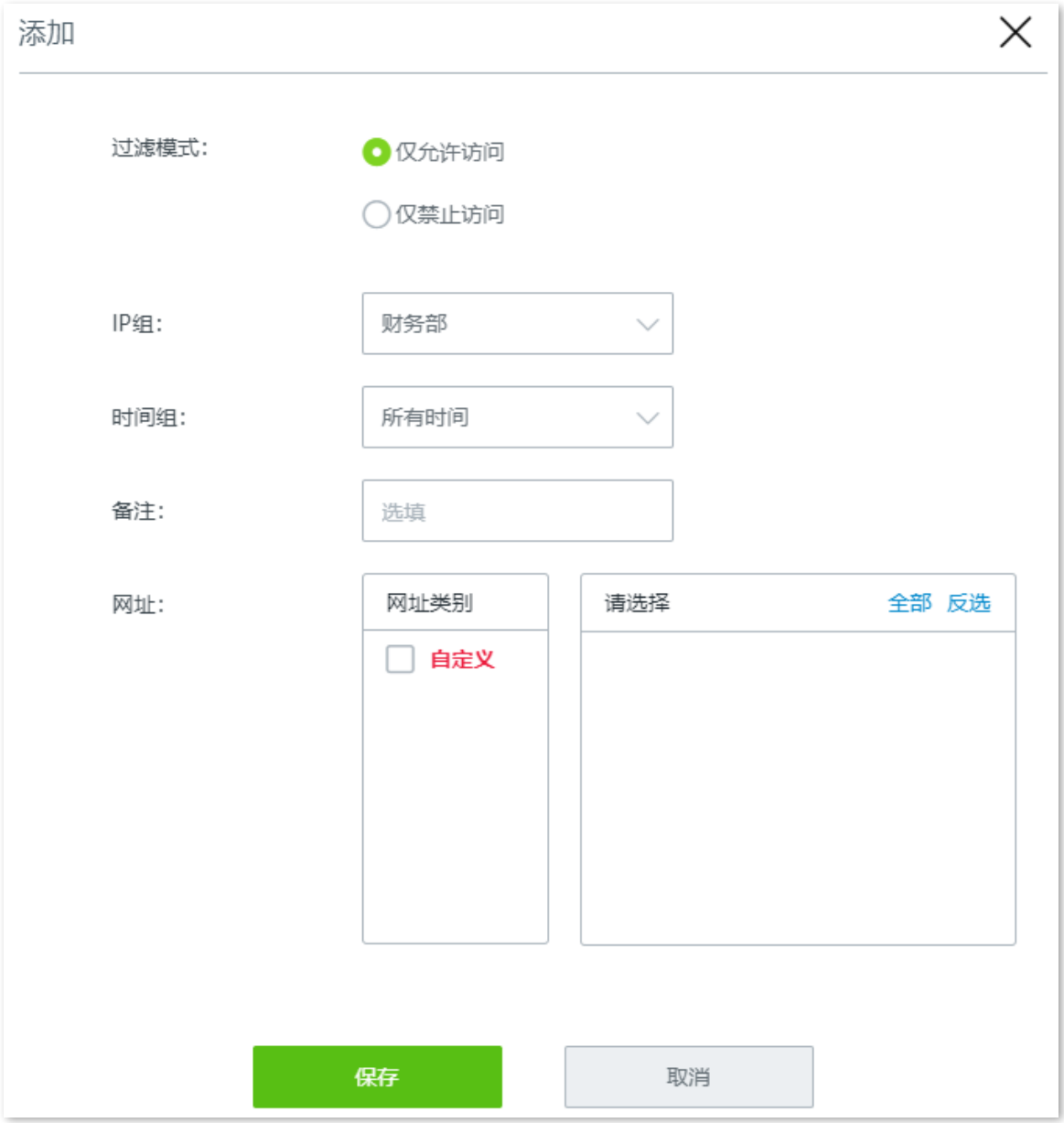
提示

- 如果路由器没有预置网址，请先自定义网址组，再添加网址过滤规则。
- 配置网站过滤规则前，请先配置好相应的 IP 组和时间组。

步骤 1 点击「行为管理」>「网站过滤」。

步骤 2 点击 +添加 。

步骤 3 在【添加】窗口配置各项参数，然后点击 保存 。


添加
过滤模式：
仅允许访问
仅禁止访问
IP组：
财务部
时间组：
所有时间
备注：
选填
网址：
网址类别
自定义
请选择
全部
反选
保存
取消

----完成

9.5.4 网站过滤配置举例

组网需求

某企业使用企业级路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），设计部门人员只能访问一些设计网站，如站酷（zcool.com.cn）、花瓣（huaban.com）、素材中国（sccnn.com）。

可以使用路由器的网站过滤功能实现上述需求。假设设计部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.10。

配置步骤

配置流程图：

配置时间组 → 配置 IP 组 → 开启网站过滤功能 → 添加网址组 → 添加网站过滤规则

步骤 1 配置时间组。

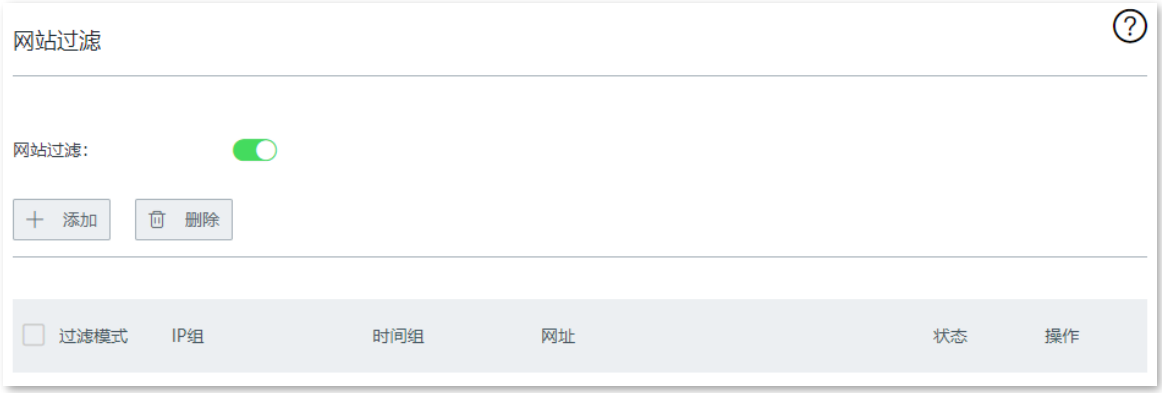
进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

步骤 2 配置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

步骤 3 开启网站过滤功能。

1. 点击「行为管理」>「网站过滤」。
2. 点击滑块至  。
3. 点击页面底端的 保存 。



步骤 4 添加网址组。

1. 点击 网址管理 。

2. 点击 新增分类 。

3. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 设置网址组名称，如“设计网站”。

(2) 输入要限制用户访问的网址，本例为“zcool.com.cn;huaban.com;sccnn.com”。

(3) （可选）设置网址组的备注信息，如“允许访问”。

步骤 5 添加网站过滤规则。

1. 点击 +添加 。

2. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 选择“过滤模式”，本例为“仅允许访问”。

(2) 选择需要限制访问网站的 IP 组，本例为“设计部”。

(3) 选择规则生效的时间组，本例为“上班时间”。

(4) （可选）设置规则备注信息，可不填。

(5) 选择要过滤的网址，本例为“设计网站”。

添加成功，如下图示。

----完成

验证配置

局域网中 IP 地址在 192.168.0.2~192.168.0.10 范围内的用户在星期一到星期五的 8:00~18:00 只能访问路由器中“设计网站”包含的网站。

10 更多设置

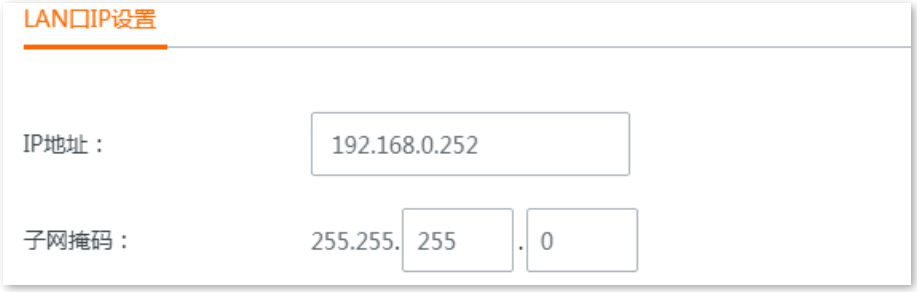
10.1 局域网设置

进入页面：点击「更多设置」>「局域网设置」。

在这里，您可以设置路由器的 LAN 口 IP 地址和 DHCP 服务器。

10.1.1 LAN 口 IP 设置

LAN 口 IP 地址是路由器对局域网的 IP 地址，也是路由器的管理 IP 地址。路由器默认的 LAN 口 IP 地址为 192.168.0.252，子网掩码为 255.255.255.0。



一般情况下，您无需修改 LAN 口设置，除非遇到 IP 地址冲突，如：路由器获得的 WAN 口 IP 地址和其 LAN 口 IP 地址处于同一网段；局域网内，有其它设备的 IP 地址也为 192.168.0.252。

修改 LAN 口 IP 地址后，系统出现如下提示。

进度条走完后，将自动重新跳转到登录页面。如果没有，请确保电脑的以太网（或本地连接）IP 地址设置为“自动获得”，之后使用新的 LAN 口 IP 地址重新尝试。

提示

如果新的 LAN 口 IP 地址与原 LAN 口 IP 地址不在同一网段，系统将自动匹配修改 DHCP 地址池，使其和新的 LAN 口 IP 地址在同一网段。

10.1.2 DHCP 服务器

DHCP 服务器能自动给局域网用户设备分配 IP 地址、子网掩码、网关地址和 DNS 等上网信息。

如果关闭此功能，需要在局域网设备上手动配置 IP 地址信息才能上网。如无特殊情况，请保持 DHCP 服务器为开启状态。

参数说明

标题项	说明
DHCP 服务器	DHCP 服务器功能开关。表示关闭，表示开启。
起始 IP 地址 结束 IP 地址	DHCP 服务器可分配的 IP 地址范围。起始 IP 地址默认为 192.168.0.2，结束 IP 地址默认为 192.168.0.254。
租约时间	DHCP 服务器分配给局域网设备的 IP 地址的有效时间，默认为 30 分钟。 当地址到期后： - 如果设备仍连接在路由器上，设备将自动续约，继续占用该 IP 地址。 - 如果设备未连接（关机、网线已拔掉、无线已断开等）到路由器，路由器将释放该 IP 地址。以后若有其它设备请求 IP 地址信息，路由器可将该 IP 地址分配给其它设备。 如无特殊需要，建议保持默认设置。
首选 DNS	DHCP 服务器分配给局域网设备的首选 DNS 服务器 IP 地址。本路由器支持 DNS 代理功能，故首选 DNS 默认为路由器的 LAN 口 IP 地址。 提示 一般情况下，建议保持默认设置。如需修改，为了使局域网设备能够正常上网，请务必确保您设置

标题项	说明
	的首选 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。
备用 DNS	DHCP 服务器分配给局域网设备的备用 DNS 服务器 IP 地址。不填表示 DHCP 服务器不分配此项。

10.2 WAN 口参数

进入页面：点击「更多设置」>「WAN 口参数」。

如果您已经正确完成联网设置，但路由器局域网的用户还是不能上网，或者上网出现问题，可以尝试修改 WAN 口参数解决。

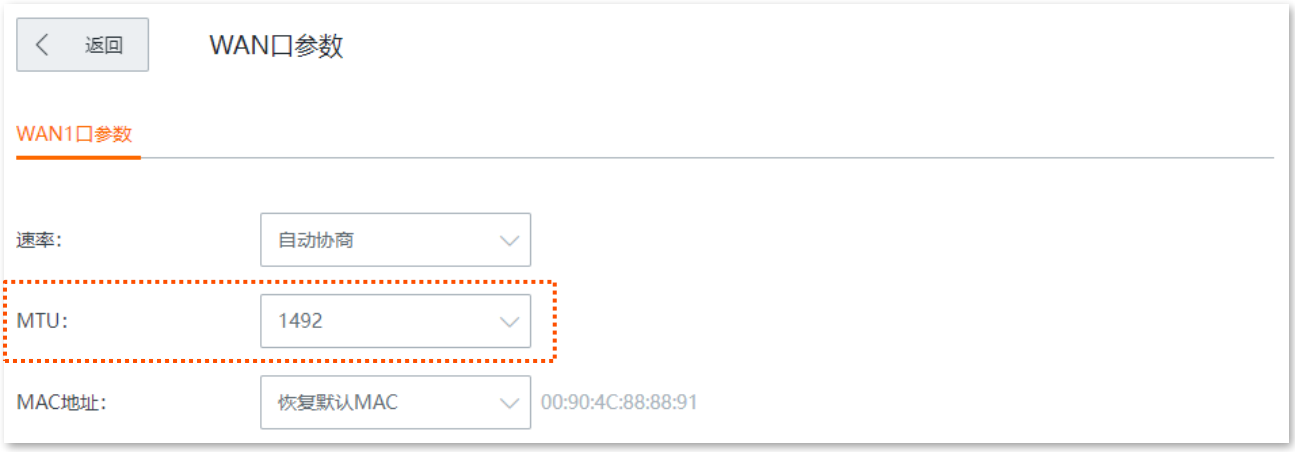
10.2.1 WAN 口速率

如果路由器 WAN 口已正确连接网线，且网线完好，但对应 WAN 口灯不亮；或者插上网线后 WAN 口灯要等待一会儿（5 秒以上）才亮。此时，可以将路由器的 WAN 口速率调为 10Mbps 半双工或 10Mbps 全双工尝试解决问题。

否则，建议 WAN 口速率保持默认设置“自动协商”。

10.2.2 MTU

MTU，即“最大传输单元”，是网络设备传输的最大数据包。联网方式为“宽带拨号”时，默认 MTU 值为 1492。联网方式为“动态 IP”或“静态 IP”时，默认 MTU 值为 1500。



一般情况下，建议保持 MTU 值为默认设置，除非您遇到以下情况：

- 无法访问某些网站、或打不开安全网站（如网银、支付宝登录页面）。
- 无法收发邮件、或无法访问 FTP 和 POP 等服务器等。

此时，可以尝试从最大值 1500 逐渐减少 MTU 值（建议修改范围 1400~1500），直到问题消失。

MTU 值应用说明

MTU 值	应用
1500	非宽带拨号、非 VPN 拨号环境下最常用的设置。
1492	用于宽带拨号环境。
1472	使用 ping 的最大值（大于此值的包会被分解）。
1468	用于一些 DHCP（动态 IP）环境。
1436	用于 VPN 或 PPTP 环境。

10.2.3 MAC 地址

当联网设置完毕后，如果路由器还是无法联网，有可能是 ISP 将上网账号信息与某一 MAC 地址（物理地址）绑定了。此时，您可以尝试通过 MAC 地址克隆（方法 1 或方法 2）解决该问题。

注意

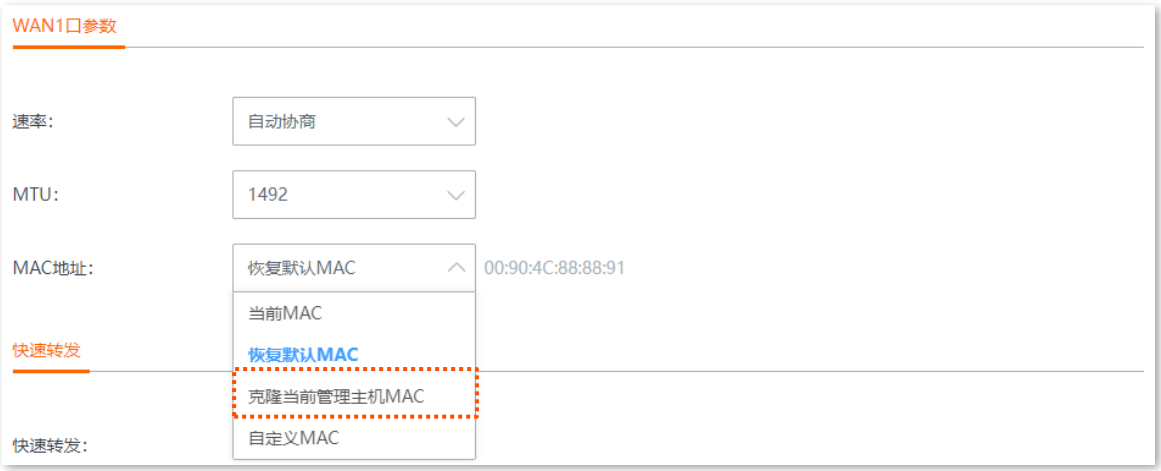
请克隆之前能正常上网的电脑 MAC 地址或能正常上网的路由器 WAN 口 MAC 地址。

方法 1：

步骤 1 使用之前能正常上网的电脑连接路由器。

步骤 2 登录路由器管理页面，点击「更多设置」>「WAN 口参数」进入设置页面，在对应 WAN 口的 MAC 地址选项框选择“克隆当前管理主机 MAC”。

步骤 3 点击页面底端的 保存 。



----完成

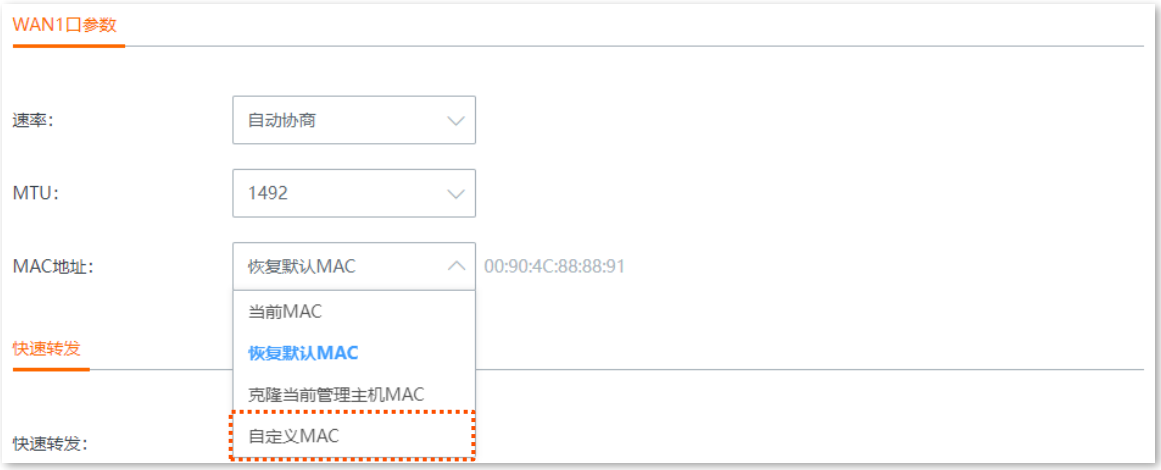
方法 2：

步骤 1 记录正确的 MAC 地址。

步骤 2 登录路由器管理页面，点击「更多设置」>「WAN 口参数」页面。

步骤 3 在对应 WAN 口的 MAC 地址选项框选择“自定义 MAC”，然后填入正确的 MAC 地址（可能是“直连宽带网线时能成功联网的电脑的 MAC 地址”或“之前能正常上网的路由器的 WAN 口 MAC 地址”）。

步骤 4 点击页面底端的 保存 。



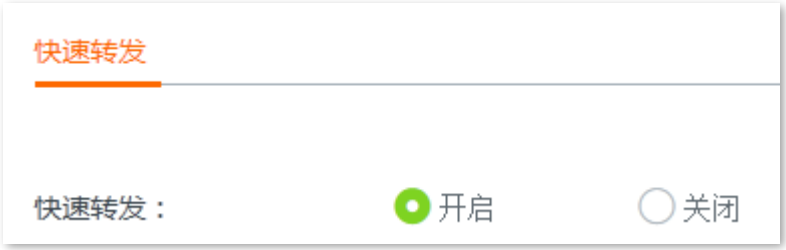
----完成

提示

如果需要将 MAC 地址恢复为出厂 MAC，请点击「更多设置」>「WAN 口参数」，在对应 WAN 口的 MAC 地址选项框选择“恢复默认 MAC”，然后点击页面底端的 保存 。

10.2.4 快速转发

路由器支持“快速转发”功能，开启此功能可以提高路由器的 NAT（网络地址转换）转发性能。



10.3 静态路由

10.3.1 概述

路由，是选择一条最佳路径把数据从源地址传送到目的地址的行为。静态路由则是手动配置的一种特殊路由，具有简单、高效、可靠等优点。合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。

通过设置目标网络、子网掩码、默认网关和接口来确定一条静态路由，其中，目标网络和子网掩码用来确定一个目标网络或主机。静态路由设置完成后，所有目的地址为静态路由目标网络的数据均直接通过该静态路由接口转发至网关地址。

> 注意
> 在大型复杂网络中完全使用静态路由时，如果网络发生故障或者拓扑发生变化，可能会出现路由不可达，并导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

进入页面：点击「更多设置」>「静态路由」。

参数说明

标题项	说明
目标网络	目的网络的 IP 地址。目标网络和子网掩码均为“0.0.0.0”表示默认路由。 提示 当在路由表中找不到与数据包的目的地址精确匹配的路由时，路由器会选择默认路由来转发该数据包。
子网掩码	目的网络的子网掩码。
默认网关	数据包从路由器的接口出去后，下一跳路由的入口 IP 地址。 默认网关为“0.0.0.0”表示直连路由，即该目标网络是路由器该接口直连的网络。
接口	数据从路由器出去的接口。请根据需要选择相应接口。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。

10.3.2 新增静态路由

注意

当静态路由规则和自定义的多 WAN 策略冲突时，静态路由优先生效。

在「更多设置」>「静态路由」页面，点击 +添加 ，然后在弹出窗口中设置各项参数，点击 保存 。

10.3.3 静态路由配置举例

组网需求

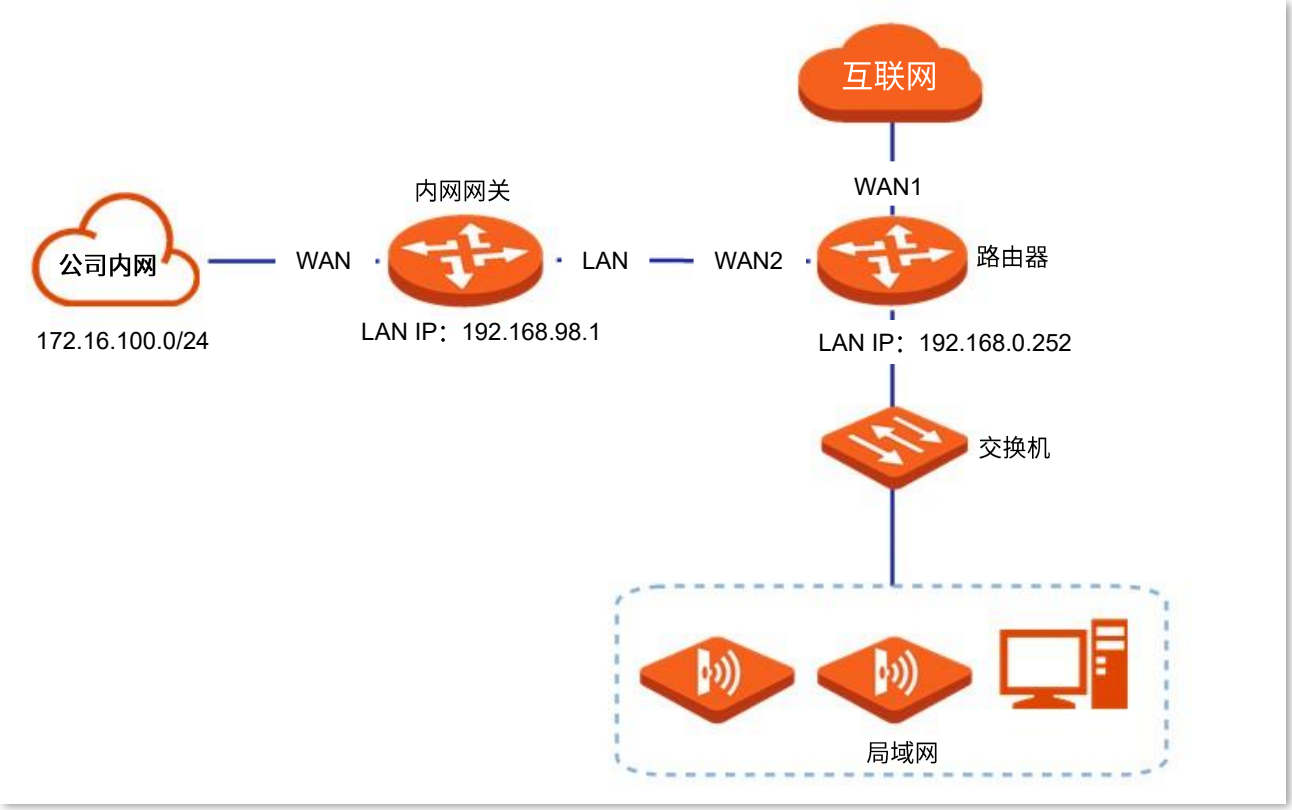
某企业使用企业级路由器进行网络搭建。互联网、公司内网在不同的网络，其中，WAN1 口通过宽带拨号接入互联网，WAN2 口通过动态 IP 接入公司内网。

