Tenda

User Guide

Web 配置指南

2.5G 口企业级路由器

*本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

www.tenda.com.cn

声明

前言

关于本指南

本指南是安装指南的补充说明文档，安装指南旨在帮助您快速使用产品，本指南详细介绍产品各功能的配置方法。

本指南适用于 Tenda 2.5G 口企业级路由器 G200、G300–F 和 G500–F。

本指南仅作为功能配置参考，不代表产品支持指南内提及的全部功能。不同型号产品或同一产品的不同版本，Web 页面的功能可能存在差异，请以实际产品的 Web 页面为准。

文中若无特殊说明：

- 以型号为 G500–F 的路由器为例进行介绍，界面截图、IP/MAC 地址等数据信息仅供示例，可能与您实际购买的产品不同，具体请以实际为准。
- 涉及到的“路由器”、“产品”均指 Tenda 2.5G 口企业级路由器。
- Web 软件版本以 V16.01.14.2 为例，不同版本的功能可能不同，请以实际为准。

约定

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。
连续菜单选择	>	进入「AP 管理」>「AP 配置」页面。
按钮	边框+底纹	点击 确定 。

本文可能用到的标识说明如下。

标识	含义
注意	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。
提示	表示对配置操作进行补充与说明。

更多服务与支持

若您遇到产品使用问题，或者您对我们有任何的意见或建议，均可以反馈给我们，我们会尽快为您解决。

Tenda 售后微信客服

邮箱：
tenda@tenda.com.cn

若您想获取相关产品的技术规格、其它手册，请扫描“更多资料”二维码或访问
https://www.tenda.com.cn/service/default.html

更多资料

若您需要查看安装视频、了解产品使用小技巧等，建议关注“Tenda 腾达”微信公众号。

Tenda 腾达

如需获取更多信息，请访问 Tenda 官网：https://www.tenda.com.cn

Tenda 官网

修订记录

文档版本	修订内容	发布日期
V2.0	- 新增漫游优化、创建 WiFi 二维码、外置服务器认证、自定义 NAT、USB 应用、局域网 IP 扫描功能说明 - 更新 LAN 口设置、Wi-Fi 高级设置、认证页面模板、认证方式、分组限速、单用户限速、多 WAN 策略、SSH 维护、VPN 功能说明	2026-01-15
V1.0	首次发行	2024-09-16

目录

1 工作模式

路由模式：设备作为路由器+无线控制器使用，提供互联网接入、路由转发、AP 管理，行为管理等功能。此模式下，设备既要处理控制报文，也要处理数据报文。

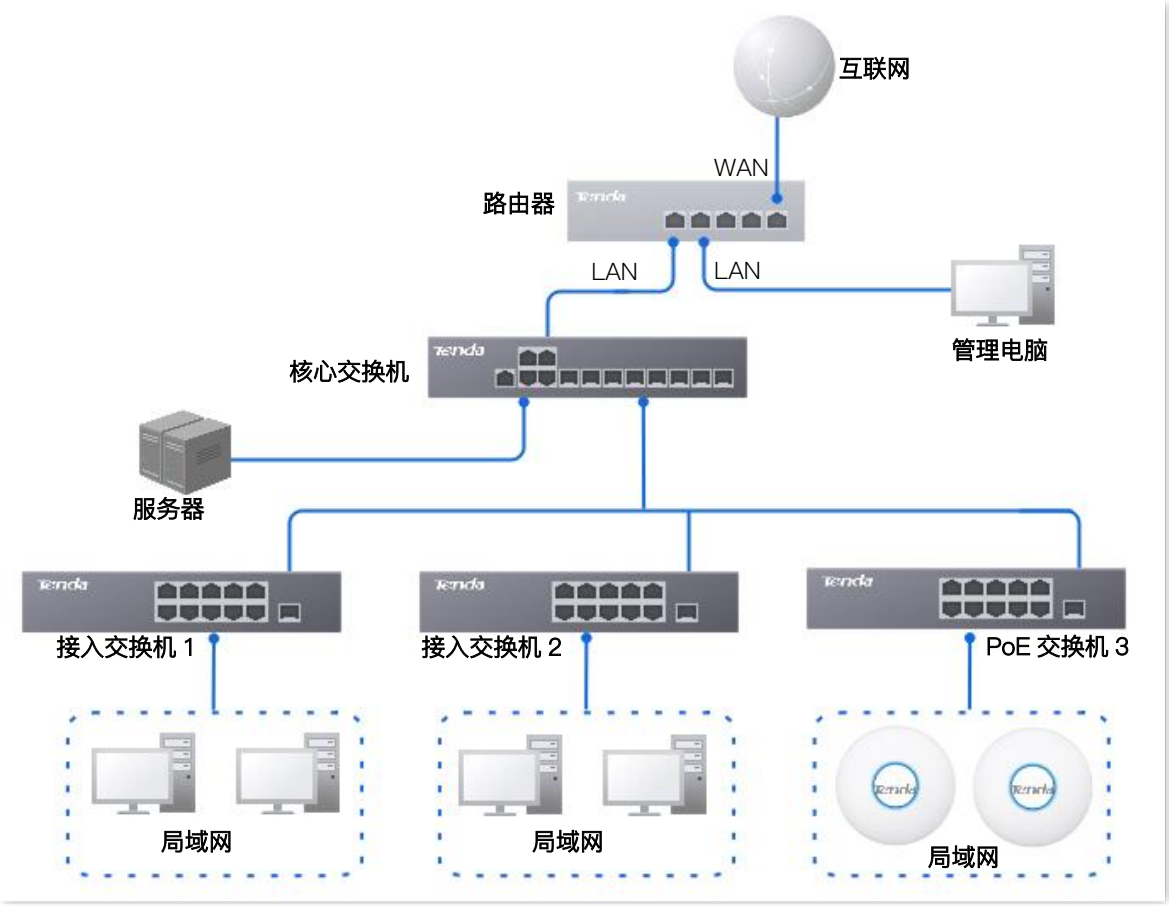
纯 AC 模式：设备作为无线控制器使用，提供 AP 管理、审计等功能，请以页面显示为准。此模式下，数据报文不再经过设备，设备只需处理控制报文。

1.1 路由模式

1.1.1 概述

路由模式下，设备作为路由器+无线控制器使用，一般部署在出口网关的位置，代理局域网上网。

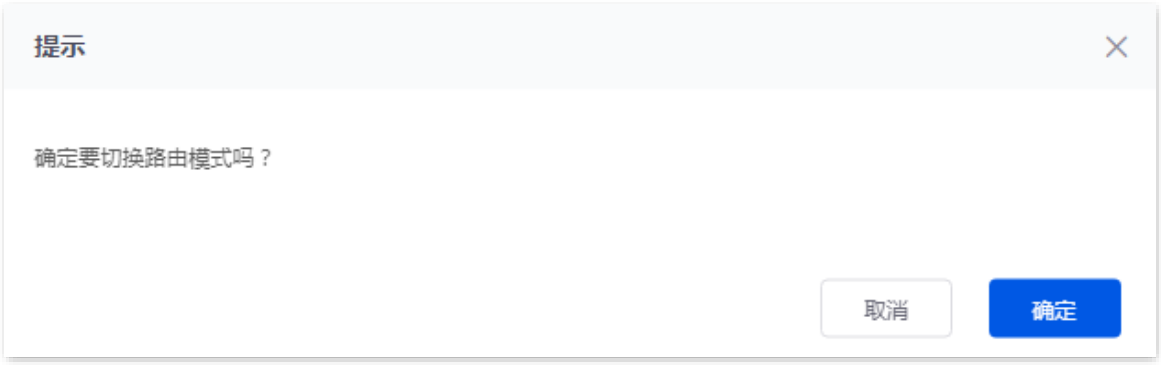
应用场景如下。



1.1.2 设置路由器工作在路由模式

步骤 1 纯 AC 模式登录到路由器 Web 管理页面，在页面右上方模式选择下拉菜单中选择“路由模式”。下图仅供参考。

步骤 2 确认提示信息后，点击 确定 。



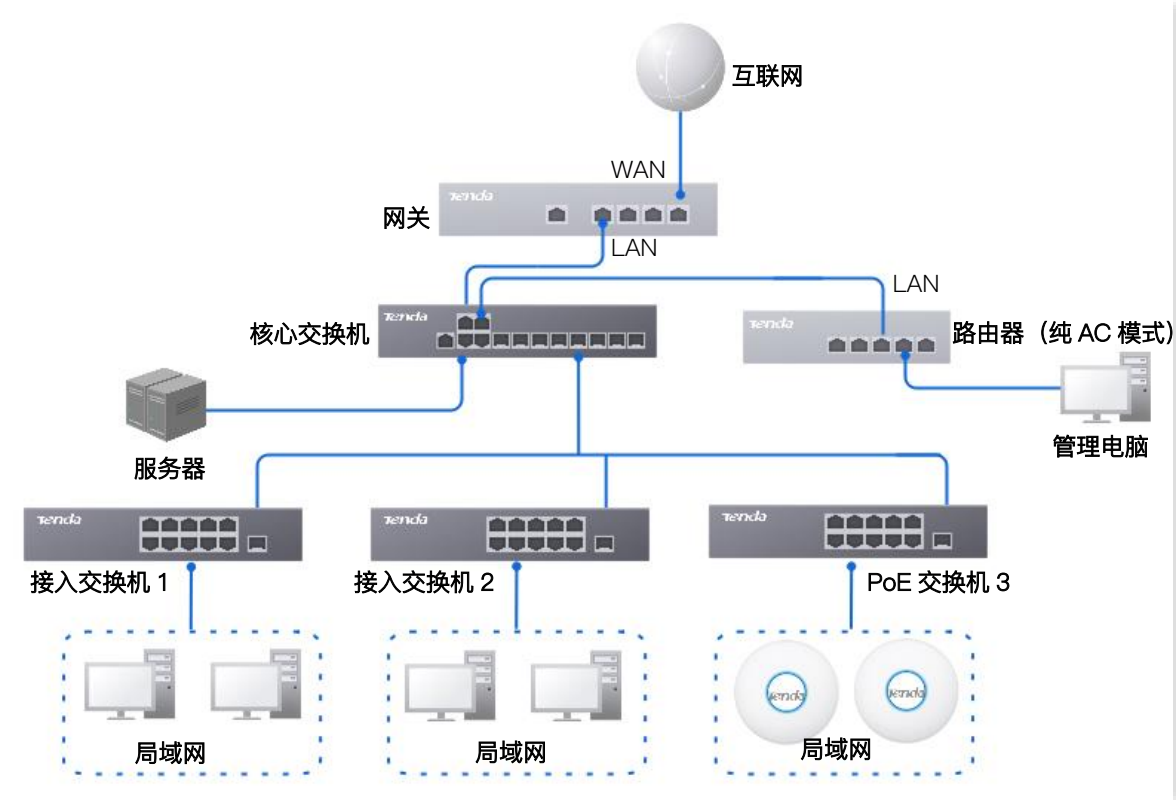
----完成

1.2 纯 AC 模式

1.2.1 概述

纯 AC 模式下，设备作为无线控制器使用，可部署在核心交换机下。仅支持部分功能。

应用场景如下。



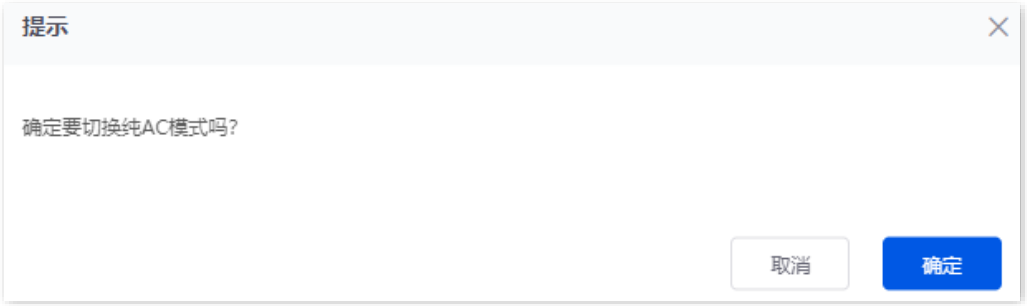
提示

纯 AC 模式下，如果您要使用路由器的远程 WEB 管理、云维护、SSH 维护功能，请先设置路由器成功联网，详见纯 AC 模式下设置路由器联网。否则配置无效。

1.2.2 设置路由器工作在纯 AC 模式

步骤 1 登录到路由器 Web 管理页面，在页面右上方的模式选择下拉菜单中选择“纯 AC 模式”。

步骤 2 确认提示信息后，点击 确定 。



----完成

2 登录 Web 管理界面

2.1 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，请参考相关路由器的快速安装指南设置（扫描更多资料二维码或前往 www.Tenda.com.cn 搜索型号查看安装指南）。其他情况，请参考下文。

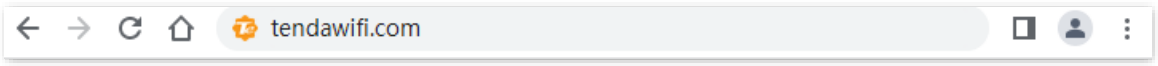
2.1.1 局域网登录

路由模式下登录设备管理页面

电脑端登录

步骤 1 用网线将管理电脑接到路由器的 LAN 口，或已连接路由器 LAN 口的交换机。

步骤 2 打开电脑上的浏览器，访问路由器的管理地址“tendawifi.com”，进入路由器的登录页面。



步骤 3 输入登录密码，点击 登录 。

----完成

提示

若提示输入密码错误，请将路由器恢复出厂设置后，重新设置。注意，恢复出厂设置后需重新设置路由器联网。

若未出现上述登录页面，请尝试使用以下办法解决：

- 确保管理电脑已连接到路由器，网线无松动现象。
- 电脑已设为“自动获得 IP 地址，自动获得 DNS 服务器地址”。
- 请在电脑浏览器的地址栏（非搜索栏）输入“http://tendawifi.com”或“http://192.168.0.252”。
- 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设置路由器联网。

成功登录路由器管理页面。

手机等无线设备端登录

适用于路由器的局域网中已连接 AP。

步骤 1 手机等无线设备连接 AP 的无线网络。

- AP 已被路由器管理：无线名称和密码为您设置的无线名称和密码。如果您未设置，默认无线名称为 Tenda_XXXXXX，其中，XXXXXX 为路由器 MAC 地址（见机身铭牌）后六位，默认无密码。
- AP 未被路由器管理：无线名称和密码为 AP 原有的无线名称和密码。

步骤 2 以手机为例，打开手机上的浏览器，在地址栏（非搜索栏）访问路由器的管理地址“tendawifi.com”，进入路由器的登录页面。

步骤 3 输入登录密码，点击 登录 。

----完成

提示

若提示输入密码错误，请将路由器恢复出厂设置后重新设置。注意，恢复出厂设置后需要重新设置路由器联网。

如果未出现上述页面，请尝试使用以下办法解决：

- 确保 AP 已正常工作，手机已连接正确的 Wi-Fi。
- 使用手机登录时，请确保已关闭手机数据流量。
- 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设置路由器联网。

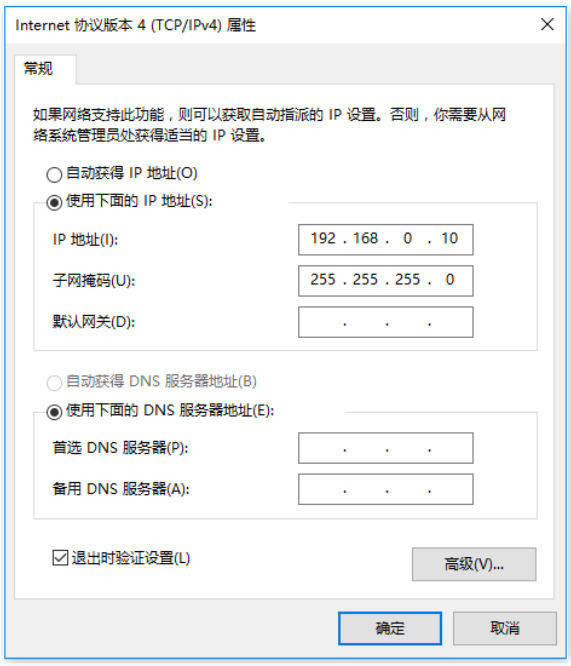
成功登录路由器管理页面。

纯 AC 模式下登录设备管理页面

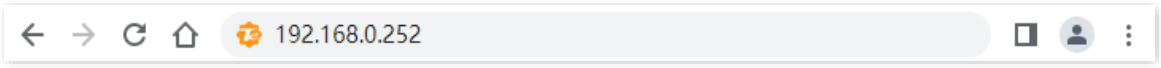
步骤 1 用网线将管理电脑接到路由器的 LAN 口，或已连接路由器 LAN 口的交换机。

步骤 2 设置管理电脑的 IP 地址，使其与路由器的 IP 地址在同一网段。

例如：路由器的默认 IP 地址为 192.168.0.252，则电脑的 IP 地址可以设为“192.168.0.*X*”（*X* 为 2~251，且未被其它设备占用），子网掩码为“255.255.255.0”。



步骤 3 在电脑上打开浏览器，访问路由器的 IP 地址（默认为“192.168.0.252”）。



步骤 4 输入登录密码，点击 登录 。

----完成

提示

若未出现上述页面，请确认管理电脑已连接到路由器，且网线无松动。

成功登录路由器管理页面。

2.1.2 远程登录

本登录方式适用于路由器已联网且开启远程 WEB 管理功能。

提示

使用此方式登录前，请确保您的终端设备已经被允许远程访问路由器。

步骤 1 在已接入互联网的终端上打开浏览器，访问路由器远程管理地址。下图仅供参考。

步骤 2 输入登录密码，点击 登录 。

---完成

成功登录路由器管理页面。

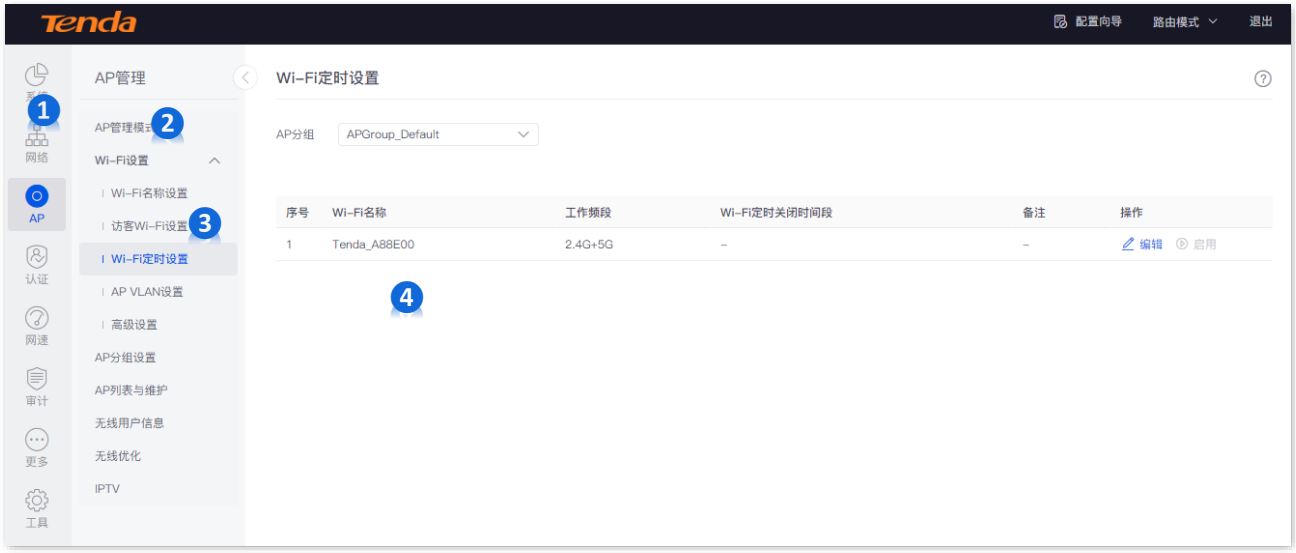
2.2 退出登录

您登录到路由器的管理页面后，如果在闲置超时时间内没有任何操作，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。

3 Web 界面简介

3.1 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、三级导航栏和配置区四部分。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	三级导航栏	
4	配置区	用户进行配置或查看配置的区域。

3.2 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
新增	用于新增配置。
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。
编辑	用于修改配置。
删除	用于删除配置。
	用于查看当前页面设置的帮助信息。
	用于查看对应设置项的帮助信息。
	自定义要显示的列表参数项，或将列表参数项显示恢复到默认状态。

4 系统状态

本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

4.1 查看联网信息

登录到路由器 Web 管理页面后，点击「系统」。

在“联网信息”模块，您可以查看路由器的联网状态。如下图所示，表示路由器已联网成功。

若显示失败信息，请点击跳转至联网设置页面，检查联网设置。图示仅供参考。

4.2 查看系统资源信息

登录到路由器 Web 管理页面后，点击「系统」。

在“系统资源信息”模块，您可以查看路由器的系统状态信息。下图仅供参考。

4.3 查看运行质量监控

登录到路由器 Web 管理页面后，点击「系统」。

在“运行质量监控”模块，您可以快速查看路由器的网络异常日志，最多显示 10 条最新日志，更多详细信息请点击页面的查看详情，跳转至网络监控日志；点击页面的立即诊断，跳转至网络诊断。

4.4 查看终端信息

登录到路由器 Web 管理页面后，点击「系统」。

在“终端信息统计”模块，您可以查看连接到路由器的用户数量和会话数、已被路由器管理的在线 AP 数和离线数、连接到 AP 的 2.4GHz 网络和 5GHz 网络的用户数。

4.5 查看端口信息

登录到路由器 Web 管理页面后，点击「系统」。

在“端口信息”模块，您可以查看路由器各端口的基本状态信息。鼠标悬浮于接口图标上，可查看该端口的物理连接状态、IP 地址等信息。

参数说明

标题项	说明
接口	路由器各接口角色及物理连接状态。 - 绿色表示已连接且协商速率为 1G 及以上。 - 橙色表示已连接且协商速率为 100M/10M。 - 灰色表示未连接。

标题项		说明
LAN 口信息	物理连接	LAN 口的连接状态。 - 已连接：接口连接正常，显示对应 LAN 口的协商速率和双工模式。 - 未检测到连接：接口未连接或连接异常。
	IP 地址	LAN 口的 IPv4 地址。
	子网掩码	LAN 口的子网掩码。
	MAC 地址	LAN 口的 MAC 地址。
	VLAN 信息	LAN 口所属的 VLAN。
WAN 口信息		WAN 口的连接状态。

4.6 查看 WAN 口实时速率

登录到路由器 Web 管理页面后，点击「系统」。

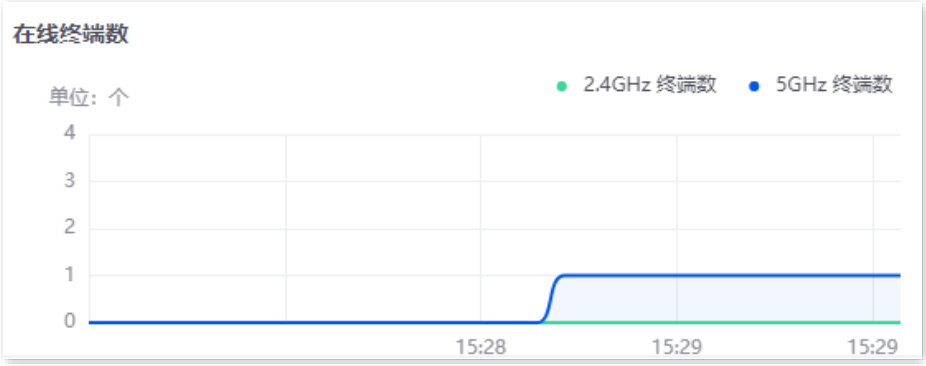
在“WAN 口实时速率”模块，您可查看路由器所有 WAN 口的上传、下载速率总和，也可查看某一 WAN 口的上传、下载速率。

点击“WAN 口实时速率”右侧的下拉框可以选择查看某一 WAN 口的实时速率。

4.7 在线终端数（纯 AC 模式）

登录到路由器 Web 管理页面后，点击「系统」。

在“在线终端数”模块，您可查看连接到 AP 的 2.4GHz 和 5GHz 网络的实时用户数变化。



5 网络设置

本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

5.1 联网设置

在这里，您可以配置路由器 WAN 口上网参数，实现局域网多台设备共享您办理的宽带服务上网（IPv4）。

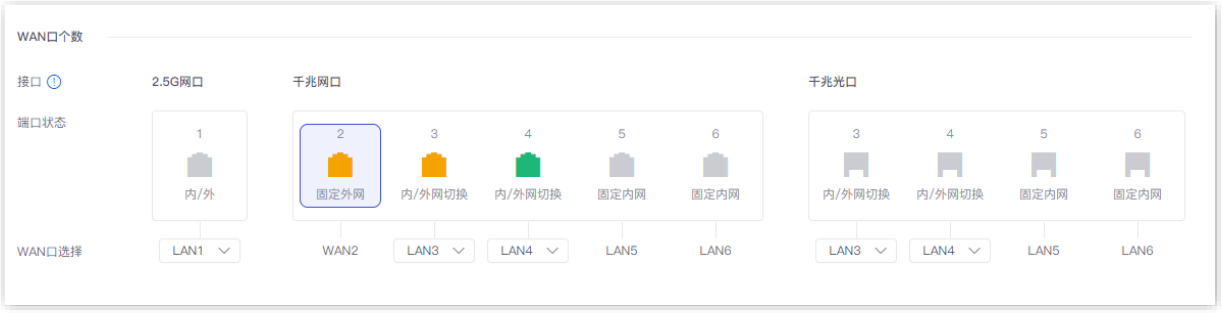
5.1.1 WAN 口个数

登录到路由器 Web 管理页面后，点击「网络」>「联网设置」，找到“WAN 口个数”模块。

您可以查看接口的速率类型，设置 WAN 口个数，查看各接口的连接状态及属性。下图仅供参考。

部分型号路由器支持光口，光口的端口类型和同编号的网（电）口相同。

- 如果光口连线后，同编号电口也连线，仅光口生效。
- 如果电口连线后，30 秒内同编号光口也连线，仅光口生效，否则仅电口生效。



参数说明

标题项	说明
接口	路由器的接口类型及最大协商速率。
端口状态	路由器接口的角色及各接口连接状态。 绿色或橙色表示接口连接正常。灰色表示接口未连接设备或连接异常。
WAN 口选择	接口当前的类型，可根据实际情况修改。

5.1.2 设置联网

登录到路由器 Web 管理页面后，点击「网络」>「联网设置」，找到“连接设置”模块。

您可以设置 WAN 口的联网参数。路由器的联网方式支持宽带拨号、动态 IP、静态 IP。

提示

- 不同型号路由器默认的 WAN 口个数不一样，具体以产品规格为准。下文以 WAN2 口设置为例，其他 WAN 口的设置方法类似。
- 各上网参数均由宽带服务商提供，如不清楚，请咨询您的宽带服务商。

宽带拨号

路由器使用宽带服务商提供的宽带账号和密码拨号上网。

设置步骤：

步骤 1 登录到路由器 Web 管理页面，点击「网络」>「联网设置」。

步骤 2 在“连接设置”模块，选择“联网方式”为“宽带拨号”。

步骤 3 输入宽带服务商提供的“宽带账号”和“宽带密码”。

步骤 4 点击 连接 。

---完成

稍等片刻，您可以在“连接状态”模块查看相关联网信息。

参数说明

标题项	说明
宽带账号 宽带密码	宽带服务商提供的宽带账号/密码。
服务器名	PPPoE 服务器的名称（Server name），也叫 AC name。用于路由器验证 PPPoE 服务器合法性。 注意 如果宽带服务商未提供，请勿填写，否则可能会导致拨号失败。
服务名	PPPoE 服务的名称（Service name）。用于 PPPoE 服务器验证路由器的合法性。 注意 如果宽带服务商未提供，请勿填写，否则可能会导致拨号失败。
首选 DNS 备用 DNS	设置 WAN 口的首选/备用 DNS 服务器地址。 当自动获取的 DNS 服务器无法正常解析网址时，您可以在此处手动指定一个正确的首选/备用 DNS 服务器。

动态 IP

路由器使用宽带服务商动态分配的 IP 地址信息上网。

设置步骤：

步骤 1 登录到路由器 Web 管理页面，点击「网络」>「联网设置」。

步骤 2 在“连接设置”模块，选择“联网方式”为“动态 IP”。

步骤 3 点击 连接 。

---完成

稍等片刻，您可以在“连接状态”模块查看相关联网信息。

参数说明

标题项	说明
首选 DNS	设置 WAN 口的首选/备用 DNS 服务器地址。 当自动获取的 DNS 服务器无法正常解析网址时，您可以在此处手动指定一个正确的首选/备用 DNS 服务器。
备用 DNS	

静态 IP

路由器使用宽带服务商提供的固定 IP 地址、子网掩码、默认网关、DNS 服务器信息上网。

设置步骤：

步骤 1 登录到路由器 Web 管理页面，点击「网络」>「联网设置」。

步骤 2 在“连接设置”模块，选择“联网方式”为“静态 IP”。

步骤 3 输入宽带服务商提供的“IP 地址”、“子网掩码”、“默认网关”和“首选/备用 DNS”。

提示

如果宽带服务商只提供一个 DNS 服务器地址，“备用 DNS”可不填。

步骤 4 点击 连接 。

---完成

稍等片刻，您可以在“连接状态”模块查看相关联网信息。

5.1.3 查看连接状态

登录到路由器 Web 管理页面后，点击「网络」>「联网设置」，找到“连接状态”模块。

在这里，您可以查看对应 WAN 口 IPv4 的网络情况，包括 WAN 口协商速率及双工模式、联网状态、联网时长，以及 IP 地址等。如下图示仅供参考。

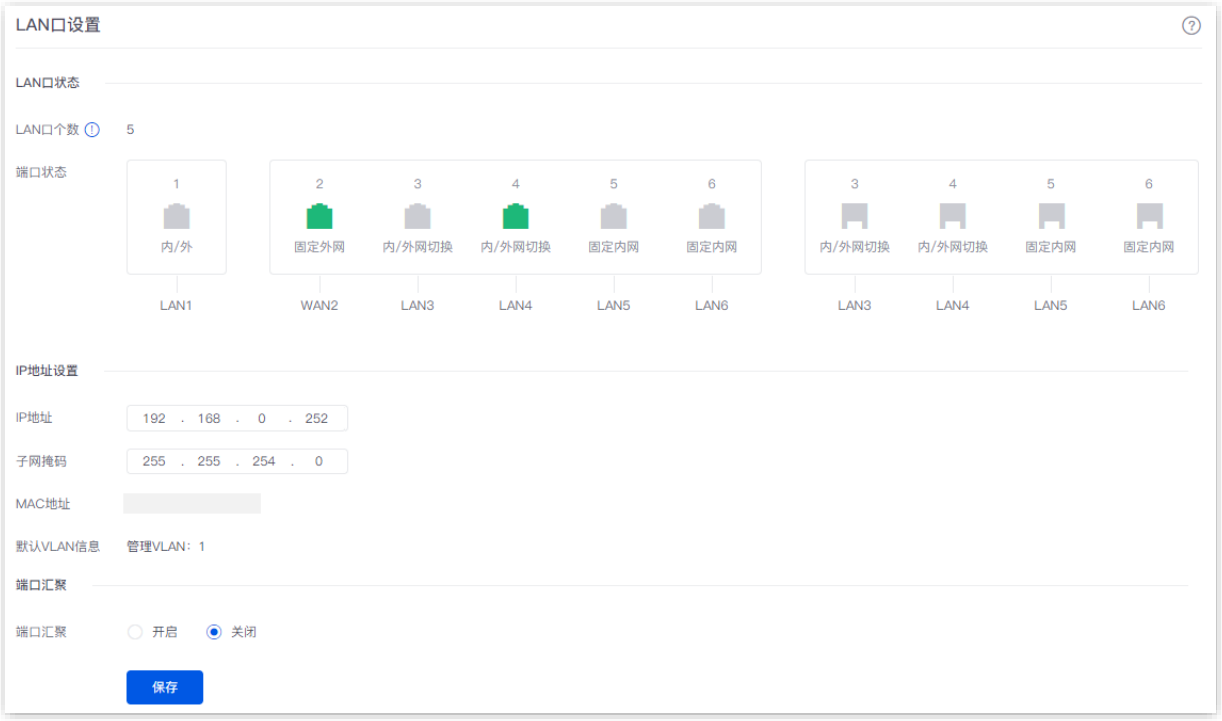
5.2 LAN 口设置

端口汇聚：本质上和交换机的链路聚合功能类似，是将多个物理端口组合在一起形成一个逻辑端口的技术。通过这种方式，可以增加链路带宽、提供链路冗余备份，增强网络的可靠性和性能。

- 动态聚合：依靠链路聚合控制协议（LACP）来自动协商和配置端口汇聚。路由器通过发送 LACP 协议数据包来发现对端设备是否支持端口汇聚，并且自动协商哪些端口可以组成聚合组。适用于对网络性能和可靠性要求较高、需要动态适应网络变化的复杂网络环境，如大型企业网络、云数据中心等。
- 静态聚合：需要手动在路由器上配置参与汇聚的端口，没有自动协商的过程。管理员需要明确指定哪些端口要组合成一个聚合组，并且要保证这些端口的相关参数（如属性、端口速率、双工模式、VLAN ID 等）一致。适用于网络结构相对简单、稳定性要求较高且对网络变化需求不高的环境，如小型企业网络、家庭网络等。

登录到路由器 Web 管理页面后，点击「网络」>「LAN 口设置」。

在这里，您可以查看 LAN 口个数以及各网口的连接状态及属性，设置默认 VLAN 接口“VLAN_Default”的 IPv4 地址相关信息，配置端口汇聚功能。



参数说明

标题项		说明
LAN 口状态	LAN 口个数	路由器的 LAN 口个数。
	端口状态	路由器接口的角色及各接口连接状态。 绿色和橙色表示接口连接正常。灰色表示接口未连接设备或连接异常。
IP 地址设置	IP 地址	VLAN_Default 接口的 IPv4 地址，连接到接口的设备可以通过 http 或 https 协议（默认为 http）访问该 IPv4 地址登录路由器的 Web 管理页面。默认为 192.168.0.252。 提示 修改 IP 地址后，您需要先禁用再启用电脑的网卡，使网卡重新获取 IP 地址。
	子网掩码	VLAN_Default 接口的子网掩码。
	MAC 地址	VLAN_Default 接口的 MAC 地址。
	默认 VLAN 信息	VLAN_Default 接口的 VLAN ID。
端口汇聚	汇聚模式	- 静态聚合：管理员需在路由器手动指定“成员端口”，并在对端指定聚合端口，以形成聚合组。 - 动态聚合：管理员指定的“成员端口”根据 LACP 协议自动与对端设备协商聚合组。

标题项		说明
LAN 口状态	LAN 口个数	路由器的 LAN 口个数。
	端口状态	路由器接口的角色及各接口连接状态。 绿色和橙色表示接口连接正常。灰色表示接口未连接设备或连接异常。
IP 地址设置	IP 地址	VLAN_Default 接口的 IPv4 地址，连接到接口的设备可以通过 http 或 https 协议（默认为 http）访问该 IPv4 地址登录路由器的 Web 管理页面。默认为 192.168.0.252。 提示 修改 IP 地址后，您需要先禁用再启用电脑的网卡，使网卡重新获取 IP 地址。
	子网掩码	VLAN_Default 接口的子网掩码。
	MAC 地址	VLAN_Default 接口的 MAC 地址。
	默认 VLAN 信息	VLAN_Default 接口的 VLAN ID。
	汇聚算法	汇聚端口间数据的分配方式，路由器和对端设备的汇聚算法需保持一致。 - 源目的 MAC：结合了源 MAC 和目的 MAC 两种算法，在数据传输时同时考虑数据帧的源 MAC 地址和目的 MAC 地址两个因素，来确定将数据帧转发到汇聚组中的哪一个端口。 - 源目的 IP：结合了源 IP 和目的 IP 两种算法，在数据传输时同时考虑数据帧的源 IP 地址和目的 IP 地址两个因素，来确定将数据帧转发到汇聚组中的哪一个端口。 - 源目的 MAC–IP–端口：结合源 MAC、目的 MAC、源 IP、目的 IP 以及端口号五种算法，精准分配数据，但也对系统性能要求较高，可能导致设备性能下降。
	MAC 地址	聚合后端口 AGG1 的 MAC 地址。系统会自动生成，也可以手动修改。
	成员端口	选择加入汇聚组的端口，端口的相关参数（如属性、端口速率、双工模式等）需一致。
	汇聚速率	当前聚合口 AGG1 的最高速率。

5.3 VLAN 设置

5.3.1 概述

VLAN（Virtual Local Area Network，虚拟局域网），是一种将局域网内的设备在逻辑上而不是在物理上划分成不同网段，从而实现虚拟工作组的技术。VLAN 的用途是将局域网交换机构成的网络中的工作站作逻辑分组，分组间隔绝广播。组内工作站位于同一个 VLAN，不管地理位置都可以像连接在同一个

网段上一样正常通讯，由于广播包隔绝，VLAN 间不能直接通信，必须通过路由器或其它三层包转发设备转发。

与传统以太网相比，VLAN 具有如下的优点：

- 控制广播域的范围：局域网内的广播报文被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强了局域网的安全性：由于报文在数据链路层被 VLAN 划分的广播域所隔离，因此各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层网络设备对报文进行三层转发。
- 灵活创建虚拟工作组：使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以访问网络。

VLAN 端口对数据包的处理方式如下表所示：

类型	接收 Tag 数据包	接收 Untag 数据包	发送数据
Access 端口	按 Tag 数据包中的 VID 转发到相应 VLAN 的其他端口	按该端口的 PVID 转发到相应 VLAN 的其他端口	删除报文的 Tag 再发送
Trunk 端口			若数据包的 VID 值与 PVID 值相同，拆除 Tag 发送；反之保留 Tag 发送

登录到路由器 Web 管理页面后，点击「网络」>「VLAN 设置」。

您可以配置 VLAN 规则。路由器默认已创建一个名称为 VLAN_Default 的 VLAN 接口，其 VLAN ID 为 1，不可编辑、删除。若 VLAN=1，则表示不带 VLAN 信息，只处理不带 VLAN 的 LAN 口的数据；若 VLAN≠1，只处理对应 VLAN 的 LAN 口的数据。

参数说明

标题项	说明
端口状态	路由器接口的类型及各接口连接状态。 绿色和橙色表示接口连接正常。灰色表示接口未连接设备或连接异常。
VLAN 设置	路由器默认创建名称为 VLAN_Default 的 VLAN，且将所有接口加入该 VLAN。点击 新增 ，可新建 VLAN，并选择是否将接口加入 VLAN。 - 不加入：接口未加入对应 VLAN，不收发携带对应 VLAN ID 的数据包。 - TAG：接口加入对应 VLAN，该接口为 Trunk 口，PVID=1，可允许多个 VLAN 通过，一般用于路由器与交换机、AP 之间连接的端口。数据处理方式参考 VLAN 端口对数据包的处理方式。 - UNTAG：接口加入对应 VLAN，该接口为 Access 口，仅允许一个 VLAN 通过，一般用于连接电脑的端口。数据处理方式参考 VLAN 端口对数据包的处理方式。 提示 如果接口同时包含 TAG 与 UNTAG VLAN，该接口为 Trunk 口，且 PVID 为 UNTAG VLAN 的 VLAN ID。
VLAN ID	VLAN 接口的 VLAN ID。 VLAN ID 是虚拟局域网的标识，用来在一个局域网划分出独立的局域网，不同的 ID 号代表不同的局域网。 提示 - 如果 VLAN ID 为“1”，则表示不带 VLAN 信息。 - 汇聚组内各端口的 VLAN ID 相同。
IP 地址	VLAN 接口的 IP 地址，该接口下的设备可以使用该 IP 地址登录路由器的 Web 管理界面。
子网掩码	VLAN 接口的子网掩码。
互访设置	VLAN 的互访策略。 - 允许：表示其它 VLAN 下的客户端可以访问本 VLAN 下的服务。 - 禁止：表示其它 VLAN 下的客户端不能访问本 VLAN 下的服务。

5.3.2 VLAN 配置举例一（路由器允许单个 VLAN）

组网需求

某企业使用路由器+胖 AP 进行网络搭建，要求访客、各部门和员工访问的网络相互隔离，并且具有不同的网络权限。

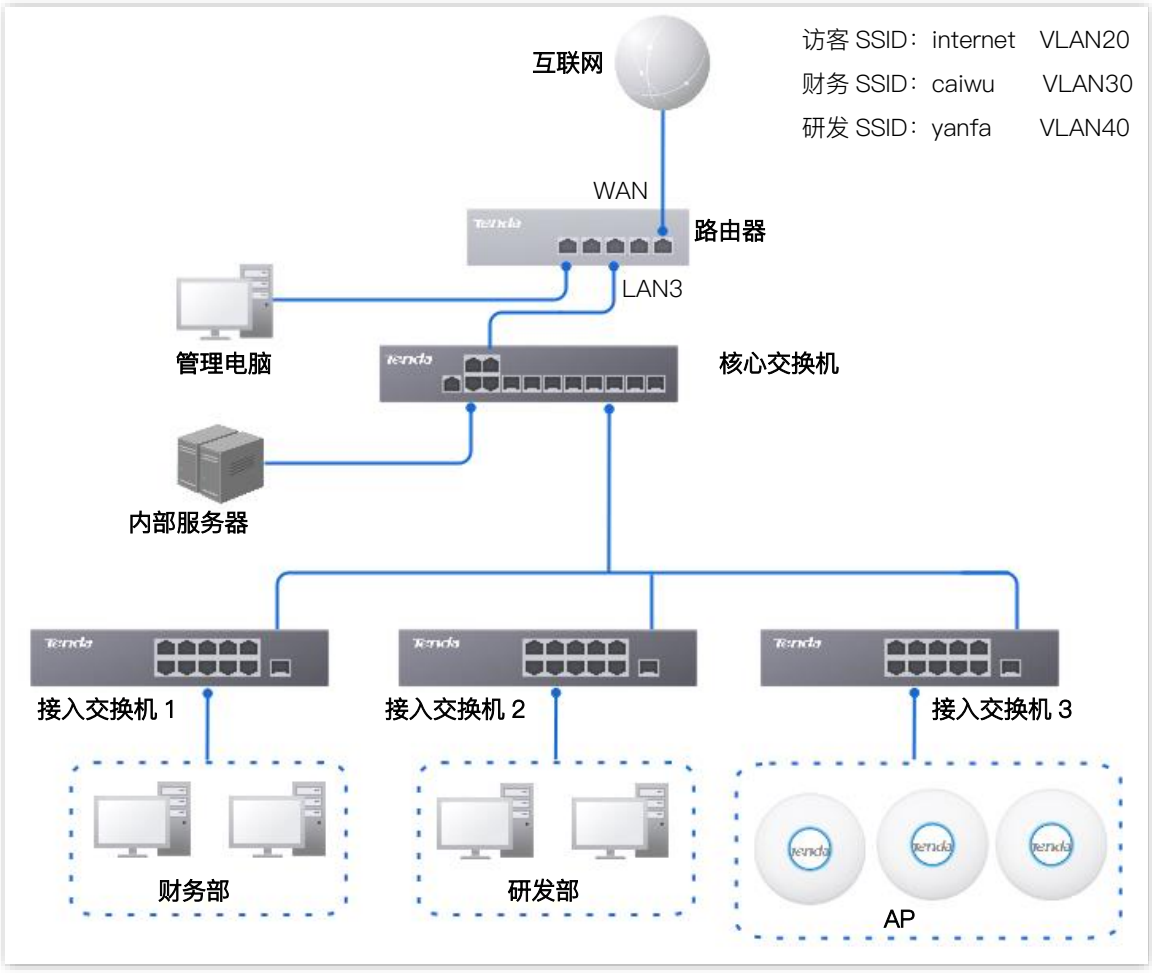
- 访客接入无线网络，只能访问互联网且与其他网络隔离。
- 财务部员工支持接入有线网络与无线网络，只能访问内网且与其他网络隔离。

- 研发部员工支持接入有线网络与无线网络，只能访问内网且与其他网络隔离。

方案设计

- 在路由器上成功管理 AP，并配置不同的 Wi-Fi 下发给 AP。
- 配置访客连接的 Wi-Fi，Wi-Fi 名称为 internet，Wi-Fi 密码为 UmXmL9UK，无线 VLAN ID 为 20。
- 配置财务部员工连接的 Wi-Fi，Wi-Fi 名称为 caiwu，Wi-Fi 密码为 CetTLb8T，无线 VLAN ID 为 30。
- 配置研发部员工连接的 Wi-Fi，Wi-Fi 名称为 yanfa，Wi-Fi 密码为 ZeFtub6m，无线 VLAN ID 为 40。
- 将财务部员工连接的有线网络划分到 VLAN30。
- 将研发部员工连接的有线网络划分到 VLAN40。
- 在交换机上配置 VLAN 转发规则。
- 在路由器和内部服务器上配置 VLAN 转发规则。

网络组网拓扑如下所示。



配置步骤

配置路由器 > 配置核心交换机 > 配置内部服务器

一、设置路由器

步骤 1 登录到路由器 Web 管理页面。

步骤 2 管理 AP。（如已管理 AP，请跳过此步）

1 点击「AP」>「AP 管理模式」。

2 开启“AP 管理模式”功能和“配置自动下发”功能。

进入「AP」>「AP 列表与维护」页面，即可查看路由器是否已成功管理 AP。

步骤 3 添加 VLAN 并配置 DHCP 服务器。

VLAN 参数示例如下表所示。

VLAN 名称	VLAN ID	IP 地址/网段	物理端口
访客	20	192.168.20.1/24	LAN3（TAG）

VLAN 的 DHCP 服务器参数示例如下表所示。

策略名称	应用接口	DHCP 类型	DHCP 配置
访客	访客	用户 DHCP	IP 地址池：192.168.20.100~192.168.20.200 子网掩码：255.255.255.0 默认网关：192.168.20.1 首选 DNS：192.168.20.1

1 添加 VLAN。

- 进入「网络」>「VLAN 设置」页面。

- 点击 新增，然后配置 VLAN 相关参数，点击 保存。

- 为“访客”VLAN 选择端口，本例为 LAN3，设置 VLAN 策略为 TAG。

2 为 VLAN 配置 DHCP 服务器。

进入「网络」>「DHCP 设置」>「DHCP 服务器」页面，点击 新增，然后配置“访客”VLAN 的用户 DHCP 服务器相关参数，点击 保存。

步骤 4 配置 AP 策略。

AP 相关策略参数示例如下表所示，其他未提及的参数保持默认设置。

AP 分组	Wi-Fi 设置	AP VLAN
分组名称：企业	所属 AP 分组：企业 Wi-Fi 名称：internet 加密方式/加密类型：WPA2-PSK/AES 密码：UmXmL9UK 无线 VLAN ID：20 最大客户端：40	所属 AP 分组：企业 AP VLAN：开启 Trunk 口：LAN0
	所属 AP 分组：企业 Wi-Fi 名称：caiwu 加密方式：WPA2-PSK/AES 密码：CetTLb8T 无线 VLAN ID：30 最大客户端：40	
	所属 AP 分组：企业 Wi-Fi 名称：yanfa 加密方式：WPA2-PSK/AES 密码：ZeFtub6m 无线 VLAN ID：40 最大客户端：40	

1 配置 AP 分组策略。

进入「AP」>「AP 分组设置」页面，点击 新增，配置 AP 分组策略，点击 保存。

2 配置 Wi-Fi。

进入「AP」>「Wi-Fi 设置」>「Wi-Fi 名称设置」页面，选择 AP 分组为“企业”，点击 新增，然后配置 Wi-Fi 相关参数，点击 保存。

3 配置 VLAN 策略。

进入「AP」>「Wi-Fi 设置」>「AP VLAN 设置」页面，选择 AP 分组为“企业”，开启“AP VLAN”功能，点击 保存 。

步骤 5 下发 AP 分组策略。

1 进入「AP」>「AP 列表与维护」页面，选择要下发 AP 分组策略的 AP，点击 AP 分组 。

2 选择名称为“企业”的 AP 分组策略，点击 保存 ，下图仅供参考。

二、配置核心交换机

在核心交换机上划分 IEEE 802.1Q VLAN，具体如下。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
路由器	20	Trunk	1
内部服务器	30，40	Trunk	1
接入交换机 1（财务部）	30	Access	30
接入交换机 2（研发部）	40	Access	40
接入交换机 3（AP）	20，30，40	Trunk	1

其他未提到的端口保持默认设置即可。具体配置方法请参考交换机的使用说明书。

三、配置内部服务器

为连接到核心交换机的端口添加 VLAN 并配置 DHCP 服务器。

步骤 1 添加 VLAN，下表参数仅供参考。

VLAN 名称	VLAN ID	IP 地址/网段	物理端口
财务	30	192.168.30.1/24	LAN
研发	40	192.168.40.1/24	LAN

步骤 2 为 VLAN 配置用户 DHCP 服务器，下表参数仅供参考。

策略名称	用户 DHCP
财务	IP 地址池：192.168.30.100~192.168.30.200 子网掩码：255.255.255.0 默认网关：192.168.30.1 首选 DNS：192.168.30.1
研发	IP 地址池：192.168.40.100~192.168.40.200 子网掩码：255.255.255.0 默认网关：192.168.40.1 首选 DNS：192.168.40.1

步骤 3 设置连接到核心交换机的端口的 VLAN。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
核心交换机	30,40	Trunk	1

具体配置方法请参考对应设备的使用说明书。

---完成

验证配置

- 访客连接无线网络“internet”时，输入无线密码“UmXmL9UK”，即可访问互联网，且与其他网络隔离。
- 财务员工连接无线网络“caiwu”时，输入无线密码“CetTLb8T”，即可访问内网，且与其他网络隔离。
- 研发员工连接无线网络“yanfa”时，输入无线密码“ZeFtub6m”，即可访问内网，且与其他网络隔离。
- 财务员工接入有线网络时，即可访问内网，且与其他网络隔离。
- 研发员工接入有线网络时，即可访问内网，且与其他网络隔离。

5.3.3 VLAN 配置举例二（路由器允许多个 VLAN）

组网需求

某企业使用路由器+胖 AP 进行网络搭建，要求访客、各部门和员工访问的网络相互隔离，并且具有不同的网络权限。

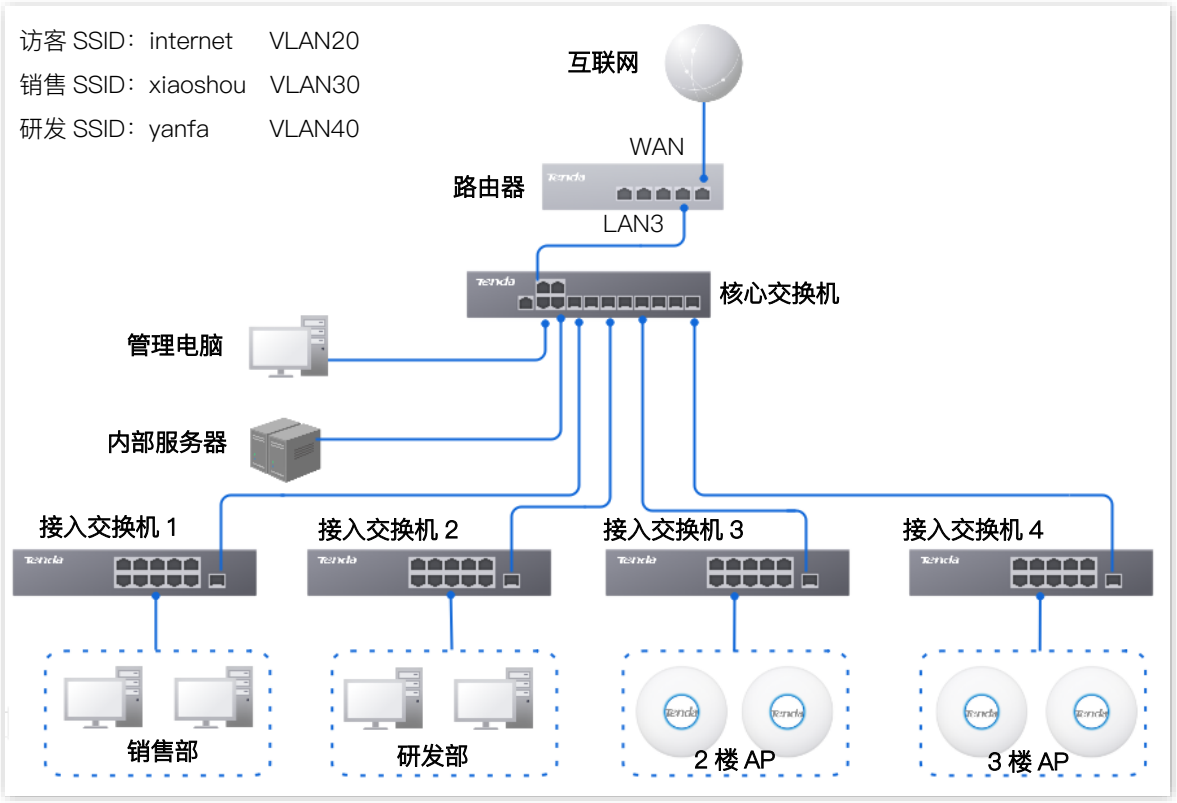
- 访客接入无线网络，只能访问互联网且与其他网络隔离。
- 销售部员工支持接入有线网络与无线网络，只能访问互联网且与其他网络隔离。

- 研发部员工支持接入有线网络与无线网络，只能访问研发内网且与其他网络隔离。
- 为了隔离管理，将管理电脑、2 楼的 AP、3 楼的 AP 划分到不同 VLAN。