要求：局域网的用户能同时访问互联网和公司内网。

方案设计

使用路由器的静态路由功能实现上述需求。

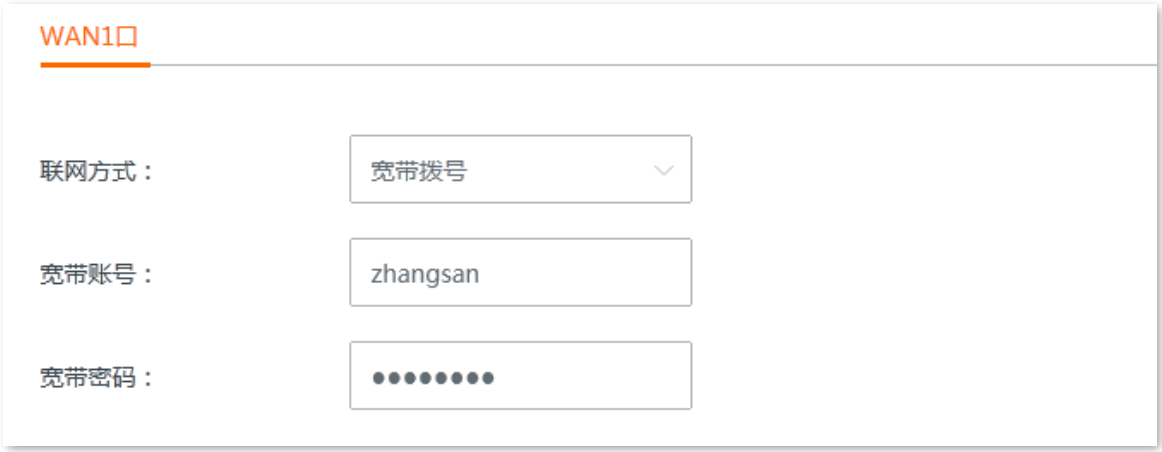
假设宽带账号和宽带密码均为 zhangsan。



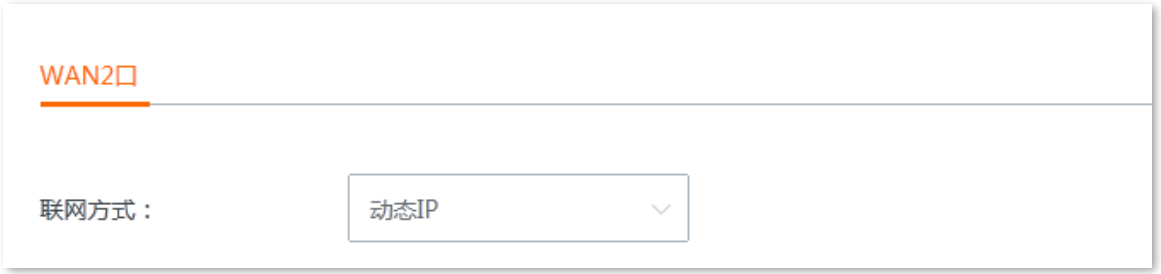
配置步骤

步骤 1 启用 2 个 WAN 口，并进行上网设置。

1. 点击「联网设置」。
2. 设置 WAN 口个数为“2”。
3. 在 WAN1 处选择“联网方式”为“宽带拨号”，输入 ISP 提供的“宽带账号”和“宽带密码”，本例均为“zhangsan”。

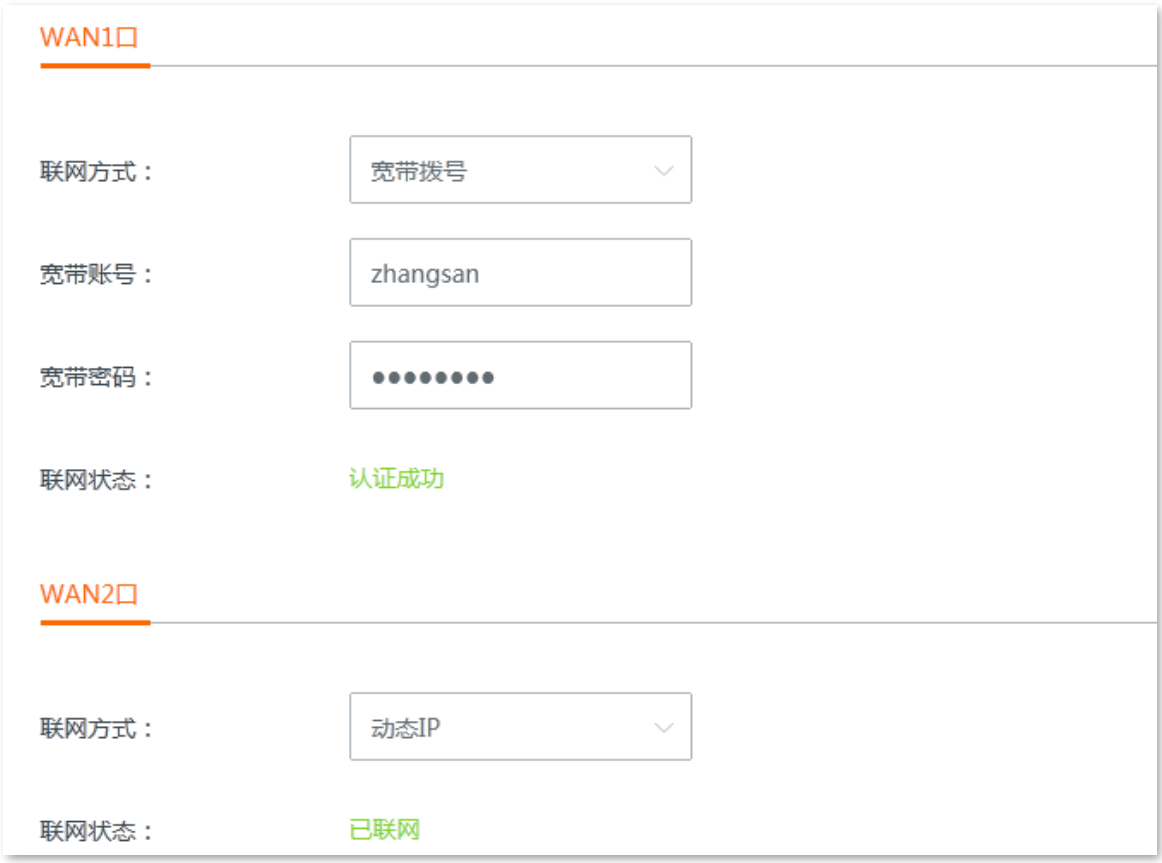


4. 设置 WAN2 口的“联网方式”为“动态 IP”。



5. 点击页面底端的 保存 ，之后按页面提示进行操作。

稍等片刻，当 WAN1 口的联网状态显示“认证成功”时，WAN1 口联网成功；当 WAN2 口的联网状态显示“已联网”时，WAN2 口联网成功。



步骤 2 配置静态路由。

1. 点击「系统状态」，查看 WAN2 获取的 IP 地址信息，假设如下：

   (1) IP 地址：192.168.98.190

   (2) 子网掩码：255.255.255.0

   (3) 默认网关：192.168.98.1

   (4) 首选 DNS：192.168.98.1

2. 添加静态路由规则。

   (1) 点击「更多设置」>「静态路由」。

   (2) 点击 +添加 。

   (3) 在【添加】窗口进行如下配置，然后点击 保存 。

   - 输入目的网络的 IP 地址，本例为“172.16.100.0”。
   - 输入目的网络的子网掩码，本例为“255.255.255.0”。
   - 输入下一跳路由的入口 IP 地址，本例为“192.168.98.1”。
   - 选择路由器与目标网络通信的接口，本例为“WAN2”。

   添加成功。

----完成

验证配置

局域网中的电脑可以同时访问互联网和公司内网。

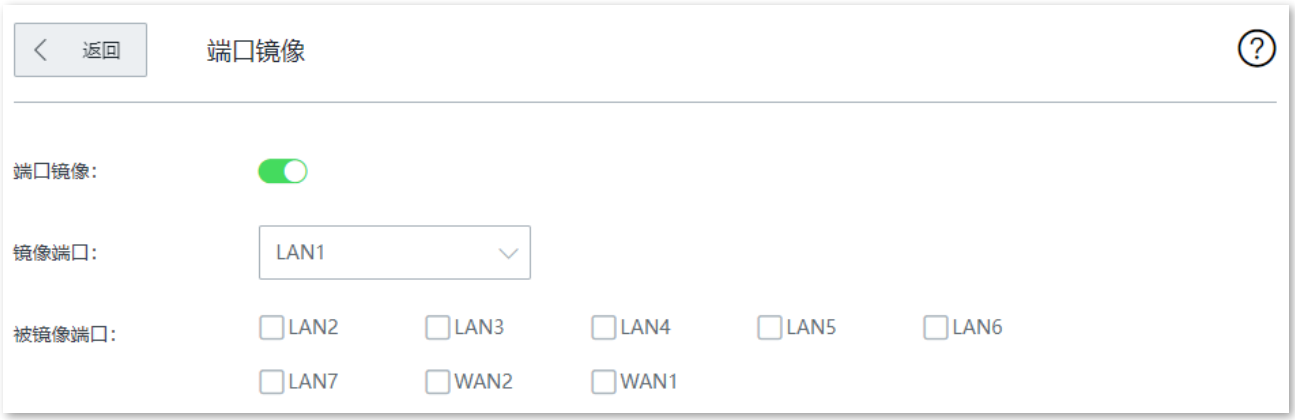
10.4 端口镜像

10.4.1 概述

通过端口镜像功能，可将路由器一个或多个端口（被镜像端口）的数据复制到指定的端口（镜像端口）。镜像端口一般接有数据监测设备，以便网络管理员实时进行流量监控、性能分析和故障诊断。

进入页面：点击「更多设置」>「端口镜像」。

端口镜像默认关闭，开启后，页面显示如下。



参数说明

标题项	说明
端口镜像	端口镜像功能开关。 表示关闭， 表示开启。
镜像端口	监控端口，该端口下的设备要安装监控软件。镜像端口默认为 LAN1，可根据需要修改。
被镜像端口	被监控端口。开启端口镜像功能后，被镜像端口的数据会被复制到镜像端口。

10.4.2 端口镜像配置举例

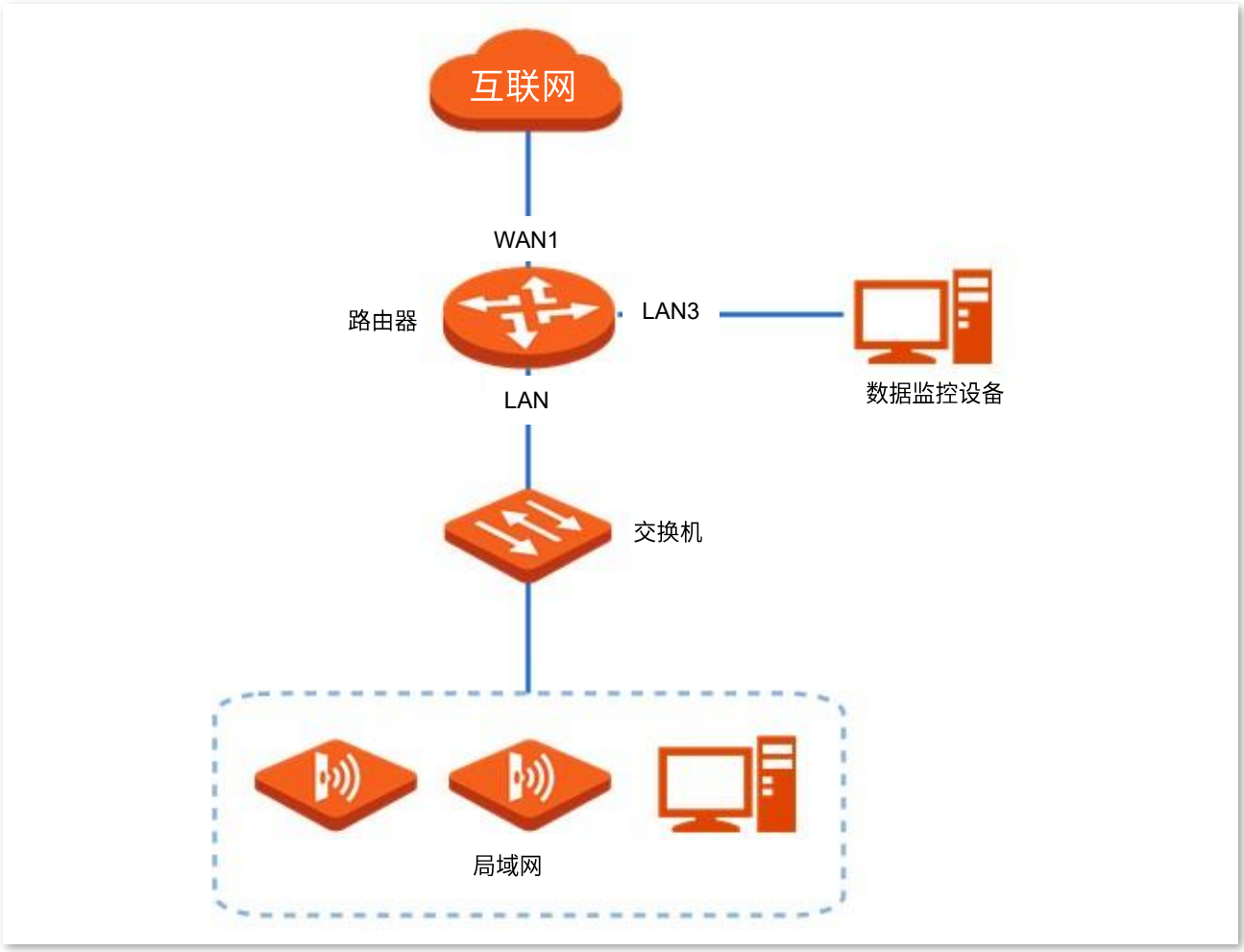
组网需求

某企业使用企业级路由器进行网络搭建，最近公司网络异常，经常上不了网，网络管理员需要捕获路由器 WAN 口、LAN 口的数据进行分析。

方案设计

使用路由器的端口镜像功能实现上述需求。

假设监控设备接在 LAN3 上，需要监控其余接口的数据。



配置步骤

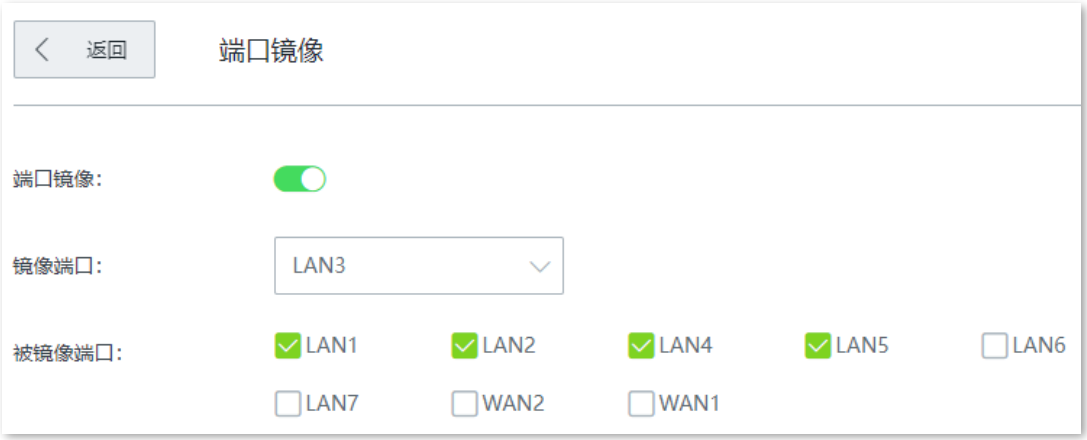
步骤 1 点击「更多设置」>「端口镜像」。

步骤 2 点击滑块至  。

步骤 3 选择“镜像端口”，本例为“LAN3”。

步骤 4 选择“被镜像端口”，本例为“WAN1、LAN2、LAN4、LAN5”。

步骤 5 点击页面底端的 保存 。



----完成

验证配置

在监控电脑上运行监控软件，如 Wireshark，可以抓取到被镜像端口的数据包。

10.5 远程 WEB 管理

10.5.1 概述

一般情况下，只有接到路由器 LAN 口或 LAN 口下的无线网络的设备才能登录路由器的管理页面。通过远程 WEB 管理功能，使您在有特殊需要时（如远程技术支持），可以通过 WAN 口远程访问路由器的管理页面。

进入页面：点击「更多设置」>「远程 WEB 管理」。

远程 WEB 管理默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
远程 WEB 管理	远程 WEB 管理功能开关。表示关闭，  表示开启。
WAN 口	路由器的 WAN 口，即远程访问路由器管理页面时所使用的 WAN 口。
远程主机的 IP 地址	可以远程访问路由器管理页面的设备的 IP 地址。 - 任意 IP 地址：互联网上任意 IP 地址的设备都能访问路由器的管理页面。为了网络安全，不建议选择此项。 - 特定 IP 地址：只有指定 IP 地址的设备能远程访问路由器的管理页面。如果该设备在局域网，则应填入该设备的网关的 IP 地址（公网 IP 地址）。

标题项	说明
远程管理地址	远程管理路由器时使用的域名。开启“远程 WEB 管理”功能后，互联网用户可以使用此域名登录到路由器管理页面。

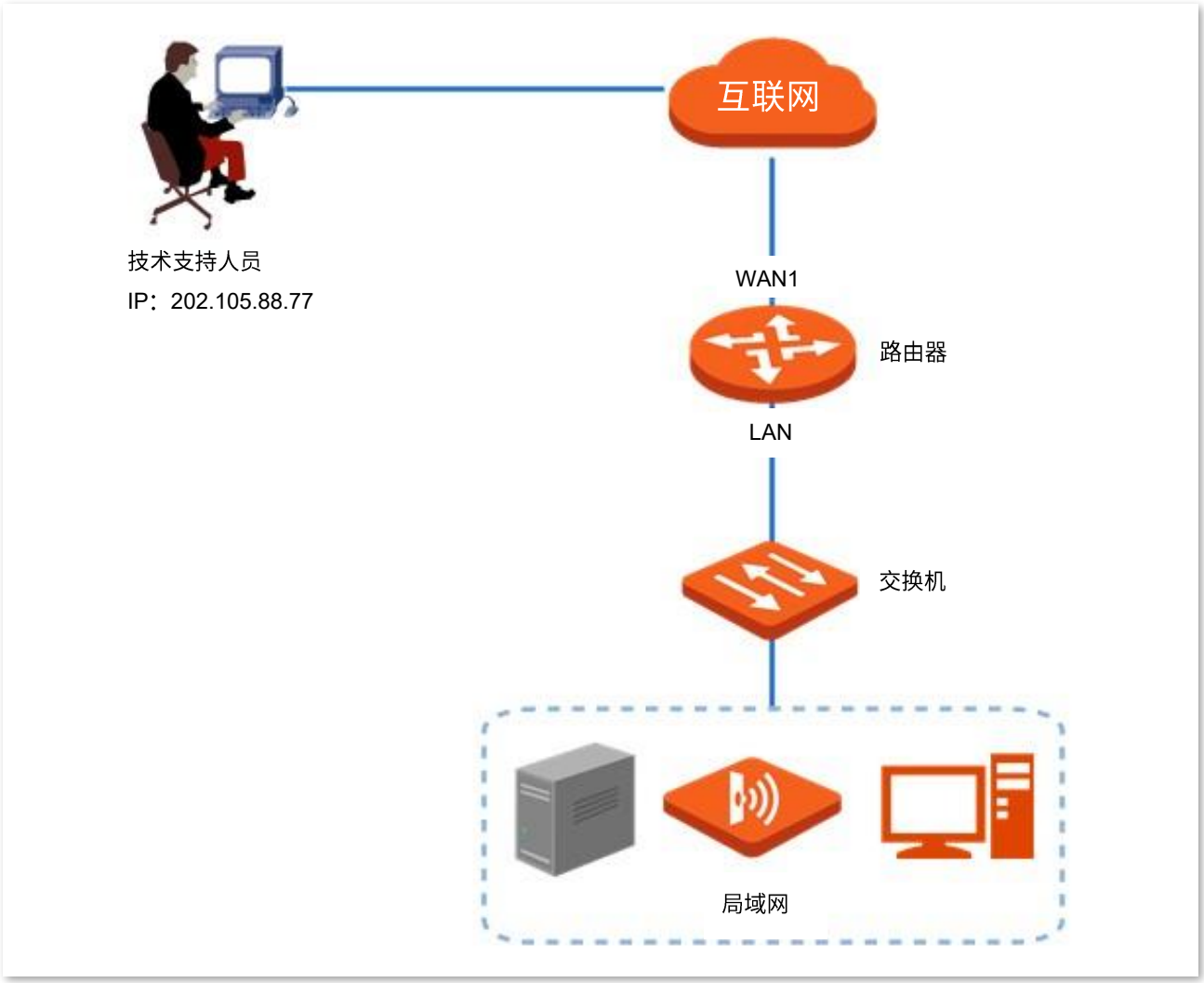
10.5.2 远程 WEB 管理配置举例

组网需求

某企业使用企业级路由器进行网络搭建，网络管理员在设置网络时遇到问题，需要 Tenda 技术支持远程登录到路由器管理页面分析并解决。

方案设计

可以采用路由器的远程 WEB 管理功能实现上述需求。



配置步骤

步骤 1 点击「更多设置」>「远程 WEB 管理」。

步骤 2 点击滑块至。

步骤 3 选择远程访问路由器时所使用的 WAN 口，本例为“WAN1”。

步骤 4 选择“特定 IP 地址”，然后输入 Tenda 技术支持的电脑的 IP 地址，本例为“202.105.88.77”。

步骤 5 点击页面底端的 保存 。

----完成

验证配置

Tenda 技术支持在其电脑（IP 地址为 202.105.88.77）上访问“http://o95ju9jc.cloud.tendacn.net:8080”，即可登录路由器管理页面并对其进行管理。

10.6 DDNS

10.6.1 概述

DDNS，Dynamic Domain Name Server，动态域名服务。当服务运行时，路由器上的 DDNS 客户端将路由器当前的 WAN 口 IP 地址传送给 DDNS 服务器，然后服务器更新数据库中域名与 IP 地址的映射关系，实现动态域名解析。

通过 DDNS 功能，可以将路由器动态变化的 WAN 口 IP 地址（公网 IP 地址）映射到一个固定的域名上。DDNS 功能通常与端口映射、DMZ 主机等功能结合使用，使外网用户可以通过域名访问路由器局域网服务器或路由器管理页面，无需再关注路由器的 WAN 口 IP 地址变化。

进入页面：点击「更多设置」>「DDNS」。

DDNS 默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
DDNS 服务	开启/关闭 DDNS 功能。
服务提供商	DDNS 的服务提供商。路由器支持的 DDNS 服务提供商有：3322、88ip、oray（花生壳）、gnway（金万维）。

标题项	说明
服务类型	该 DDNS 账号的类型。仅在服务提供商为 oray 时显示此参数。
用户名	登录 DDNS 服务的用户名/密码。
密码	即在 DDNS 服务提供商网站上注册的登录用户名及对应登录密码。
域名	在 DDNS 服务商处申请的域名信息。设置为除 oray 外的其他 DDNS 提供商时，需要手动输入在对应网站上申请的域名。
状态	显示 DDNS 服务的运行状态。

10.6.2 DDNS 配置举例

组网需求

某企业使用企业级路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。现需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