方案设计

- 在路由器上成功管理 AP，并配置不同的 Wi-Fi 下发给 AP。
- 配置访客连接的 Wi-Fi，Wi-Fi 名称为 internet，Wi-Fi 密码为 UmXmL9UK，VLAN ID 为 20。
- 配置销售部员工连接的 Wi-Fi，Wi-Fi 名称为 xiaoshou，Wi-Fi 密码为 CetTLb8T，VLAN ID 为 30。
- 配置研发部员工连接的 Wi-Fi，Wi-Fi 名称为 yanfa，Wi-Fi 密码为 ZeFtub6m，VLAN ID 为 40。
- 将 2 楼 AP 划分到 VLAN2。
- 将 3 楼 AP 划分到 VLAN3。
- 将管理电脑划分到 VLAN50。
- 将销售部员工连接的有线网络划分到 VLAN30。
- 将研发部员工连接的有线网络划分到 VLAN40。
- 在核心交换机上配置 VLAN 转发规则。
- 在路由器和内部服务器上配置 VLAN 转发规则。

网络组网拓扑如下所示。



配置步骤

配置路由器 > 配置核心交换机 > 配置内部服务器

一、设置路由器

步骤 1 登录到路由器 Web 管理页面。

步骤 2 管理 AP。（如已管理 AP，请跳过此步）

1 点击「AP」>「AP 管理模式」。

2 开启“AP 管理模式”功能和“配置自动下发”功能。

进入「AP」>「AP 列表与维护」页面，即可查看路由器是否已成功管理 AP。

步骤 3 添加 VLAN 并配置 DHCP 服务器。

VLAN 参数示例如下表所示。

VLAN 名称	VLAN ID	IP 地址/网段	物理端口
访客	20	192.168.20.1/24	LAN3（TAG）
销售部	30	192.168.30.1/24	LAN3（TAG）
管理电脑	50	192.168.50.1/24	LAN3（TAG）
2 楼 AP	2	192.168.2.1/24	LAN3（TAG）
3 楼 AP	3	192.168.3.1/24	LAN3（TAG）

VLAN 的 DHCP 服务器参数示例如下表所示。

策略名称	应用接口	DHCP 类型	DHCP 配置
访客	访客	用户 DHCP	IP 地址池：192.168.20.100~192.168.20.200 子网掩码：255.255.255.0 默认网关：192.168.20.1 首选 DNS：192.168.20.1
销售部	销售部	用户 DHCP	IP 地址池：192.168.30.100~192.168.30.200 子网掩码：255.255.255.0 默认网关：192.168.30.1 首选 DNS：192.168.30.1
管理电脑	管理电脑	用户 DHCP	IP 地址池：192.168.50.100~192.168.50.200 子网掩码：255.255.255.0 默认网关：192.168.50.1 首选 DNS：192.168.50.1
2 楼 AP	2 楼 AP	AP DHCP	IP 地址池：172.10.20.100~172.10.20.200 子网掩码：255.255.255.0 默认网关：172.10.20.1 首选 DNS：172.10.20.1
3 楼 AP	3 楼 AP	AP DHCP	IP 地址池：172.10.30.100~172.10.30.200 子网掩码：255.255.255.0 默认网关：172.10.30.1 首选 DNS：172.10.30.1

1 添加 VLAN。

- 进入「网络」>「VLAN 设置」页面。
- 点击 新增，然后配置 VLAN 相关参数，点击 保存。

- 为 VLAN 选择端口，本例为 LAN3，设置 VLAN 策略为 TAG。

2 为 VLAN 配置 DHCP 服务器。

进入「网络」>「DHCP 设置」>「DHCP 服务器」页面，点击 新增，然后配置 VLAN 的用户 DHCP 服务器和 AP DHCP 服务器相关参数，点击 保存。

步骤 4 配置 AP 策略。

AP 相关策略参数示例如下表所示，其他未提及的参数保持默认设置。

AP 分组	Wi-Fi 设置	AP VLAN
分组名称：2 楼 AP	所属 AP 分组：2 楼 AP Wi-Fi 名称：internet 加密方式/加密类型：WPA2-PSK/AES 密码：UmXmL9UK 无线 VLAN ID：20 最大客户端：40	所属 AP 分组：2 楼 AP AP VLAN：开启 管理 VLAN：2 Trunk 口：LAN0
	所属 AP 分组：2 楼 AP Wi-Fi 名称：xiaoshou 加密方式：WPA2-PSK/AES 密码：CetTLb8T 无线 VLAN ID：30 最大客户端：40	
	所属 AP 分组：2 楼 AP Wi-Fi 名称：yanfa 加密方式：WPA2-PSK/AES 密码：ZeFtub6m 无线 VLAN ID：40 最大客户端：40	
分组名称：3 楼 AP	所属 AP 分组：3 楼 AP Wi-Fi 名称：internet 加密方式/加密类型：WPA2-PSK/AES 密码：UmXmL9UK 无线 VLAN ID：20 最大客户端：40	所属 AP 分组：3 楼 AP AP VLAN：开启 管理 VLAN：3 Trunk 口：LAN0
	所属 AP 分组：3 楼 AP Wi-Fi 名称：xiaoshou 加密方式：WPA2-PSK/AES 密码：CetTLb8T 无线 VLAN ID：30 最大客户端：40	
	所属 AP 分组：3 楼 AP Wi-Fi 名称：yanfa 加密方式：WPA2-PSK/AES 密码：ZeFtub6m 无线 VLAN ID：40 最大客户端：40	

1 配置 AP 分组策略。

进入「AP」>「AP 分组设置」页面，点击 新增 ，配置 AP 分组策略，点击 保存 。

2 进入「AP」>「Wi-Fi 设置」>「Wi-Fi 名称设置」页面，配置 Wi-Fi。

- 选择 AP 分组为“2 楼 AP”，点击 新增，然后配置 Wi-Fi 相关参数，点击 保存。

- 选择 AP 分组为“3 楼 AP”，点击 新增，然后配置 Wi-Fi 相关参数，点击 保存。

3 进入「AP」>「Wi-Fi 设置」>「AP VLAN 设置」页面，配置 VLAN 策略。

- 选择 AP 分组为“2 楼 AP”，开启“AP VLAN”功能，设置“管理 VLAN”为“2”，点击 保存。

- 选择 AP 分组为“3 楼 AP”，开启“AP VLAN”功能，设置“管理 VLAN”为“3”，点击 保存 。

步骤 5 为 2 楼 AP 下发 AP 分组策略。

1 进入「AP」>「AP 列表与维护」页面，勾选 2 楼的 AP，点击 AP 分组 。下图仅供参考。

2 选择名称为“2 楼 AP”的 AP 分组策略，点击 保存，下图仅供参考。

步骤 6 参考**步骤 5** 为 3 楼 AP 下发 AP 分组策略。

二、配置核心交换机

在核心交换机上划分 IEEE 802.1Q VLAN，具体如下。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
路由器	2，3，20，30，50	Trunk	1
管理电脑	50	Access	50
内部服务器	40	Access	40
接入交换机 1（财务部）	30	Access	30
接入交换机 2（研发部）	40	Access	40
接入交换机 3（2 楼 AP）	2，20，30，40	Trunk	1
接入交换机 4（3 楼 AP）	3，20，30，40	Trunk	1

其他未提到的端口保持默认设置即可。具体配置方法请参考交换机的使用说明书。

三、配置内部服务器

为连接到核心交换机的端口添加 VLAN 并配置 DHCP 服务器。

步骤 1 添加 VLAN，下表参数仅供参考。

VLAN 名称	VLAN ID	IP 地址/网段	物理端口
研发	40	192.168.40.1/24	LAN

步骤 2 为 VLAN 配置用户 DHCP 服务器，下表参数仅供参考。

策略名称	用户 DHCP
研发	IP 地址池：192.168.40.100~192.168.40.200 子网掩码：255.255.255.0 默认网关：192.168.40.1 首选 DNS：192.168.40.1

步骤 3 设置连接到核心交换机的端口的 VLAN。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
核心交换机	40	Access	40

具体配置方法请参考对应设备的使用说明书。

---完成

验证配置

- 访客连接无线网络“internet”时，输入无线密码“UmXmL9UK”，即可访问互联网，且与其他网络隔离。
- 销售员工连接无线网络“销售”时，输入无线密码“CetTLb8T”，即可访问互联网，且与其他网络隔离。
- 研发员工连接无线网络“yanfa”时，输入无线密码“ZeFtub6m”，即可访问内网，且与其他网络隔离。
- 销售员工接入有线网络时，即可访问互联网，且与其他网络隔离。
- 研发员工接入有线网络时，即可访问内网，且与其他网络隔离。
- 管理电脑既可访问互联网，又可访问路由器 Web 页面（使用 VLAN 设置中任一 VLAN 的 IP 地址均可）。

5.4 DHCP 设置

5.4.1 概述

当网络存在以下需求时，可以通过 DHCP 服务器完成网络设备的 IP 地址配置。

- 网络规模大，为每台网络设备手工配置网络参数的工作量较大。
- 网络中设备数量远远大于该网络可使用的 IP 地址数量，而同一时间上网的设备数目却不多。

- 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

本路由器提供了 DHCP 服务器，可给 DHCP 客户端自动分配 IP 地址信息。

DHCP 服务器

IP 地址分配机制如下：

1. 路由器接收到 DHCP 客户端发送的 IP 地址分配请求时，根据 DHCP 客户端 MAC 地址查询 DHCP 静态分配表。如果该 DHCP 客户端在静态分配表内，则把对应的 IP 地址分配给该 DHCP 客户端；否则，则执行下一步。
2. 路由器从请求报文中识别出 DHCP 客户端类型（用户或 AP）及所属 VLAN，然后根据识别出的信息选择对应 VLAN 接口的相应类型 DHCP 服务器策略来分配 IP 地址。

DHCP 静态分配

通过 DHCP 静态分配功能，您可以让指定客户端始终获得预设的 IP 地址，避免“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。

5.4.2 DHCP 服务器

登录到路由器 Web 管理页面后，点击「网络」>「DHCP 设置」>「DHCP 服务器」。

您可以配置基于 VLAN 接口的 DHCP 服务器。

参数说明

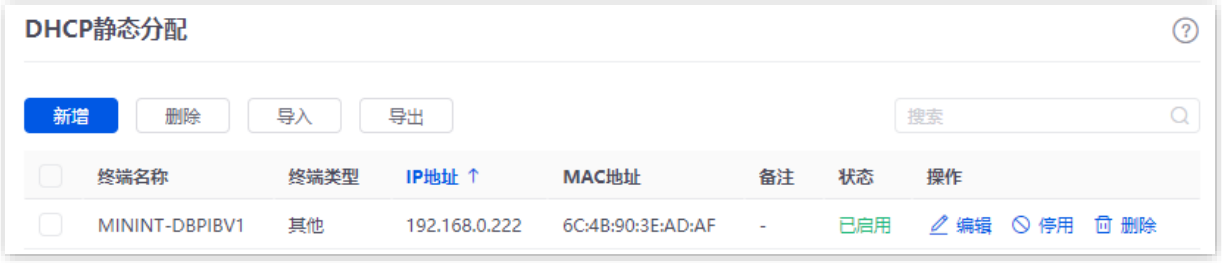
标题项	说明
DHCP 类型	本路由器的 VLAN 接口支持用户 DHCP 和 AP DHCP 两种 DHCP 类型。 - 用户 DHCP：给终端设备分配 IP 地址。 - AP DHCP：给 Tenda AP 分配 IP 地址。
应用接口	DHCP 服务器规则生效的 VLAN 接口，需先在 VLAN 设置页面配置 VLAN 接口。
客户端地址	DHCP 地址池，即 DHCP 服务器可分配给客户端的 IP 地址范围。
子网掩码	DHCP 服务器分配给客户端的子网掩码。
网关	DHCP 服务器分配给客户端的网关地址。

标题项	说明
首选 DNS	DHCP 服务器分配给客户端的首选/备用 DNS 服务器 IP 地址。 注意 为了使局域网设备能够正常上网，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。
备用 DNS	
租约时间	DHCP 服务器分配给客户端的 IP 地址的有效时间。 - 当 IP 地址到期后，如果该客户端仍连接在路由器上，客户端将自动续约，继续占用该 IP 地址。 - 当 IP 地址到期后，如果客户端未连接（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。以后若有其它客户端请求 IP 地址信息，路由器可将该 IP 地址分配给其它客户端。

5.4.3 DHCP 静态分配

登录到路由器 Web 管理页面后，点击「网络」>「DHCP 设置」>「DHCP 静态分配」。

您可以配置静态 IP 地址分配策略，还可以导入/导出静态 IP 地址列表。如果设备已连接路由器，可在 DHCP 列表页面快速将设备加入静态分配。否则，请点击 新增 手动填写静态分配规则。



5.4.4 DHCP 列表

登录到路由器 Web 管理页面后，点击「网络」>「DHCP 设置」>「DHCP 列表」。

您可以对从本路由器获取 IP 地址的终端设备进行如下操作。

- 查看设备的终端名称、获取的 IP 地址等设备信息。
- 可以单个或批量将分配好 IP 地址的设备加入到静态分配列表，使 DHCP 服务器始终给该设备分配同一个 IP 地址。加入成功后，设备将出现在“DHCP 静态分配”列表。

6 AP 管理

本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

6.1 概述

路由器集成了无线控制器的功能，可以管理 Tenda 公司胖 AP，为 AP 统一配置无线网络，对 AP 进行批量维护，可以大大减少您管理大型无线网络时的工作量。

AP 要能被路由器管理，首先需要发现并加入路由器。路由器作为主路由使用时，AP 加入路由器的步骤如下：

步骤 1 AP 获取到自身的 IP 地址。

Tenda 公司的胖 AP 支持 DHCP 客户端功能。当 AP 启动后，会自动从 DHCP 服务器获取到 IP 地址、网关 IP 地址、DNS 服务器的 IP 地址等。

步骤 2 AP 获取到路由器的 IP 地址。

路由器会定期在网络中广播自己的 IP 地址，AP 监听广播，即可获取到路由器的 IP 地址。

步骤 3 AP 向路由器发起加入请求。

AP 获取到路由器的 IP 地址后，即向该地址发起加入请求。

步骤 4 路由器回应 AP 的加入请求，AP 成功加入路由器。

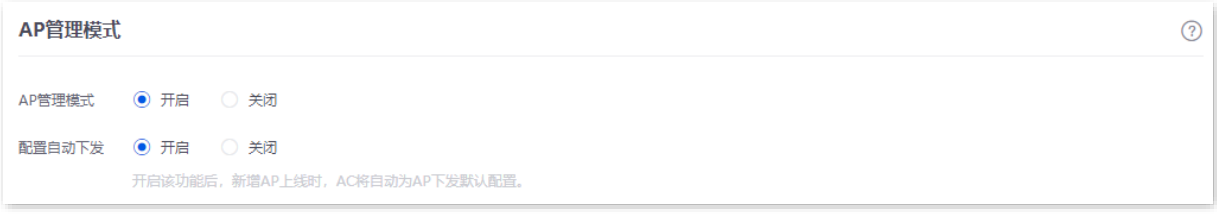
6.2 配置向导

步骤	任务	任务说明
1	配置网络	**可选。** 路由器默认已创建一个名称为 VLAN_Default 的 VLAN 接口，该接口的默认 IP 地址为 192.168.0.252，配置了 User_DHCP_Default 和 AP_DHCP_Default 策略。
2	设置 AP 管理模式	**可选。** 路由器已默认开启“AP 管理模式”和“配置自动下发”功能。
3	配置 AP 分组	**可选。** 路由器默认已创建一条名称为“APGroup_Default”的 AP 分组策略。
4	配置 Wi-Fi	**可选。** 路由器默认已为“APGroup_Default”分组创建了名称为“Tenda_XXXXXX”（XXXXXX 为路由器 MAC 地址后六位）的 Wi-Fi 网络。
5	配置 AP VLAN	**可选。** 默认关闭，如果要为 AP 配置 VLAN，请开启。
6	将 AP 划分到 AP 分组	**可选。** 将已管理上的 AP 划分到 AP 分组。默认已划分到“APGroup_Default”。

6.3 AP 管理模式

登录到路由器 Web 管理页面后，点击「AP」>「AP 管理模式」。

您可以开启或关闭 AP 管理和配置自动下发功能，默认开启 AP 管理和配置自动下发功能。



参数说明

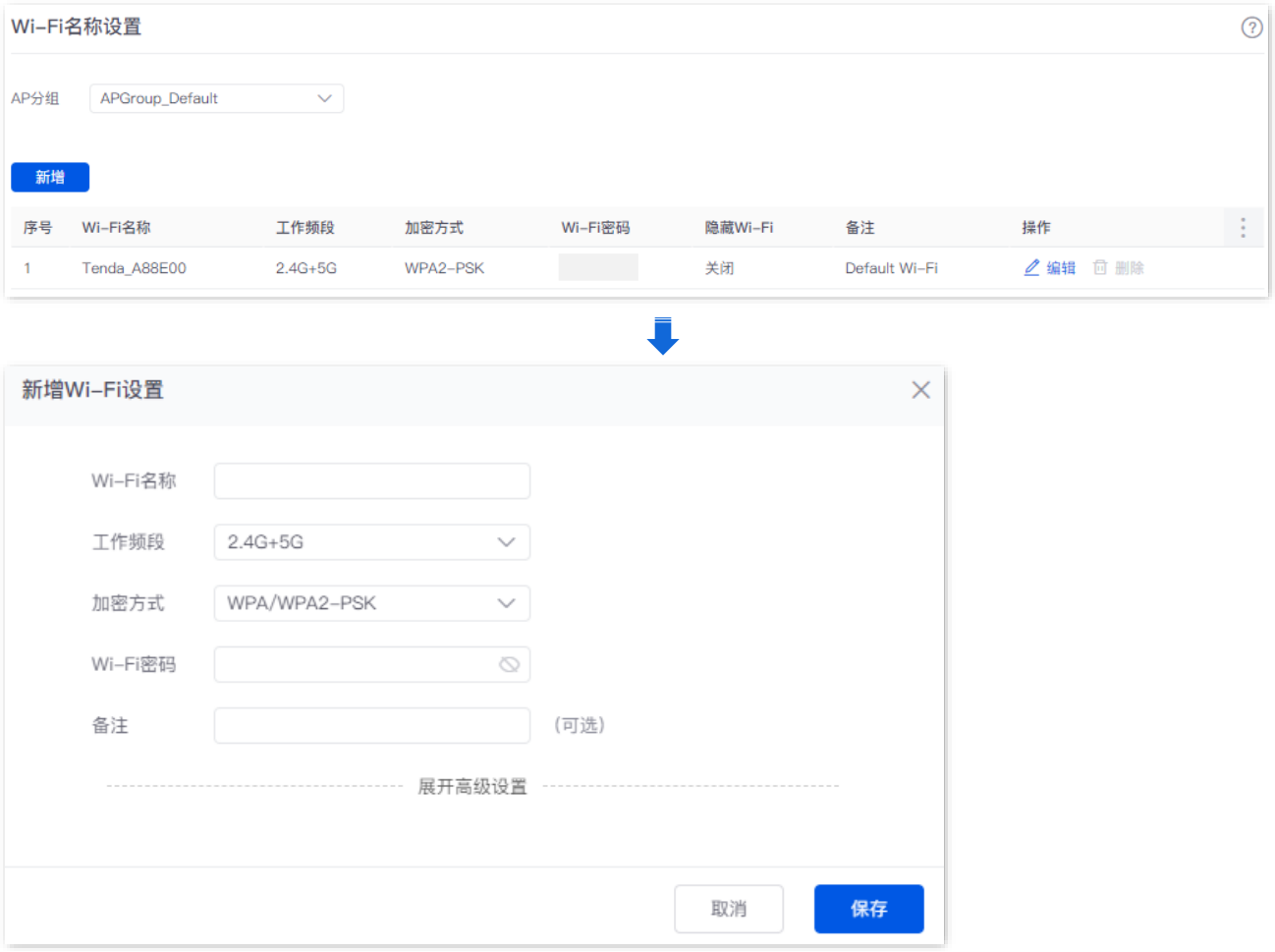
标题项	说明
AP 管理模式	开启/关闭 AP 管理功能。
配置自动下发	开启后，新上线的 AP 或离线 AP 重新上线时，路由器自动将 AP 加入到默认分组（APGroup_Default），即给 AP 下发默认配置。

6.4 Wi-Fi 设置

6.4.1 Wi-Fi 名称设置

登录到路由器 Web 管理页面后，点击「AP」>「Wi-Fi 设置」>「Wi-Fi 名称设置」。

您可以为 AP 分组里的 AP 配置 Wi-Fi。系统默认为 APGroup_Default 创建了一条 Default Wi-Fi，点击 新增 可以新增 Wi-Fi。



参数说明

标题项	说明
AP 分组	选择无线网络所属的 AP 分组，请提前配置 AP 分组。
Wi-Fi 名称	无线网络的名称。
工作频段	无线网络的生效频段。 提示 如 AP 只支持 2.4GHz，则可以选择 2.4GHz 或 2.4GHz&5GHz；若选择 5GHz，则配置无效。

标题项	说明
加密方式	无线网络的加密方式。 - 不加密：无线网络不加密，用户无需密码即可接入网络。为了保障网络安全，不建议选择此项。 - WPA-PSK、WPA2-PSK、WPA/WPA2-PSK：采用预共享密钥认证，用户设置的密钥只用来验证身份，数据加密密钥由 AP 基于加密规则 TKIP 或 AES 来自动生成，解决了 WEP 静态密钥的漏洞，适合个人或家庭用户用于保证无线安全。 WPA/WPA2-PSK 表示 AP 同时兼容 WPA-PSK、WPA2-PSK 两种安全模式，安全性更高。 - WPA3-SAE、WPA3-SAE/WPA2-PSK：采用预共享密钥认证，WPA3-SAE/AES 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。 WPA3-SAE/WPA2-PSK 表示 AP 同时兼容 WPA2-PSK/AES、WPA3-SAE/AES 两种安全模式，安全性更高。 - WPA-企业、WAP2-企业：使用 802.1x 对用户进行认证，而不再使用手工设定的预共享密钥，数据加密密钥由 AP 基于加密规则 TKIP 或 AES 来自动生成，适合企业等高安全要求的无线网络使用。
加密类型	加密方式为 WPA-PSK、WPA2-PSK、WPA3-SAE、WPA3-SAE/WPA2-PSK、WPA-企业、WAP2-企业时使用的数据加密算法。点击**--展开高级设置--**可见。 - AES：高级加密标准。 - TKIP：临时密钥完整性协议。相较于 AES，采用 TKIP 时，AP 只能使用较低的无线速率（最大 54Mbps）。 - TKIP&AES：兼容 TKIP 和 AES。
Wi-Fi 密码	加密方式为 WPA-PSK、WPA2-PSK、WPA3-SAE、WPA3-SAE/WPA2-PSK 时的预共享密钥，即用户在连接无线网络时需要输入对应的无线密码。
密钥更新周期	加密方式为 WPA-PSK、WPA2-PSK、WPA3-SAE、WPA3-SAE/WPA2-PSK 时数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。0 表示不更新。点击**--展开高级设置--**可见。
Radius 服务器地址	加密方式为 WPA-企业、WAP2-企业时，RADIUS 认证服务器的 IP 地址/认证密钥/认证端口。
认证密钥	
认证端口	
隐藏 Wi-Fi	开启后，无线网络名称会隐藏。无线终端连接无线网络时，需要手动添加，在一定程度上增强了无线网络的安全性。点击**--展开高级设置--**可见。
客户端隔离	开启后，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。点击**--展开高级设置--**可见。
最大客户端数	该无线网络最多允许接入的客户端数量。点击**--展开高级设置--**可见。
无线 VLAN ID	对应无线网络所属的 VLAN。

6.4.2 访客 Wi-Fi 设置

访客 Wi-Fi 与其他网络相互隔离，接入到访客 Wi-Fi 的终端设备仅可访问互联网，无法互相访问，也无法访问局域网。

当您需要为访客开放 Wi-Fi 时，可以开启访客 Wi-Fi，满足客访客的上网需求，同时保证主网络安全，防止个人信息泄露。

登录到路由器 Web 管理页面后，点击「AP」>「Wi-Fi 设置」>「访客 Wi-Fi 设置」。

您可以为 AP 分组里的 AP 配置访客 Wi-Fi。该功能默认关闭。下图仅供参考。

- 开启双频合一：访客 Wi-Fi 的 2.4GHz、5GHz 网络的 Wi-Fi 名称、Wi-Fi 密码均相同，只显示一个 Wi-Fi 名称。您连接访客 Wi-Fi 时，将会自动连接到网络质量最好的访客 Wi-Fi。
- 关闭双频合一：访客 Wi-Fi 的 2.4GHz、5GHz 网络分开显示，您连接任意一个访客 Wi-Fi 都可以上网。
- 其他参数请参考 Wi-Fi 名称设置的参数说明。

6.4.3 Wi-Fi 定时设置

登录到路由器 Web 管理页面后，点击「AP」>「Wi-Fi 设置」>「Wi-Fi 定时设置」。

您可以配置 Wi-Fi 在指定时间段关闭。在 Wi-Fi 定时关闭时间段内，智能手机等无线设备无法搜索到该 Wi-Fi。点击 设置 Wi-Fi 定时关闭规则。

6.4.4 AP VLAN 设置

登录到路由器 Web 管理页面后，点击「AP」>「Wi-Fi 设置」>「AP VLAN 设置」。

您可以为 AP 分组里的 AP 配置 VLAN 策略，包括 AP VLAN 启用状态、管理 VLAN、Trunk 口等。该功能默认关闭。

参数说明

标题项	说明
AP 分组	选择 AP VLAN 所属的 AP 分组，请提前配置 AP 分组。
AP VLAN	开启/关闭 AP 的 802.1Q VLAN 功能。
PVID	AP Trunk 口默认所属的 VLAN ID。
管理 VLAN	AP 的管理 VLAN ID。 更改管理 VLAN 后，AP 需要重新连接到新的管理 VLAN 端口，才能被路由器管理。

标题项	说明
Trunk 口	作为 AP Trunk 口的有线 LAN 口。Trunk 口允许所有 VLAN 通过。 注意 启用 802.1Q VLAN 功能后，至少要选择一个 LAN 口作为 Trunk 口。如果使用本策略的 AP 只有一个 LAN 口，请选择 LAN0 为 Trunk 口，否则可能会导致配置失败。
LAN 口	非 Trunk 口的有线 LAN 口对应的 VLAN ID。当使用本策略的 AP 有两个 LAN 口时，才需设置。不可编辑的有线 LAN 口为 Trunk 口。 提示 启用 802.1Q VLAN 功能后，非 Trunk 口的有线 LAN 口和 SSID 所在的无线接口都为 Access 口，其 PVID 与自身的 VLAN ID 相同。

6.4.5 高级设置

登录到路由器 Web 管理页面后，点击「AP」>「Wi-Fi 设置」>「高级设置」。

您可以为 AP 分组里的 AP 配置高级策略，下图仅供参考。

参数说明

标题项	说明
AP 分组	选择 AP 分组，请提前配置 AP 分组。
LED 灯	开启/关闭分组内 AP 的 LED 灯显示。
广播报文限制	限制广播报文的传输速率，默认为 200pps（每秒 200 个以内）。广播报文过多可能会导致广播风暴，使网络瘫痪，请合理设置。
组播报文限制	限制组播报文的传输速率，默认为 200pps（每秒 200 个以内），组播流量过大时，可能会影响网络的整体性能。
日志通知	开启后，AP 的告警信息将显示到「工具」>「日志中心」>「运行日志」的“AP 告警日志”和“AP 运行日志”类别中。
AP 故障告警	开启/关闭 AP 的故障告警功能。 开启后，如果 AP 出现故障（如：重启、离线、上线等），AP 将发出告警信息。通知告警信息的方式为日志通知。
AP 流量告警	开启/关闭 AP 的流量告警功能。 开启后，如果 AP 的流量达到“流量告警阈值”，AP 将发出告警信息。通知告警信息的方式为日志通知。
AP 接入数告警	开启/关闭 AP 接入数告警功能。 开启后，如果接入 AP 的无线客户端达到“接入数告警阈值”，AP 将发出告警信息。通知告警信息的方式为日志通知。
重启设定	自动重启类型。 - 定时重启：AP 在指定的日期的时间点自动重启一次。 - 循环重启：AP 每隔一个指定的“重启间隔时间”自动重启一次。
统一登录账号	AP Web 管理页面的登录用户名与密码。
统一登录密码	
确认登录密码	再一次输入 AP Web 管理页面的登录密码。

6.5 AP 分组设置

登录到路由器 Web 管理页面后，点击「AP」>「AP 分组设置」。

您可以配置 AP 分组策略，以便 Wi-Fi 设置引用，为 AP 分组配置 Wi-Fi 等策略。

系统默认已创建一条名称为“APGroup_Default”的 AP 分组。

6.6 AP 列表与维护

6.6.1 概述

登录到路由器 Web 管理页面后，点击「AP」>「AP 列表与维护」。

您可以查看 AP 列表，给 AP 下发相应的策略以及对 AP 进行重启、升级等相关维护操作。已管理的 AP 默认加入 APGroup_Default 分组。

按钮说明

按钮	说明
同步配置	AP 将使用所属 AP 分组的策略配置替换当前配置。
AP 分组	AP 引用的 AP 分组策略，需先在 AP 分组设置页面配置好。
模式切换	开启/关闭 AP 的云维护功能，或切换云维护的管理模式。详情可参考设置 AP 云维护功能。 提示 部分 AP 不支持云维护功能，请以实际为准。

参数说明

标题项	说明
5G 优先	开启后，当 2.4GHz 和 5GHz 两个频段的无线名称（不能含中文字符）和密码都相同，且无线客户端支持双频 Wi-Fi 时，客户端优先从 5GHz 频段接入 AP 无线网络。
管理模式	AP 的云维护状态。如果要设置 AP 的云维护功能，可参考设置 AP 云维护功能。 提示 部分 AP 不支持云维护功能，请以实际为准。
管理 VLAN	AP 的管理 VLAN ID，与数据 VLAN 做区分。
有线口 VLAN	AP 有线口默认所属的 VLAN ID。

6.6.2 下发策略给 AP

步骤 1 登录到路由器 Web 管理页面。

步骤 2 （若已配置，跳过）配置 AP 分组，详情可参考 AP 分组设置。

步骤 3 （若已配置，跳过）为 AP 分组配置无线策略，详情可参考 Wi-Fi 设置。

步骤 4 下发策略给 AP。

1 点击「AP」>「AP 列表与维护」。

2 选择要下发策略的在线 AP，点击 AP 分组 。下图仅供参考。

3 在“选择 AP 分组策略”的下拉菜单中选择 AP 要加入的 AP 组，点击 保存 。下图仅供参考。

---完成

将 AP 加入某一 AP 组后，AP 将应用该 AP 组内关联的相关策略。

6.6.3 批量设置

通过“批量设置”可以对已选择 AP 进行统一详细配置。

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「AP」>「AP 列表与维护」。

步骤 3 选择要进行详细配置的在线 AP，点击 批量设置 。下图仅供参考。

步骤 4 根据实际情况配置相关参数，点击 保存 。下图仅供参考。

提示

保持不变表示不修改对应配置，和上次配置保持一致。

---完成

已选中 AP 的相关配置将重新下发。

基本参数说明

标题项	说明
AP 分组	AP 引用的 AP 分组策略，需先在 AP 分组设置页面配置好。
射频状态	开启/关闭该频段的射频策略，“保持不变”表示不修改 AP 对应频段的射频开关状态。
网络模式	无线传输标准。您可以参考以下说明选择合适的无线网络模式。 2.4GHz 频段： - 11b：AP 工作在 802.11b 无线网络模式。 - 11g：AP 工作在 802.11g 无线网络模式。 - 11b/g：AP 工作在 802.11b/g 无线网络模式。 - 11b/g/n：AP 工作在 802.11b/g/n 无线网络模式。 - 11b/g/n/ax：AP 工作在 802.11b/g/n/ax 无线网络模式。 - 11b/g/n/ax/be：AP 工作在 802.11b/g/n/ax/be 无线网络模式。 5GHz 频段： - 11a：AP 工作在 802.11a 无线网络模式。 - 11ac：AP 工作在 802.11ac 无线网络模式。 - 11a/n：AP 工作在 802.11a/n 无线网络模式。 - 11a/n/ac/ax：AP 工作在 802.11a/n/ac/ax 无线网络模式。 - 11a/n/ac/ax/be：AP 工作在 802.11a/n/ac/ax/be 无线网络模式。
信道带宽	AP 的无线频段带宽。 - 20M：AP 只能使用 20MHz 的频段带宽。 - 40M：AP 只能使用 40MHz 的频段带宽。 - 80M：AP 只能使用 80MHz 的信道带宽。仅 5GHz 的无线网络支持。 - 160M：AP 只能使用 160MHz 的信道带宽。仅 5GHz 的无线网络支持。 - 自动：AP 根据周围环境，自动调整其频段带宽。 - 保持不变：不修改 AP 对应频段的信道带宽。
信道	AP 的工作信道。 - 自动：AP 自动检测各信道利用率，并据此选择合适的工作信道。 如果使用 AP 无线网络时，经常出现掉线、卡顿或网速慢的问题，可尝试修改 AP 的信道来解决问题。您可以通过工具软件（如 WiFi 分析仪）检测周边较少用到、干扰较小的信道。 - 保持不变：不修改 AP 对应频段的信道。
功率	AP 的无线发射功率。 发射功率越大，则无线覆盖范围更广。但适当的减少发射功率更有助于提高无线网络的性能和安全性。
RSSI	AP 可接受的无线设备信号强度，信号强度低于此值的设备将无法接入 AP。 当环境中存在多个 AP 时，正确设置接入信号强度限制可以确保无线设备主动连接到信号比较强的 AP。

标题项	说明
客户端老化时间	AP 在该时间段内没有接收到客户端任何流量，则 AP 会自动断开该客户端的连接。
抗干扰模式	选择设备的干扰抑制模式。仅 2.4GHz 支持。 - 0：禁用所有抗干扰。 - 1：启用同频段干扰抑制，如微波炉、手机、蓝牙设备造成的同频干扰，一般用于干扰较小的环境。 - 2：强制启用无线电干扰抑制，主要用在无线信号干扰源在 30 个以下的场景，一般用于干扰较大的环境。 - 3：自动启用无线电干扰抑制，一般用于干扰很大的环境。 - 4：自动启用无线电干扰抑制并降低噪声。一般用于无线信号干扰源超过 30 个的环境，如高密场景等。 - 保持不变：不修改 AP 的抗干扰模式。
空口调度	启用后，可以让不同速率的用户获得相同的空口时间，提升高速率用户体验。
WMM	WMM（WiFi Multimedia）是一种无线 QoS 协议，用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的服务质量。
SSID 隔离	开启后，不同 SSID 下的设备之间不能互相通信。
APSD	Automatic Power Save Delivery，自动省电模式。是 Wi-Fi 联盟的 WMM 省电认证协议。开启“APSD”后，可降低 AP 的电能消耗。
5G 优先	开启后，当 2.4GHz 和 5GHz 两个频段的无线名称（不能含中文字符）和密码都相同，且无线客户端支持双频 Wi-Fi 时，客户端优先从 5GHz 频段接入 AP 无线网络。

6.6.4 设置 AP 云维护功能

通过“模式切换”，可以开启/关闭 AP 的云维护功能，或切换云维护的管理模式。

开启 AP 云维护功能

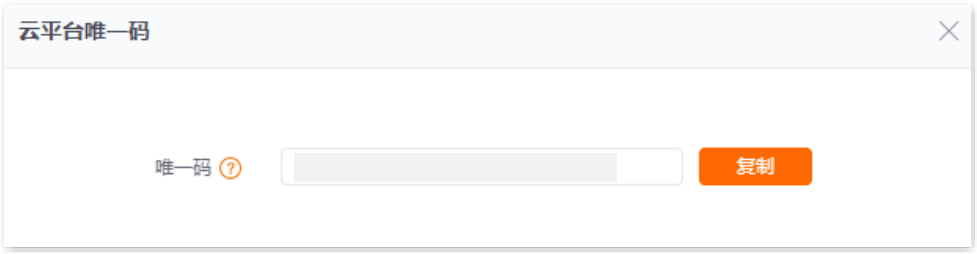
步骤 1 获取云平台唯一码。

提示

- 如果路由器已开启云维护功能，且要将 AP 与路由器添加到同一个项目，可在「更多」>「维护服务」>「云维护」页面获取云平台唯一码。
- 开启 AP 的云维护功能前，请确保 AP 已联网。

1 访问 https://cloudfi.tenda.com.cn，进入 Tenda 掌中宝云平台 Web。

2 点击 Tenda 掌中宝云平台 Web 页面右上角的“新建”>“云平台唯一码”，然后复制该云平台唯一码。



步骤 2 开启 AP 的云维护功能。

1 登录到路由器 Web 管理页面，点击「AP」>「AP 列表与维护」。

2 选择需要开启云维护功能的 AP，然后点击 模式切换 。下图仅供参考。

3 开启“云维护”功能，根据实际需要选择管理模式，如“云托管”。

4 输入已获取的云台唯一码，开启“设备信息上报”功能。

5 点击 确定 。

----完成

AP 开启“云维护”功能后，可以通过 Tenda 掌中宝云平台 Web（https://cloudfi.tenda.com.cn ）或“Tenda

掌中宝”App 管理 AP。

参数说明

标题项	说明
管理模式	云维护的管理模式。 - 云托管：适用于集中统一管理项目并配置维护项目的场景。AP 可被 Tenda 掌中宝云管理系统管理，且相关功能的配置信息仅由 Tenda 掌中宝云管理系统下发。 - 本地托管：适用于集中统一管理并查看项目的场景。AP 可被 Tenda 掌中宝云管理系统管理，但是功能不能修改，所有功能的配置需在路由器或 AP 的 Web 管理页面完成。
云平台唯一码	用于指定设备关联的云平台账号。可以在 Tenda 掌中宝云平台 Web 管理页面（https://cloudfi.tenda.com.cn）或掌中宝 App 获取。
设备信息上报	开启后，AP 才能被云平台管理，AP 的配置信息将会上报到云平台。

6.7 无线用户信息

登录到路由器 Web 管理页面后，点击「AP」>「无线用户信息」。

您可以查看连接到 AP 的终端设备的基本信息。

6.8 胖 AP 管理配置举例

组网需求

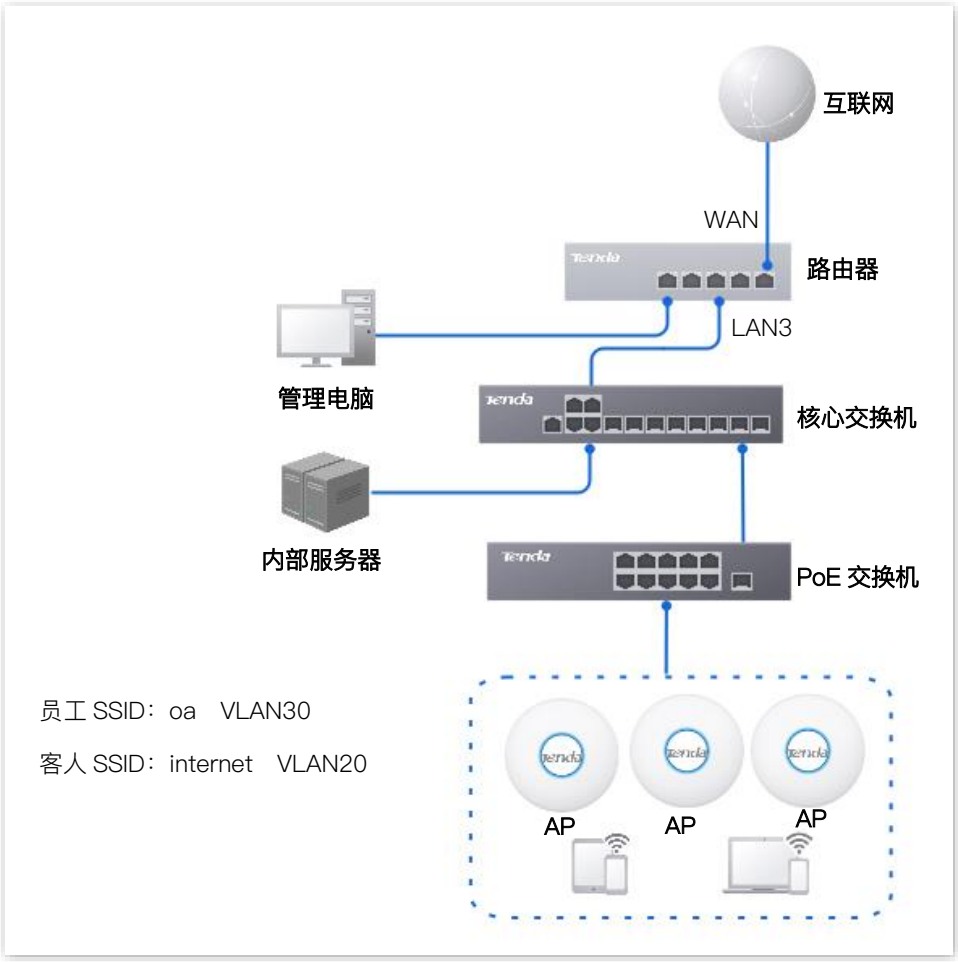
某酒店使用路由器+胖 AP 进行网络搭建，要求客人和员工访问的网络相互隔离，并且客人只能访问互联网，员工只能访问内网。

方案设计

- 在路由器上成功管理 AP，并配置不同的 Wi-Fi 下发给 AP。
- 配置客人连接的 Wi-Fi，Wi-Fi 为 internet，Wi-Fi 密码为 UmXmL9UK，无线 VLAN ID 为 20。

- 配置员工连接的 Wi-Fi，Wi-Fi 名称为 oa，Wi-Fi 密码为 CetTLb8T，无线 VLAN ID 为 30。
- 在核心交换机上配置 VLAN 转发规则。
- 在路由器和内部服务器上配置 VLAN 转发规则。

网络组网拓扑如下所示。



配置步骤

配置路由器 → 配置核心交换机 → 配置内部服务器

一、配置路由器

步骤 1　登录到路由器 Web 管理页面。

步骤 2　管理 AP。（如已管理 AP，请跳过此步）

1　点击「AP」>「AP 管理模式」。

2　开启“AP 管理模式”和“配置自动下发”功能。

进入「AP」>「AP 列表与维护」页面，即可查看路由器是否已成功管理 AP。

步骤 3 给路由器添加 VLAN 并配置 DHCP 服务器。

VLAN 参数示例如下表所示。

VLAN 名称	VLAN ID	IP 地址/网段	物理端口
客人	20	192.168.20.1/24	LAN3（TAG）

VLAN 的 DHCP 服务器参数示例如下表所示。

策略名称	应用接口	DHCP 类型	DHCP 配置
客人	客人	用户 DHCP	IP 地址池：192.168.20.100~192.168.20.200 子网掩码：255.255.255.0 默认网关：192.168.20.1 首选 DNS：192.168.20.1

1 添加 VLAN。

- 进入「网络」>「VLAN 设置」页面。
- 点击 新增，然后配置 VLAN 相关参数，点击 保存。

- 为“客人”VLAN 选择端口，本例为 LAN3，设置 VLAN 策略为 TAG。

2 为 VLAN 配置 DHCP 服务器。

进入「网络」>「DHCP 设置」>「DHCP 服务器」页面，点击 新增 ，然后配置“客人”VLAN 的用户 DHCP 服务器相关参数，点击 保存 。

步骤 4 配置 AP 策略。

AP 相关策略参数示例如下表所示，其他未提及的参数保持默认设置。

AP 分组	Wi-Fi 设置	AP VLAN
分组名称：酒店	所属 AP 分组：酒店 Wi-Fi 名称：internet 加密方式/加密类型：WPA2-PSK/AES 密码：UmXmL9UK VLAN ID：20	所属 AP 分组：酒店 AP VLAN：开启
	所属 AP 分组：酒店 Wi-Fi 名称：oa 加密方式：WPA2-PSK/AES 密码：CetTLb8T VLAN ID：30	

1 配置 AP 分组策略。

进入「AP」>「AP 分组设置」页面，点击 新增 ，配置 AP 分组策略，点击 保存 。

2 配置 Wi-Fi。

进入「AP」>「Wi-Fi 设置」>「Wi-Fi 设置」页面，选择 AP 分组为“酒店”，点击 新增 ，然后配置 Wi-Fi 相关参数，点击 保存 。

3 配置 VLAN 策略。

进入「AP」>「Wi-Fi 设置」>「AP VLAN 设置」页面，选择 AP 分组为“酒店”，开启“AP VLAN”功能，点击 保存 。

步骤 5 下发 AP 分组策略。

1 进入「AP」>「AP 列表与维护」页面，选择要下发 AP 分组策略的 AP，点击 AP 分组 。

2 选择名称为“酒店”的 AP 分组策略，点击 保存，下图仅供参考。

二、配置核心交换机

在核心交换机上划分 IEEE 802.1Q VLAN，具体如下。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
AP	20,30	Trunk	1
路由器	20	Trunk	1
内部服务器	30	Access	30

其他未提到的端口保持默认设置即可。具体配置方法请参考交换机的使用说明书。

三、配置内部服务器

为连接到核心交换机的端口添加 VLAN 并配置 DHCP 服务器。

步骤 1 添加 VLAN，下表参数仅供参考。

VLAN 名称	VLAN ID	IP 地址/网段	物理端口	端口属性
员工	30	192.168.30.1/24	LAN	Access

步骤 2 为 VLAN 配置用户 DHCP 服务器，下表参数仅供参考。

策略名称	用户 DHCP
员工	IP 地址池：192.168.30.100~192.168.30.200 子网掩码：255.255.255.0 默认网关：192.168.30.1 首选 DNS：192.168.30.1

步骤 3 设置连接到核心交换机的端口的 VLAN。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
交换机	30	Access	30

具体配置方法请参考对应设备的使用说明书。

---完成

验证配置

连接到“internet”的用户只能访问互联网；连接到“oa”的用户只能访问公司内网。

6.9 IPTV

6.9.1 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。

登录到路由器 Web 管理页面后，点击「AP」>「IPTV」。

IPTV 功能默认关闭，下图仅供参考。

参数说明

标题项		说明
IPTV 设置	IPTV 口选择	指定路由器的一个 LAN 口作为 IPTV IN 口，用于连接光猫的 IPTV 口。LAN 端口号查看“系统”页面的“接口信息”。
	IPTV 功能	开启或关闭路由器的 IPTV 功能。
	VLAN 设置	IPTV 业务 VLAN ID。 - 若开通 IPTV 业务时，宽带服务商没有提供 VLAN 相关信息，请保持“通用 IPTV”或选择“自定义 VLAN”，勾选“不带 VLAN Tag”。 - 若开通 IPTV 业务时，宽带服务商提供了 VLAN ID 值，请选择“自定义 VLAN”，勾选“带 VLAN Tag”，并输入相应的 VLAN ID 值。 - 若是上海地区的 IPTV 业务，请选择“上海地区”，然后选择相应的 VLAN 值。
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。
	指定网口	AP 与路由器 IPTV 口建立 IPTV 数据透传通道的有线网口。该网口需要连接到 IPTV 机顶盒。 提示 该网口固定指定网口 LAN1。

6.9.2 仅观看 IPTV 节目

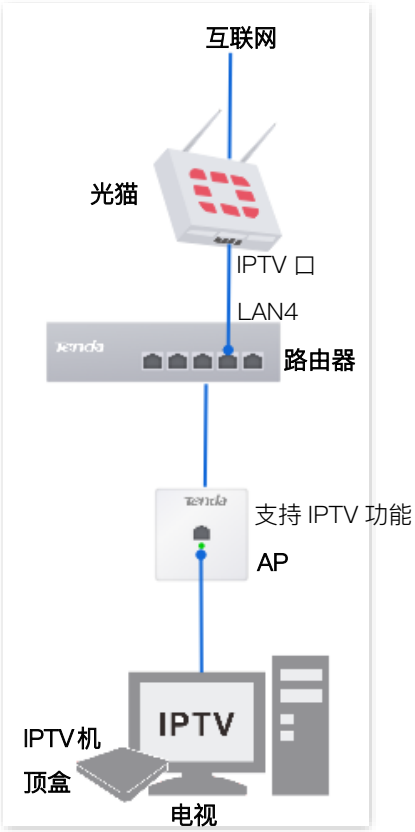
组网需求

某旅馆的宽带业务包含 IPTV 业务。宽带服务商提供了 IPTV 账号和密码，未提供 IPTV 业务的 VLAN ID。

要求：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

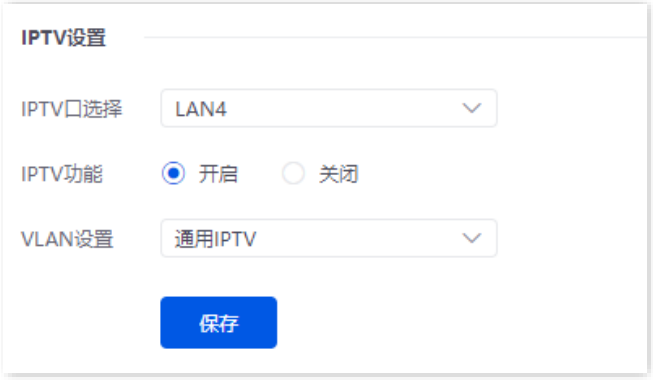
步骤 1 配置路由器。

1 登录到路由器 Web 管理页面。

2 点击「AP」>「IPTV」。

3 开启路由器 IPTV 功能并指定 IPTV 端口。

- 选择路由器作为 IPTV 的 LAN 口，本例为“LAN4”。
- 选择“IPTV 功能”为“开启”。
- 点击 保存 。



4 指定 AP 作为 IPTV 口的有线网口，下图仅供参考。

- 在 AP 列表找到要连接 IPTV 机顶盒的 AP，点击 。
- 勾选指定网口，点击 保存 。

成功指定 AP 的 IPTV 口。

步骤 2 设置您的 IPTV 机顶盒。

使用宽带服务商提供的 IPTV 账号和密码在 IPTV 机顶盒上进行拨号。

----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。

6.9.3 上网+观看 IPTV 节目

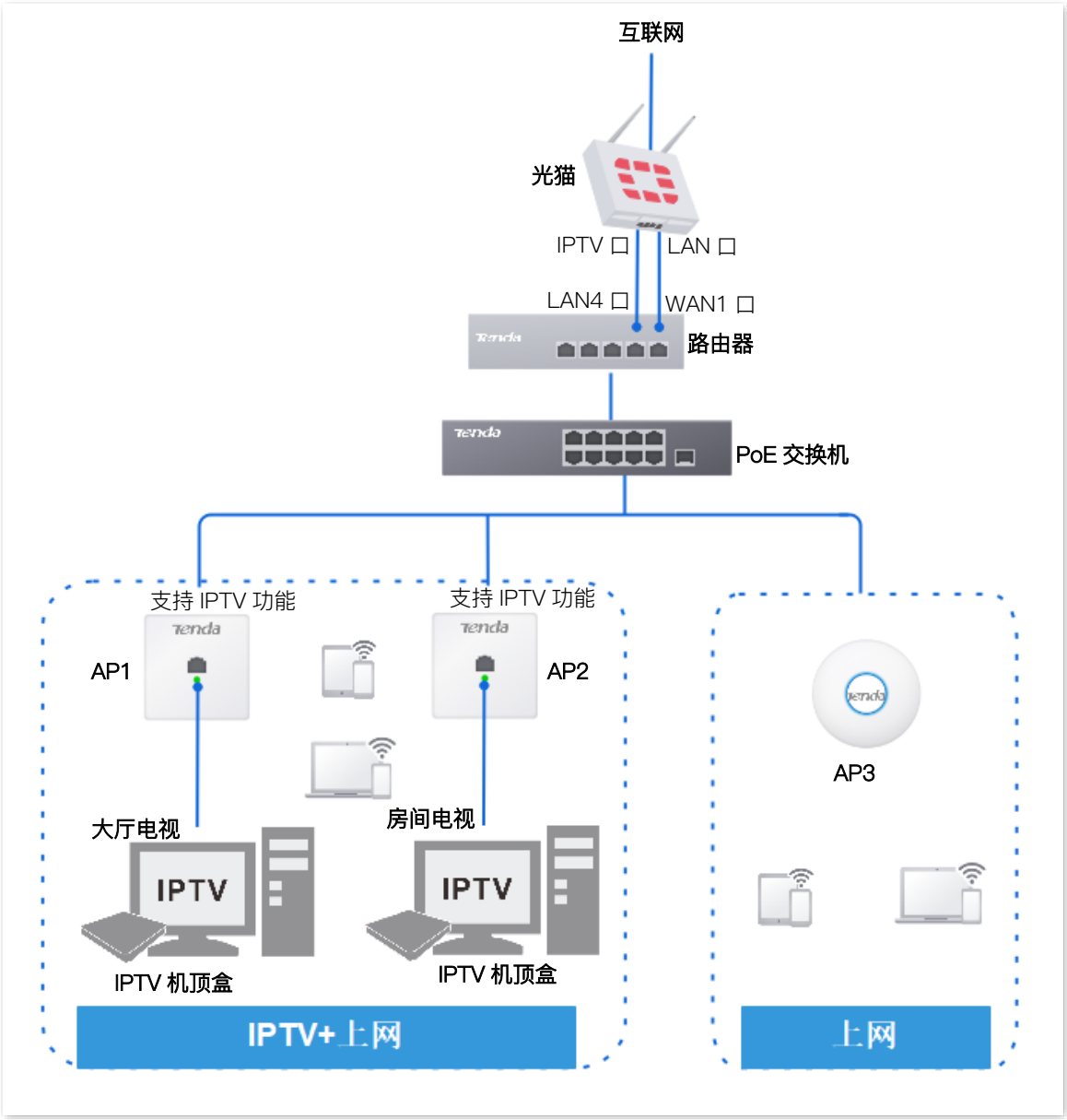
组网需求

某酒店的宽带业务中包含 IPTV 业务。宽带服务商提供了 IPTV 账号和密码，且提供了 IPTV 业务的 VLAN ID（此处以 VLAN ID 为 10 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 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