方案设计

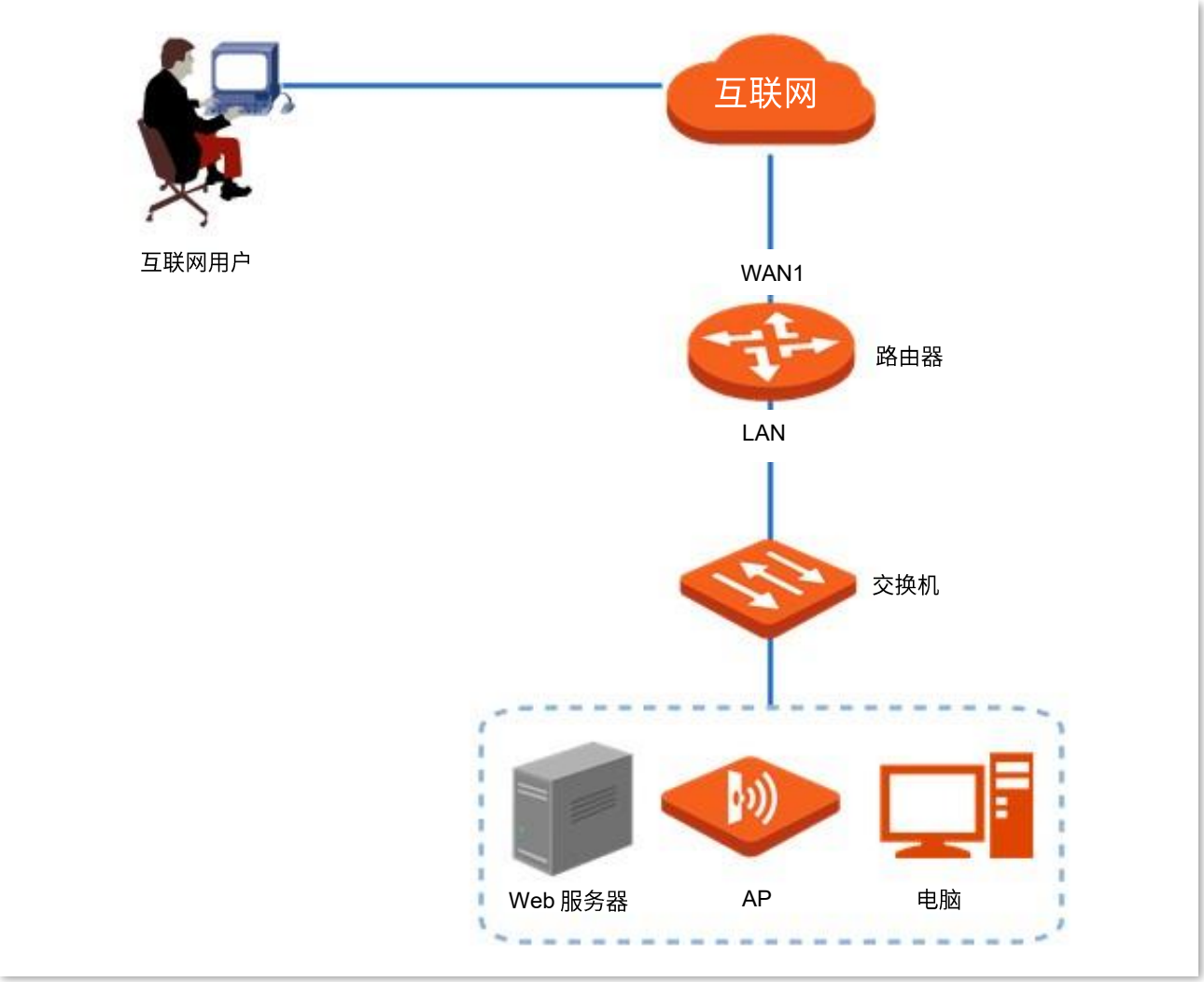
- 使用端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。
- 使用 DDNS 功能让互联网用户可以通过固定域名访问企业内部 Web 服务器，防止因 WAN 口 IP 地址变化导致访问失败。
- 使用静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.0.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999

提示

- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在设置端口映射时，建议将外网端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。
- 内网端口和外网端口可设置为不同的端口号。



配置步骤

配置流程图：

配置端口映射 → 给服务器主机分配固定 IP 地址 → 配置 DDNS

步骤 1 配置端口映射。

在「更多设置」>「端口映射」页面，配置如下规则。若有需要，可参考新增端口映射规则。

步骤 2 给服务器主机分配固定 IP 地址。

1. 点击「静态 IP 分配」，找到“手动分配 IP 地址”模块。

2. 点击 添加 。

3. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 设置固定分配给服务器主机的 IP 地址，本例为“192.168.0.250”。

(2) 输入服务器主机的 MAC 地址，本例为“C8:9C:DC:60:54:69”。

固定 IP 地址分配完成，如下图示。

步骤 3 配置 DDNS。

1. 注册域名。

登陆到 DDNS 服务提供商网站进行注册。假设您到 3322 网站注册的用户名为 zhangsan，密码为 123456，申请到的域名为 zhangsan.3322.org。

2. 登录到路由器的管理页面，设置 DDNS。

(1) 点击「更多设置」>「DDNS」，找到对应 WAN 口模块，本例为“WAN1 口”。

(2) 选择“DDNS 服务”为“开启”。

(3) 选择您申请域名的 DDNS 提供商，本例为“3322”。

(4) 输入您在 DDNS 服务提供商网站注册的用户名及对应登录密码，本例分别为“zhangsan”和“123456”。

(5) 输入您从 DDNS 服务提供商网站申请的域名，本例为“zhangsan.3322.org”。

(6) 点击页面底端的 保存 。

DDNS 服务配置完成，刷新一下页面，稍等片刻。当 WAN1 口“状态”显示为“已联网”时，连接成功。

----完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://对应 WAN 口域名”可以成功访问内网服务器。添加端口映射规则时，如果设置的外网端口号不是内网服务的默认端口号，访问格式为“内网服务应用层协议名称://对应 WAN 口域名:外网端口”。

在本例中，访问地址为“http://zhangsan.3322.org:9999”。

提示

配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保您填写的内网端口是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。

10.7 端口映射

10.7.1 概述

默认情况下，广域网中的用户不能访问局域网内的设备。利用端口映射功能，您可以开放路由器的一个或多个服务端口（TCP 或 UDP），并将这些端口映射到指定的局域网服务器，使路由器能够将发送到该端口的服务请求转发到对应的局域网服务器。这样，广域网中的用户就能够访问局域网服务器，局域网也能避免受到侵袭。

进入页面：点击「更多设置」>「端口映射」。

参数说明

标题项	说明
内网服务器 IP 地址	内网服务器的 IP 地址。
内网端口	内网服务器的服务端口。
外网端口	路由器开放给广域网用户访问的端口。
协议	内网服务使用的传输层协议类型。“全部”表示 TCP 和 UDP。设置时，如果不确定服务的协议类型，可以选择“全部”。
端口（接口）	内网服务映射的 WAN 口，即广域网用户访问局域网服务器时使用的 WAN 口。
状态	规则的状态，可根据需要开启或关闭。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。

10.7.2 新增端口映射规则

在「更多设置」>「端口映射」页面，点击 +添加 ，然后在弹出窗口中设置各项参数，点击 保存 。

10.7.3 端口映射配置举例

组网需求

某企业使用企业级路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。现需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

方案设计

- 使用端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。假设路由器开放的外网端口为 9999。
- 使用静态 IP 分配功能防止因 Web 服务器 IP 地址改变导致互联网用户访问企业内部 Web 服务器失败。

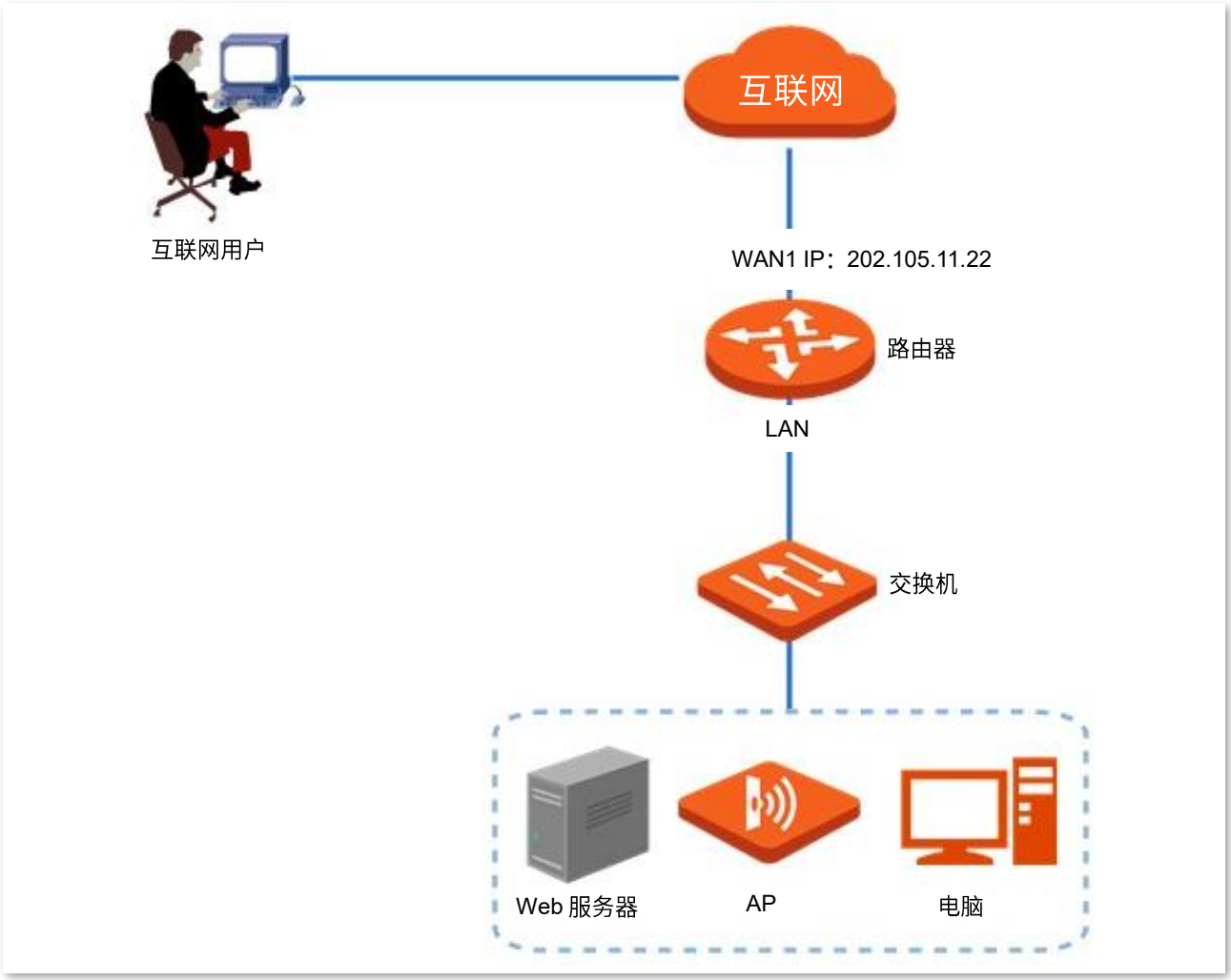
假设 Web 服务器信息如下：

- 服务器地址：192.168.0.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69

- 服务端口：9999

提示

- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在设置端口映射时，建议将外网端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。
- 内网端口和外网端口可设置为不同的端口号。



配置步骤

配置流程图：

配置端口映射 → 给服务器主机分配固定 IP 地址

步骤 1 配置端口映射。

1. 点击「更多设置」>「端口映射」。

2. 点击 +添加 。

3. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 输入 Web 服务器的 IP 地址，本例为“192.168.0.250”。

(2) 输入内网端口，即 Web 服务器使用的端口，本例为“9999”。

(3) 输入外网端口，即路由器开放给广域网用户访问的端口，如“9999”。

(4) 选择 Web 服务器使用的协议“TCP”，如果您不清楚，可以选择“全部”。

(5) 选择互联网用户访问局域网服务器时使用的 WAN 口，本例为“WAN1”。

端口映射规则配置完成，如下图示。

步骤 2 给服务器主机分配固定 IP 地址。

1. 点击「静态 IP 分配」，找到“手动分配 IP 地址”模块。
2. 点击 添加 。

3. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) 设置固定分配给服务器主机的 IP 地址，本例为“192.168.0.250”。

(2) 输入服务器主机的 MAC 地址，本例为“C8:9C:DC:60:54:69”。

固定 IP 地址分配完成，如下图示。

----完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址”可以成功访问内网服务器。如果设置的外网端口号不是内网服务的默认端口号，访问格式为“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址:外网端口”。

在本例中，访问地址为“http://202.105.11.22:9999”。

您可以在「系统状态」页面找到路由器 WAN 口当前 IP 地址。

如果该 WAN 口开启了 DDNS，还可使用“内网服务应用层协议名称://该 WAN 口域名:外网端口”访问。

提示

配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保您填写的内网端口是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。

10.8 DMZ 主机

10.8.1 概述

将局域网中的某台电脑设置为 DMZ 主机后，该电脑与互联网通信时将不受限制。例如：某台电脑正在进行视频会议或在线游戏，可将该电脑设置为 DMZ 主机使视频会议和在线游戏更加顺畅。另外，在互联网用户需要访问局域网资源时，也可将该服务器设置为 DMZ 主机。

注意

- 将设备设置成 DMZ 主机后，该设备相当于完全暴露于外网，路由器的防火墙对该设备不再起作用。
- 黑客可能会利用 DMZ 主机对本地网络进行攻击，请不要轻易使用 DMZ 主机功能。
- DMZ 主机上的安全软件、杀毒软件以及系统自带防火墙，可能会影响 DMZ 主机功能，使用本功能时，请暂时关闭。不使用 DMZ 主机时，建议关闭该功能，并且打开 DMZ 主机上的防火墙、安全卫士和杀毒软件。

进入页面：点击「更多设置」>「DMZ 主机」。

DMZ 主机默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
DMZ 主机	开启/关闭 DMZ 主机功能。
DMZ 主机 IP 地址	要设置为 DMZ 主机的局域网设备的 IP 地址。
VPN 端口过滤	开启/关闭 VPN 端口过滤功能。 开启后，启用 DMZ 功能时，由路由器的 VPN 服务响应外网的 VPN 请求。

标题项	说明
	注意 路由器已开启 VPN 功能的情况下，开启 DMZ 主机功能时，请同时开启“VPN 端口过滤”功能。

10.8.2 DMZ 主机配置举例

组网需求

某企业使用企业级路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。现需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

方案设计

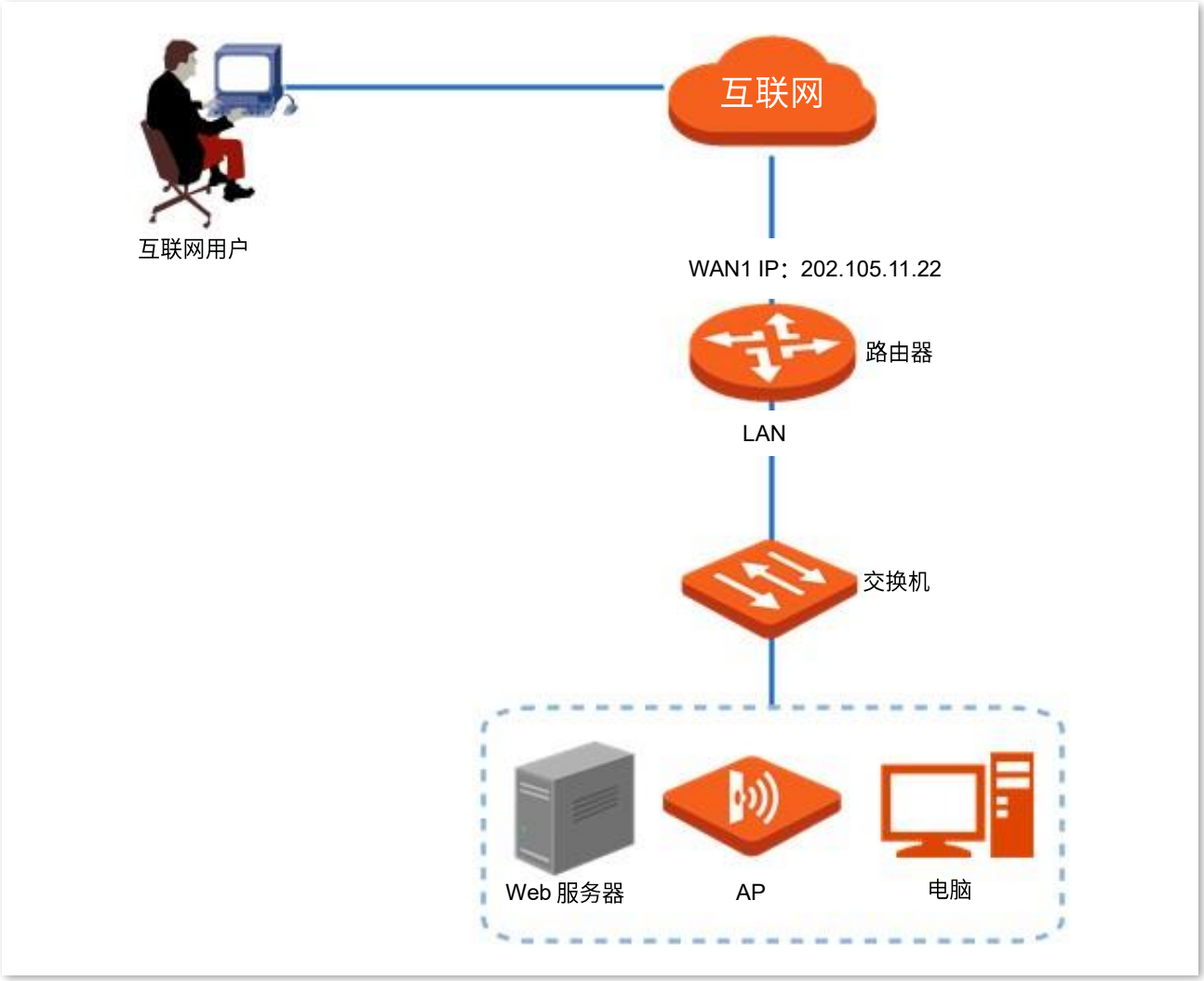
- 使用 DMZ 主机功能实现互联网用户访问企业内部 Web 服务器的需求。
- 使用静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.0.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999

提示

- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在使用 DMZ 主机功能时，建议将内网服务端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。



配置步骤

配置流程图：

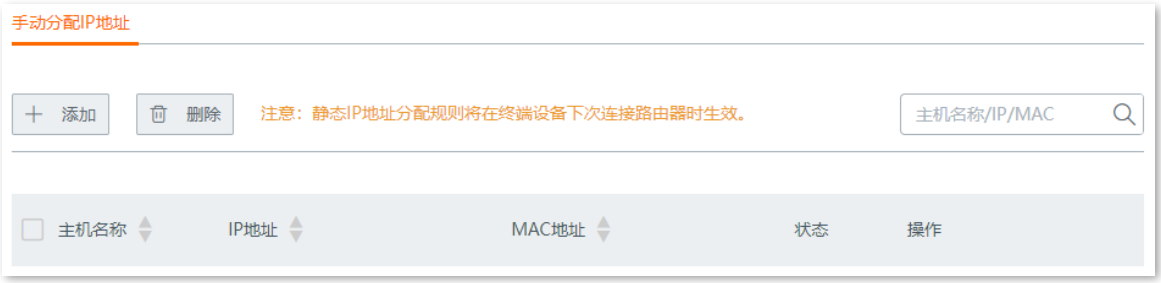
配置 DMZ 主机 → 给 DMZ 主机分配固定 IP 地址

步骤 1 配置 DMZ 主机。

1. 点击「更多设置」>「DMZ 主机」，找到对应 WAN 口模块。
2. 选择“DMZ 主机”为“开启”。
3. 输入局域网内要设置为 DMZ 主机的设备的 IP 地址，本例为“192.168.0.250”。
4. 点击页面底端的 保存 。

步骤 2 给 DMZ 主机分配固定 IP 地址。

1. 点击「静态 IP 分配」，找到“手动分配 IP 地址”模块。
2. 点击 添加 。



3. 在【添加】窗口进行如下配置，然后点击 保存 。

(1) IP 地址：设置固定分配给服务器主机的 IP 地址，本例为“192.168.0.250”。

(2) MAC 地址：输入服务器主机的 MAC 地址，本例为“C8:9C:DC:60:54:69”。

固定 IP 地址分配完成，如下图示。

----完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址”可以成功访问内网服务器。如果内网服务端口不是默认端口号，访问格式为“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址:内网服务端口”。

在本例中，访问地址为“http://202.105.11.22:9999”。

您可以在「系统状态」页面找到路由器 WAN 口当前 IP 地址。

如果该 WAN 口开启了 DDNS，还可使用“内网服务应用层协议名称://对应 WAN 口域名:内网服务端口”访问。

提示

配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，可能是 DMZ 主机上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。

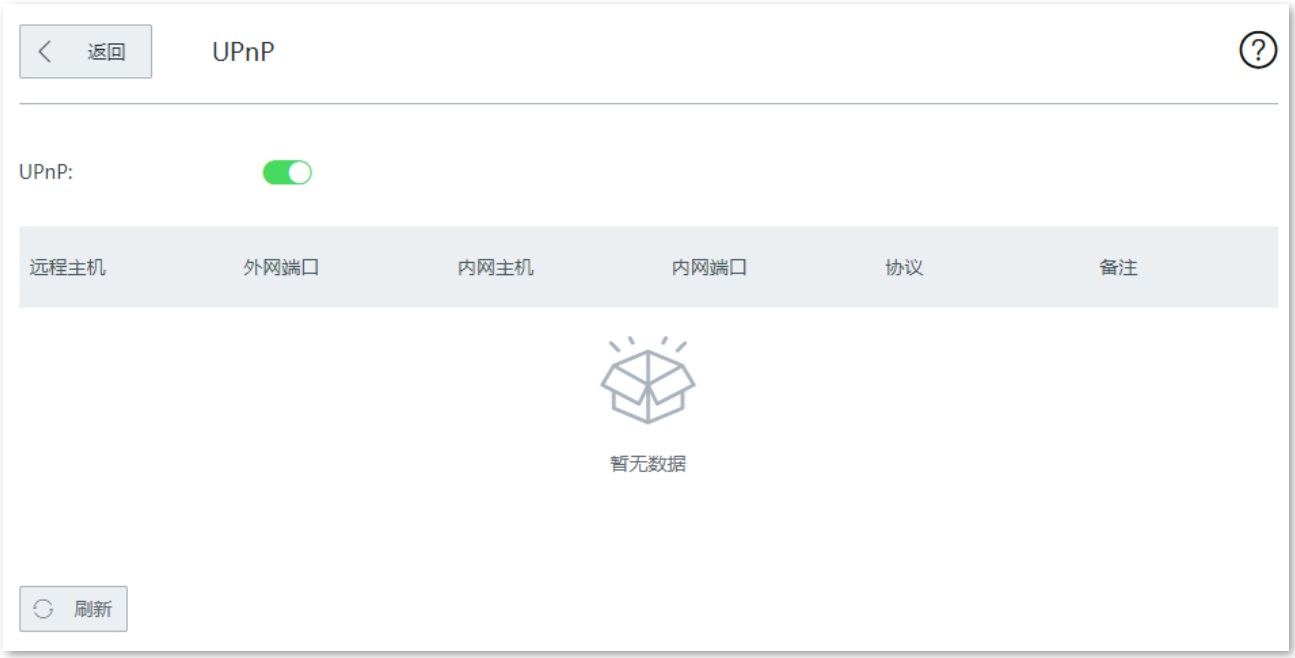
10.9 UPnP

10.9.1 概述

UPnP，Universal Plug and Play，通用即插即用。开启 UPnP 功能后，路由器可以为内网中支持 UPnP 的程序（如迅雷、BitComet、AnyChat 等）自动打开端口，使应用更加顺畅。

10.9.2 开启 UPnP

在「更多设置」>「UPnP」页面，点击滑块至  。



开启 UPnP 功能后，当局域网中运行支持 UPnP 的程序（如迅雷等）时，可以在此页面看到应用程序发出请求时提供的端口转换信息。如下图示例。

UPnP:

远程主机	外网端口	内网主机	内网端口	协议	备注
anywhere	42094	192.168.0.110	28795	TCP	PTL-D8C4976CAE...
anywhere	28795	192.168.0.110	28795	UDP	PTL-D8C4976CAE...
anywhere	28795	192.168.0.110	28796	TCP	PTL-D8C4976CAE...
anywhere	20741	192.168.0.110	12345	UDP	MiniTP SDK
anywhere	20741	192.168.0.110	54321	TCP	MiniTP SDK

10.10 攻击防御

路由器支持的攻击防御类型有：ARP 攻击防御、DDoS 防御、IP 攻击防御和防 WAN 口 Ping。

- ARP 防御：路由器可以识别局域网的 ARP 欺骗，并记录攻击者的 MAC 地址。
- DDoS 防御：DDoS 攻击，即分布式拒绝服务（Distributed Denial of Service）攻击。利用 DDoS 攻击，攻击者可以消耗目标系统资源，使该目标系统无法提供正常服务。路由器可以防御的 DDoS 攻击类型包括：ICMP Flood、UDP Flood、SYN Flood。
- IP 攻击防御：路由器可以按照要求拦截具有一些特殊 IP 选项的数据包，这些 IP 选项包括：IP Timestamp Option、IP Security Option、IP Stream Option、IP Record Route Option、IP Loose Source Route Option 及非法 IP 选项等。
- 防 WAN 口 Ping：广域网主机 Ping 路由器 WAN 口 IP 地址时，路由器可以自动忽略该 Ping 请求，防止暴露自己，同时防范外部的 Ping 攻击。

进入页面：点击「更多设置」>「攻击防御」。

参数说明

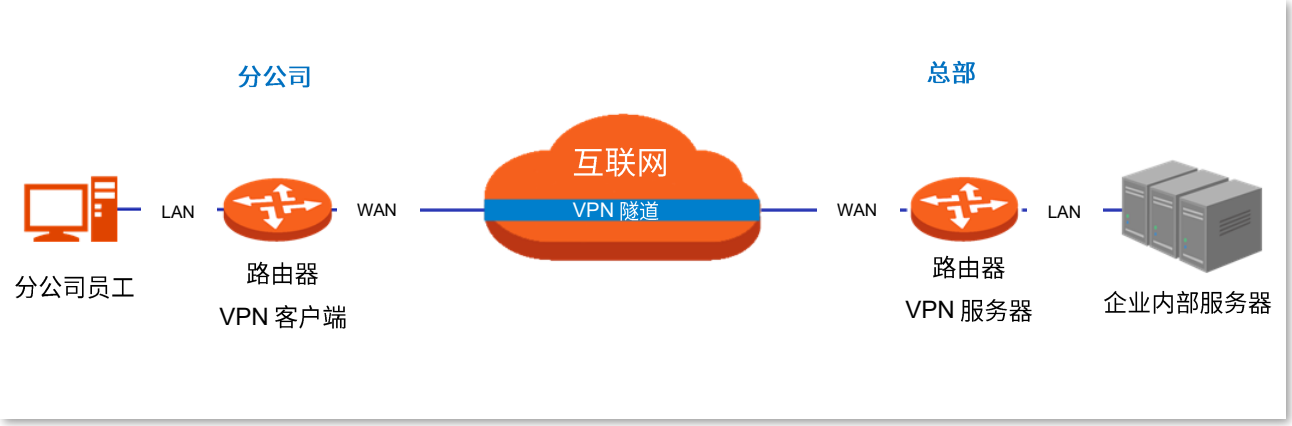
标题项		说明
攻击防御	ARP 防御	启用/禁用 ARP 防御功能。
	ARP 广播间隔	路由器发送 ARP 查询报文的间隔。
DDoS 防御	ICMP Flood 阈值	一秒钟内，如果路由器收到来自局域网同一主机的 ICMP 请求包超过此阈值，则认为路由器正受到 ICMP Flood 攻击。
	UDP Flood 阈值	一秒钟内，如果路由器收到来自局域网同一主机的 UDP 包超过此阈值，则认为路由器正受到 UDP Flood 攻击。
	SYN Flood 阈值	一秒钟内，如果路由器收到来自局域网同一主机的 TCP SYN 包超过此阈值，则认为路由器正受到 SYN Flood 攻击。
IP 攻击防御	IP Timestamp Option	启用后，路由器将拦截局域网中带有 Internet Timestamp 选项的 IP 包。
	IP Security Option	启用后，路由器将拦截局域网中带有 Security 选项的 IP 包。
	IP Stream Option	启用后，路由器将拦截局域网中带有 Stream ID 选项的 IP 包。
	IP Record Route Option	启用后，路由器将拦截局域网中带有 Record Route 选项的 IP 包。
	IP Loose Source Route Option	启用后，路由器将拦截局域网中带有 Loose Source Route 选项的 IP 包。
	非法 IP 选项	启用后，路由器将检查局域网 IP 包的完整性、正确性，如果不符合，则拦截。
防 WAN 口 Ping		启用/禁用路由器的防 WAN 口 Ping 功能。默认“禁用”。 启用防 WAN 口 Ping 功能后，路由器自动忽略互联网主机对其 WAN 口 IP 地址的 Ping，以防止暴露自己，同时防范外部的 Ping 攻击。

10.11 VPN 服务

10.11.1 概述

VPN（Virtual Private Network，虚拟专用网），是一个建立在公用网络（通常是互联网）上的专用网络，这个专用网络只在逻辑上存在，并没有实际物理线路。VPN 技术广泛应用于企业网络，用来实现企业分公司与总部的资源共享，同时确保这些资源不会暴露给互联网上的其他用户。

VPN 的典型网络拓扑图如下。



本系列路由器支持的 VPN 服务有：

- PPTP/L2TP VPN 服务器
- PPTP/L2TP VPN 客户端
- IPSec

VPN 服务器

本路由器可以作为 PPTP/L2TP 服务器，接受 PPTP/L2TP 客户端的连接。

进入页面：点击「更多设置」>「VPN 服务器」。

VPN 服务器默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
VPN 服务器	VPN 服务器功能开关。表示关闭，表示开启。 开启后，路由器作为 VPN 服务器。
服务器类型	路由器使用的 VPN 协议类型，PPTP 或 L2TP。PPTP 和 L2TP 都是二层 VPN 隧道协议，使用 PPP（点到点协议）进行数据封装，并都为数据增添额外首部。 - PPTP：路由器作为 PPTP 服务器，接受 PPTP 客户端的连接。 - L2TP：路由器作为 L2TP 服务器，接受 L2TP 客户端的连接。
WAN 口	VPN 服务器与客户端建立 VPN 隧道的 WAN 口。该 WAN 口的 IP 地址或域名是 VPN 客户端的“服务器 IP 地址/域名”。
加密	只有 PPTP VPN 才支持此选项。 是否启用 128 位数据加密。客户端、服务器双方的加密设置需保持一致，否则将不能正常通信。
IPSec 加密	只有 L2TP VPN 才支持此选项。 是否启用 IPSec 加密。如果要进行 IPSec 加密，请选择封装模式为“传输模式”的 IPSec 规则。

标题项	说明
地址池	VPN 服务器可分配给 VPN 客户端的 IP 地址范围。
最大用户数	VPN 服务器最多支持的 VPN 客户端数量。系统固定为 32 个。
用户名	VPN 用户账号和密码，即 VPN 用户进行 PPTP/L2TP 拨号（VPN 连接）时需要输入的用户名/密码。
密码	
是否网络	VPN 客户端类型。 - 是：VPN 客户端是一个网络时选择。此时，需要设置 VPN 客户端的“网段”、“子网掩码”参数。 - 否：VPN 客户端是一台主机。
网段	VPN 客户端为一个网络时，在此输入客户端的内网网络号。
子网掩码	VPN 客户端为一个网络时，在此输入客户端内网的子网掩码。
备注	该账号的描述信息。
状态	该账号的使用状态，可以根据需要启用或禁用。
操作	可对账号进行如下操作： - 点击 可以修改账号。 - 点击 可以删除账号。

新增 PPTP/L2TP 用户账号：

在「更多设置」>「VPN 服务器」页面，点击 +添加 ，然后在【添加】窗口中配置各项参数，点击 保存 。


添加
用户名：
密码：
是否网络：
是
否
备注：
选填
保存
取消

VPN 客户端

本路由器可以作为 PPTP/L2TP 客户端连接到 PPTP/L2TP 服务器。

进入页面：点击「更多设置」>「VPN 客户端」。

VPN 客户端默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
VPN 客户端	VPN 客户端功能开关。表示关闭，  表示开启。 开启后，路由器作为 VPN 客户端。
客户端类型	路由器使用的 VPN 协议类型，PPTP 或 L2TP。PPTP 和 L2TP 都是二层 VPN 隧道协议，使用 PPP（点到点协议）进行数据封装，并都为数据增添额外首部。 - PPTP：要连接的 VPN 服务器是 PPTP 服务器时，选择此项。 - L2TP：要连接的 VPN 服务器是 L2TP 服务器时，选择此项。
WAN 口	路由器进行 VPN 拨号时使用的 WAN 口。
服务器 IP 地址/域名	要拨入的 VPN 服务器的 IP 地址或域名，一般是对端 VPN 路由器上开启了“PPTP/L2TP 服务器”功能的 WAN 口的 IP 地址或域名。
用户名	输入 PPTP/L2TP 用户账号，即 VPN 服务器分配的用户名和密码。
密码	
加密	根据 VPN 服务器配置选择是否启用数据加密。请和服务器配置保持一致，否则不能正常通信。只有 PPTP VPN 才支持此选项。
VPN 代理上网	开启后，局域网内的用户通过 VPN 服务器端路由器上网。
服务器内网网段	VPN 服务器端局域网的网段。
服务器内网子网掩码	VPN 服务器端局域网的子网掩码。
状态	当前 VPN 的连接状态。

IPSec

IPSec（IP Security，IP 安全性）是一系列协议的集合，用来实现在互联网上安全、保密地传送数据。

IPSec 相关概念如下：

- **封装模式**

  封装模式，即 IPSec 传输的数据的封装模式。IPSec 支持“隧道模式”和“传输模式”两种。

  - 隧道模式：增加新的 IP 头，通常用于两个安全网关之间的通讯。用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。
  - 传输模式：不改变原有 IP 头部，通常用于主机和主机之间的通信。只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。

- **安全网关**

  指具有 IPSec 功能的网关设备（安全加密路由器），安全网关之间可以利用 IPSec 对数据进行安全保护，保证数据不被偷窥和篡改。

- **IPSec 对等体**

  IPSec 的两个端点被称为 IPSec 对等体，要在两个对等体（安全网关）之间安全传输数据，首先要在两者之间建立安全联盟（Security Association，SA）。

- **SA**

  SA（Security Association，安全联盟）是通信对等体间对某些要素的约定。如，使用哪种协议（AH、ESP 还是两者结合）、协议的封装模式（传输模式、隧道模式）、加密算法（DES、3DES、AES）、特定流中保护数据的共享密钥以及密钥的生命周期等。SA 具有以下特征：

  - 由{SPI，IP 目的地址，安全协议标识符}三元组唯一标识。
  - 它决定了对报文进行何种处理：协议、算法、密钥。
  - 每个 IPSec SA 都是单向的，并且是具有生命周期的。
  - SA 可以手工建立或由 IKE（Internet Key Exchange，互联网密钥交换）协商生成。IKE 协议分为 IKEv1 和 IKEv2 两个版本，本路由器支持 IKEv1，下文中涉及的 IKE 均指 IKEv1。

新增 IPSec 连接

在「更多设置」>「IPSec」页面，点击 +添加 ，然后在出现的页面配置各项参数，点击 保存 。

参数说明

标题项	说明
IPSec	开启/关闭 IPSec 功能。
WAN 口	IPSec 生效的 WAN 口，IPSec 对端设备的“远端网关地址”需填为此接口的 IP 地址。
封装模式	IPSec 数据的封装模式。 - 隧道模式：通常用于两个安全网关之间的通讯。

标题项	说明
	- 传输模式：通常用于主机和主机、主机与网关之间的通信。
隧道名称	该 IPSec 连接的名称。
协商模式	IPSec 隧道的协商模式。 - 初始者模式：主动向对端发起连接。 - 响应者模式：等待对端发起连接。  请勿将 IPSec 隧道两端都设置为“响应者模式”，否则会导致 IPSec 隧道建立失败。
隧道协议	为 IPSec 提供安全服务的协议。 - AH：Authentication Header，鉴别首部。该协议主要提供数据完整性校验功能，若数据报文在传输过程中被篡改，则接收方将在完整性验证时丢弃该报文。 - ESP：Encapsulating Security Payload，封装安全性载荷。该协议可以对数据的完整性进行检查，还对数据进行加密，这样，即使报文在传输过程中被截获，截取方也难以获取到真实信息。 - AH+ESP：同时使用上述两种协议。
远端网关地址	IPSec 隧道对端网关的 IP 地址或域名。
本地内网网段/前缀长度	本路由器局域网的网段/前缀长度。例如：本路由器的 LAN 口 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0，则本地内网网段/前缀长度可填为 192.168.0.0/24。
远端内网网段/前缀长度	IPSec 隧道对端网关局域网的网段/前缀长度。若对端是一台特定主机，则此参数设置为“该设备的 IP 地址/32”。
密钥协商方式	建立 IPSec 安全隧道的密钥协商方式。本路由器支持“自动协商”和“手动设置”。 - 自动协商：默认模式。通过 IKE 自动建立 SA，并进行动态维护、删除，降低了手工配置的复杂度，简化 IPSec 的使用、管理工作。自动建立的 SA 有生命周期，会定时更新，增强了安全性。 - 手动设置：用户手动设置加密/认证算法及密钥来建立 SA。手动建立的 SA 没有生命周期限制，除非手动删除，否则永不过期，因此有安全隐患。该方式常用于调试阶段。

密钥协商方式--自动协商

自动协商时，为了保证信息的私密性，IPSec 通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由 IKE 完成。IKE 是 ISAKMP、Oakley、SKEME 这三个协议的混合体。

- ISAKMP：Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议，该协议为交换密钥和 SA 协商提供了一个框架。
- Oakley：密钥确定协议，该协议描述了密钥交换的具体机制。
- SKEME：安全密钥交换机制，该协议描述了与 Oakley 不同的另一种密钥交换机制。

IKE 协商过程分为两个阶段：

阶段 1：通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在阶段 2 中安全交换更多信息。

阶段 2：使用阶段 1 中建立的 ISAKMP SA 为 IPSec 的安全性协议协商参数，创建 IPSec SA，用于对双方的通信数据进行保护。

密钥协商方式为“自动协商”时，如下图。

参数说明

标题项	说明
认证方式	显示为“共享密钥方式”，表示 IPSec 双方事先通过某种方式协商好一个双方共享的密钥字符串。
预共享密钥	输入协商时所用的预共享密钥，需要与对端网关设备保持一致。最长为 128 字符。
DPD 检测	开启/关闭对等体检测功能。 通过 DPD 检测可以检测远端的隧道站点是否有效。
DPD 检测周期	发送 DPD 报文的周期。 路由器会按照设置的周期定时发送 DPD 报文。如果 DPD 报文在有效时间内没有得到远端的确认，则重新初始化本地到远端的 IPSec SA。

点击显示高级设置可显示自动协商的高级参数。点击后，页面如下图示。


点击隐藏
阶段1
模式：
Main
加密算法：
DES
完整性验证算法：
SHA1
Diffie-Hellman分组：
768
本地ID类型：
IP地址
对端ID类型：
IP地址
密钥生命周期：
3600
阶段2
PFS：
开启
关闭
加密算法：
DES
完整性验证算法：
SHA1
Diffie-Hellman分组：
768
密钥生命周期：
3600

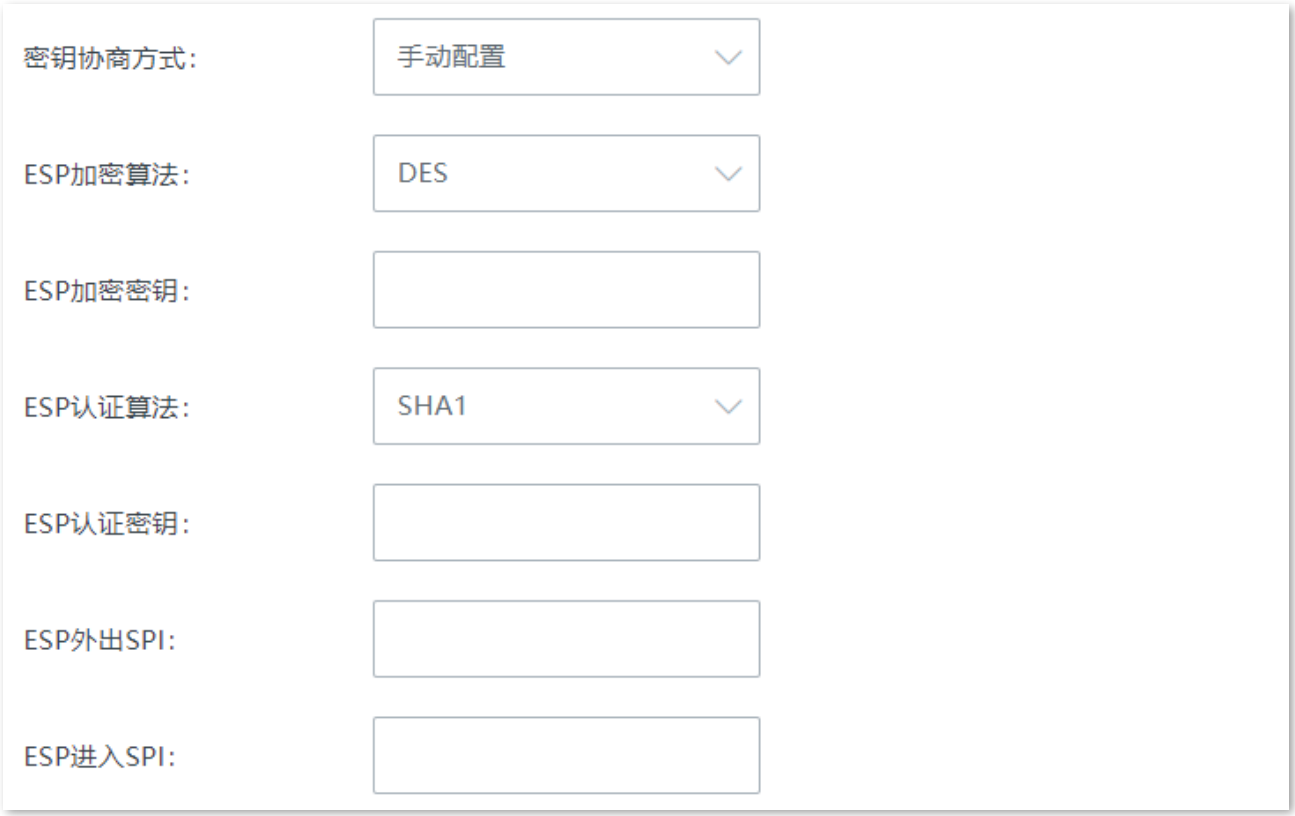
参数说明

标题项	说明
模式	IKE 阶段 1 的交换模式，该交换模式必须与对端设置相同。 - Main：主模式，此模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。 - Aggressive：野蛮模式，又称主动模式，此模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。
加密算法	应用于 IKE 会话的加密算法。路由器支持以下加密算法： - DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。 - AES（Advanced Encryption Standard，高级加密标准）：AES 128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。
完整性验证算法	应用于 IKE 会话的验证算法。路由器支持以下验证算法： - MD5：Message Digest Algorithm，消息摘要算法。对一段消息产生 128bit 的消息摘要，防止消息被篡改。 - SHA1：Secure Hash Algorithm，安全散列算法。对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。
Diffie-Hellman 分组	Diffie-Hellman 算法的组信息，用于产生加密 IKE 隧道的会话密钥。
本地 ID 类型	本地网关标识。 - IP 地址：本地路由器使用对应 WAN 口 IP 地址与对端网关协商。 - FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“本地 ID”输入框中输入任意字符串，用于与对端网关协商。“本地 ID”与远端网关的“对端 ID”必须相同。 注意 “本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）。
对端 ID 类型	对端网关标识。 - IP 地址：本地网关默认对端网关使用其 WAN 口 IP 地址进行协商。 - FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“对端 ID”输入框中输入任意字符串，用于与本地网关协商。“对端 ID”与远端网关的“本地 ID”必须相同。 注意 “本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）。
密钥生命周期	IPSec SA 的生存时间。
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）特性使得 IKE 阶段 2 协商生成一个新的密钥材料，该密钥材料与阶段 1 协商生成的密钥材料没有任何关联，这样即使 IKE1 阶段 1 的密钥被破

标题项	说明
	解，阶段 2 的密钥仍然安全。 如果没有使用 PFS，阶段 2 的密钥将根据阶段 1 生成的密钥材料来产生，一旦阶段 1 的密钥被破解，用于保护通信数据的阶段 2 密钥也岌岌可危，这将严重威胁到双方的通信安全。

密钥协商方式-手动设置

密钥协商方式为“手动设置”时，如下图（以隧道协议为“AH+ESP”时为例）。



参数说明

标题项	说明
ESP 加密算法	当隧道协议选择“ESP”时需设置 ESP 加密算法。路由器支持以下加密算法： - DES：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。 - AES：AES128/192/256 表示使用长度为 128/192/256bit 的密钥进行加密。
ESP 加密密钥	ESP 加密密钥。IPSec 通信双方设置需保持一致。

标题项	说明
ESP/AH 认证算法	当隧道协议选择“ESP”时，需设置 ESP 认证算法；当隧道协议选择“AH”时，需设置 AH 认证算法。路由器支持以下验证算法： - MD5：对一段消息产生 128bit 的消息摘要，防止消息被篡改。 - SHA1：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。
ESP/AH 认证密钥	当隧道协议选择“ESP”时，需设置 ESP 认证密钥；当隧道协议选择“AH”时，需设置 AH 认证密钥。 IPSec 通信双方设置需保持一致。
ESP/AH 外出 SPI	外出 SPI 参数。 SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“进入 SPI”值相同。
ESP/AH 进入 SPI	进入 SPI 参数。 SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“外出 SPI”值相同。

10.11.2 PPTP/L2TP VPN 服务配置举例

组网需求

某企业总部和分公司都使用企业级路由器进行网络搭建，并成功接入互联网。分公司员工需要经过互联网访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

方案设计

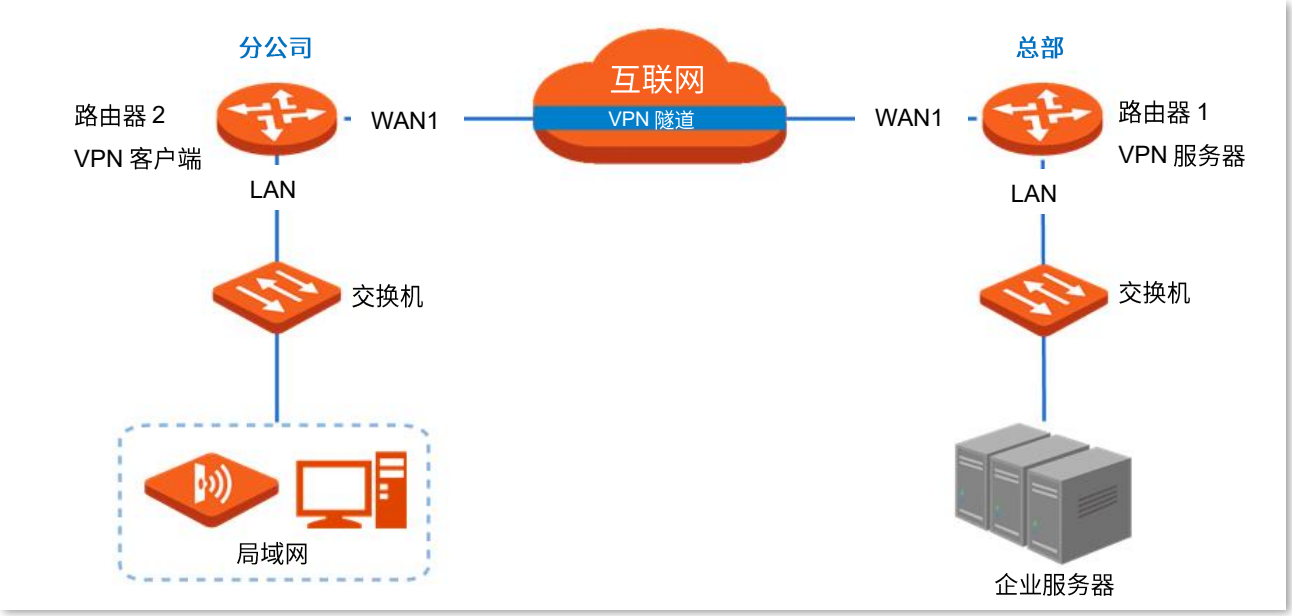
将一台路由器设置为 VPN 服务器，另一台设置为 VPN 客户端，实现远端用户经互联网安全访问企业内部局域网的需求。本例以 PPTP VPN 为例说明，L2TP VPN 的设置方法类似。

假设将路由器 1 设置为 PPTP 服务器，基本信息如下：

- PPTP 服务器分配的用户名、密码均为 fengongsi1。
- PPTP 服务器 IP 地址为 202.105.11.22。
- PPTP 服务器对数据启用加密。
- PPTP 服务器内网为 192.168.0.0/24。
- PPTP 服务器建立 VPN 隧道的接口为 WAN1。

假设将路由器 2 设置为 PPTP 客户端基本信息如下：

- PPTP 客户端内网为 192.168.1.0/24。
- 路由器与 PPTP 服务器建立隧道的接口为 WAN1。



配置步骤

配置流程图：

设置路由器 1 为 VPN 服务器 > 设置路由器 2 为 VPN 客户端

步骤 1 设置路由器 1 为 VPN 服务器。

1. 开启 PPTP 服务器。

(1) 登录路由器 1 的 WEB 管理界面，点击「更多设置」>「VPN 服务器」。

(2) 点击滑块至  。

(3) 进行如下配置，然后点击页面底端的 保存 。

- 选择 VPN 服务器类型，本例为“PPTP”。
- 指定 VPN 服务器与客户端建立隧道的 WAN 口，本例为“WAN1”。
- 选择“加密”为“开启”。

2. 配置 PPTP/L2TP 用户。

(1) 点击「更多设置」>「VPN 服务器」，找到“PPTP/L2TP 用户”模块。

(2) 点击 +添加 。

(3) 在【添加】窗口进行如下配置，然后点击 保存 。

- 输入 VPN 客户端进行 VPN 连接时所用的用户名，本例为“fengongsi1”。
- 输入对应用户名的密码，本例为“fengongsi1”。
- 选择“是否网络”为“是”。
- 输入 VPN 客户端局域网的网段，本例为“192.168.1.0”。
- 输入子网掩码为“255.255.255.0”。
- 输入该用户账号的描述信息，如“分公司 1”。