一、配置 IPTV 业务

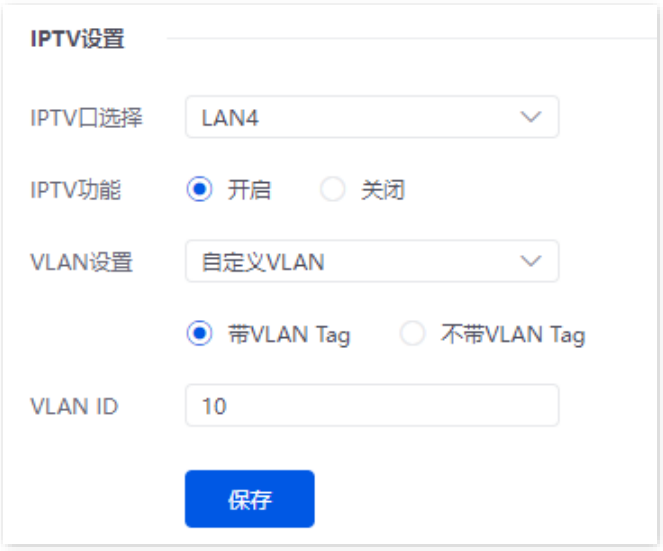
步骤 1 配置路由器。

1 登录到路由器 Web 管理页面。

2 点击「AP」>「IPTV」。

3 开启路由器 IPTV 功能与指定 IPTV IN 端口。

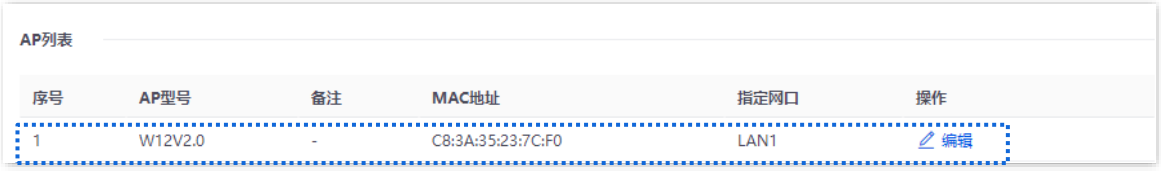
- 选择路由器作为 IPTV IN 口的 LAN 口，本例为“LAN4”。
- 选择“IPTV 功能”为“开启”。
- 选择“VLAN 设置”为“自定义 VLAN”，勾选“带 VLAN Tag”，“VLAN ID”为“10”。
- 点击 保存 。



4 指定 AP1（支持 IPTV 功能）的有线网口。

- 在 AP 列表，找到待连接 IPTV 机顶盒的 AP1，点击 。
- 勾选指定网口，点击 保存 。

成功指定 AP 的 IPTV 口。



5 重复**步骤 1** 的 4，指定其他 AP2（支持 IPTV 功能）的有线网口。

步骤 2 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

二、配置上网业务

具体请参考联网设置将路由器联网。

验证配置

完成配置后，您可以同时观看 IPTV 节目和上网。

6.10 无线优化

登录到路由器 Web 管理页面后，点击「AP」>「无线优化」。

您可以优化 AP 的无线性能，通过调整 AP 的功率、无线信道、无线频宽等，以获得更好的无线体验，从而打造优质的无线网络。

提示

- AP 分组内至少有 2 个支持无线优化功能的 AP，本功能才能正常使用。
- 优化过程中，无线网络将断开，请在网络相对空闲时优化。

6.10.1 立即自动优化无线网络

自动优化，即网络管理员主动发起自动优化无线网络任务。

参数说明

标题项	说明
应用场景	根据 AP 的使用场景选择应用场景。
优化策略	选择合适的优化策略。 - 漫游体验优先：以漫游体验优先，用于 AP 部署密度较高的场景，最大化的提升漫游体验，确保客户端连接到信号好的 AP，可能降低 Wi-Fi 的最大覆盖范围。 - 覆盖范围优先：以 Wi-Fi 覆盖范围为先，用于 AP 部署密度较低的场景，最大化的提升覆盖范围，尽可能地确保客户端成功接入 AP，漫游灵敏度可能会降低。

6.10.2 定时自动优化无线网络

网络管理员预先设置好定时优化的时间，之后系统将在预定的时间自动进行无线网络优化任务。

在“定时优化”模块，点击 定时优化安排 ，可进行定时优化无线网络配置。配置完成后，如果到时间点后，将自动进行无线优化。系统已默认为 APGroup_Default 创建了一条优化策略，默认禁用。

6.10.3 手动优化无线网络

网络管理员手动输入信道、频宽、发射功率等参数来优化无线网络。

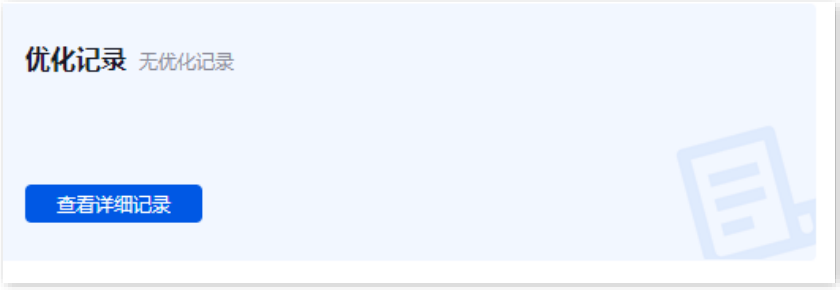
找到要手动优化无线网络的 AP，点击该 AP 表项后的编辑，根据实际请情况修改信道、频宽、发射功率等参数，点击保存。下图仅供参考。

参数说明

标题项	说明
2.4G 接入阈值	“5G 优先”功能开启时，如果 AP 接收到的终端 5GHz 信号强度低于该值，则让双频用户连接到 AP 的 2.4GHz 网络。
2.4G 漫游阈值	终端在移动到两个或多个 AP 覆盖范围的临界区域时，如果接收到的 2.4GHz 信号强度低于该值，终端会自动连接到信号更好的 AP，并断开原有 AP 的连接。
5G 接入阈值	“5G 优先”功能开启时，如果 AP 接收到的终端 5GHz 信号强度不低于该值，则让双频用户优先连接到 AP 的 5GHz 网络。
5G 漫游阈值	终端在移动到两个或多个 AP 覆盖范围的临界区域时，如果接收到的 5GHz 信号强度低于该值，终端会自动连接到信号更好的 AP，并断开原有 AP 的连接。

6.10.4 查看无线优化记录

在“优化记录”模块，您可以查看 AP 的优化的信息，最多显示 3 条，可点击 查看详细记录 查看更多信息。



6.11 漫游优化

登录到路由器 Web 管理页面后，点击「AP」>「漫游优化」。

您可以优化 AP 的漫游性能，通过调整 AP 与终端间的漫游阈值，以获得更好的漫游体验，打造优质的无线网络。

参数说明

标题项	说明
2.4GHz 漫游切换阈值 5GHz 漫游切换阈值	终端在 2.4GHz 或 5GHz 频段内接收到当前 AP 的信号强度低于阈值时，自动切换至相邻信号更好的 AP。
频段间漫游安全阈值	终端连接到 AP 的 2.4GHz（或 5GHz）频段时，如果接收到 AP 的 2.4GHz（或 5GHz）信号小于此阈值，终端将自动连接至另一频段。
AP 间漫游安全阈值	终端连接到当前 AP 后，如果终端移动位置，导致接收的信号强度低于此阈值，终端将自动切换至信号更好的 AP。
快速漫游	无线漫游指终端设备在移动到两个或多个 AP 覆盖范围的临界区域时，自动连接到信号更好的 AP，并断开原有 AP 的连接。前提是这些 AP 的 Wi-Fi 名称、安全模式和 Wi-Fi 密码相同。 - 802.11k：无线局域网频谱资源测量协议。开启后协助终端扫描环境中潜在的可漫游目标 AP，解决是否应该漫游、什么时候需要漫游的问题。 - 802.11v：无线网络管理协议。开启后协助终端进行漫游目标 AP 的选择，解决漫游到哪个 AP 的问题。 - 802.11r：快速 BSS 转换协议。开启后可以消除无线重关联过程中的握手开销，减少漫游时间，解决怎样快速漫游的问题。

6.12 创建 WiFi 二维码

您可以手动创建 AP WiFi 的二维码并下载。其他人通过微信扫描该二维码，可连接到对应的 Wi-Fi。

设置步骤：

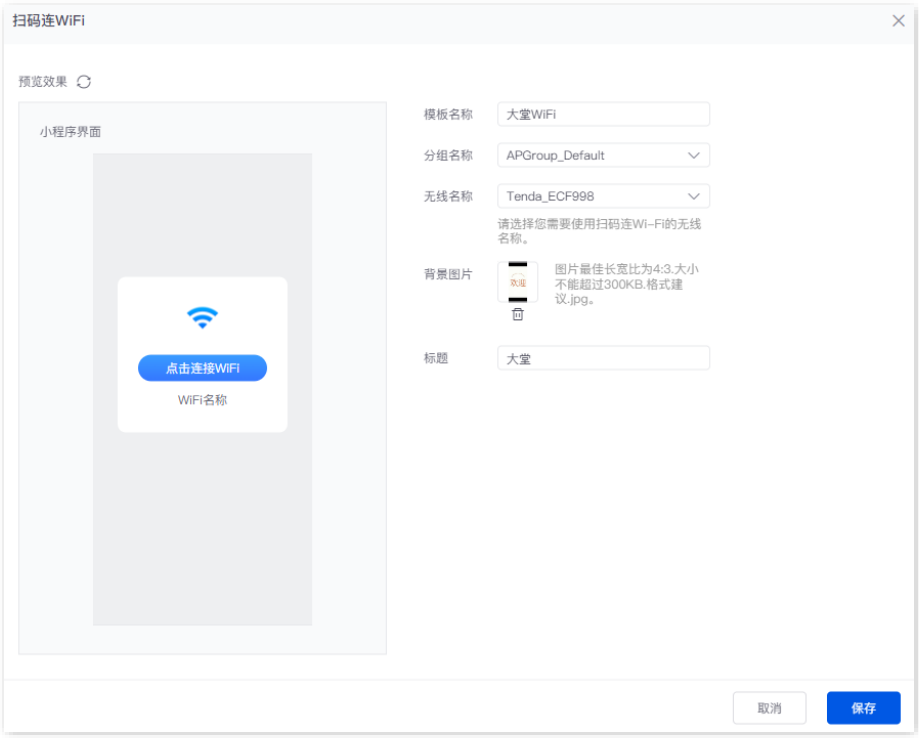
步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「AP」>「扫码连 WiFi」。

步骤 3 点击 。

步骤 4 根据实际情况设置 Wi-Fi 生成二维码的参数并保存。

- 设置模板名称，如“大堂 WiFi”。
- 选择 AP 所在的分组，如“APGroup_Default”。
- 选择 Wi-Fi，如“Tenda_ECF998”。
- 选择一张图片作为扫描二维码后显示的背景图。
- 设置标题，如“大堂”。



----完成

生成的页面如下图所示。您可以下载二维码并打印粘贴到任意位置。在 WiFi 覆盖范围内，其他人直接通过微信扫描该二维码即可连接到 WiFi。

7 认证管理

本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

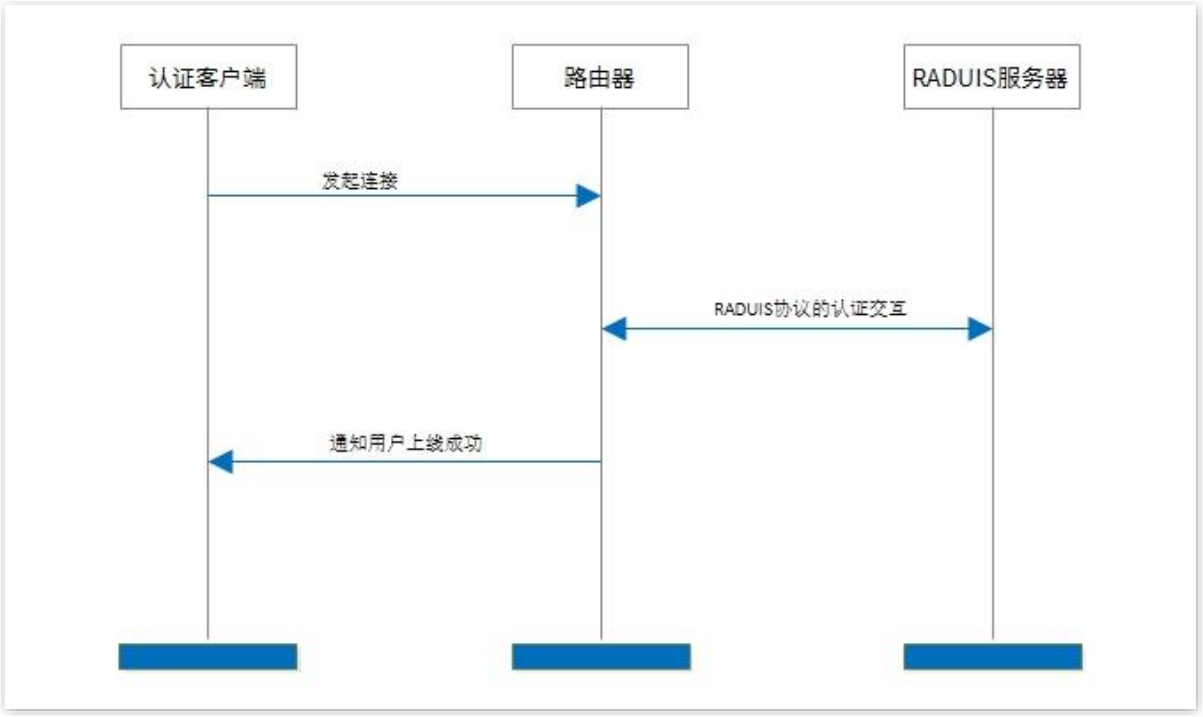
7.1 概述

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。开启认证后，连接到路由器认证网络的终端设备，需要认证成功后才能访问互联网。终端设备认证成功后，如果终端设备断开连接后又重新连接到路由器，可能需要重新认证。认证策略基于 VLAN 接口生效。

路由器支持本地服务器认证和外置服务器认证。

- 本地服务器认证：路由器启用本地服务器认证后，用户认证工作在路由器上完成；即认证用户保存在路由器上，认证页面也由路由器生成。
- 外置服务器认证：路由器启用外置服务器认证后，外置 RADIUS 服务器完成用户认证和计费。

外置服务器认证的工作原理如下图。



步骤 1 认证客户端使用 HTTP 协议发起连接请求。

步骤 2 路由器将请求重定向到本地认证页面，用户在认证页面输入用户名和密码。

步骤 3 路由器根据获取的用户名和密码，与 RADIUS 服务器进行 RADIUS 协议的认证交互，对用户进行认证、计费。

步骤 4 路由器通知认证客户端上线成功。

7.2 配置向导

7.2.1 本地服务器认证

步骤	任务	任务说明
1	配置认证页面	**必选。** 手动创建一个认证页面模板。
2	配置认证方式	**必选。** 根据实际场景需要，配置一条或多条认证方式策略。
3	配置时间策略	**必选。** 根据实际场景需要，在时间组页面配置相应的时间策略。
4	配置认证策略	**必选。**
5	配置计费策略	**可选。** 在配置认证账号时，可根据需要选择计费策略来进行流量收费。
6	配置认证账号	**可选。** 如果认证方式是账号密码认证或随机码认证，则需要配置认证账号。
7	配置免认证主机	**可选。** 如果要让设备无需认证即可连入互联网，则需要配置免认证主机。

提示

若需配置 PPPoE 认证方式，请配置 PPPoE 服务器并勾选客户端强制认证（必选）、配置计费策略（可选）、配置认证账号（必选）、配置免认证主机（可选）、关闭 PPPoE 服务器应用接口下的 DHCP 服务器（必选）。

7.2.2 外置服务器认证

步骤	任务	任务说明
1	配置 VPN 客户端	**必选。** 配置路由器为 VPN 客户端，拨号接入 RADIUS 服务器。
2	配置认证页面	**必选。** 手动创建图片或文本模板。
3	配置账号密码认证	**必选。** 根据实际场景需要，配置账号密码认证方式策略。
4	配置时间策略	**必选。** 根据实际场景需要，在时间组页面配置相应的时间策略。
5	配置外置服务器参数	**必选。** 根据实际场景需要，配置外置服务器的认证策略和计费策略。
6	配置认证策略	**必选。**
7	配置免认证主机	**可选。** 如果要让设备无需认证即可连入互联网，则需要配置免认证主机。

7.3 配置认证页面

7.3.1 图片模板

图片模板可应用于短信认证、邮箱认证、账号密码认证、一键认证、随机码认证。系统已经预置了一个图片模板认证页面，您可以根据需要编辑或者创建新的图片模板认证页面。

登录到路由器 Web 管理页面后，点击「认证」>「认证模板」>「认证页面」，然后点击 手动创建 可新增图片模板认证页面。

参数说明

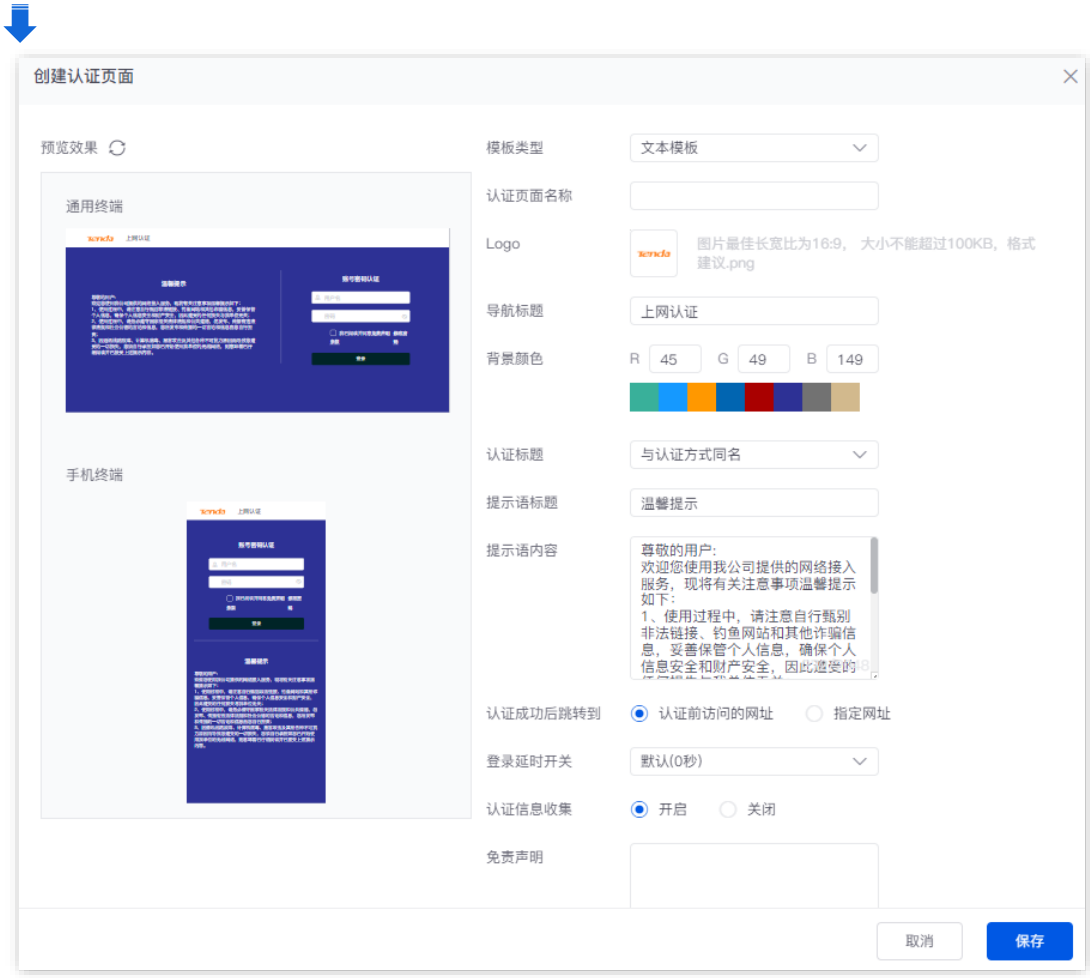
标题项	说明
背景图片	认证页面的背景图片。 提示 当上传了两或三张背景图片后，认证页面将会轮流播放这些图片。
图片 1 链接	背景图片链接的网址。配置后在认证页面点击背景图片即可访问该网址。 注意 链接需要为 http 网址，否则功能不生效。
认证成功后跳转到	用户通过认证后自动跳转到的网址。 - 认证前访问的网址：通过认证后，浏览器跳转到认证前访问的网址。例如用户访问百度时，跳转到认证页面，认证成功后就会跳转到百度页面。 - 指定网址：通过认证后，浏览器跳转到此处设置的网址。
登录延时开关	用户输入认证信息，点击“登录”后，页面停留的时间。
认证信息收集	开启后，请写入免责声明。

标题项	说明
免责声明	认证页面的免责声明信息，用户在登录时需勾选同意免责声明才能登录。

7.3.2 文本模板

文本模板可应用于短信认证、邮箱认证、账号密码认证、一键认证、随机码认证，您可以根据需要创建文本模板认证页面。

登录到路由器 Web 管理页面后，点击「认证」>「认证模板」>「认证页面」，然后点击 手动创建 ，模板类型选择文本模板即可新增文本模板认证页面。



参数说明

标题项	说明
认证页面名称	认证页面模板名称。
背景颜色	认证页面的背景色，可修改。
认证标题	认证页面的认证标题。 - 与认证方式同名：与认证方式名称保持一致。例如，配置账号密码认证时，使用该认证页面模板，认证标题为“账号密码认证”。 - 自定义名称：自定义认证页面的认证标题。
提示语标题	认证页面的提示语标题。
提示语内容	认证页面的提示语内容。
认证成功后跳转到	用户通过认证后自动跳转到的网址。 - 认证前访问的网址：通过认证后，浏览器跳转到认证前访问的网址。例如用户访问百度时，跳转到认证页面，认证成功后就会跳转到百度页面。 - 指定网址：通过认证后，浏览器跳转到此处设置的网址。
登录延时开关	用户输入认证信息，点击“登录”后，页面停留的时间。
认证信息收集	开启后，请写入免责声明。
免责声明	认证页面的免责声明信息，用户在登录时需勾选同意免责声明才能登录。

7.3.3 公众号模板

公众号模板可应用于公众号认证。系统已经预置了一个公众号模板认证页面，您可以根据需要编辑或者创建新的公众号模板认证页面。

登录到路由器 Web 管理页面后，点击「认证」>「认证模板」>「认证页面」，然后点击 手动创建 ，模板类型选择公众号模板，即可新增公众号模板认证页面。

参数说明

标题项	说明
认证页面名称	认证页面模板名称。
Logo	点击后可替换图片。
说明	认证页面显示的文字，用来提示用户或者宣传。可自定义。
上传二维码	上传用来上网认证的公众号的二维码。

7.4 配置认证方式

7.4.1 短信认证

开启短信认证后，用户需要在认证页面输入有效的手机号获取验证码进行认证，认证成功后才能访问互联网。

短信供应商，即，给指定手机号下发授权验证码的供应商，目前支持对接的短信供应商包括：阿里云、腾讯云、吉信通、NEXMO。你也可以选择“自定义 HTTP 对接”使用其他短信供应商。

注意

您需先在对应的短信供应商办理短信包套餐，然后再将申请到的对接信息配置到路由器。

登录到路由器 Web 管理页面，点击「认证」>「认证模板」>「认证方式」，点击 新增 即可新增短信认证策略。下图仅供参考。

参数说明

标题项	说明
微信放行时间	用户未认证时，可使用微信的时间，0 表示不放行。
闲置超时时间	用户认证成功后，在闲置超时时间内没有任何操作，需要重新认证。
认证有效期	用户认证成功后，上网时间超过该有效期后，需要重新认证。
有效性测试	检测路由器与短信供应商对接是否成功。此处输入手机号，然后点击 测试 按钮，如果对接成功，该手机号将会收到带验证码的短信。

7.4.2 邮箱认证

开启邮箱认证后，用户上网时，需要在认证页面中输入邮箱获取验证码进行认证，认证成功后才能访问互联网。

登录到路由器 Web 管理页面，点击「认证」>「认证模板」>「认证方式」，点击 新增 即可新增邮箱认证策略。

参数说明

标题项	说明
微信放行时间	用户未认证时，可使用微信的时间，0 表示不放行。
闲置超时时间	用户认证成功后，在闲置超时时间内没有任何操作，需要重新认证。
认证有效期	用户认证成功后，上网时间超过该有效期后，需要重新认证。
共享用户数	允许同时使用同一个邮箱认证上网的用户数。
邮箱账号	发送验证码邮件的电子邮箱账号。
邮箱密码	发送验证码邮件的电子邮箱账号对应的密码。
SMTP 服务器地址	SMTP 服务器的地址/端口。 Simple Mail Transfer Protocol，简单邮件传输协议，SMTP 服务器是邮件代发服务器，各邮件服务商的 SMTP 服务器地址和端口不同，需用户自行查询。
SMTP 服务器端口	

标题项	说明
有效性测试	检测路由器与邮件服务器对接是否成功。 此处输入邮箱地址后点击 测试 按钮，如果对接成功，该邮箱将会收到带验证码的邮件。
邮件内容	验证码邮件的内容。

7.4.3 账号密码认证

开启账号密码认证后，用户需要在认证页面输入用户名和密码进行认证，认证成功后才能访问互联网。用户名和密码需预先在「认证」>「账号管理」>「账号管理」页面配置好。

登录到路由器 Web 管理页面，点击「认证」>「认证模板」>「认证方式」，点击 新增 即可新增账号密码认证策略。

参数说明

标题项	说明
微信放行时间	用户未认证前时，可使用微信的时间，0 表示不放行。
闲置超时时间	用户认证成功后，在闲置超时时间内没有任何操作，需要重新认证。
认证有效期	用户认证成功后，上网时间超过该有效期后，需要重新认证。
首次登录强制修改密码	开启后，用户首次认证成功时，需要修改账号的密码后才能上网。