添加完成，如下图示。

步骤 2 设置路由器 2 为 VPN 客户端。

1. 登录路由器 2 的 WEB 管理界面，点击「更多设置」>「VPN 客户端」。
2. 点击滑块至。
3. 进行如下配置，然后点击 保存 。

(1) 选择“客户端类型”与 VPN 服务器侧一致，本例为“PPTP”。

(2) 指定 VPN 客户端与服务器建立隧道的 WAN 口，本例为“WAN1”。

(3) 输入 VPN 服务器侧作为隧道出口的 WAN 口的 IP 地址/域名，本例为“202.105.11.22”。

(4) 输入 VPN 服务器分配的用户名，本例为“fengongsi1”。

(5) 输入 VPN 服务器分配的用户名对应的密码，本例为“fengongsi1”。

(6) 选择“加密”为“开启”，与 VPN 服务器侧配置保持一致。

(7) 输入 VPN 服务器内网的网段，本例为“192.168.0.0”。

(8) 输入 VPN 服务器内网的子网掩码，本例为“255.255.255.0”。

当页面的状态显示为“已联网”时，VPN 连接成功。如下图示。

----完成

之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。

验证配置

下文以分公司访问总部 FTP 服务器为例。公司总部的项目资料放在 FTP 服务器中，假设服务器信息如下：

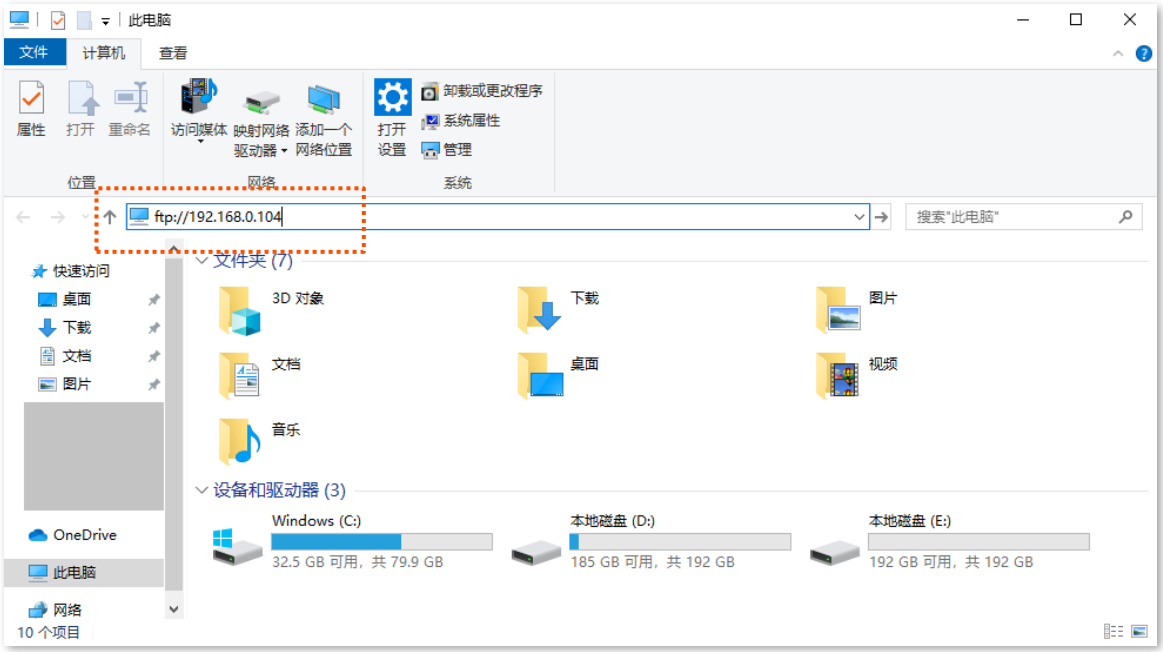
- FTP 服务器 IP 地址为 192.168.0.104
- FTP 服务端口为 21
- FTP 服务器登录用户名和密码均为 zhangsan

当分公司员工访问总部项目资料时，步骤如下：

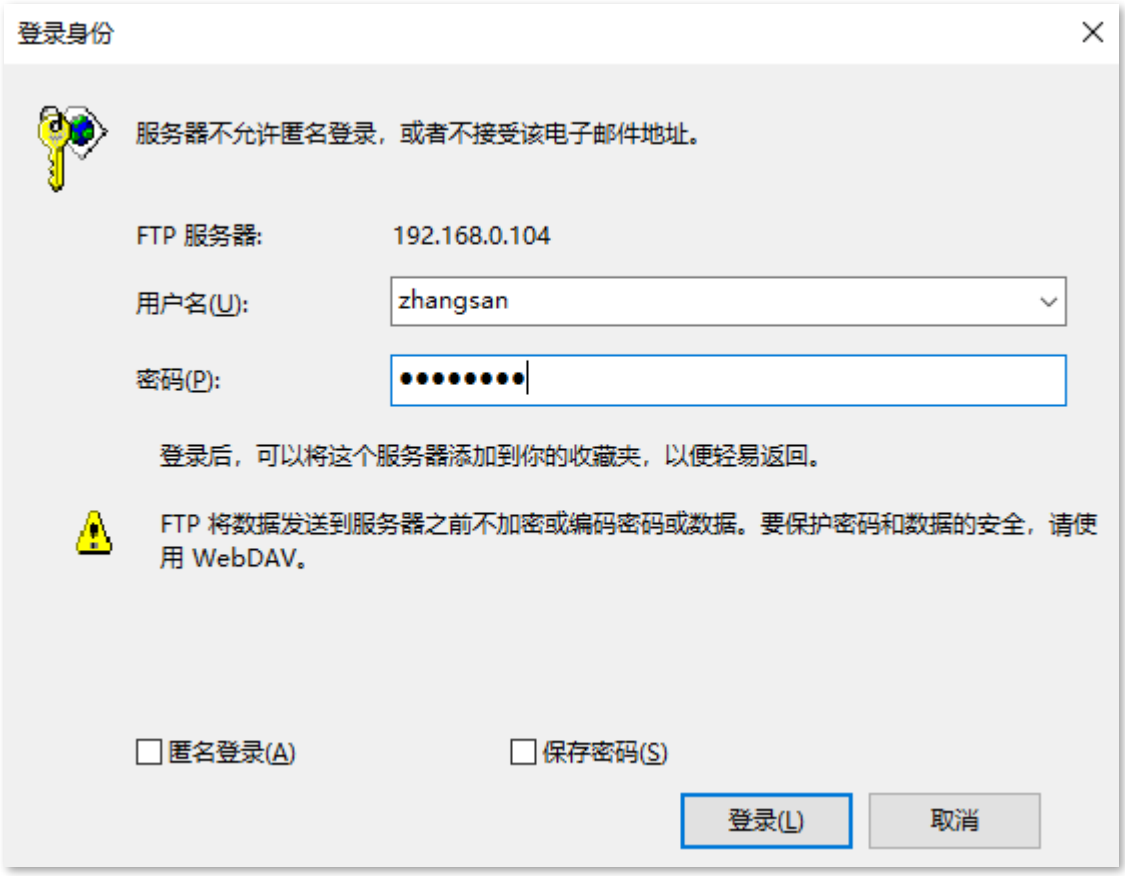
步骤 1 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 ftp://192.168.0.104。

提示

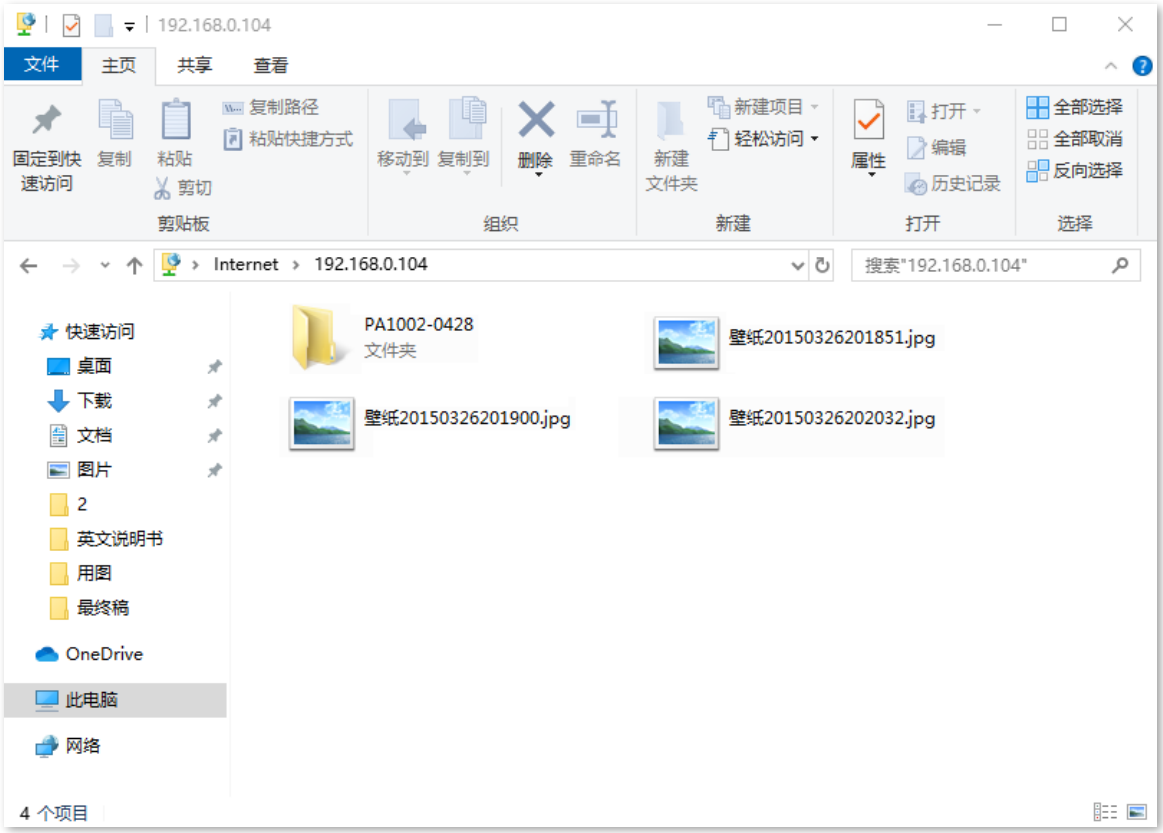
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



步骤 2 输入登录用户名和密码，本例均为“zhangsan”，然后点击 登录 。


登录身份
服务器不允许匿名登录，或者不接受该电子邮件地址。
FTP 服务器:
192.168.0.104
用户名(U):
zhangsan
密码(P):
登录后，可以将这个服务器添加到你的收藏夹，以便轻易返回。
FTP 将数据发送到服务器之前不加密或编码密码或数据。要保护密码和数据的安全，请使用 WebDAV。
匿名登录(A)
保存密码(S)
登录(L)
取消

访问成功。


192.168.0.104
文件
主页
共享
查看
固定到快速访问
复制
粘贴
剪切
复制路径
粘贴快捷方式
剪贴板
移动到
复制到
删除
重命名
组织
新建项目
轻松访问
新建文件夹
新建
属性
打开
编辑
历史记录
打开
全部选择
全部取消
反向选择
选择
Internet › 192.168.0.104
搜索"192.168.0.104"
快速访问
桌面
下载
文档
图片
2
英文说明书
用图
最终稿
OneDrive
此电脑
网络
PA1002-0428
文件夹
壁纸20150326201851.jpg
壁纸20150326201900.jpg
壁纸20150326202032.jpg
4 个项目

10.11.3 IPSec VPN 配置举例

组网需求

某企业总部和分公司都使用企业级路由器进行网络搭建，并成功接入互联网。分公司员工需要经过互联网访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

方案设计

在 2 台路由器上均建立 IPSec 隧道，实现远端用户经互联网安全访问企业内部局域网的需求。

假设将路由器 1 部署在总部，基本信息如下：

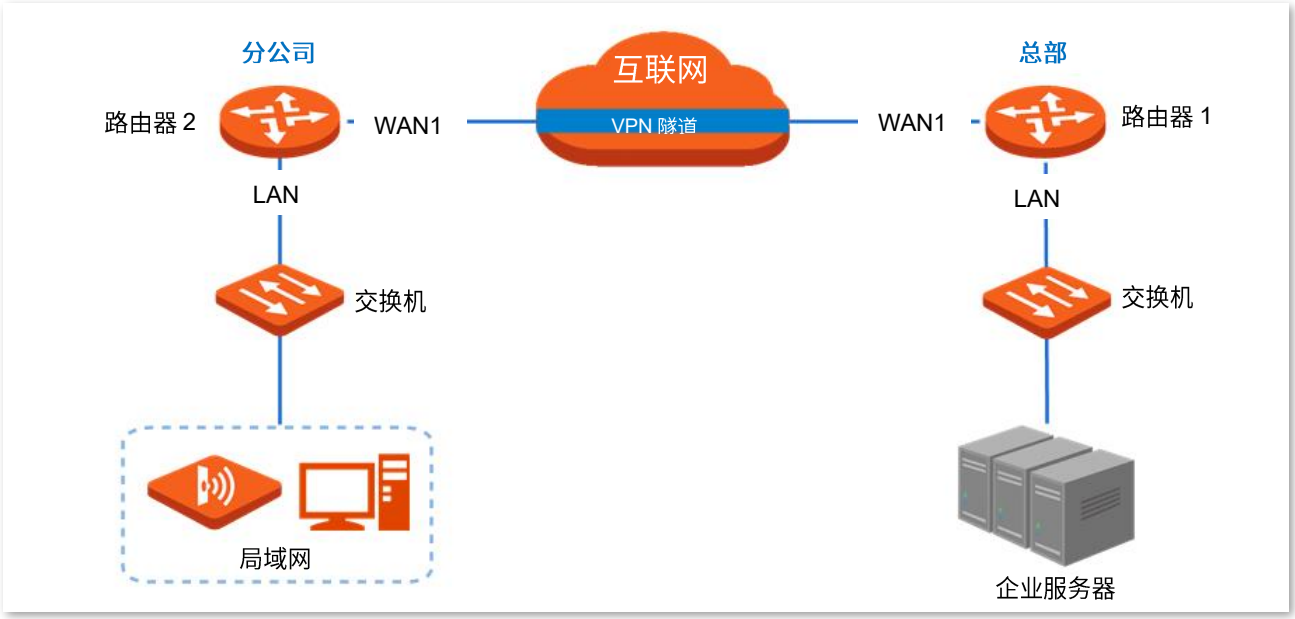
- 建立 IPSec 隧道的接口为 WAN1。
- WAN1 IP 地址为 202.105.11.22。
- 局域网网络为 192.168.0.0/24。

假设将路由器 2 部署在分公司，基本信息如下：

- 建立 IPSec 隧道的接口为 WAN1。
- WAN1 IP 地址为 202.105.88.77。
- 局域网网络为 192.168.1.0/24。

假设两台路由器的 IPSec 连接基本信息如下：

- 封装模式为隧道模式。
- 密钥协商方式为自动协商。
- 预共享密钥为 12345678。



配置步骤

配置流程图：

设置路由器 1 → 设置路由器 2

注意

配置过程中，如果需要设置 IPSec 连接的高级选项，请保持两台路由器的设置参数一致。

步骤 1 设置路由器 1。

1. 登录路由器 1 的 WEB 管理界面，点击「更多设置」>「IPSec」。
2. 点击 +添加 。

3. 在“添加”页面进行如下配置，然后点击页面底端的 保存 。
   (1) 选择本条 IPSec 隧道绑定的 WAN 口，本例为“WAN1”。
   (2) 选择“封装模式”为“隧道模式”。
   (3) 为本条隧道设置一个名称，如“IPSec_1”。
   (4) 设置本隧道的协商模式，本例为“初始者模式”。
   (5) 设置“远端网关地址”为对端路由器上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.88.77”。
   (6) 输入本路由器内网的网段/前缀长度，本例为“192.168.0.0/24”。
   (7) 输入对端路由器内网的网段/前缀长度，本例为“192.168.1.0/24”。
   (8) 设置协商时所用的预共享密钥，本例为“12345678”。

添加完成，如下图示。

步骤 2 设置路由器 2。

1. 登录路由器 2 的 WEB 管理界面，点击「更多设置」>「IPSec」。

2. 点击 +添加 。

3. 在“添加”页面进行如下配置。

   (1) 选择本条 IPSec 隧道绑定的 WAN 口，本例为“WAN1”。

   (2) 选择“封装模式”为“隧道模式”。

   (3) 为本条隧道设置一个名称，如“IPSec_1”。

   (4) 设置本隧道的协商模式，本例为“响应者模式”。

   (5) 设置“远端网关地址”为对端路由器上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.11.22”。

   (6) 输入本路由器内网的网段/前缀长度，本例为“192.168.1.0/24”。

   (7) 输入对端路由器内网的网段/前缀长度，本例为“192.168.0.0/24”。

   (8) 输入协商时所用的预共享密钥，本例为“12345678”。

4. 点击页面底端的 保存 。

添加完成，如下图示。

----完成

验证配置

当规则的“隧道状态”显示为“已连接”时，IPSec 隧道建立成功。之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。

10.11.4 L2TP over IPSec VPN 配置举例

组网需求

某企业使用企业级路由器进行网络搭建，并成功接入互联网。出差的员工需要访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

方案设计

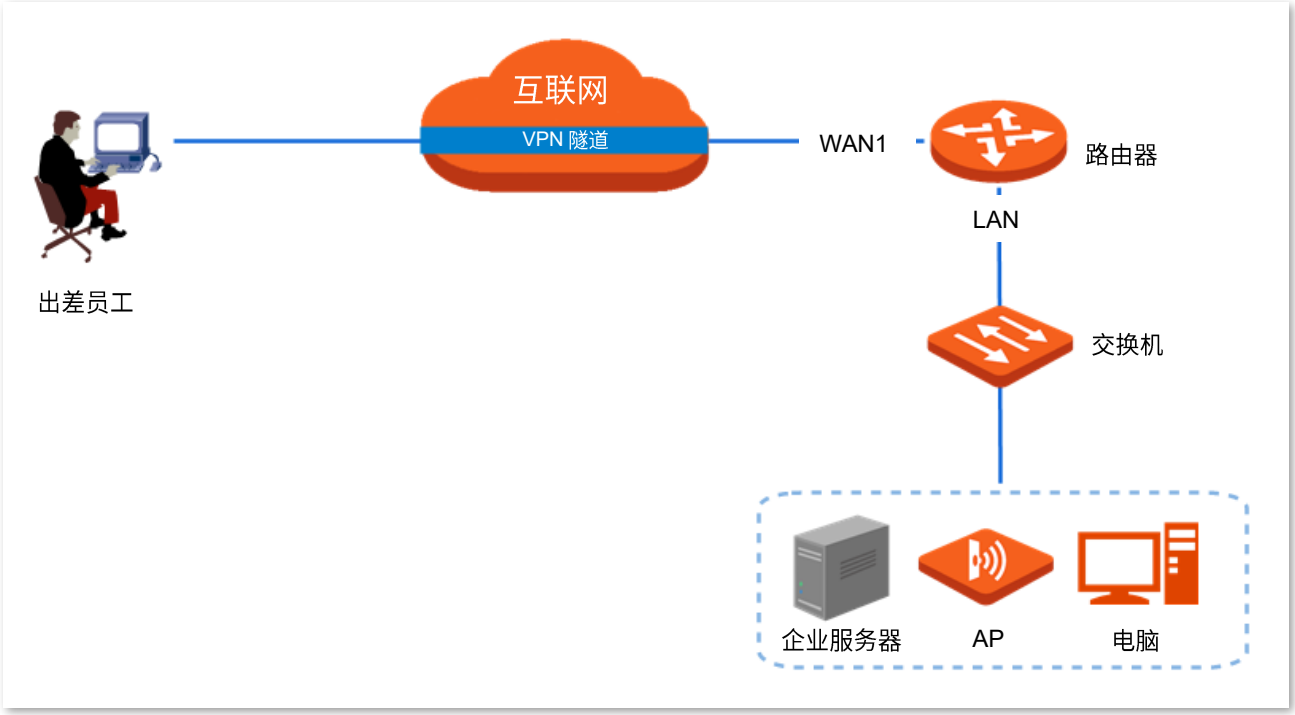
在企业级路由器上建立 IPSec 隧道，并开启 L2TP 服务器，实现远端用户经互联网安全访问企业内部局域网的需求。

假设基本信息如下：

- 路由器建立 IPSec 隧道的接口为 WAN1。
- 路由器建立 L2TP VPN 隧道的接口为 WAN1。
- WAN1 IP 地址为 202.105.11.22。
- 局域网网络为 192.168.0.0/24。

假设路由器的 IPSec 连接基本信息如下：

- 封装模式为传输模式。
- 密钥协商方式为自动协商。
- 预共享密钥为 12345678。



配置步骤

配置流程图：

建立 IPSec 连接 → 开启 L2TP 服务器 → 添加 PPTP/L2TP 用户账号

步骤 1 建立 IPSec 连接。

1. 点击「更多设置」>「IPSec」。
2. 点击 +添加 。

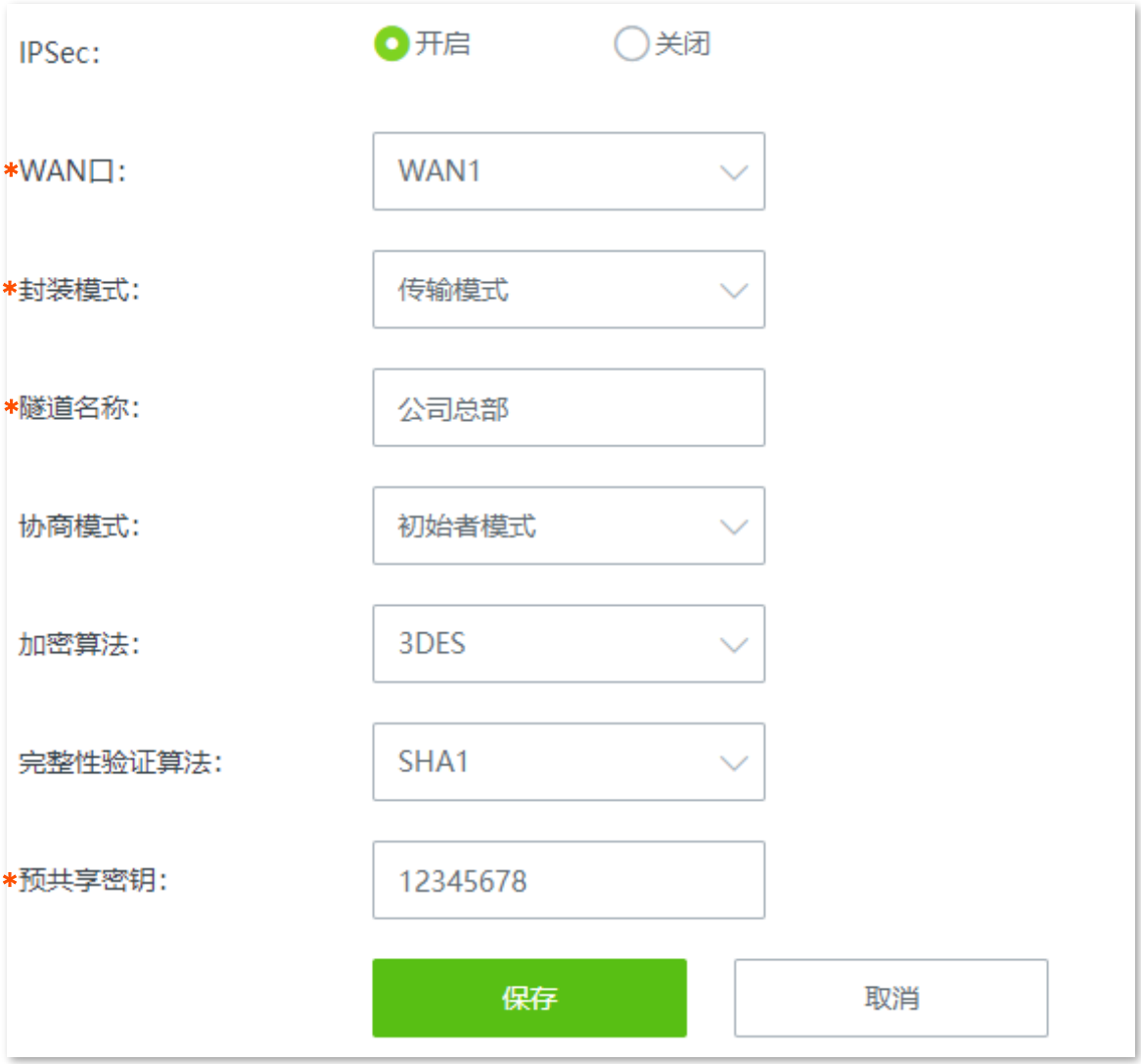
3. 在“添加”页面进行如下配置，然后点击 保存 。

(1) 选择本条 IPSec 连接绑定的 WAN 口，本例为“WAN1”。

(2) 选择“封装模式”为“传输模式”。

(3) 为本连接设置一个隧道名称，如“公司总部”。

(4) 设置共享密钥，用于出差员工建立 VPN 连接时输入，本例为“12345678”。



添加成功。

步骤 2 开启 L2TP 服务器。

1. 点击「更多设置」>「VPN 服务器」。
2. 点击滑块至  。
3. 选择“服务器类型”为“L2TP”。
4. 指定 VPN 服务器与客户端建立隧道的 WAN 口，本例为“WAN1”。
5. 选择要进行 IPSec 加密的 IPSec 隧道，本例为“公司总部”。
6. 点击页面底端的 保存 。

步骤 3 添加 PPTP/L2TP 用户账号。

1. 点击「更多设置」>「VPN 服务器」，找到“PPTP/L2TP 用户”模块。
2. 点击 +添加 。

3. 在【添加】窗口进行如下配置，然后点击 保存 。
   (1) 设置 VPN 客户端进行 VPN 连接时所用的用户名及对应的密码，如均设置为“zhangsan”。
   (2) 选择“是否网络”为“否”。
   (3) （可选）设置该用户账号的备注信息，如“张三”。


添加
用户名:
zhangsan
密码:
••••••••
是否网络:
是
否
备注:
张三
保存
取消

添加完成，如下图示。


PPTP/L2TP用户
添加
删除
用户名
是否网络
网段
子网掩码
备注
状态
操作
zhangsan
否
--
--
张三

----完成

验证配置

出差员工进行 VPN 拨号

场景 1：出差员工在电脑（以 Windows 10 为例）上连接 VPN。

步骤 1 建立 VPN 连接。

1. 点击桌面右下角图标，选择“网络和 Internet 设置”。

2. 点击“VPN”，点击“添加 VPN 连接”。

3. 设置 VPN 参数，然后点击 保存 。

(1) 选择“VPN 提供商”为“Windows（内置）”。

(2) 设置 VPN 连接名称，如“VPN 访问”。

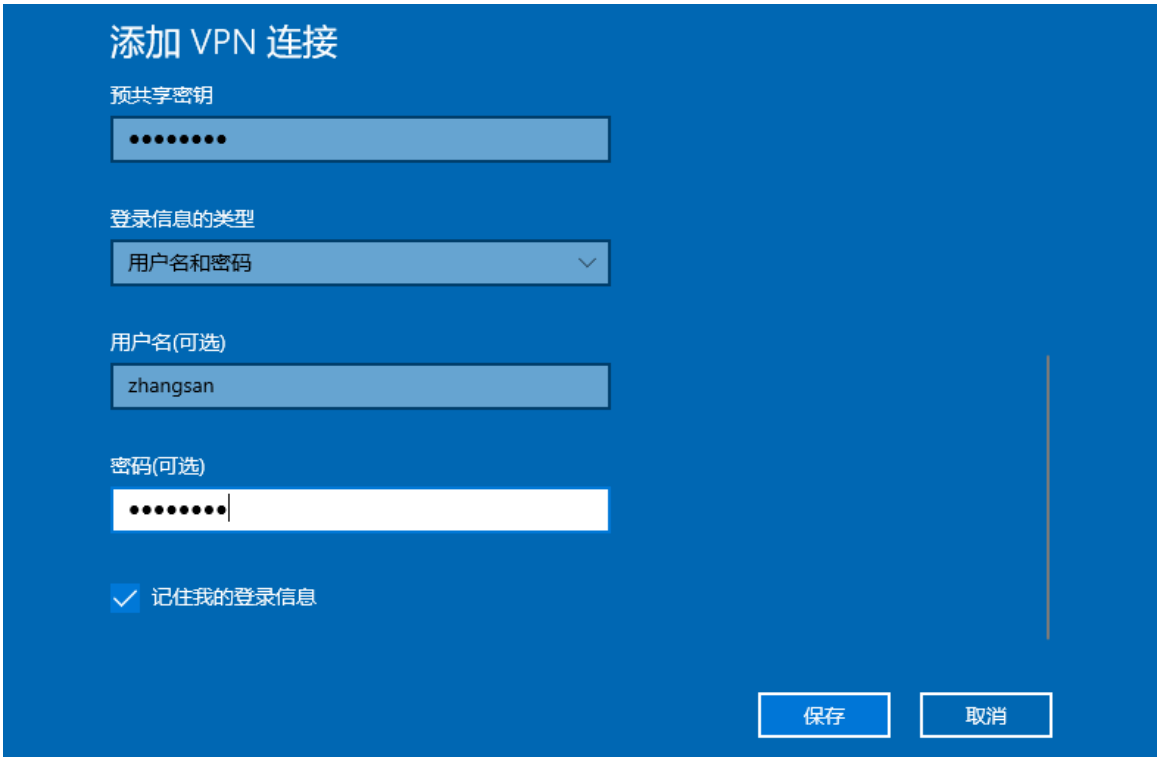
(3) 输入 PPTP 服务器的 IP 地址，本例为“202.105.11.22”。

(4) 选择 VPN 类型，本例为“使用预共享密钥的 L2TP/IPsec”。

(5) 输入 IPSec 隧道设置的预共享密钥，本例为“12345678”。

(6) 向下拉动滚动条，选择登录信息的类型，本例为“用户名和密码”。

(7) 输入 L2TP 服务器允许拨入的用户名及其密码，本例均为“zhangsan”。



4. 点击“VPN 访问”，点击 连接 。

稍等片刻，连接成功。即可根据总部提供的账号信息进行访问。

场景 2：出差员工在移动设备（以 iOS 系统为例）上连接 VPN。

步骤 1 点击手机上的“设置”图标 。

步骤 2 点击“VPN”。

步骤 3 点击“添加 VPN 配置…”。

步骤 4 设置 VPN 连接相关参数。

1. 选择“类型”为“L2TP”。
2. 在“描述”选项设置此 VPN 连接的名称，如“总部”。
3. 输入 L2TP 服务器的 IP 地址，本例为“202.105.11.22”。
4. 输入 L2TP VPN 的用户账号及对应的密码，本例均为“zhangsan”。

5. 输入 IPSec 隧道设置的预共享密钥，本例为“12345678”。
6. 点击“完成”。

步骤 5 点击 。

稍等片刻，当“状态”变为“已连接”时，拨号成功。

出差员工访问总部

下文以分公司访问总部 FTP 服务器为例。总部的项目资料放在 FTP 服务器中，假设服务器信息如下：

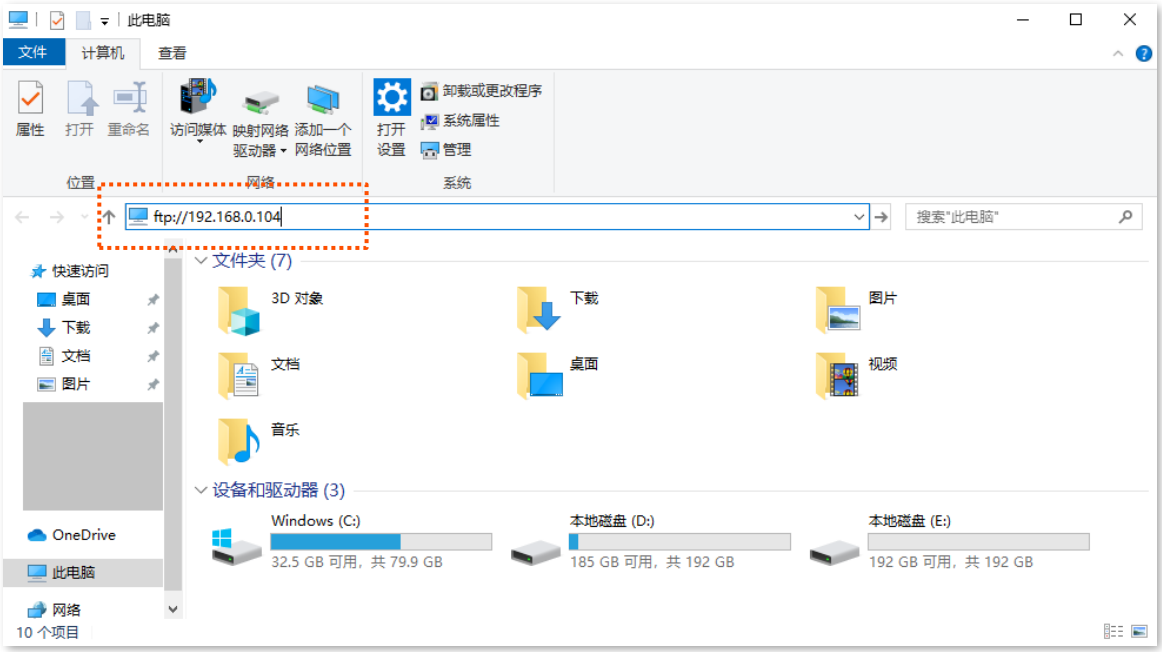
- FTP 服务器 IP 地址为 192.168.0.104
- FTP 服务端口为 21
- FTP 服务器登录用户名和密码均为 zhangsan

当分公司员工访问总部项目资料时，步骤如下：

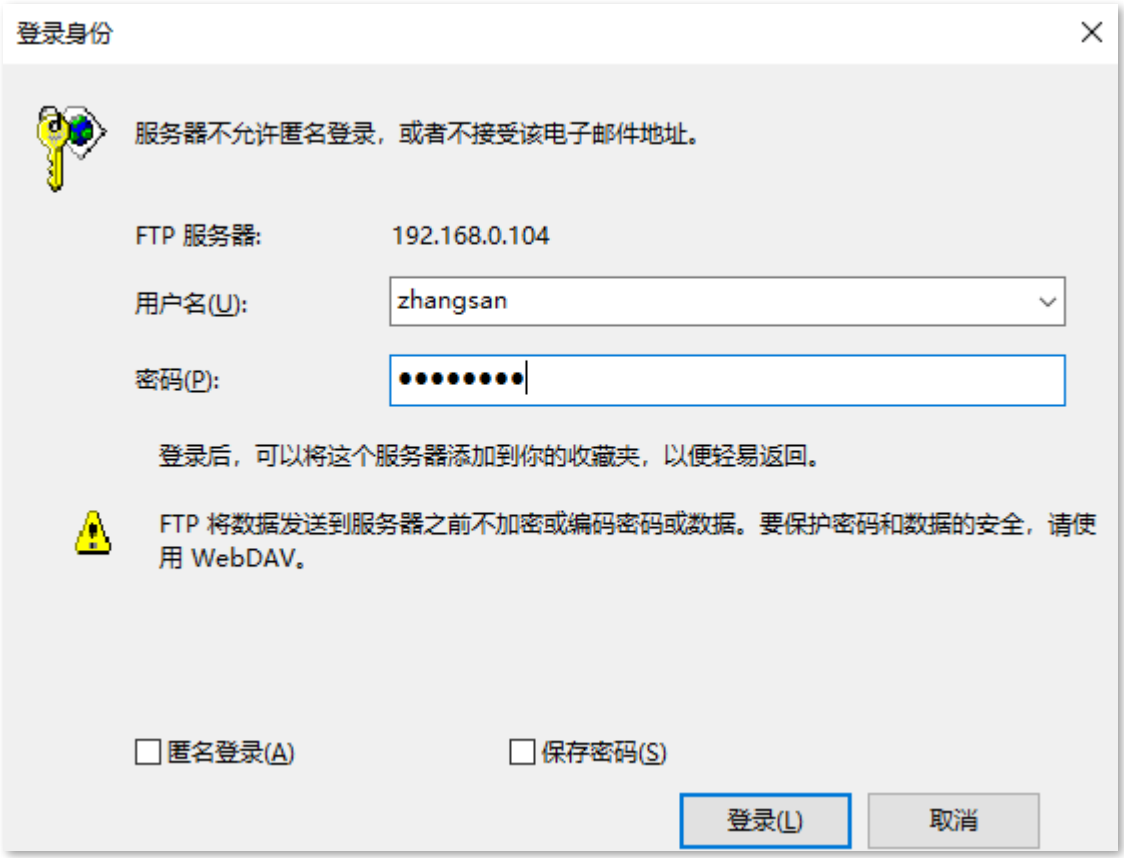
步骤 1 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 ftp://192.168.0.104。

提示

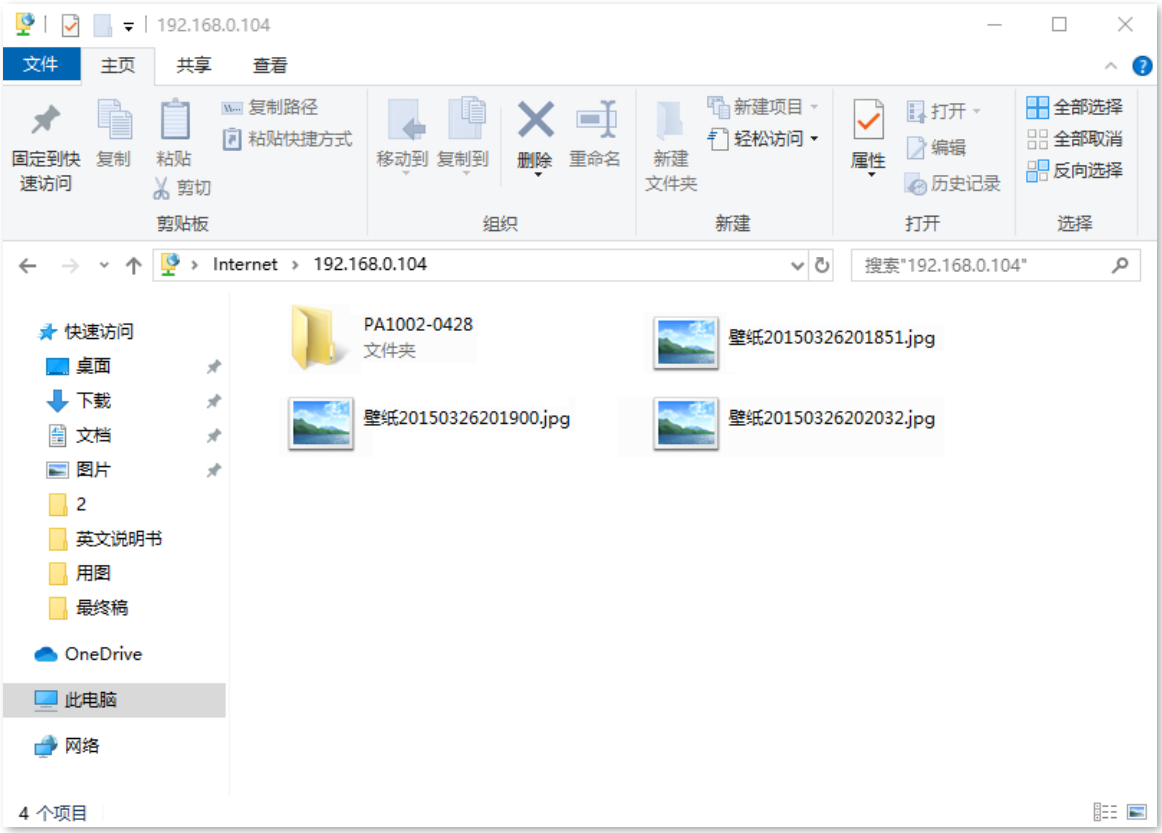
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



步骤 2 输入登录用户名和密码，本例均为“zhangsan”，然后点击 登录 。



访问成功。



提示

如果要使用移动端（智能手机、平板电脑等）访问 FTP 服务器，移动端需要成功安装 FTP 客户端才能访问。

10.12 多 WAN 策略

10.12.1 概述

在“多 WAN 策略”模块，您可以设置多 WAN 策略和广域网线路检测。

- **多 WAN 策略**

  路由器启用多个 WAN 口后，可允许多条宽带同时接入，实现带宽叠加。当多个 WAN 口同时工作时，合理的设置多 WAN 策略可以大幅提升路由器的带宽利用率。

- **广域网线路检测**

  启用广域网线路检测功能后，路由器会周期性地检测路由器 WAN 口与“检测地址”（一般为广域网地址）的连通情况。当检测到 1 个或多个 WAN 口联网失败时，连接到路由器的用户不能通过该 WAN 口访问互联网。

进入页面：点击「更多设置」>「多 WAN 策略」。

参数说明

标题项	说明
多 WAN 策略	路由器多个 WAN 口同时工作时采用的数据转发策略。 - 智能负载均衡：自动分配流量，系统自动寻找流量最小的 WAN 口通信。 - 自定义：用户根据实际需要，为某一源 IP 地址的流量指定 WAN 口进行转发。

标题项	说明
广域网线路检测	开启后，路由器会周期性地检测 WAN 口与“检测地址”的连通情况。
检测地址	需检测的目标主机的 IP 地址或域名。
检测间隔	执行广域网线路检测的时间间隔，默认 5 分钟检测一次。

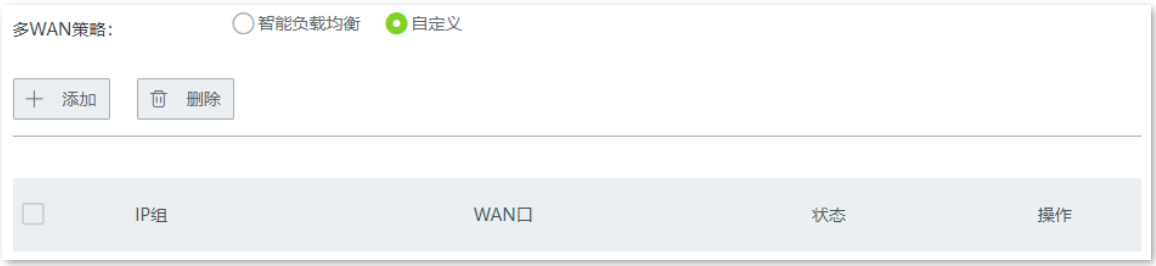
10.12.2 自定义多 WAN 策略

提示

- 自定义多 WAN 策略前，请先配置好相应的 IP 组。
- 如果多 WAN 策略和静态路由器规则冲突，静态路由器优先级高。

步骤 1 点击「更多设置」>「多 WAN 策略」。

步骤 2 选择“多 WAN 策略”为“自定义”，然后点击页面底端的 保存 。



步骤 3 点击 +添加 ，然后在弹出窗口配置各项参数，点击 保存 。

----完成

参数说明

标题项	说明
状态	是否启用该规则。
IP 组	规则引用的 IP 组，以指定规则对应的用户。IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。
WAN 口	对应 IP 组数据流量使用的 WAN 口。

10.12.3 自定义多 WAN 策略配置举例

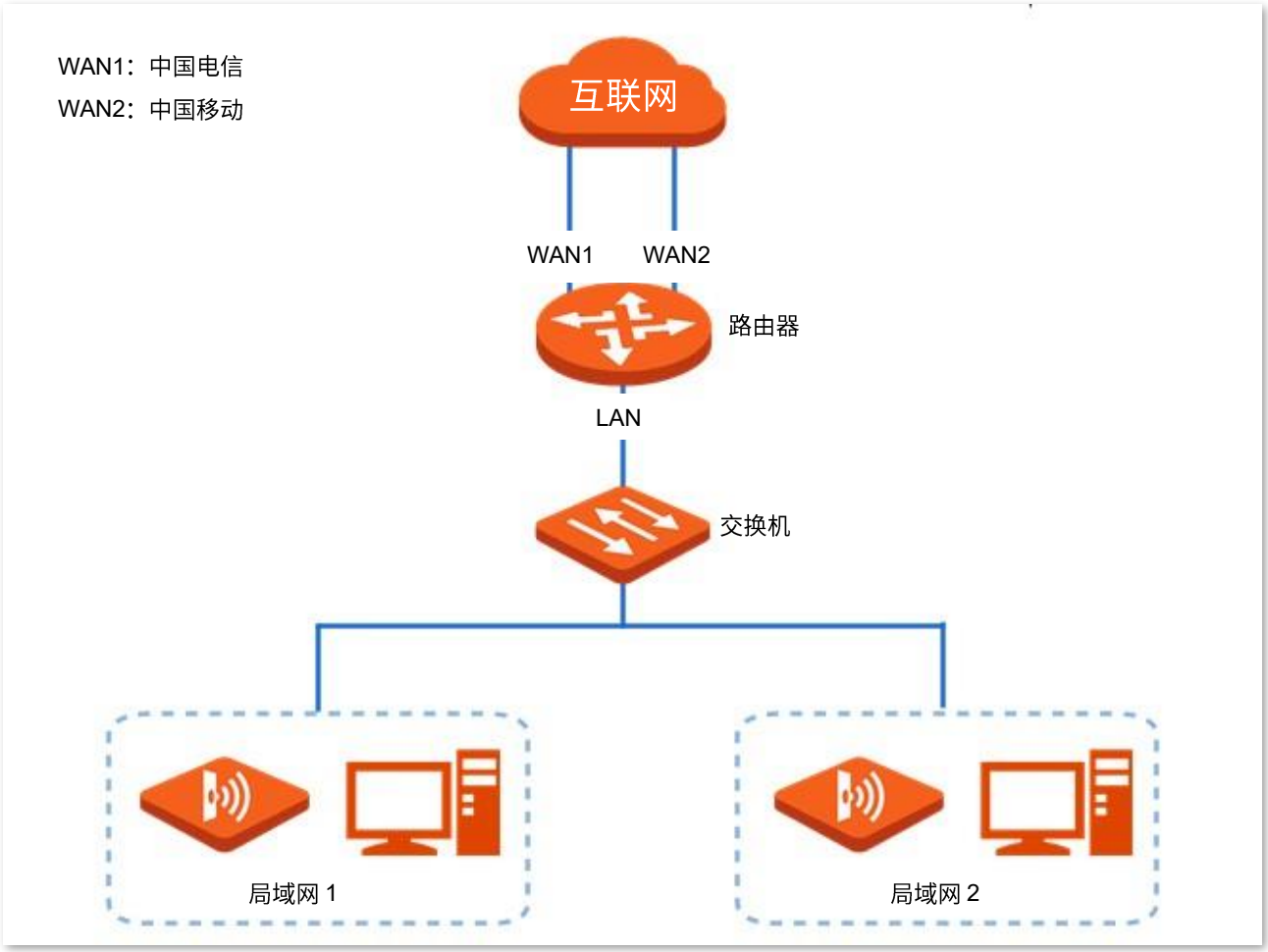
组网需求

某企业使用企业级路由器进行网络搭建，为了满足企业网络需求，办理了两条宽带线路（中国电信和中国移动），并且已经成功访问互联网。为了实现负载均衡，现要求局域网中：

- 局域网 1：IP 地址在 192.168.0.2~192.168.0.100 范围内的设备通过电信宽带访问互联网。
- 局域网 2：IP 地址在 192.168.0.101~192.168.0.250 范围内的设备通过移动宽带访问互联网。

方案设计

可以使用路由器的多 WAN 策略功能实现上述需求。



配置步骤

配置流程图：

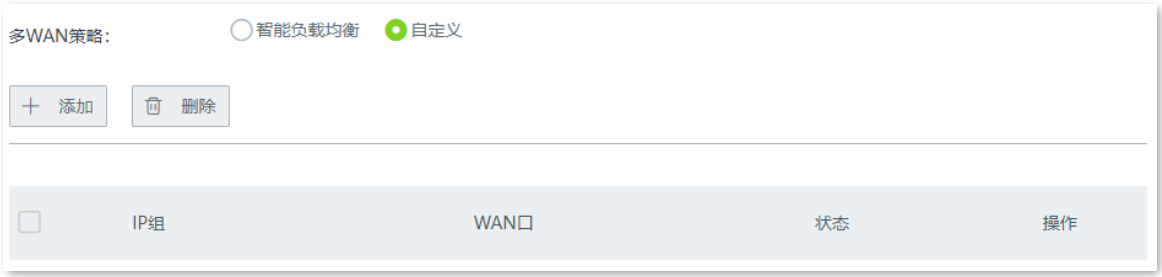
配置 IP 组 → 开启自定义多 WAN 策略 → 自定义多 WAN 策略规则

步骤 1 配置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，参考新增 IP 组，配置如下 IP 组。

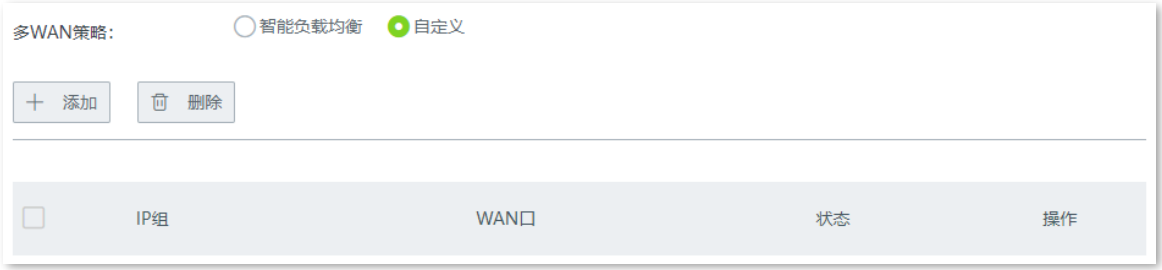
步骤 2 开启自定义多 WAN 策略功能。

1. 点击「更多设置」>「多 WAN 策略」。
2. 选择“多 WAN 策略”为“自定义”。
3. 点击页面底端的 保存 。



步骤 3 自定义多 WAN 策略规则。

1. 点击 +添加 。



2. 在【添加】窗口进行如下配置，然后点击 保存 。

   (1) 选择规则生效的 IP 组，本例为“IP 组 1”。

   (2) 选择该 IP 组数据流量使用的 WAN 口，本例为“WAN1”。

3. 重复步骤 3 的 1~2 小步，添加“IP 组 2”的 WAN 口策略。

   添加成功，如下图示。

----完成

验证配置

IP 地址在 192.168.0.2~192.168.0.100 范围内的局域网设备访问外网时，数据流量由 WAN1 口转发；IP 地址在 192.168.0.101~192.168.0.250 范围内的局域网设备访问外网时，数据流量由 WAN2 口转发。