7.4.4 一键认证

开启一键认证后，用户上网时，只需要在弹出的认证页面点击“立即上网”，即可访问互联网。

登录到路由器 Web 管理页面，点击「认证」>「认证模板」>「认证方式」，点击 新增 即可新增一键认证策略。

参数说明请参考账号密码认证参数说明。

7.4.5 随机码认证

开启随机码认证后，用户上网时，需要在认证页面中输入随机码进行认证，认证成功后才能访问互联网。随机码需要预先在随机码账号中配置好。

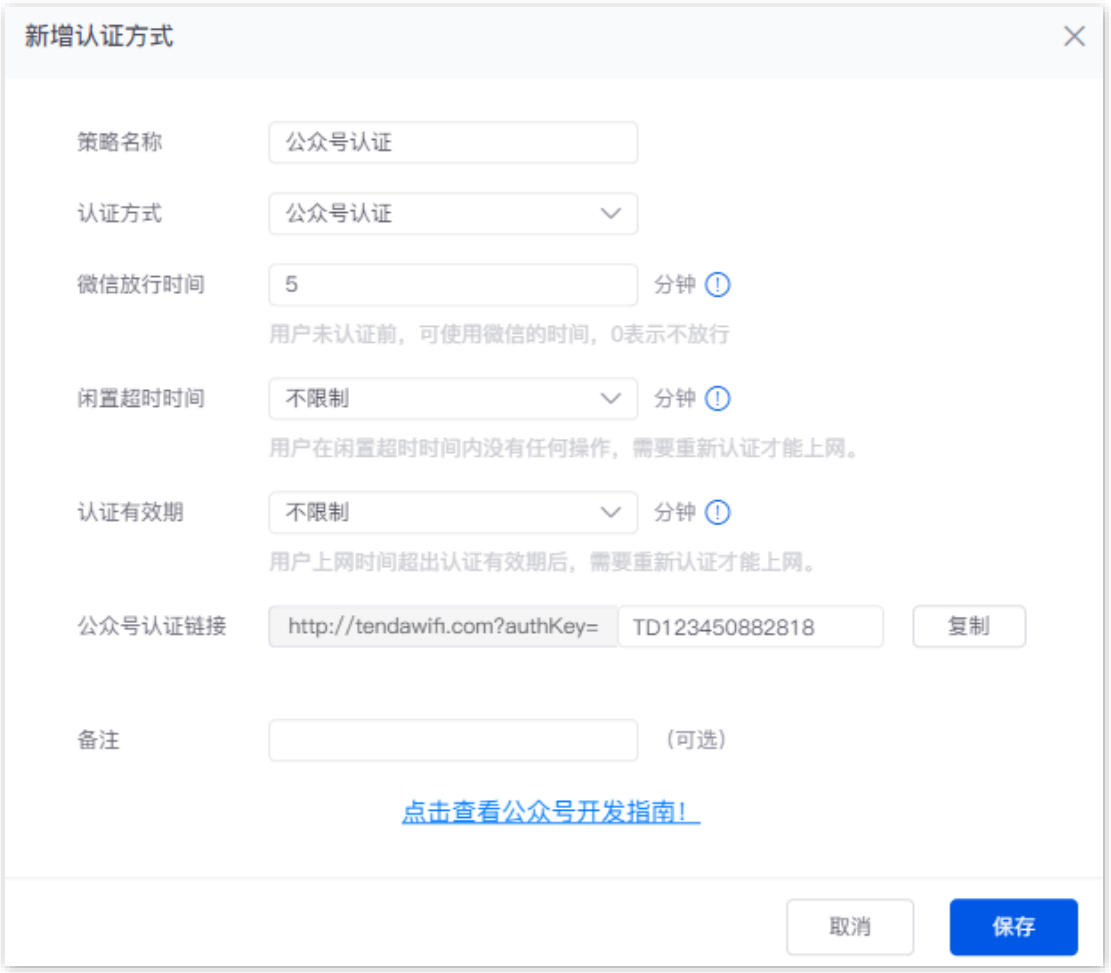
登录到路由器 Web 管理页面，点击「认证」>「认证模板」>「认证方式」，点击 新增 即可新增随机码认证策略。

参数说明请参考账号密码认证参数说明。

7.4.6 公众号认证

开启公众号认证后，用户通过手机连接局域网 Wi-Fi 上网时，需要微信扫描认证页面的二维码进行认证，认证成功后才能访问互联网。

登录到路由器 Web 管理页面，点击「认证」>「认证模板」>「认证方式」，点击 新增 即可新增公众号认证策略。



参数说明：

标题项	说明
微信放行时间	用户未认证时，可使用微信的时间，0 表示不放行。
闲置超时时间	用户认证成功后，在闲置超时时间内没有任何操作，需要重新认证。
认证有效期	用户认证成功后，上网时间超过该有效期后，需要重新认证。
公众号认证链接	用户在公众号认证后，跳转的显示页面。

配置公众号认证：

步骤 1 在您的公众号页面增加上网认证的按钮，如“我要上网”。

1 登录微信公众平台。

在 IE/Firefox/Chrome 等浏览器中输入：HTTPS://mp.weixin.qq.com/，输入您公众号注册的用户名和密码，点击“登录”可登录公众平台。

2 配置“我要上网”按钮。

在导航上，找到“自定义菜单”。根据您的实际情况增加一级菜单或子菜单。然后填写以下信息并保存发布。下图仅供参考。

提示

如果增加的是子菜单，请在公众号模板的“说明栏”写出按钮的具体路径，如“请扫码二维码通过公众号点击一级菜单名>我要上网即可开启免费上网”。

- 在“名称”栏填入上网认证按钮名称，如“我要上网”。
- “消息类型”选择“跳转网页”，并在“网页链接”栏填入“公众号认证”页面的“公众号认证链接”。

步骤 2 配置路由器。

1 登录到路由器 Web 管理页面。

2 配置公众号模板。

3 配置公众号认证方式。

4 配置时间策略。

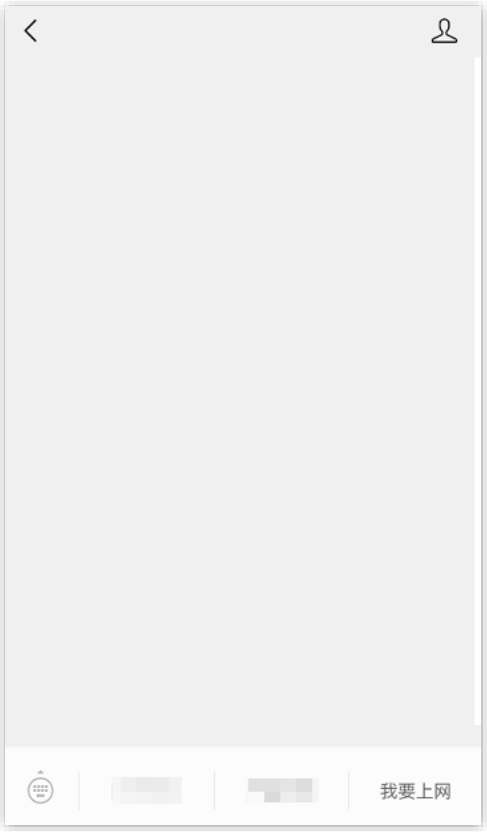
5 配置认证策略。

----完成

在时间策略配置的时间段内，手机、平板等连接路由器下接 AP 的 Wi-Fi 后，会自动打开浏览器并弹出上面小程序模板配置的二维码页面。然后用微信扫描该二维码，进入到公众号，点击“我要上网”即可上网了。下图仅供参考。

提示

连接 Wi-Fi 后，请尽快在认证方式页面设置的微信放行时间内扫码认证，否则因网络不通，微信扫码失败。

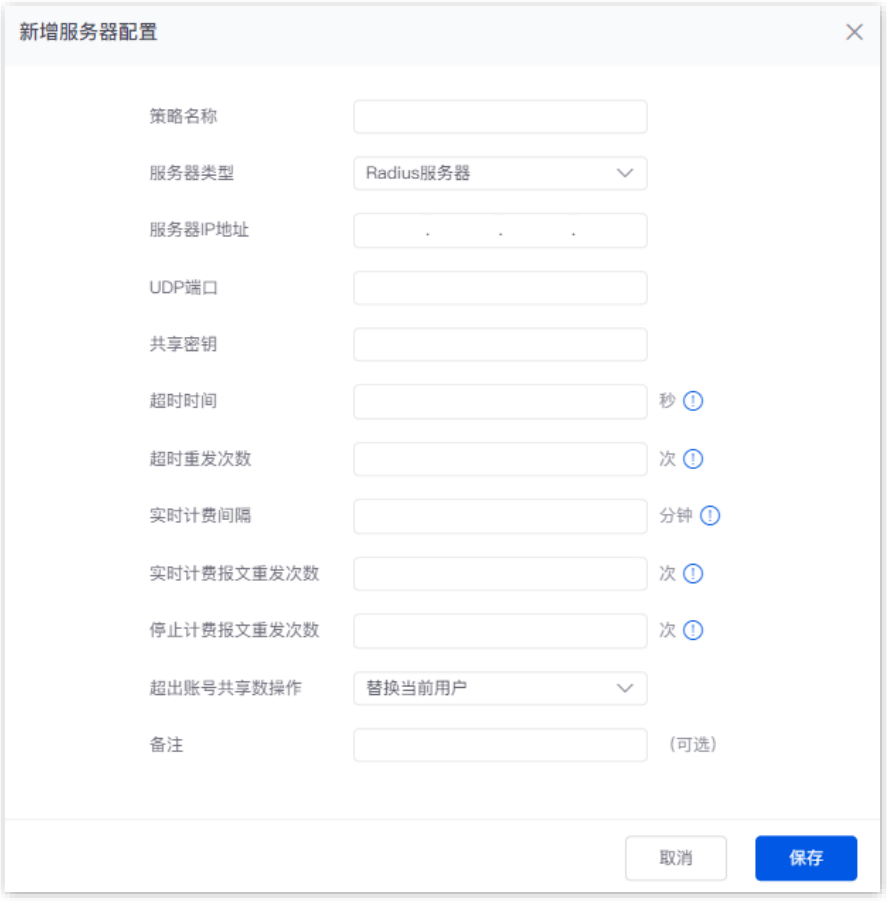


7.5 外置服务器配置

路由器启用外置 Radius 服务器认证时，计费策略、用户信息都存储在 Radius 服务器上。用户认证校验工作也在 Radius 服务器上完成。

登录到路由器 Web 管理页面后，点击「认证」>「服务器配置」。

点击 新增 即可新增 Radius 服务器。下图仅供参考。一个 Radius 服务器需配置一条 Radius 认证策略和一条 Radius 计费策略。



参数说明

标题项	说明
服务器类型	选择 Radius 服务器。
服务器 IP 地址	Radius 服务器的 IP 地址。
UDP 端口	Radius 认证服务器端口号。需要与 Radius 服务器的认证端口保持一致。一般认证端口号为 1812，计费端口为 1813。
共享密钥	Radius 认证服务器上配置的共享密钥。
超时时间	等待 Radius 认证服务器响应时间。如果超过该时间，路由器自动重发请求。
超时重发次数	Radius 认证服务器响应超时后，路由器重发请求的次数。
实时计费间隔	Radius 认证服务器每次计费的间隔。每隔设定的时间，路由器会向 RADIUS 服务器发送一次在线用户的计费信息。实时计费间隔的取值对 NAS 和 RADIUS 服务器的性能有一定的要求，取值越小，对二者的性能要求越高。
实时计费报文重发次数	路由器向 RADIUS 服务器发出实时计费请求没有得到响应时，路由器重发实时计费请求的次数。
停止计费报文重发次数	路由器向 RADIUS 服务器发出停止计费请求没有得到响应时，路由器重发停止计费请求的次数。

标题项	说明
超出账号共享数操作	当 Radius 服务器账号使用用户数量超过账号共享数时，Radius 服务器对用户的操作。 - 替换当前用户：按时间先后顺序，将最早通过该账号认证的用户踢下线，新认证的用户可以通过认证。 - 限制登录：新认证用户将无法通过认证，已认证用户不受影响。除非有已认证用户下线，新认证用户才可以通过认证。

7.6 配置认证策略

登录到路由器 Web 管理页面后，点击「认证」>「认证策略」。

您可以基于 VLAN 接口配置对应的认证策略。

参数说明

标题项	说明
应用接口	认证策略生效的接口，请提前配置 VLAN 接口。
认证页面	认证策略使用的认证页面。需预先在认证页面配置好。
认证方式	认证策略使用的认证方式。需预先在认证方式页面配置好。
认证账号方式	认证方式为账号密码认证时可配置。 - 内置账号：使用本地服务器认证，账号密码由账号管理页面配置。 - 外置 Radius：使用外置服务器认证。
主认证 Radius	“认证账号方式“选择“外置 Radius”时可配置。 主认证 Radius 服务器，用于用户认证。需预先在服务器配置页面配置好。
备认证 Radius	“认证账号方式“选择“外置 Radius”时可配置。 备认证 Radius 服务器，作为备用认证服务器。需预先在服务器配置页面配置好。
主计费 Radius	“认证账号方式“选择“外置 Radius”时可配置。 主计费 Radius 服务器，用于认证完成后的实时计费。需预先在服务器配置页面配置好。
备计费 Radius	“认证账号方式“选择“外置 Radius”时可配置。 备计费 Radius 服务器，作为备用计费服务器。需预先在服务器配置页面配置好。
时间策略	认证策略生效的时间段。需预先在时间组页面配置好。

7.7 PPPoE 服务器

登录到路由器 Web 管理页面后，点击「认证」>「PPPoE 服务器」。

您可以配置路由器为 PPPoE 服务器，并配置 PPPoE 认证。接入对应接口的客户端需要通过宽带拨号认证才能上网。宽带账号和密码需预先在「认证」>「账号管理」>「账号管理」页面中配置好。

点击 新增 即可新增 PPPoE 服务器。

参数说明

标题项	说明
PPPoE 服务器名称	PPPoE 服务器的名称，用户自定义即可。
应用接口	PPPoE 服务器认证应用的接口。
PPPoE 服务器 IP 地址	PPPoE 服务器的 IP 地址，也是客户端的网关地址，需与客户端地址池在同一网段。用户自定义即可。

标题项	说明
客户端起始 IP 地址	客户端 IP 地址池，即 PPPoE 服务器可分配给 PPPoE 客户端的 IP 地址范围。
客户端结束 IP 地址	
首选 DNS	PPPoE 服务器分配给客户端的首选/备用 DNS 服务器 IP 地址。 注意 为了使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。
备用 DNS	
LCP 探测间隔时间	路由器发送 LCP（Link Control Protocol，链路控制协议）探测报文的时间间隔。
LCP 探测失败次数	路由器未收到 LCP 探测报文，则表示探测失败。当一条连接的 LCP 探测失败次数超过设置的数值时，路由器将会断开该连接。
客户端强制认证	开启后，接入应用接口的客户端必须通过宽带拨号认证才能上网。
客户端隔离	开启后，拨号用户之间不能互相通信。

7.8 账号管理

7.8.1 用户列表

登录到路由器 Web 管理页面后，点击「认证」>「账号管理」>「用户列表」。

您可以查看和导出认证用户信息，批量断开在线用户的连接，也可以批量删除离线状态的认证用户信息。

按钮&参数说明

标题项	说明
断开	断开选中的在线用户的连接。已认证的在线用户需要重新认证才可以上网。免认证的在线用户将自动重新连接来上网。
删除	删除选中的离线用户信息。
认证类型	认证用户的认证方式。 配置为免认证主机的用户显示为“免认证”，未配置认证策略的用户显示为“自动认证”。

标题项	说明
认证账号	用户使用的认证账号、邮箱、手机号、真实姓名或随机码等。
认证接口	认证用户所在的路由器接口。

7.8.2 账号管理

概述

登录到路由器 Web 管理页面后，点击「认证」>「账号管理」>「账号管理」。

您可以添加用户进行账号密码认证或 PPPoE 认证上网时使用的账号。

您可以给账号配置计费策略和上传/下载速率来完成认证计费及流控功能，也可以对已有账号进行充值、查看充值记录等计费功能相关操作。

按钮&参数说明

标题项	说明
分组	给认证账号分组，使用对应账号进行认证的用户都将加入对应的用户组中。
账号 密码	认证账号的用户名和密码。
用户分组	认证账号所属的用户组。
计费策略	该用户认证上网的计费策略。需预先在计费策略页面配置好。“不使用”表示该账号不开启计费功能。
上传限速（最大上传限速） 下载限速（最大下载限速）	该账号的最大上传/下载速率。 提示 如果选择了计费策略，则自动填充计费策略中配置的最大上传/下载速率。如果不选择计费策略，则可以手动配置。
账户金额	账号余额。选择计费策略后，需要输入。

标题项	说明
计费开始时间	账号生效时间。 注意 如果不选择计费策略，则可以手动输入开始时间。
到期时间 （结束时间）	使用该账号上网的有效期。使用该账号认证并成功联网后，如果上网时间超出有效期，需要重新充值才能上网。 注意 选择计费策略，输入账户金额后，路由器自动计算而成。如果不选择计费策略，则手动设置结束时间。
连接数（最大连接数）	该账号最大允许的并发连接数，即路由器最大允许同时处理该账号发起的会话数。 当有多人同时使用该账号时，每人的并发连接数为所设定的值。
共享用户数	允许同时使用该账号认证上网的用户数量。 注意 如果开启了“绑定 MAC”功能，则会将最先使用该账号认证上网成功的几个 MAC 地址绑定，其他 MAC 则不能使用该账号认证上网。例如，共享用户数为 2，则路由器会将最先使用该账号认证成功的两个 MAC 地址与该账号绑定，其他 MAC 地址对应的设备无法共享该账号认证上网。
绑定 MAC	开启后，路由器会将最先使用该账号认证上网成功的几个 MAC 地址与该账号绑定。
固定 IP	配置后，只有本 IP 地址对应的设备才能使用该账号认证上网。默认为不固定。 注意 PPPoE 认证时，固定 IP 地址功能不会生效。

账号详情及充值记录

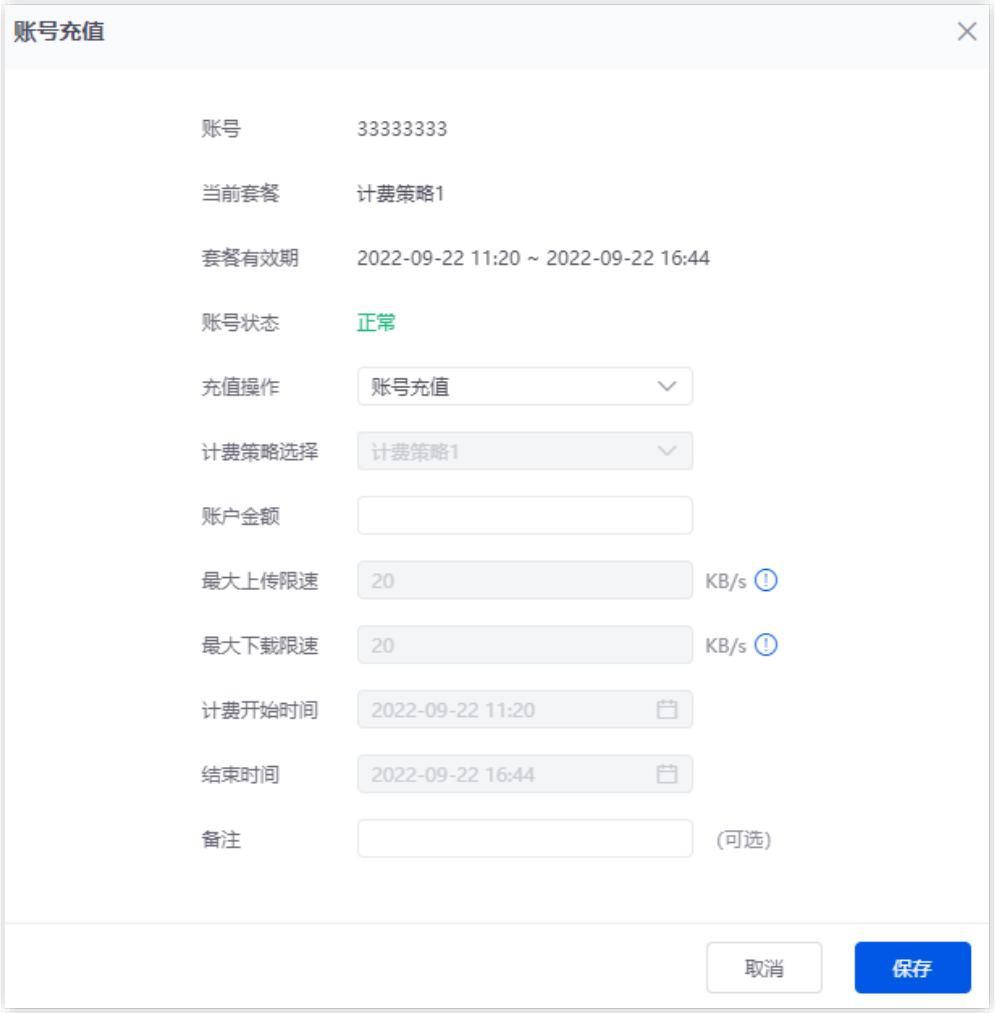
点击相应账号后的 详情 按钮，您可以在弹出的“账号详情”模块查看账号详细信息，在“操作记录”模块查看账号充值记录。下图仅供参考。

账号充值

点击相应账号后的 充值 按钮，您可以在弹出的窗口中充值金额或变更计费策略。下图仅供参考。

注意

如果账号没有引用计费策略，您可以手动更改到期时间来给账号充值。



参数说明

标题项	说明
充值操作	您可以选择“账号充值”来续费当前套餐，也可以选择“变更计费策略”来变更套餐。 注意 变更计费策略会将原账户金额和有效期都清零。
计费策略选择	账号引用的计费策略。当“充值操作”选择为“变更计费策略”时，您可以在此处选择变更后的计费策略。
账户金额	此次充值的金额。 提示 账号没有引用计费策略，即“计费策略选择”为“不使用”时，不允许输入充值金额。
最大上传速率 最大下载速率	账号当前的最大上传/下载速率。 提示 如果账号变更为不引用计费策略，即“充值操作”为“变更计费策略”且“计费策略选择”为“不选择”时，需手动输入。
计费开始时间	账号生效时间。
结束时间	使用该账号上网的有效期。使用该账号认证并成功联网后，如果上网时间超出有效期，需要重新充值才能上网。 提示 账号没有引用计费策略，即“计费策略选择”为“不使用”时，需手动输入。

7.8.3 计费策略

登录到路由器 Web 管理页面后，点击「认证」>「账号管理」>「计费策略」。

您可以根据实际计费需求配置相应的计费策略。

参数说明

标题项	说明
有效期	计费策略的计费周期。
套餐价格	一个计费周期的套餐金额。例如：有效期为 1 小时，套餐价格为 2 元，那么该计费策略是 2 元/小时。
最大上传速率	使用该计费策略的账号的最大上传/下载速率。
最大下载速率	

7.8.4 免认证策略

登录到路由器 Web 管理页面后，点击「认证」>「账号管理」>「免认证策略」。

您可以为一些特殊设备（例如：网络摄像机）配置免认证策略，这些设备不需要认证，即可连入互联网。

参数说明

标题项	说明
免认证策略	免认证策略类型。包括终端唯一信息、终端类型。
免认证条件	免认证策略的条件，只有符合该条件的终端设备才可以进行免认证上网。 当“免认证策略”选择“按终端唯一信息”时，支持下面三种免认证条件。 - 按手机号：开启短信认证时，配置手机号免认证，可无需获取验证码即可认证成功。 - 按 IP：根据设备 IP 地址来匹配免认证设备。 - 按 MAC：根据设备 MAC 地址来匹配免认证设备。 当“免认证策略”选择“终端类型”时，支持下面三种免认证条件。 - 有线终端免认证：有线连接路由器所在局域网的设备免认证。 - 无线终端免认证：无线连接路由器所在局域网的设备免认证。 - 手机终端免认证：被识别为手机终端类型的设备免认证。
免认证内容	只有符合该内容的的设备才可以进行免认证上网。需要进行二次判断，先判断是否符合免认证条件，再判断免认证内容，只有两者都判断通过时，才会免认证。“–”表示无认证内容。

7.8.5 随机码账号

登录到路由器 Web 管理页面后，点击「认证」>「账号管理」>「随机码账号」。

您可以添加用户进行随机码认证上网时使用的随机码。下图仅供参考。

参数说明

标题项	说明
随机码	认证时使用的随机码。
创建时间	随机码创建的时间。
创建条数	创建随机码的个数。
账号有效期	随机码的有效时长。
过期时间	随机码到期时间，到期后随机码失效。路由器根据“账号有效期”和“创建时间”自动计算而成。
备注	点击 ✎ 可以对随机码进行备注。
流量限额	随机码可以使用的总下载流量，超过流量后该随机码不能上网。
可用时长	允许该随机码单次在线的最长时间，到期后需再次认证。
共享用户数	允许同时使用该随机码认证上网的用户数量。 注意 随机码默认开启绑定 MAC 地址，例如共享用户数为 2，则路由器会将最先使用该随机码认证成功的两个 MAC 地址与该随机码绑定，其他 MAC 地址的设备无法使用该随机码认证上网。
已使用数	已使用该随机码认证上网的用户数。
随机码标题	随机码的标题。打印时显示于打印页面的正上方，您可以用于广告推广，例如：“XX 欢迎您！”

7.9 出租屋网络认证计费举例（本地服务器）

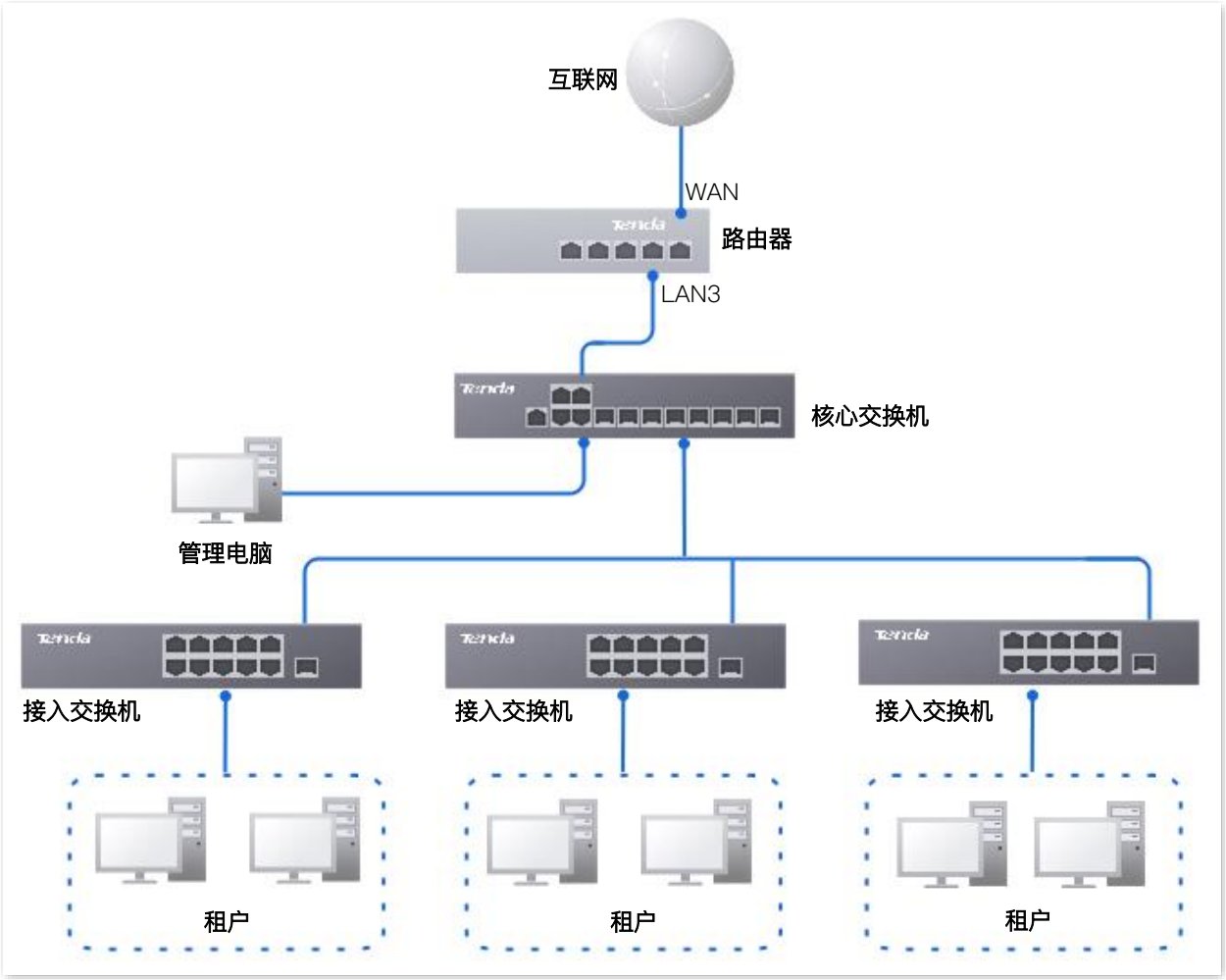
7.9.1 组网需求

某小区公寓网络使用路由器作为出口网关，各租户连接到公寓网络拨号上网时，需要按月付费。

公寓网络具体要求如下：

- 所有租户通过宽带拨号方式上网。
- 公寓提供 30 元/月的 20M 带宽和 100 元/月的 100M 带宽两种套餐供租户选择。
- 为方便管理，公寓管家的电脑无需认证即可连入互联网。