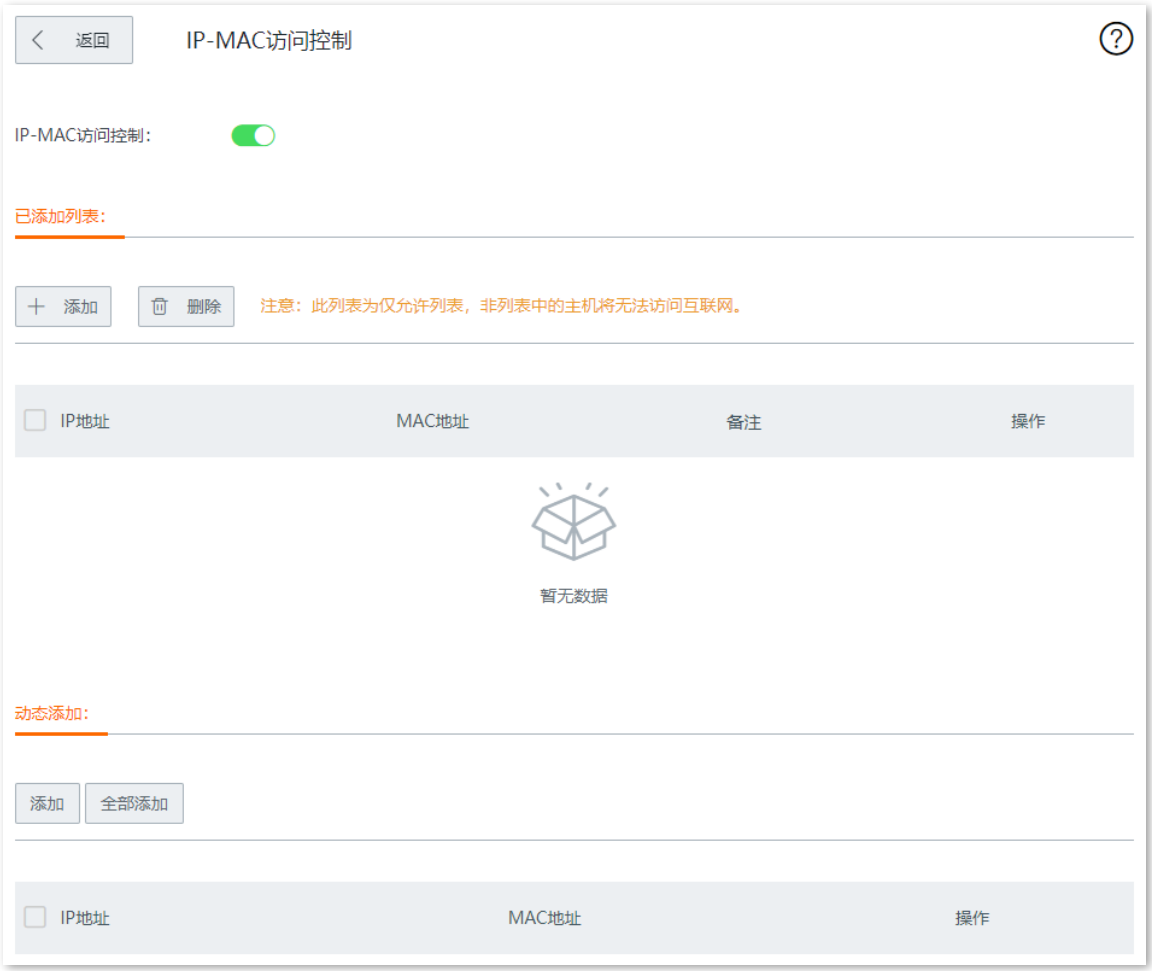
10.13 IP-MAC 访问控制

10.13.1 概述

启用 IP-MAC 访问控制功能后，路由器仅允许与“已添加列表”中的 IP 地址和 MAC 地址匹配的用户访问互联网，其他用户禁止访问互联网。

进入页面：点击「更多设置」>「IP-MAC 访问控制」。

IP-MAC 访问控制功能默认关闭，开启后，如下图所示。



参数说明

标题项		说明
IP-MAC 访问控制		IP-MAC 访问控制功能开关，表示关闭，表示开启。
已添加列表	添加	点击此按钮可手动添加相应 IP 地址和其对应的 MAC 地址。
	删除	点击此按钮可删除选中的已添加的规则。

标题项		说明
	IP 地址	显示已添加的 IP 地址。
	MAC 地址	显示 IP 地址对应的 MAC 地址。
	备注	显示对应规则描述。若动态添加或手动添加时未设置备注信息，将不显示。
	操作	可对已添加的规则进行修改或删除操作。
动态添加	添加	连接到路由器的客户端信息将会显示在动态列表中。点击此按钮可将已选中的规则添加到“已添加列表”。
	全部添加	点击此按钮可将动态列表中的所有规则添加到“已添加列表”。
	IP 地址	显示连接到路由器的客户端的 IP 地址。
	MAC 地址	显示连接到路由器的客户端的 IP 地址对应的 MAC 地址。
	操作	点击对应规则后的添加，即可将该规则快速添加到“已添加列表”。

10.13.2 IP-MAC 访问控制配置举例

组网需求

某企业使用路由器进行网络搭建。公司禁止员工访问互联网，只允许招聘组的员工使用固定的电脑和 IP 地址访问互联网。

方案设计

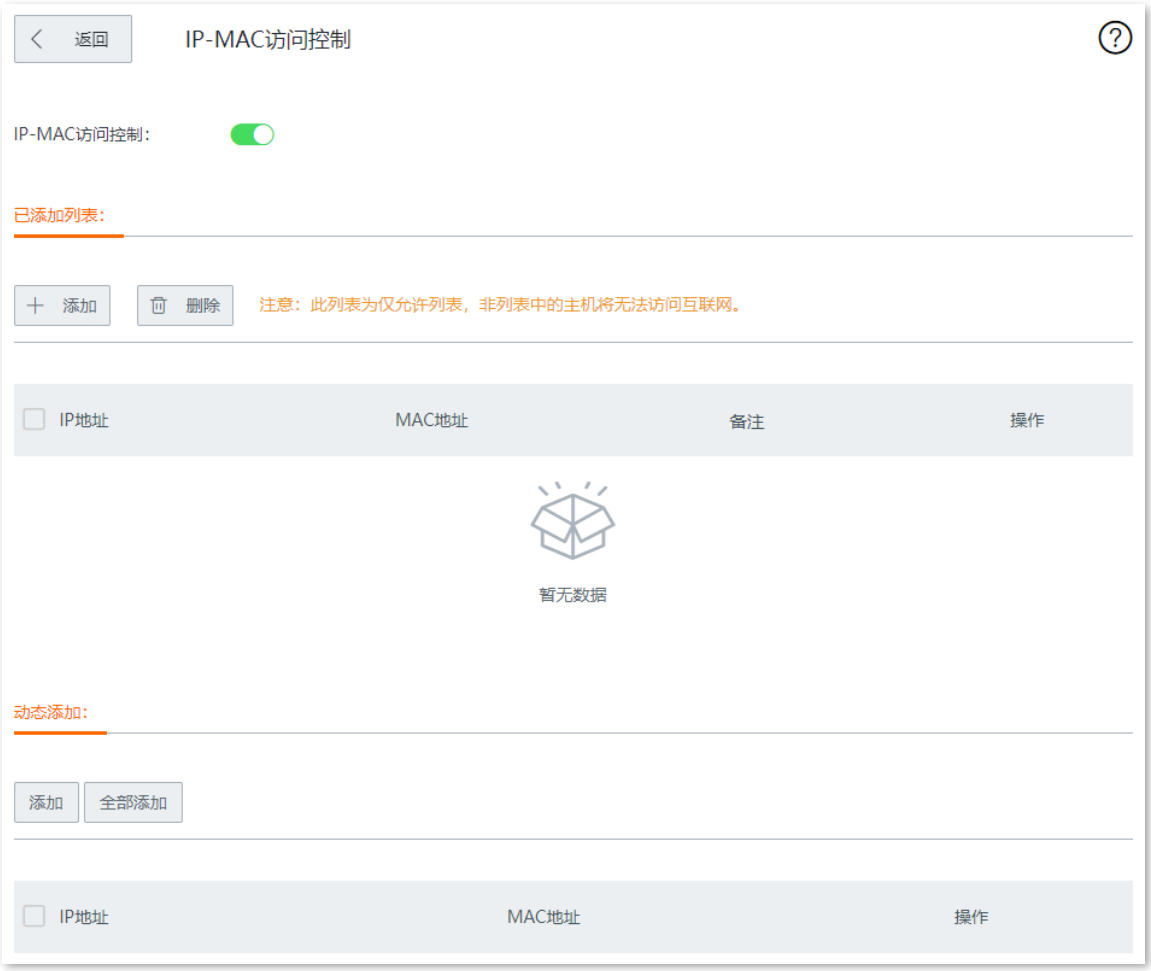
可以通过 IP-MAC 访问控制功能实现。首先需要知道允许上网的招聘人员使用的电脑的 IP 地址和 MAC 地址，假设它们分别为：192.168.0.11、50:2B:73:13:05:18；192.168.0.12、50:2B:73:D5:75:A6；192.168.0.164，50:2B:73:C9:C9:C8。

配置步骤

步骤 1 点击「更多设置」>「IP-MAC 访问控制」。

步骤 2 点击滑块至  。

步骤 3 点击页面底端的 保存 。



步骤 4 添加 IP-MAC 访问控制规则。

- 如果用户没有连接到路由器，请参考如下操作：

1. 点击 +添加 。

2. 在弹出的对话框输入要添加的 IP 地址和 MAC 地址信息，点击 保存 。

- 如果要设置的客户端已经连接路由器，可在“动态添加”列表中找到对应设备并点击添加。

----完成

添加成功，如下图示。

验证配置

MAC 地址为 50:2B:73:C9:C9:C8 的客户端需要配置 192.168.0.164 的 IP 地址才能访问互联网。

MAC 地址为 50:2B:73:13:05:18 的客户端需要配置 192.168.0.11 的 IP 地址才能访问互联网。

MAC 地址为 50:2B:73:D5:75:A6 的客户端需要配置 192.168.0.12 的 IP 地址才能访问互联网。

10.14 IPv6

注意

本路由器仅 WAN1 口支持 IPv6 功能，请将带有 IPv6 业务的宽带连接到 WAN1 口，然后再进行本章配置。

10.14.1 概述

IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，属于 IPv4 的升级版，解决了当前 IPv4 在地址空间等方面的不足之处。

IPv6 地址总长度为 128 比特，通常分为 8 组，每组为 4 个十六进制数的形式，每组十六进制数间用冒号分隔。一个 IPv6 地址可以分为如下两部分：

- 网络前缀：n 比特，相当于 IPv4 地址中的网络 ID。
- 接口标识：128-n 比特，相当于 IPv4 地址中的主机 ID。

进入页面：点击「更多设置」>「IPv6」。

IPv6 功能默认关闭，开启后，如下图所示。

10.14.2 IPv6 WAN 设置

本路由器支持通过“自动获取”、“PPPoEv6”和“静态 IPv6 地址”3 种方式接入 IPv6 网络，请根据下表说明选择相应的联网方式。

如果	您可以查看
- 上级设备为网络运营商，且运营商未提供具体上网参数 - 上级设备的 LAN 口启用了 DHCPv6 功能	自动获取
上级设备为网络运营商，且运营商提供了支持 IPv6 业务的宽带账号和宽带密码	PPPoEv6

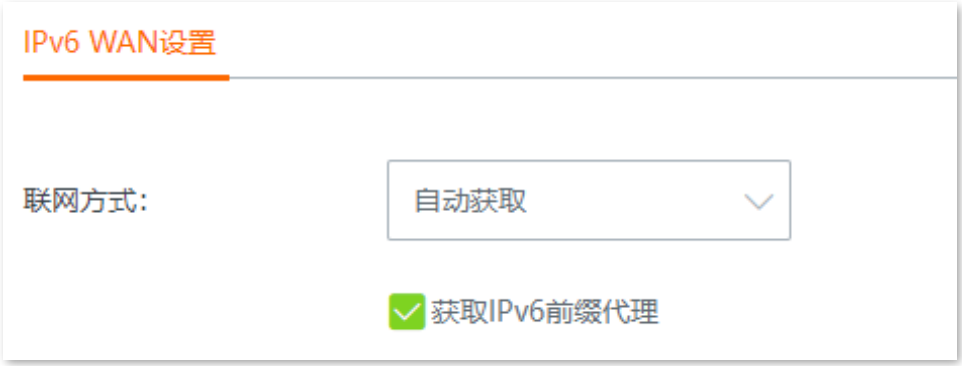
如果	您可以查看
- 上级设备为网络运营商，且网络运营商提供了一组用于上网的固定 IPv6 地址，包括 IP 地址、子网掩码、默认网关、DNS 服务器信息 - 上级设备的 LAN 口未启用 DHCPv6 功能	静态 IPv6 地址

提示

如果 WAN 口直连运营商网络时，请确保您已开通 IPv6 互联网服务。如果不确定，请先与您的网络运营商联系。

自动获取

自动获取，即通过 DHCPv6 方式获取地址上网。

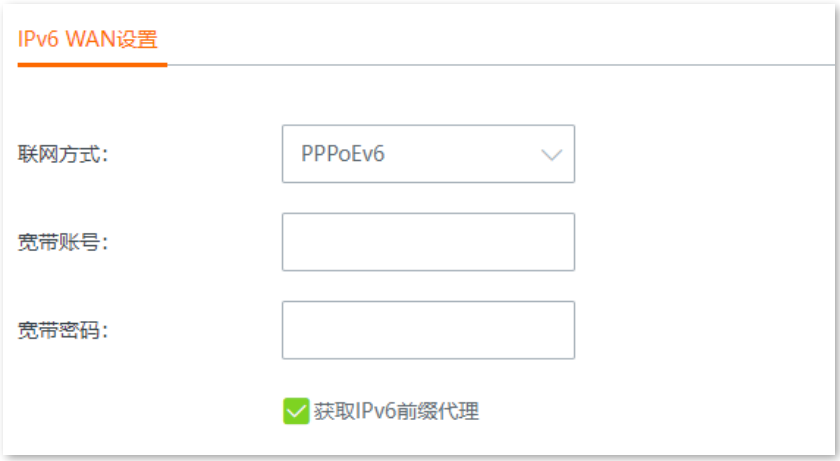


参数说明

标题项	说明
联网方式	请选择自动获取。
获取 IPv6 前缀代理	勾选后，路由器将自动从上级服务器获取 LAN 口 IPv6 地址前缀。该前缀用于为 LAN 侧设备生成 IPv6 地址。 提示 如果路由器无法获取前缀，可能是上级设备不支持下发 PD 前缀，请联系您的网络运营商处理。

PPPoEv6

PPPoEv6，即通过使用带 IPv6 业务的宽带账号和密码进行拨号上网。

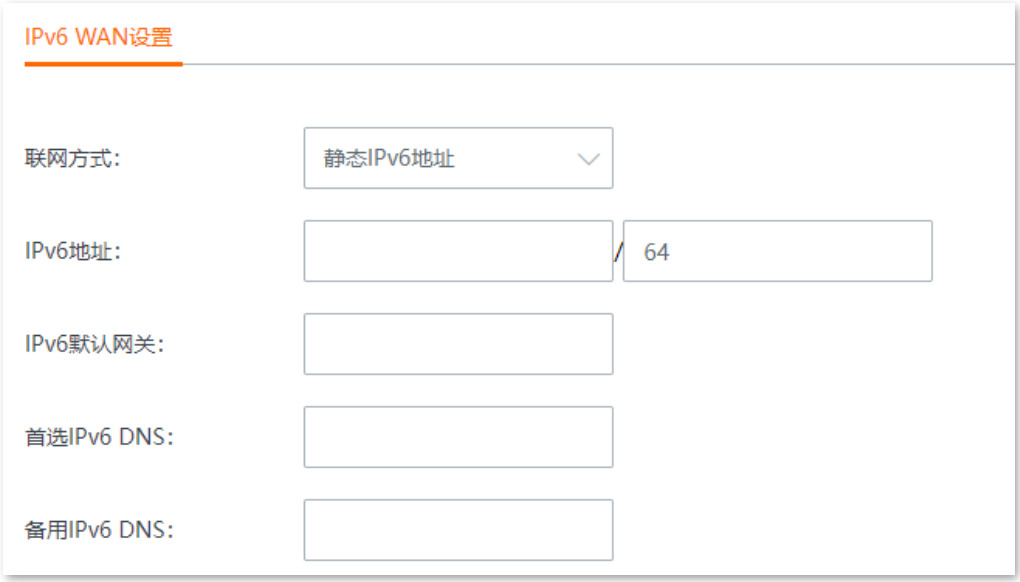


参数说明

标题项	说明
联网方式	请选择 PPPoEv6。
宽带账号 宽带密码	宽带拨号上网使用的账号和密码，一般由网络运营商提供。
获取 IPv6 前缀代理	勾选后，路由器将自动从上级服务器获取 LAN 口 IPv6 地址前缀。该前缀用于为 LAN 侧设备生成 IPv6 地址。 提示 如果路由器无法获取前缀，可能是上级设备不支持下发 PD 前缀，请联系您的网络运营商处理。

静态 IPv6 地址

静态 IPv6 地址，即需要手动输入 WAN 口的 IPv6 地址信息上网。



参数说明

标题项	说明
联网方式	请选择静态 IPv6 地址。
IPv6 地址	IPv6 上网地址信息。 提示 如果网络运营商只提供一个 DNS 地址，“备用 DNS”可以不填。
IPv6 默认网关	
首选 IPv6 DNS	
备用 IPv6 DNS	

10.14.3 IPv6 LAN 设置

为保证局域网设备能够访问 IPv6 网络，需合理设置路由器 LAN 口的 IPv6 参数。

参数说明

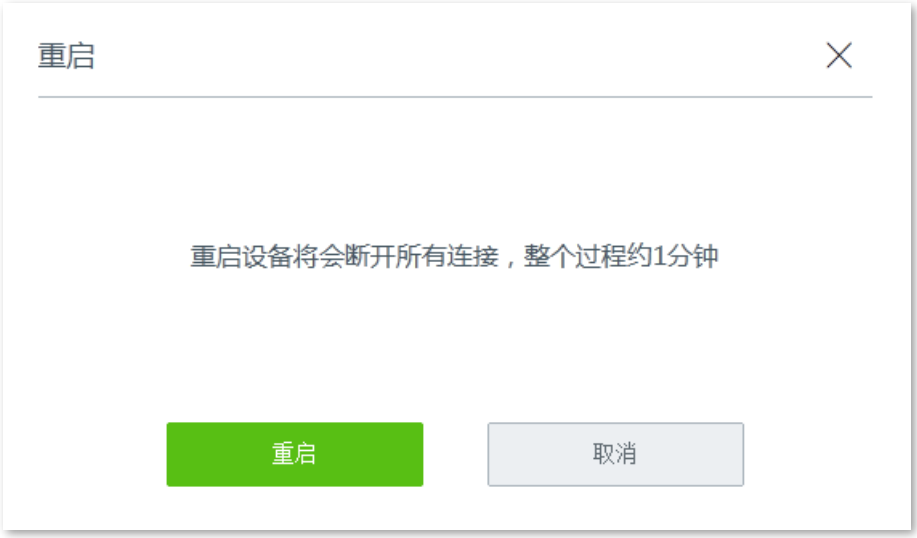
标题项	说明
IPv6 LAN 地址	LAN 口 IPv6 地址设置方式。 - 自动配置：路由器根据 LAN 口 MAC 地址自动生成 LAN 口 IPv6 地址的接口标识。 - 手动配置：手动设置 IPv6 地址。
LAN 前缀	LAN 口 IPv6 地址的网络前缀。 - 自动配置：路由器从上级设备获取 LAN IPv6 地址前缀。 - 手动配置：手动设置 LAN IPv6 地址前缀。
DHCPv6	开启后，DHCPv6 服务器可以为客户端分配 IPv6 地址/前缀和其他网络配置参数。
DHCPv6 地址分配方式	DHCPv6 服务器分配 IPv6 地址信息的方式。 - 无状态：即 DHCPv6 无状态配置。客户端的 IPv6 地址仍然通过路由通告方式（地址无状态自动配置）自动生成，DHCPv6 服务器只分配除 IPv6 地址以外的网络配置参数，如 DNS 服务器地址等。 - 有状态：即 DHCPv6 有状态配置。DHCPv6 服务器给客户端自动分配 IPv6 地址/前缀及其他网络配置参数（如 DNS 服务器地址等）。用户需手动配置起始 ID 和结束 ID。
起始 ID	有状态 DHCPv6 地址分配方式需要配置此项。 DHCPv6 服务器可分配的 IPv6 地址中最后一段地址范围。
结束 ID	范围：1~ffff
IPv6 DNS	LAN 口 IPv6 DNS 设置方式。 - 自动配置：从上级设备获取 IPv6 DNS 地址。 - 手动配置：手动设置 IPv6 DNS 地址。
首选 IPv6 DNS	输入网络运营商提供的 IPv6 DNS 地址。
备用 IPv6 DNS	提示 如果网络运营商只提供一个 DNS 地址，“备用 IPv6 DNS”可以不填。

11 系统维护

11.1 重启

当您设置的某项参数不能正常生效时，可以尝试重启路由器解决。

重启步骤：在「系统维护」>「重启」页面，确认信息后，点击 重启 。



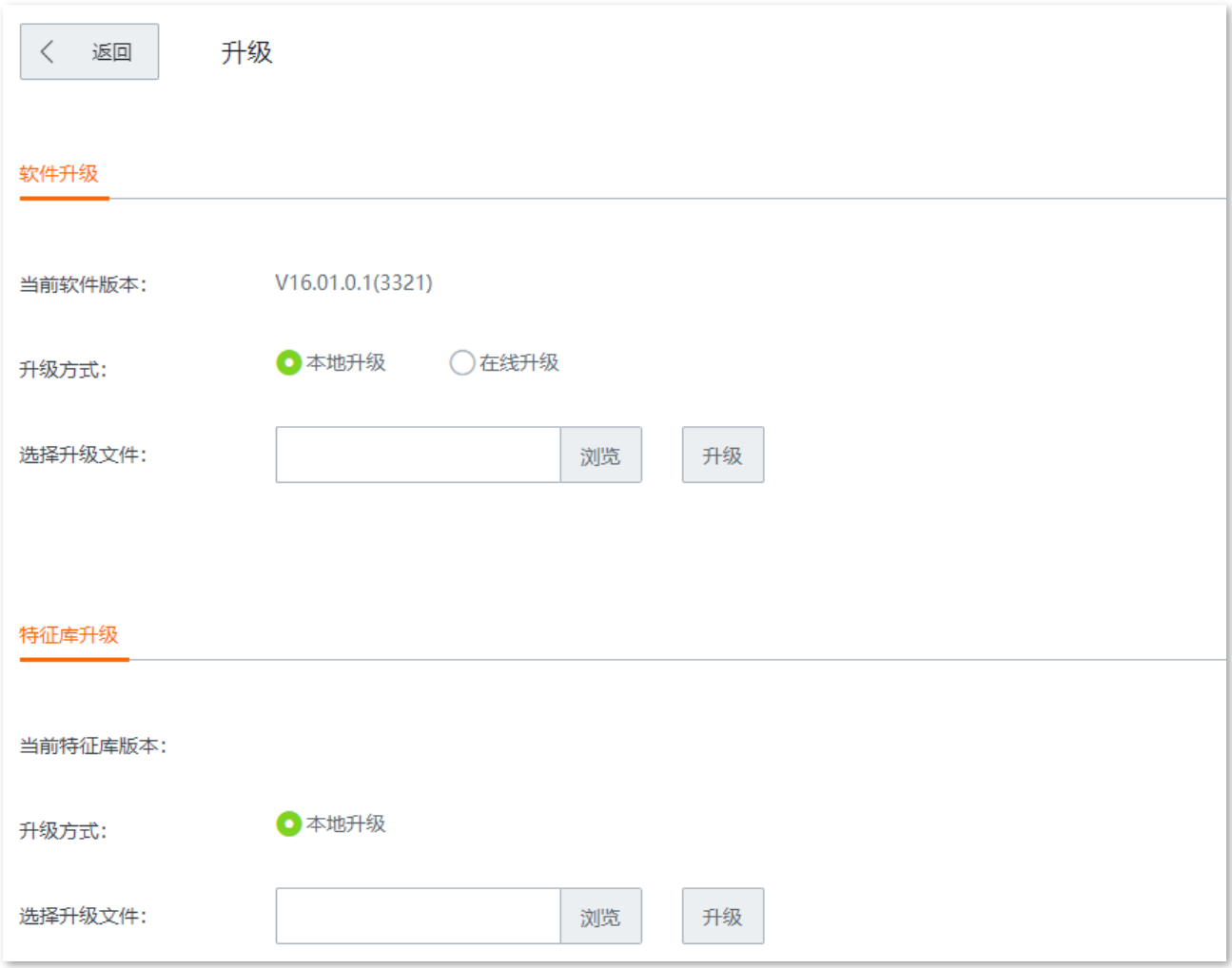
11.2 升级

11.2.1 概述

进入页面：点击「系统维护」>「升级」。

在这里，您可以对路由器进行软件升级和特征库升级。

- 软件升级：您可以通过升级软件，体验更多功能，获得更好的用户体验。路由器支持“本地升级”和“在线升级”两种升级方式。默认为“本地升级”。
- 特征库升级：更新路由器行为管理模块的 URL 特征库。升级特征库不会对路由器系统软件产生影响。路由器暂时仅支持“本地升级”。