组网拓扑图如下所示：



7.9.2 方案设计

- 配置基于 VLAN 接口的 PPPoE 认证。
- 配置管家电脑的免认证策略。
- 配置认证账号。

7.9.3 配置步骤

配置路由器 配置核心交换机

一、配置路由器

步骤 1 登录到路由器 Web 管理页面。

步骤 2 添加 VLAN 并配置 DHCP 服务器。

VLAN 参数示例如下表所示。

VLAN 名称	VLAN ID	IP 地址/网段	物理端口
租户	20	192.168.20.1/24	LAN3（UNTAG）

VLAN 的 DHCP 服务器参数示例如下表所示。

策略名称	应用接口	用户 DHCP	AP DHCP
租户	租户	IP 地址池：192.168.20.100~192.168.20.200 子网掩码：255.255.255.0 默认网关：192.168.20.1 首选 DNS：192.168.20.1	/

1 进入「网络」>「VLAN 设置」页面，添加 VLAN。

- 点击 新增，配置 VLAN 相关参数，点击 保存。

- 为“租客”VLAN 选择端口，本例为 LAN3，设置 VLAN 策略为 UNTAG。

2 为 VLAN 配置 DHCP 服务器。

进入「网络」>「DHCP 设置」>「DHCP 服务器」页面，点击 新增 ，然后配置“租户”VLAN 的用户 DHCP 服务器相关参数，点击 保存 。

步骤 3 配置 PPPoE 服务器及认证。

PPPoE 认证参数示例如下表所示，其他未提及的参数保持默认设置。

PPPoE 服务器相关参数
PPPoE 服务器名称：PPPoE_1
应用接口：租户
PPPoE 服务器地址：192.168.30.1
客户端起止 IP 地址：192.168.30.100~192.168.30.200
首选 DNS：192.168.30.1
LCP 探测间隔时间：10 秒
LCP 探测失败次数：10 次
客户端强制认证：是

进入「认证」>「PPPoE 服务器」页面，点击 新增 ，然后配置 PPPoE 服务器及认证等相关参数，点击 保存 。

步骤 4 配置宽带套餐。

宽带套餐参数示例如下表所示。

20M 套餐	100M 套餐
策略名称：20M	策略名称：100M
有效期：30 天	有效期：30 天
套餐价格：30 元	套餐价格：100 元
最大上传速率：5120KB/s	最大上传速率：10240KB/s
最大下载速率：20480KB/s	最大下载速率：102400KB/s

进入「认证」>「账号管理」>「计费策略」页面，点击 新增 ，然后配置套餐计费策略相关参数，点击 保存 。

步骤 5 配置租户的认证账号。

账号认证相关参数示例如下表所示，其他未提及的参数保持默认设置。

用户组	认证账号
分组名称：租户 PPPoE 认证 用户组类型：认证用户组	账号：门牌号 密码：门牌号+电话号码 用户分组：租户 PPPoE 认证 计费策略：20M 或 100M 用户金额：根据实际设置 共享用户数：1

1 添加用户组。

进入「审计」>「分组策略」>「用户组」页面，点击 新增 ，然后创建一个 PPPoE 认证用户组，点击 保存 。

2 添加认证账号并加入用户组。

进入「认证」>「账号管理」>「账号管理」页面，点击 新增 ，然后配置认证账号相关参数，点击 保存 。下图仅供参考。

3 参照 2 配置其他租户的认证账号。

步骤 6 配置免认证策略。

假设免认证电脑的 MAC 地址为 44:37:E6:12:34:56。

进入「认证」>「账号管理」>「免认证策略」页面，点击 新增 ，然后配置免认证策略相关参数，点击 保存 。

二、配置核心交换机

在核心交换机上划分 IEEE 802.1Q VLAN，具体如下。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
路由器	20	Access	20
接入交换机	20	Access	20
管理电脑	20	Access	20

其他未提到的端口保持默认设置即可。具体配置方法请参考交换机的使用说明书。

---完成

7.9.4 配置验证

公寓管家的电脑（MAC 地址为 44:37:E6:12:34:56）无需认证，即可上网。

租客访问网络时，需要进行宽带拨号连接。

在路由器上拨号

适用于租户用路由器接入公寓网络宽带网口的场景，关于路由器的设置，请参考对应型号的说明书。

步骤 1 进入租户路由器的管理页面。

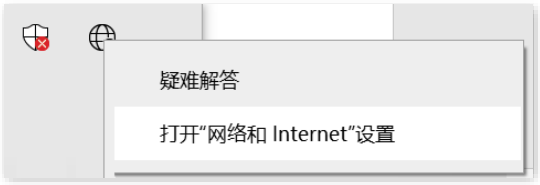
步骤 2 设置“联网方式”为“宽带拨号”，然后输入认证账号密码保存设置。

设置完成后，租户可以连接到路由器上网了。

在电脑上拨号（以 Window 10 为例说明）

适用于租户直接用电脑接入公寓网络宽带网口的场景。（以 Window 10 为例说明）

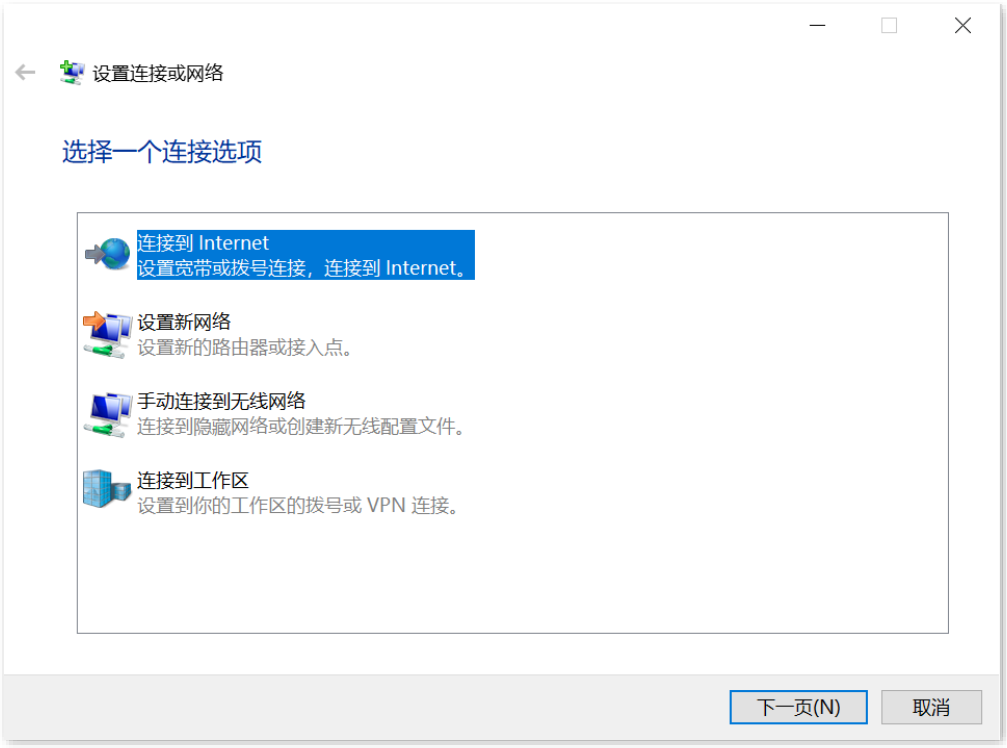
步骤 1 鼠标右击桌面右下角的网络图标，点击**打开“网络和 Internet”设置**。



步骤 2 点击左侧栏的**拨号**。

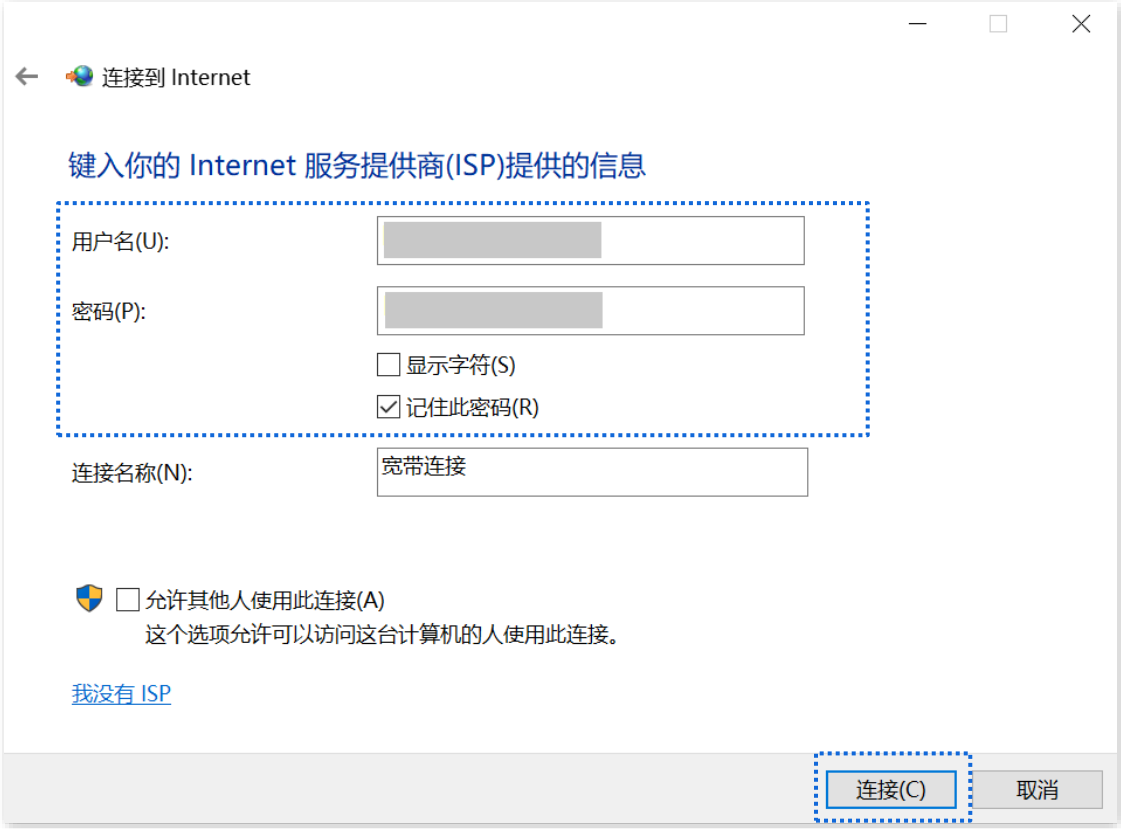
步骤 3 点击**设置新连接**。

步骤 4 选择**连接到 Internet**，然后点击 下一页 。



步骤 5 点击**宽带（PPPoE）（R）**。

步骤 6 填写 PPPoE 认证用户名和密码，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。

7.10 出租屋网络认证计费举例（外置服务器）

7.10.1 组网需求

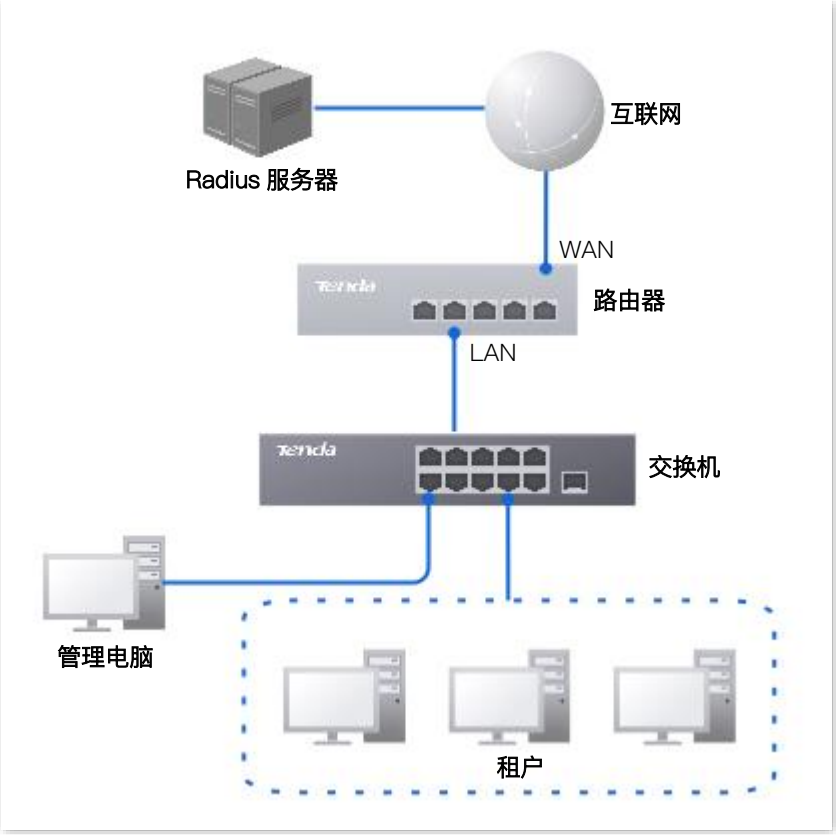
某小区公寓网络使用路由器作为出口网关，各租户连接到公寓网络通过账号密码认证上网时，需要按月付费。假设计费系统部署在 Radius 服务器上，Radius 服务器上配置参数如下：

- Radius 服务器是 PPTP 服务器，WAN 口 IP 地址：1.10.10.1，内网 IP 网段：10.150.0.0/24
- Radius 服务器登录用户名/密码：admin
- Radius 服务器共享密码：UmXmL9UK
- Radius 服务器上添加认证用户名和密码：internet-auth

公寓网络具体要求如下：

- 所有租户通过账号密码认证方式上网。
- 为方便管理，公寓的管理电脑无需认证即可连入互联网。

组网拓扑图如下所示：



7.10.2 方案设计

- 配置路由器为 PPTP 客户端来访问 Radius 服务器。
- 配置账号密码认证。
- 配置管理电脑的免认证策略。

7.10.3 配置步骤

配置 Radius 服务器 → 配置路由器

一、配置 Radius 服务器

步骤 1 在 Radius 服务器上配置一个 VPN 服务器并配置拨入 VPN 的用户名和密码。

VPN 参数示例如下表所示。

VPN 类型	服务端 IP（保持界面默认配置）	用户名和密码	IP
PPTP 服务器	10.150.0.1	admin	10.150.0.90

步骤 2 在 Radius 服务器上配置对应 VPN 的 NAS 设备信息，即对端 AC 设备。注意 IP 地址需要与上一步

新建的 VPN 的 IP 地址相同。

NAS 参数示例如下表所示。

名称	IP	共享密钥
PPTP	10.150.0.90	UmXmL9UK

步骤 3 在 Radius 服务器上配置认证用户名和密码，如“internet-auth”。

具体配置方法请参考对应 Radius 服务器的说明书。

二、配置路由器

步骤 1 登录到路由器 Web 管理页面。

步骤 2 路由器为 PPTP 客户端连接到 Radius 服务器。

PPTP 客户端参数示例如下表所示，其他未提及的参数保持默认设置。

对端 PPTP 服务器相关参数
服务器 WAN 口 IP 地址：1.10.10.1
服务器内网 IP 网段：10.150.0/24
登录用户名/密码：admin

进入「更多」>「VPN 客户端」页面，开启 VPN 客户端功能。然后配置 PPTP 客户端的相关参数，点击 保存 。

当页面的状态显示已连接时，路由器成功建立 VPN 连接，可以访问 Radius 服务器。

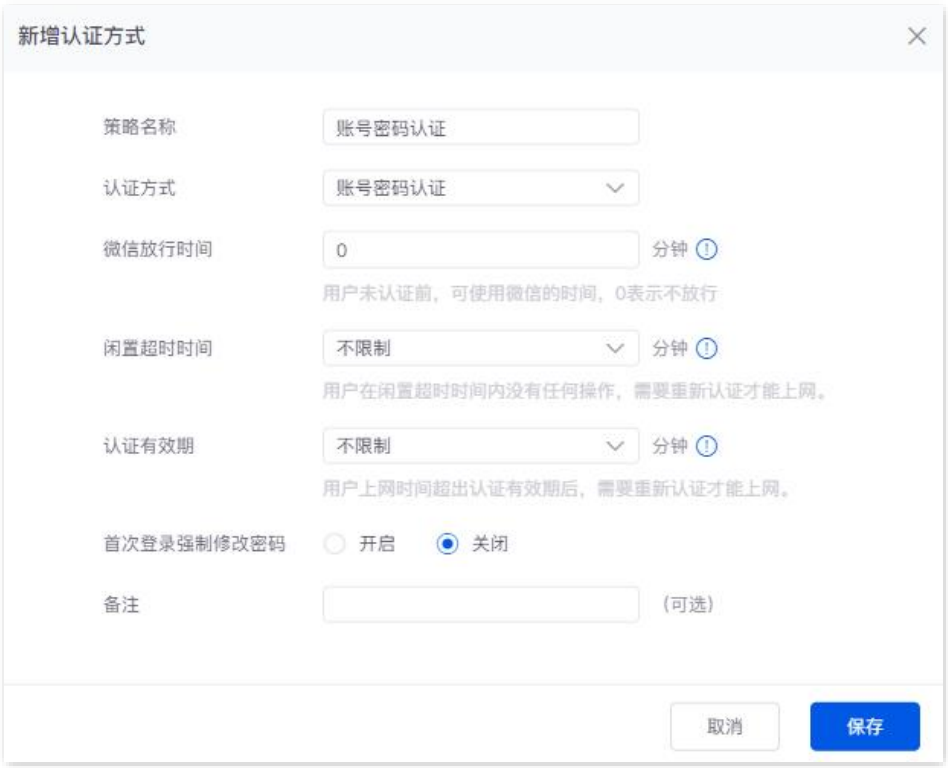
步骤 3 配置外置 Radius 服务器认证。

1 配置图片认证模板。

进入「认证」>「认证模板」>「认证页面」页面，点击＋，创建一个图片模板。下图仅供参考。

2 配置账号密码认证方式。

进入「认证」>「认证模板」>「认证方式」页面，点击 新增，新增账号密码认证。下图仅供参考。



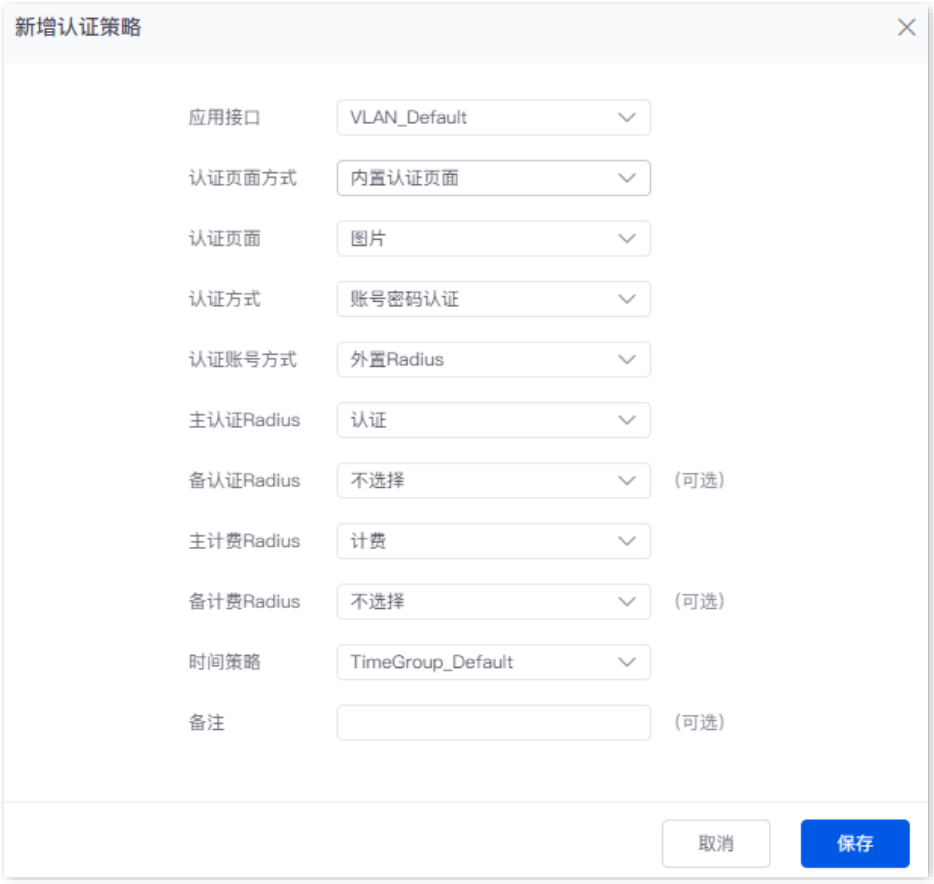
3 配置外置 Radius 服务器。

进入「认证」>「服务器配置」页面，点击 新增 ，新增一条认证策略（端口号 1812）和一条计费策略（端口号 1813）。下图仅供参考。

4 配置认证策略。

进入「认证」>「认证策略」页面，点击 新增 ，新增租户的认证策略。

注意：“认证账号方式”选择“外置 Radius”，“主认证 Radius”和“主计费 Radius”分别选择**服务器配置**页面配置的认证和计费策略。



步骤 4 配置免认证策略。

假设免认证电脑的 MAC 地址为 44:37:E6:12:34:56。

进入「认证」>「账号管理」>「免认证策略」页面，点击 新增 ，然后配置免认证策略相关参数，点击 保存 。

---完成

7.10.4 配置验证

公寓管家的电脑（MAC 地址为 44:37:E6:12:34:56）无需认证，即可上网。

租客访问网络时，需要进行账号密码认证。

通过路由器上网

适用于租户用路由器接入公寓网络宽带网口的场景，关于路由器的设置，请参考对应型号的说明书。

步骤 1 进入租户路由器的管理页面。

步骤 2 设置“联网方式”为“动态 IP”，并保存设置。

手机、平板可以连接路由器 Wi-Fi，然后访问任意网页，在弹出的认证页面输入账号密码（internet-auth）点击登录。认证后即可上网。

电脑可以连接路由器 Wi-Fi 或通过网线连接路由器 LAN 口，然后访问任意网页，在弹出的认证页面输入认证的账号和密码（internet-auth）点击登录。认证后即可上网。

通过电脑上网

适用于租户直接用电脑接入公寓网络宽带网口的场景。电脑接入公寓网络宽带网口后，访问任意网页，在弹出的认证页面输入认证的账号和密码（internet-auth）点击登录。认证后即可上网。

8 网速控制

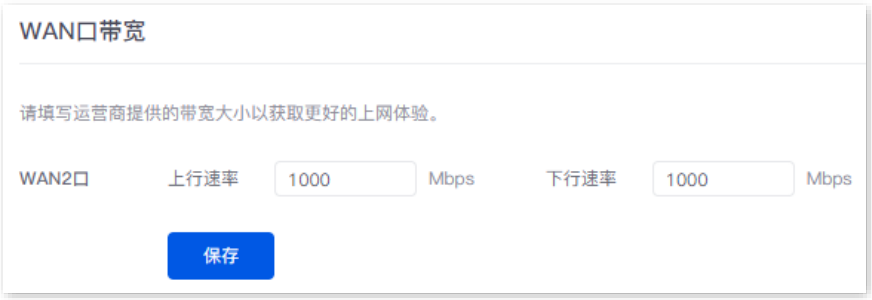
本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

8.1 WAN 口带宽

登录到路由器 Web 管理页面后，点击「网速」>「WAN 口带宽」。

您可以设置 WAN 口带宽参数，当网络设置为多 WAN 时可以分别对多个 WAN 口设置带宽参数。

正确地配置 WAN 口带宽参数，可以让分组限速策略能够更加准确地给局域网用户分配带宽。



参数说明

标题项	说明
上行速率	填入所办理的宽带的带宽值。不清楚时，可以咨询您的宽带服务商。
下行速率	

8.2 分组限速

外网带宽总是有限的，所以网络管理员需要对用户进行网速控制，使有限的带宽资源得到合理分配，有效利用外网资源。

8.2.1 分组限速配置举例

组网需求

某企业使用路由器进行网络搭建。

要求：局域网中采购部（IP 地址为 192.168.0.2~192.168.0.50）的每个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。对于局域网其他设备，不限制使用带宽。

方案设计

可以采用路由器的网速控制功能中的“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

配置时间组 → 配置 IP 组 → 添加分组限速策略

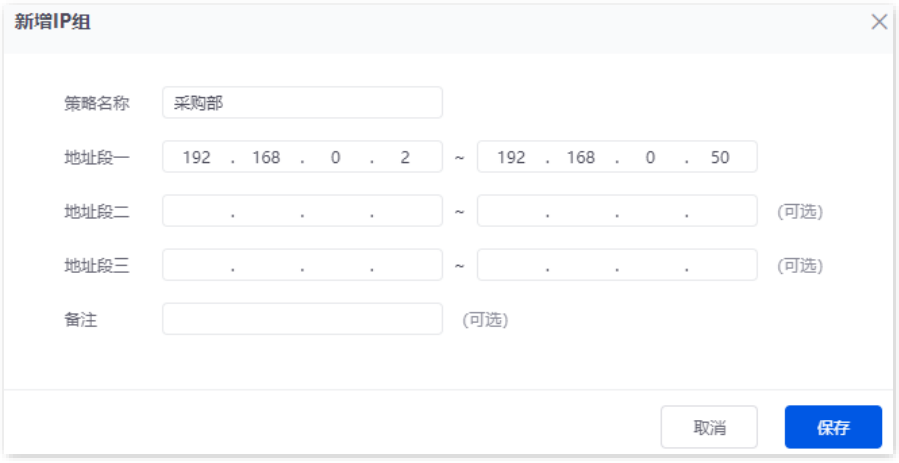
步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置时间组。