参数说明

标题项	说明
本地升级	先访问 Tenda 官方网站 www.tenda.com.cn，搜索相应产品型号，下载升级文件到本地电脑，然后再进行升级。
在线升级	仅“软件升级”支持。 联网后，路由器系统自动检测是否有新的升级文件，并显示检测结果。如果检测到新的软件版本，您可以根据需要进行升级。升级时，点击 下载并升级 ，系统将自动下载升级文件，并进行升级。

11.2.2 软件本地升级

提示

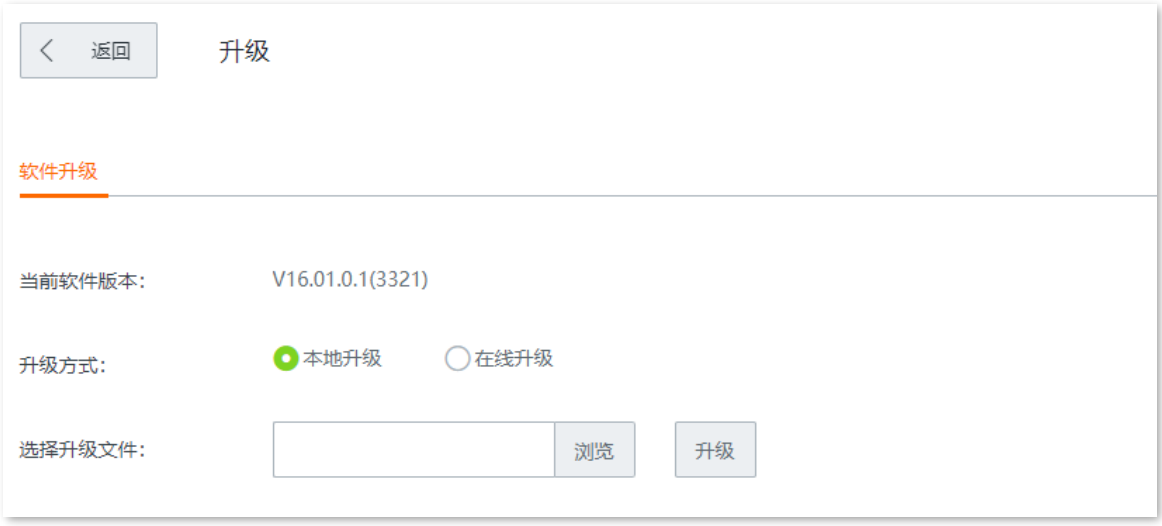
- 为避免路由器损坏，请使用正确的升级文件进行升级。一般情况下，软件升级文件的文件后缀为.bin。
- 升级过程中，请勿断开路由器电源。

步骤 1 访问 Tenda 官网 www.tenda.com.cn，下载对应型号路由器的软件升级文件到本地电脑并解压。

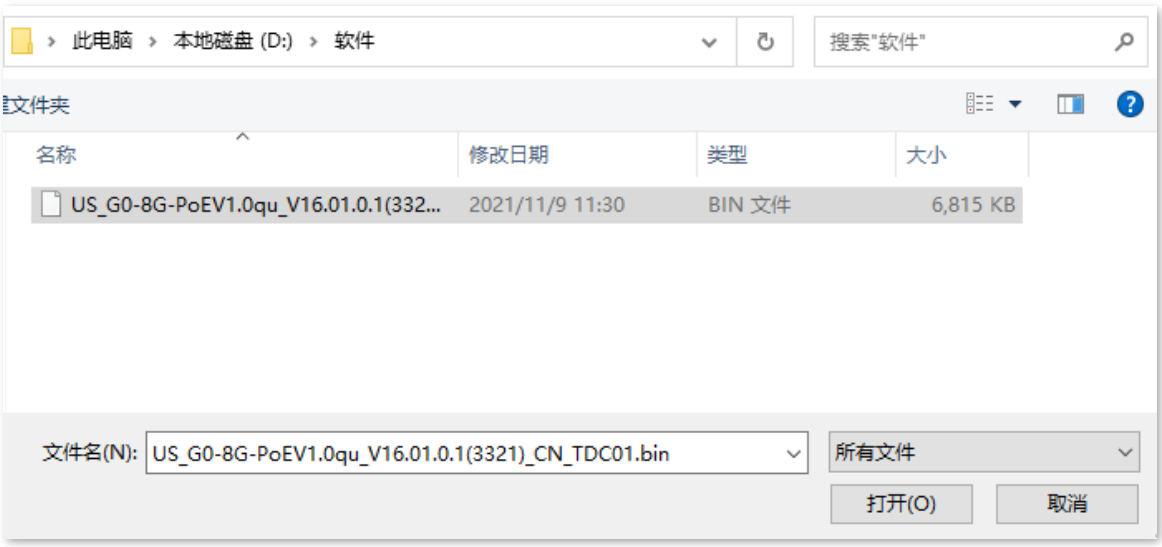
步骤 2 进入路由器的「系统维护」>「升级」页面，找到“软件升级”模块。

步骤 3 选择“升级方式”为“本地升级”。

步骤 4 点击 浏览 。



步骤 5 找到并载入相应目录下已解压的升级软件（文件后缀为.bin）。



步骤 6 点击 升级 。

----完成

等待进度条走完即可。进度条走完后，您可重新登录路由器，进入「系统维护」>「升级」页面，在“软件升级”模块或“系统状态”页面查看路由器当前的软件版本号来确认是否升级成功。

提示

为了更好的体验高版本软件的稳定性及增值功能，路由器升级完成后，建议将路由器恢复出厂设置，然后重新配置路由器。

11.2.3 特征库本地升级

提示

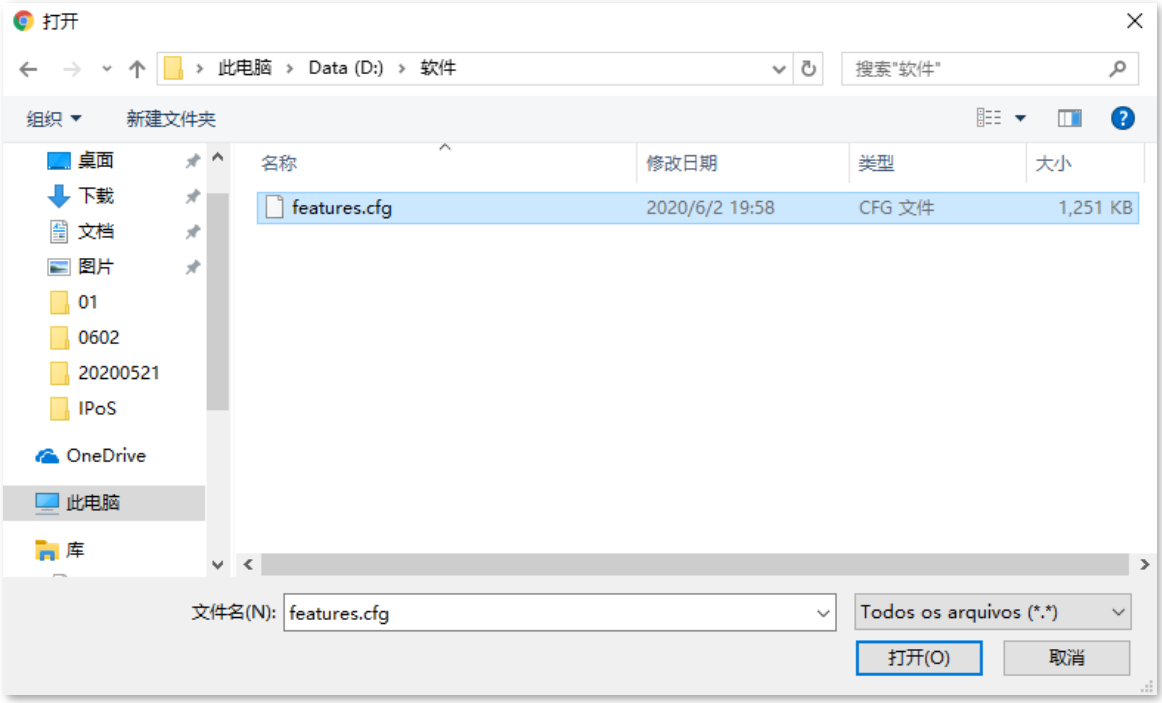
- 为避免路由器损坏，请使用正确的升级文件进行升级。一般情况下，特征库升级文件的文件后缀为.cfg。
- 升级过程中，请勿断开路由器电源。

步骤 1 访问 Tenda 官网 www.tenda.com.cn，下载对应型号的路由器最新的特征库文件并存放到本地电脑。

步骤 2 进入路由器的「系统维护」>「升级」页面，找到“特征库升级”模块。

步骤 3 点击 浏览 。

步骤 4 找到并载入相应目录下的特征库文件。



步骤 5 点击 升级 。

----完成

稍等片刻，当页面的“当前特征库版本”显示版本号时，升级成功。此时“网站过滤”页面的“网址管理”已成功导入分类好的网址。

11.3 复位

11.3.1 概述

进入页面：点击「系统维护」>「复位」。

当局域网用户不能访问互联网，且无法定位问题原因时；或您需要登录路由器的管理页面，但是却忘记登录密码时，可以将路由器复位后重新设置。路由器支持软件复位和硬件复位两种方式。

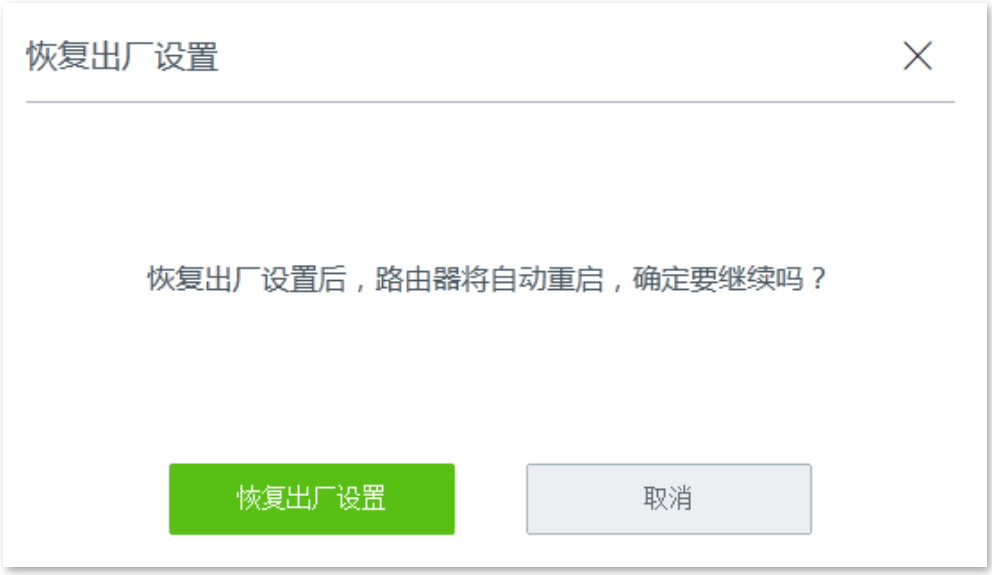
复位后，路由器的 LAN 口 IP 地址为 192.168.0.252。

提示

- 复位后，路由器的所有设置将会恢复到出厂状态，您需要重新设置路由器才能上网。请谨慎使用复位操作。
- 为避免损坏路由器，复位过程中，请确保路由器供电正常。

11.3.2 软件复位

在「系统维护」>「复位」页面，确认信息后，点击 恢复出厂设置 。



11.3.3 硬件复位

使用此方式时，您无需进入路由器管理页面就可以复位路由器。操作方法如下：

路由器 SYS 灯闪烁状态下，用尖状物按住路由器的复位按钮（Reset）约 8 秒，待指示灯全亮时松开。当 SYS 灯重新闪烁时，路由器恢复出厂设置成功。

11.4 密码管理

11.4.1 概述

进入页面：点击「系统维护」>「密码管理」。

在这里，您可以修改路由器的登录密码。首次配置路由器时，需要设置登录密码。

11.4.2 修改登录密码

步骤 1 点击「系统维护」>「密码管理」。

步骤 2 在账号类型对应的密码输入框中修改登录密码。

步骤 3 点击页面底端的 保存 ，弹出确认界面，点击 保存 。

----完成

页面将会跳转到登录页面，此时输入刚才设置的密码，然后点击 登录 即可重新登录到路由器的管理页面。

11.5 定时重启

11.5.1 概述

进入页面：点击「系统维护」>「定时重启」。

在这里，您可以设置路由器在空闲时间周期性地定时自动重启，预防路由器长时间运行导致其出现性能下降、不稳定等现象。

11.5.2 定时重启路由器

提示

定时重启时间以路由器的系统时间为准，为避免重启时间出错，请确保路由器的系统时间准确。

步骤 1 点击「系统维护」>「定时重启」。

步骤 2 点击滑块至。

步骤 3 选择路由器自动重启的时间点，如“3 时 0 分”。

步骤 4 设置重启日期。

步骤 5 点击页面底端的 保存 。

----完成

如上图设置完成后，每个星期四的凌晨 3 点，路由器将自动重启。

11.6 备份与恢复

11.6.1 概述

进入页面：点击「系统维护」>「备份与恢复」。

使用备份功能，可以将路由器当前的配置信息保存到本地电脑；使用恢复功能，可以将路由器配置还原到之前备份的配置。

如，当您对路由器进行了大量的配置，使其在运行时拥有较好的状态和性能，或更符合对应环境的需求，此时建议对该配置进行备份；当您对路由器进行了升级、复位等操作后，可以恢复路由器原有的配置文件。

11.6.2 备份配置

步骤 1 点击「系统维护」>「备份与恢复」。

步骤 2 点击 备份 。

提示

若页面出现类似“由于此类型的文件可能会损坏你的设备，RouterCfm.cfg 被阻止。”的提示，请选择“保留”。

----完成

浏览器将下载文件名为 RouterCfm.cfg 的配置文件。

11.6.3 恢复配置

步骤 1 点击「系统维护」>「备份与恢复」。

步骤 2 点击 浏览 ，选择并加载之前备份的配置文件（文件后缀为.cfg）。

步骤 3 点击 恢复 。

----完成

将出现重启进度提示，请耐心等待。路由器重启后配置恢复完成。

11.7 系统日志

进入页面：点击「系统维护」>「系统日志」。

路由器的系统日志记录了系统的启动、宽带拨号、时间同步、设备登录、WAN 口连接等情况，如遇网络故障，可以利用路由器的系统日志信息进行问题排查。

点击 导出日志 ，可以导出路由器的系统日志到本地电脑。

点击“日志类型”后的下拉框，可按日志类型查看系统日志。日志类型分系统日志、攻击日志、错误日志三种。

日志记录时间以路由器的系统时间为准，为确保日志记录时间准确，请先准确设置路由器的系统时间。可以到系统时间页面校准路由器的系统时间。

提示

- 路由器仅记录其最近一次启动后的事件信息。
- 断电后重新通电、软件升级、恢复设置、复位等操作都会导致路由器重启。

11.8 诊断工具

11.8.1 概述

进入页面：点击「系统维护」>「诊断工具」。

在这里，您可以进行 Ping/Traceroute 检测。

- Ping：用于检测网络的连通性和连通质量。
- Traceroute：用于检测数据包从路由器到目标主机所经过的路由。

11.8.2 执行 Ping

假设要检测路由器到 Tenda 官网（www.tenda.com.cn）的链路是否畅通。

设置步骤：

步骤 1 点击「系统维护」>「诊断工具」。

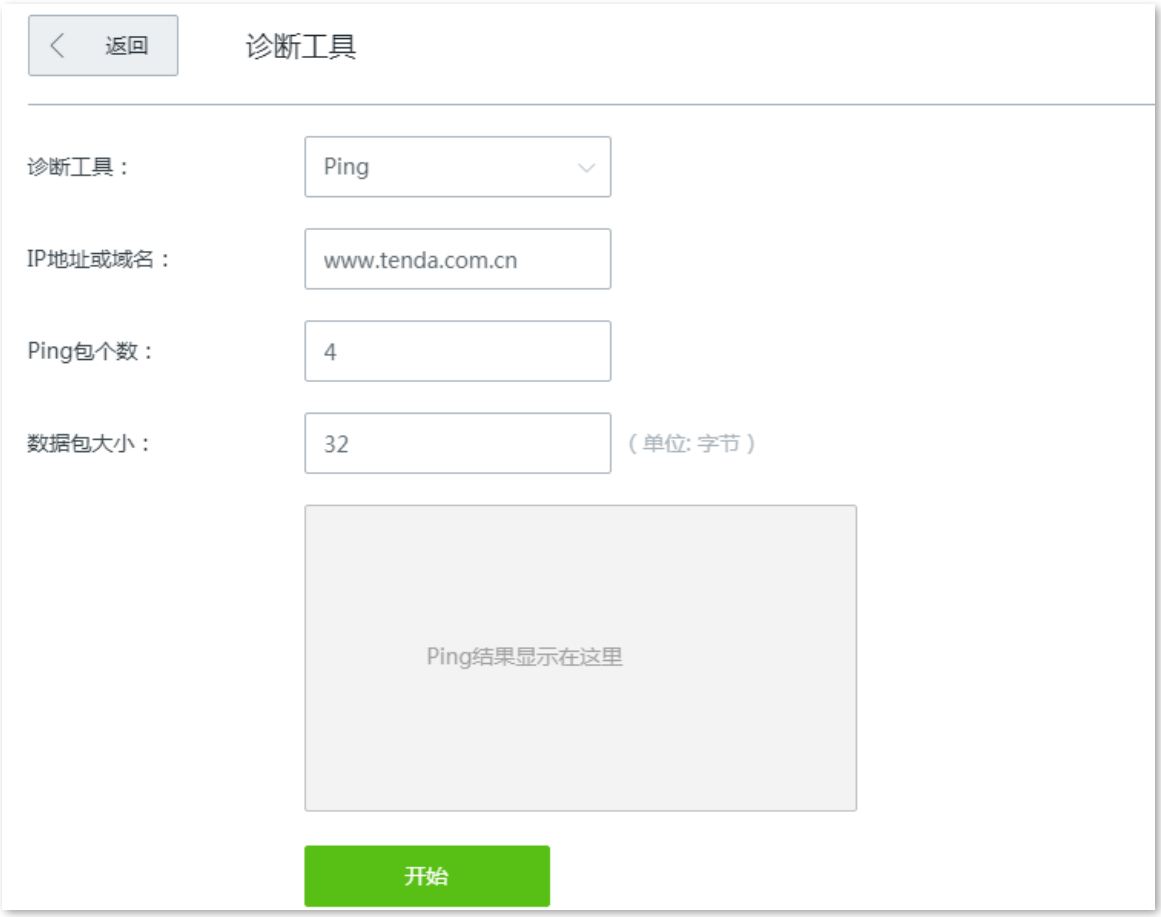
步骤 2 选择“诊断工具”为“Ping”。

步骤 3 输入目的 IP 地址或域名，本例为“www.tenda.com.cn”。

步骤 4 设置 ping 发送的数据包的个数，建议保持默认设置。

步骤 5 设置 ping 发送的数据包的大小，建议保持默认设置。

步骤 6 点击 开始 。



----完成

稍后，诊断结果将显示在页面下方。如下图示。

11.8.3 执行 Traceroute

假设要检测路由器到 Tenda 官网（www.tenda.com.cn）所经过的路由。

设置步骤：

步骤 1 点击「系统维护」>「诊断工具」。

步骤 2 选择“诊断工具”为“Traceroute”。

步骤 3 输入目的 IP 地址或域名，本例为“www.tenda.com.cn”。

步骤 4 点击 开始 。

----完成

稍后，诊断结果将显示在页面下方。如下图示例。


返回
诊断工具
诊断工具：
Traceroute
IP地址或域名：
www.tenda.com.cn
traceroute to www.tenda.com.cn(14.215.177.38), 30 hops max, 38 byte packets
1 172.16.200.1 (172.16.200.1) 0.430 ms 0.347 ms 0.341 ms
2 192.168.20.1 (192.168.20.1) 7.284 ms 1.384 ms 1.534 ms
3 192.168.21.254 (192.168.21.254) 0.652 ms 0.466 ms 0.661 ms
停止

11.9 系统时间

进入页面：点击「系统维护」>「系统时间」。

在这里，您可以设置路由器的系统时间。

为了保证路由器基于时间的功能正常生效，需要确保路由器的系统时间准确。路由器支持网络校时和手动设置两种时间设置方式，默认为“网络校时”。

11.9.1 网络校时

使用此方式时，系统时间自动同步互联网上的时间服务器。只要路由器成功连接到互联网就能自动校准其系统时间，无需重新设置。

设置完成后，您可以进入「系统状态」页面，查看路由器的系统时间是否校对准确。

参数说明

标题项	说明
系统时间	路由器系统时间的设置方式。
校时周期	路由器向互联网上的时间服务器校对系统时间的时间间隔。
选择时区	路由器当前所在地区的标准时区。

11.9.2 手动设置

手动设置路由器的系统时间。使用此方式时，路由器每次重启后，您都需要重新设置系统时间。选择“手动设置”时，页面展开的相关参数如下图所示。

设置完成后，您可以进入「系统状态」页面，查看路由器的系统时间是否校对准确。

参数说明

标题项	说明
系统时间	路由器系统时间的设置方式。
日期	可以直接在此处输入正确的时间，也可以点击 复制管理主机时间 将正在管理路由器的电脑的时间同步到路由器。
时间	

11.10 功能使用列表

进入页面：点击「系统维护」>「功能使用列表」。

在这里，您可以查看路由器当前已启用、未启用的功能列表。点击相应功能可以跳转到其配置页面。

附录

默认参数

路由器主要参数的默认设置如下表。

参数		默认设置
设备登录	管理 IP 地址	192.168.0.252
	管理员密码	无
LAN 口设置	IP 地址	192.168.0.252
	子网掩码	255.255.255.0
DHCP 服务器	DHCP 服务器	开启
	起始 IP 地址	192.168.0.2
	结束 IP 地址	192.168.0.254
	租约时间	30 分钟
	首选 DNS	192.168.0.252
AP 管理	开启	
UPnP	关闭	
系统时间	网络校时	

缩略语

缩略语	全称
AES	高级加密标准（Advanced Encryption Standard）
AH	鉴别首部（Authentication Header）
APSD	自动省电模式（Automatic Power Save Delivery）
ARP	地址解析协议（Address Resolution Protocol）
DDNS	动态域名服务（Dynamic Domain Name Server）
DDoS	分布式拒绝服务（Distributed Denial of Service）
DES	数据加密标准（Data Encryption Standard）
DHCP	动态主机配置协议（Dynamic Host Configuration Protocol）
DNS	域名系统（Domain Name System）
DPD	失效对等体检测（Dead Peer Detection）
ESP	封装安全载荷（Encapsulating Security Payload）
FQDN	完全合格域名（Fully Qualified Domain Name）
GMT	格林威治时间（Greenwich Mean Time）
HTTP	超文本传送协议（HyperText Transfer Protocol）
ICMP	网际控制报文协议（Internet Control Message Protocol）
IKE	互联网密钥交换（Internet Key Exchange）
IP	网际协议（Internet Protocol）
ISP	互联网服务提供商（Internet Service Provider）
LAN	局域网（Local Area Network）
L2TP	二层隧道协议（Layer 2 Tunneling Protocol）

缩略语	全称
MAC	媒体接入控制（Medium Access Control）
NAT	网络地址转换（Network Address Translation）
PPP	点对点协议（Point to Point Protocol）
PPTP	点对点隧道协议（Point to Point Tunneling Protocol）
SA	安全联盟（Security Association）
SSID	服务集标识符（Service Set IDentifier）
SSL	安全套接层（Secure Sockets Layer)
SPI	安全参数索引（Security Parameter Index）
TCP	传输控制协议（Transmission Control Protocol）
UDP	用户数据报协议（User Datagram Protocol）
URL	统一资源定位符（Uniform Resource Locator）
UPnP	通用即插即用（Universal Plug and Play）
WAN	广域网（Wide Area Network）
WMM	无线多媒体（Wi-Fi multi-media）