进入「审计」>「分组策略」>「时间组」页面，配置如下时间组。

步骤 3 配置 IP 组。

点击「审计」>「分组策略」>「IP 组」，配置如下 IP 组。



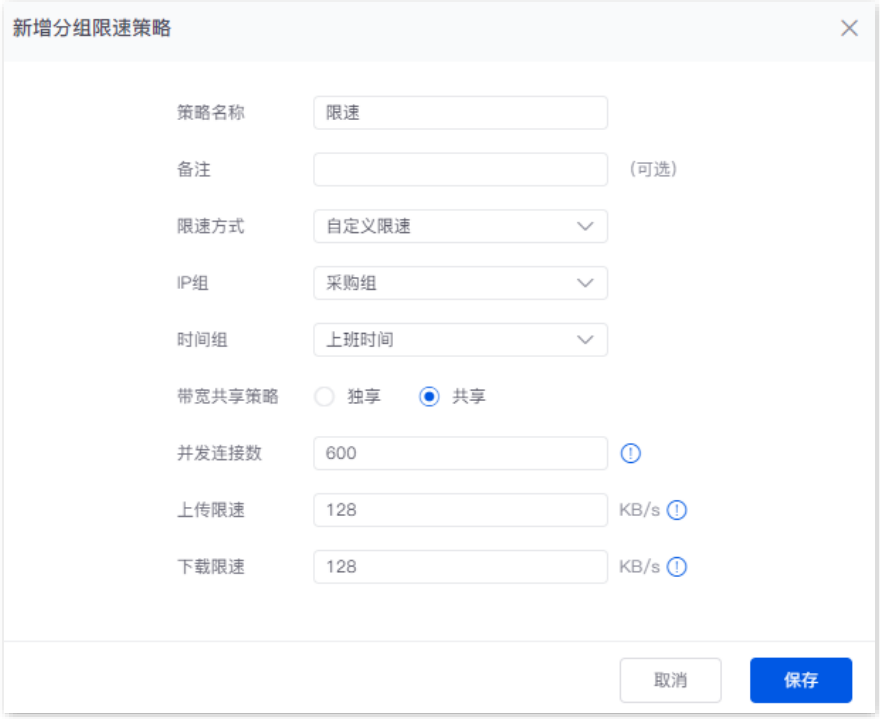
步骤 4 添加分组限速策略。

分组限速策略参数示例如下所示。

策略名称：限速	并发连接数：600
IP 组：采购部	终端设备的最大上传/载速率：128KB/s
时间组：上班时间	

1 点击「网速」>「分组限速」，然后点击 新增 。

2 配置分组限速策略相关参数，点击 保存 。



---完成

验证配置

IP 地址在 192.168.0.2~192.168.0.50 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。

8.2.2 参数说明

标题项	说明
IP 组	分组限速策略生效的 IP 地址范围。需先在 IP 组页面配置好 IP 组策略。
时间组	分组限速策略生效的时间。需先在时间组页面配置好时间组策略。
共享带宽策略	IP 组内用户享受设置的带宽的方式。 - 共享：IP 组内所有用户共享设置的带宽。 - 独享：每个用户单独享受设置的带宽。
并发连接数	受控用户所能使用的最大连接数。0 表示不限制。
上传限速	受控用户的最大上传/下载速率。0 表示不限速。
下载限速	

8.3 单用户限速

登录到路由器 Web 管理页面后，点击「网速」>「单用户限速」。

您可以根据实际需要，将连接到路由器的用户限制最大上传/下载速率、拉黑、分配固定 IP。拉黑的用户在设置的拉黑时长内无法通过路由器上网；拉黑时长到期后或解除拉黑，设备可继续通过路由器上网。图示仅供参考。

参数说明

标题项	说明
限速	限制对应用户的最大上传/下载速率。
拉黑	将对应用户拉黑并设置拉黑时长，或解除拉黑。
加入静态分配	将对应用户获得的 IP 始终分配给该用户。
限速	限制已勾选用户的最大上传/下载速率。
拉黑	将已勾选用户拉黑并设置拉黑时长，或解除拉黑。
加入静态分配	将已勾选用户获得的 IP 始终分配给对应用户。

9 行为与审计

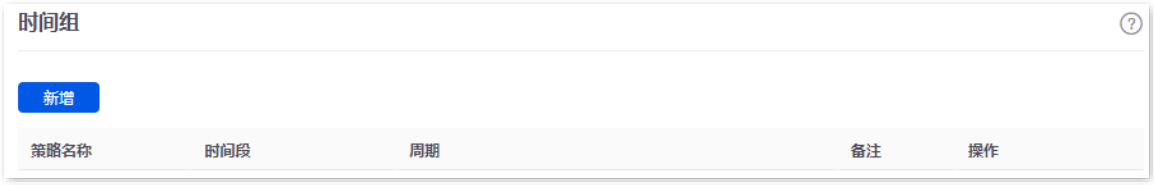
本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

9.1 分组策略

9.1.1 配置时间组

步骤 1 登录到路由器 Web 管理页面，点击「审计」>「分组策略」>「时间组」。

步骤 2 点击 新增 。



步骤 3 配置时间组相关参数，点击 保存 。

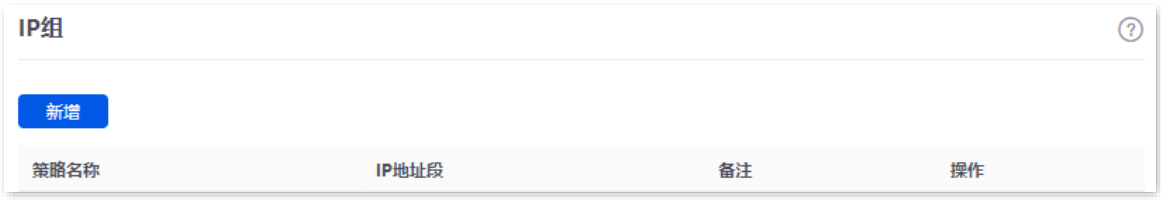
- 时间段：当前时间组策略包含的时间段。最多包含三个时间段，时间段之间不能重复。
- 周期：时间组生效的日期。

---完成

9.1.2 配置 IP 组

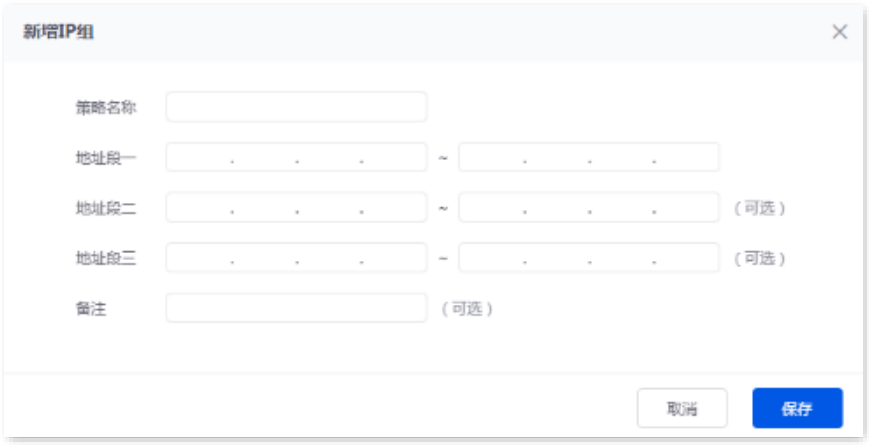
步骤 1 登录到路由器 Web 管理页面，点击「审计」>「分组策略」>「IP 组」。

步骤 2 点击 新增 。



步骤 3 配置 IP 组相关参数，点击 保存 。

地址段：当前 IP 组策略包含的 IP 地址段。最多包含三个 IP 地址段，地址段之间不能重复。



---完成

9.1.3 配置用户组

提示

路由器默认已添加 2 条用户组：User_Default 和 VPNUser_Default。默认用户组不支持删除与编辑操作。

步骤 1 登录到路由器 Web 管理页面，点击「审计」>「分组策略」>「用户组」。

步骤 2 点击 新增 。

步骤 3 配置用户组相关参数，点击 保存 。

- “用户组类型”为“认证用户组”时，如果该用户组被账号管理引用，凡是通过该账号和密码认证的用户都属于该认证用户组。
- “用户组类型”为“VPN 用户组”时，如果该用户组被用户管理引用，凡是通过该用户名和密码进行 VPN 拨号的用户都属于该 VPN 用户组。

---完成

9.2 上网过滤

9.2.1 IP 过滤

登录到路由器 Web 管理页面后，点击「审计」>「上网过滤」>「IP 过滤」。

您可以通过配置 IP 地址过滤规则来允许或禁止局域网主机连接到路由器上网。

IP 过滤配置举例

组网需求

某企业使用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。

方案设计

可以采用用路由器的 IP 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 192.168.0.2~192.168.0.50。

配置步骤

配置时间组 > 配置 IP 组 > 添加 IP 过滤策略

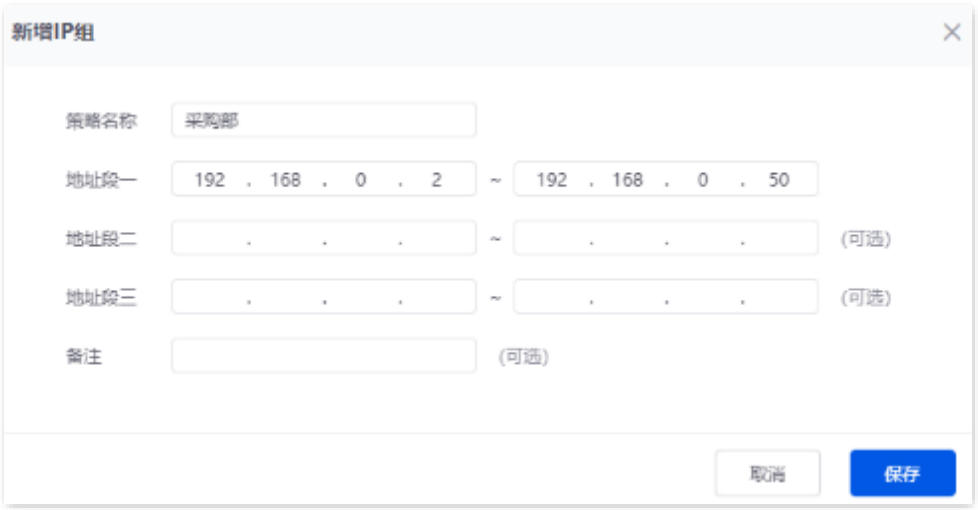
步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置时间组。

进入「审计」>「分组策略」>「时间组」页面，配置如下时间组。

步骤 3 配置 IP 组。

进入「审计」>「分组策略」>「IP 组」页面，配置如下 IP 组。



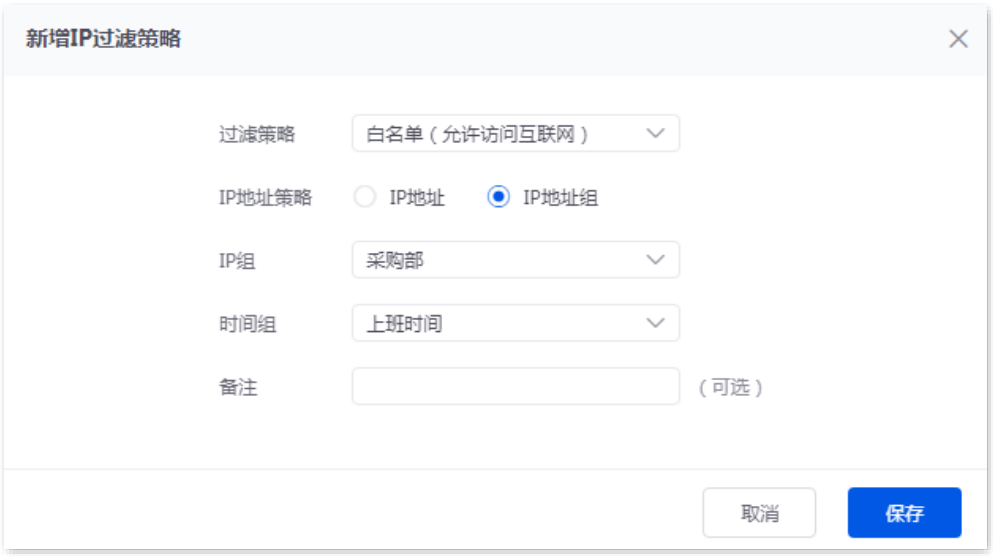
步骤 4 添加 IP 过滤策略。

IP 过滤策略参数示例如下所示。

过滤策略：白名单（允许访问互联网）	IP 组：采购部
IP 地址策略：IP 地址组	时间组：上班时间

1 点击「审计」>「上网过滤」>「IP 过滤」，然后点击 新增 。

2 配置 IP 过滤策略相关参数，点击 保存 。



3 去勾选“允许列表外的主机或设备访问互联网”，确认弹窗提示信息后，点击 确定 。

---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 192.168.0.2~192.168.0.50 范围内）才能上网，使用其他员工的电脑不能上网。

参数说明

标题项	说明
过滤策略	IP 地址的过滤模式。 - 黑名单（禁止访问互联网）：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。 - 白名单（允许访问互联网）：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。
IP 地址策略	若需要过滤某一个 IP 地址，“IP 地址策略”选择“IP 地址”并输入 IP 地址；如果需要过滤一个或几个 IP 地址段，“IP 地址策略”选择“IP 地址组”并选择对应的 IP 组策略即可。
IP 地址或 IP 组	IP 地址组策略应事先在「审计」>「分组策略」>「IP 组」页面配置好。
时间组	选择时间组策略，指定 IP 地址过滤策略生效的时间。 时间组策略应事先在「审计」>「分组策略」>「时间组」页面配置好。
允许列表外的主机或设备访问互联网	- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问互联网。 - 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都不能访问互联网。 注意 只有配置了白名单后才能取消勾选。

9.2.2 MAC 过滤

登录到路由器 Web 管理页面后，点击「审计」>「上网过滤」>「MAC 过滤」。

您可以通过配置 MAC 地址过滤规则来允许和禁止局域网主机连接到本路由器上网。

MAC 过滤配置举例

组网需求

某企业使用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。

方案设计

可以采用路由器的 MAC 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

配置时间组 > 添加 MAC 过滤策略

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置时间组。

点击「审计」>「分组策略」>「时间组」，配置如下时间组。

步骤 3 添加 MAC 地址过滤策略。

MAC 地址过滤策略参数示例如下所示。

过滤策略：白名单（允许访问互联网）　MAC 地址：CC:3A:61:71:1B:6E　时间组：上班时间

1 点击「审计」>「上网过滤」>「MAC 过滤」，然后点击 新增 。

2 配置 MAC 过滤策略相关参数，点击 保存 。

提示

如果您需要同时过滤多个 MAC 地址，MAC 地址之间请用“;”隔开。

3 去勾选“允许列表外的主机或设备访问互联网”，确认弹窗提示信息后，点击 确定 。

---完成

验证配置

在星期一到星期五的 8:00~18:00，局域网中，采购人员只有使用 MAC 地址为 CC:3A:61:71:1B:6E 的电脑才能上网，使用其他员工的电脑不能上网。

参数说明

标题项	说明
过滤策略	MAC 地址的过滤模式。 - 黑名单（禁止访问互联网）：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。 - 白名单（允许访问互联网）：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。
MAC 地址	需要上网过滤的 MAC 地址。
时间组	选择时间组策略，指定 MAC 地址过滤策略生效的时间。 时间组策略应事先在「审计」>「分组策略」>「时间组」页面配置好。
备注	MAC 地址过滤策略的备注信息。

标题项	说明
状态	MAC 地址过滤策略的状态。
允许列表外的主机或设备访问互联网	- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问互联网。 - 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都不能访问互联网。 注意 只有配置了白名单后才能取消勾选。

9.2.3 端口过滤

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。

登录到路由器 Web 管理页面后，点击「审计」>「上网过滤」>「端口过滤」。

您可以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。

端口过滤配置举例

组网需求

某企业使用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），禁止采购部门员工浏览网页（浏览网页服务默认的端口号是 80）。

方案设计

可以采用路由器的端口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 192.168.0.2~192.168.0.50。

配置步骤

配置时间组 → 配置 IP 组 → 添加端口过滤策略

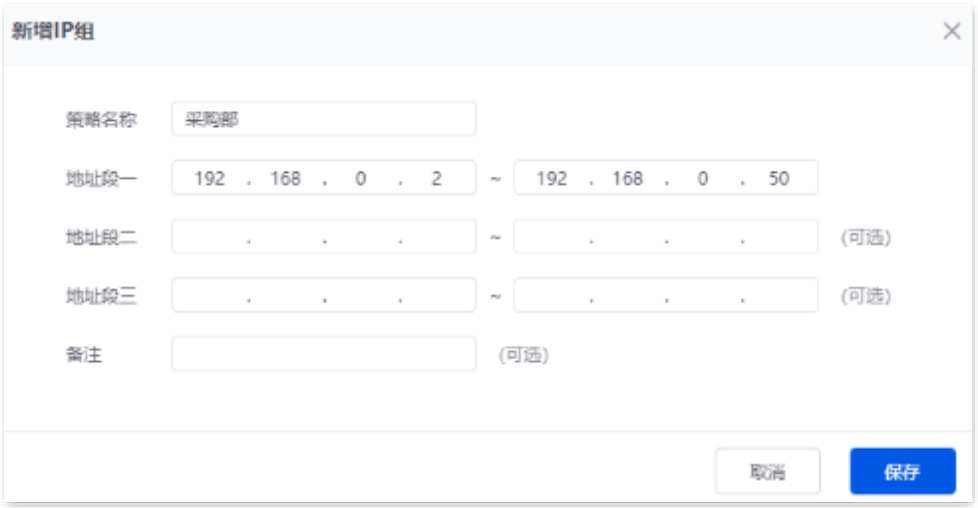
步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置时间组。

进入「审计」>「分组策略」>「时间组」页面，配置如下时间组。

步骤 3 配置 IP 组。

进入「审计」>「分组策略」>「IP 组」页面，配置如下 IP 组。



步骤 4 添加端口过滤策略。

端口过滤策略参数示例如下所示。

IP 组：采购部	时间组：上班时间
端口：80	协议：TCP&UDP

1 点击「审计」>「上网过滤」>「端口过滤」，然后点击 新增 。

2 配置端口过滤策略相关参数，点击 保存 。

提示

- 如果需要同时过滤多个不连续端口，端口号之间请用“;”隔开，如“80;20”。
- 如果需要过滤多个连续端口号，请用“~”表示，如“75~80”。

---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 192.168.0.2~192.168.0.50 范围内的电脑不能进行网页浏览服务。

参数说明

标题项	说明
IP 组	选择 IP 组策略，指定端口过滤策略生效的 IP 地址范围。 IP 组策略应事先在「审计」>「分组策略」>「IP 组」页面配置好。
时间组	选择时间组策略，指定 MAC 地址过滤策略生效的时间。 时间组策略应事先在「审计」>「分组策略」>「时间组」页面配置好。

标题项	说明
端口	禁止访问的服务的端口。
协议	禁止访问的服务的协议。

9.2.4 无线 MAC 过滤

登录到路由器 Web 管理页面后，点击「审计」>「上网过滤」>「无线 MAC 过滤」。

您可以通过配置无线 MAC 地址过滤策略来允许和禁止局域网内移动用户连接指定的无线网络上网。

无线 MAC 地址过滤配置举例

组网需求

某企业使用路由器进行网络搭建，该路由器下接有 AP（已被路由器管理），且已为 AP 下发了无线网络“VIP”。现需要配置路由器，让该无线网络仅供几个成员接入。

方案设计

可以采用路由器的无线 MAC 地址过滤功能实现上述需求。假设仅允许 3 台无线设备在上班时间连接无线网络“VIP”，MAC 地址分别为：D8:38:0D:00:00:01、D8:38:0D:00:00:02、D8:38:0D:00:00:03。

配置步骤

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置无线 MAC 地址过滤策略。

无线 MAC 地址过滤策略参数示例如下表所示。

过滤策略	AP 分组/Wi-Fi 名称（已预先配置）	MAC 地址
白名单（允许访问互联网）	APGroup_Default/VIP	D8:38:0D:00:00:01;D8:38:0D:00:00:02;D8:38:0D:00:00:03

进入「审计」>「上网过滤」>「无线 MAC 过滤」页面，点击 新增，配置无线 MAC 过滤策略相关参数，点击 保存。

----完成

验证配置

只有上述 3 台无线设备才可以接入无线网络“VIP”，其他设备无法接入该无线网络。

参数说明

标题项	说明
过滤策略	无线 MAC 地址过滤有以下两种方式： - 黑名单（禁止访问互联网）：指定 MAC 地址的用户在对应时间段内禁止通过指定的无线网络来访问互联网，在其他时间段内可以通过该无线网络来访问互联网。 - 白名单（允许访问互联网）：指定 MAC 地址的用户在对应时间段内可以通过指定的无线网络访问互联网，在其他时间段内不可以通过该无线网络来访问互联网。
AP 分组	选择无线 MAC 地址过滤策略生效 Wi-Fi 所属的分组。
Wi-Fi 名称	选择 Wi-Fi 名称，指定无线 MAC 地址过滤策略生效的 Wi-Fi。 Wi-Fi 名称应事先在「AP」>「Wi-Fi 设置」页面配置好。
MAC 地址	需要过滤的 MAC 地址。

9.2.5 URL 过滤

登录到路由器 Web 管理页面后，点击「审计」>「上网过滤」>「URL 过滤」。

您可以允许或禁止用户访问指定网址，以规范局域网用户上网行为。

URL 过滤配置举例

需求场景

某企业使用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址，如站酷（zcool.com.cn）、花瓣（huaban.com）、素材中国（sccnn.com）。其他人员不能访问互联网。

方案设计

可以采用路由器的 URL 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 192.168.0.60~192.168.0.100。

配置步骤

配置时间组 → 配置 IP 组 → 添加 URL 过滤策略

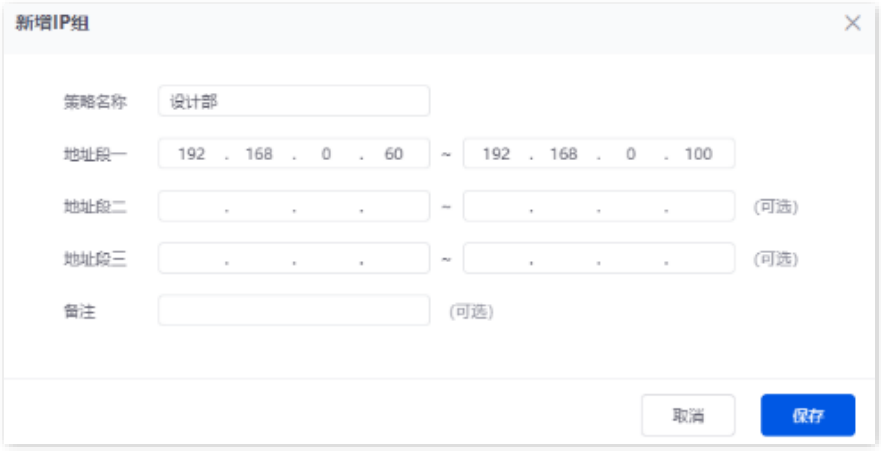
步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置时间组。

进入「审计」>「分组策略」>「时间组」页面，配置如下时间组。

步骤 3 配置 IP 组。

进入「审计」>「分组策略」>「IP 组」页面，配置如下 IP 组。



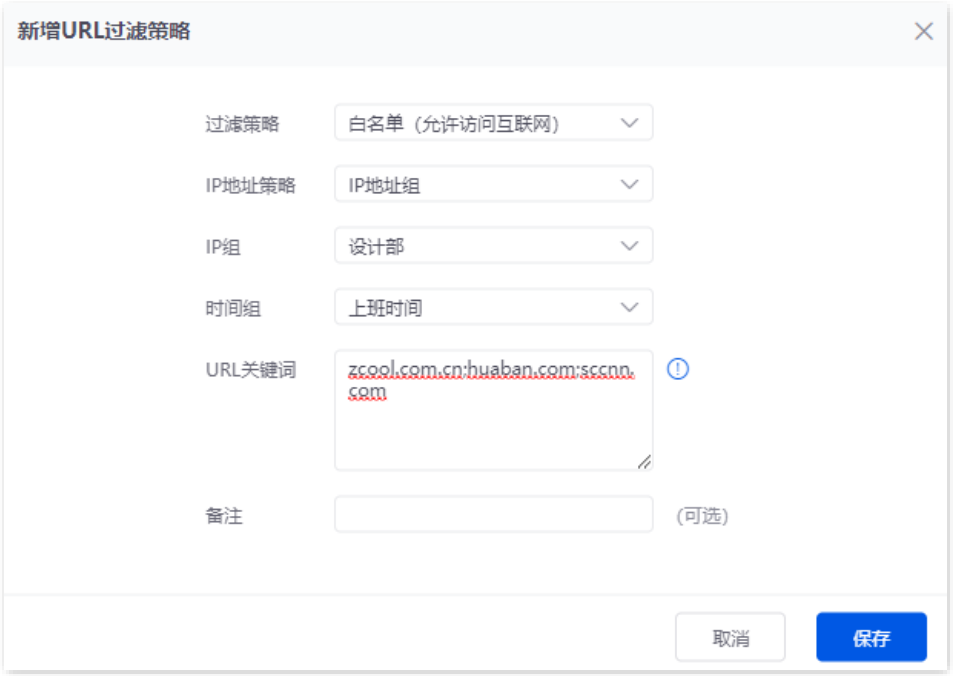
步骤 4 添加 URL 过滤策略。

URL 过滤策略参数示例如下所示。

过滤策略：白名单（允许访问互联网）	时间组：上班时间
IP 地址策略：IP 地址组	URL 关键词：zcool.com.cn;huaban.com;sccnn.com
IP 组：设计部	

1 点击「审计」>「上网过滤」>「URL 过滤」，然后点击 新增 。

2 配置 URL 过滤策略相关参数，点击 保存 。



3 去勾选“允许列表外的主机或设备访问互联网”，确认弹窗提示信息后，点击 确定 。

---完成

验证配置

局域网中 IP 地址在 192.168.0.60~192.168.0.100 范围内的电脑在星期一到星期五的 8:00~18:00 只能访问网址 zcool.com.cn、huaban.com 和 sccnn.com。其他电脑不能上网。

参数说明

标题项	说明
过滤策略	网址过滤模式。 - 黑名单（禁止访问互联网）：指定 IP 地址的用户在对应时间段内禁止访问指定网址，可以访问其他网址，在其他时间段内可以访问所有网址。 - 白名单（允许访问互联网）：指定 IP 地址的用户在对应时间段内可以访问指定网址，不可以访问其他网址，在其他时间段内可以访问所有网址。
IP 地址策略 IP 地址或 IP 组	如果需要过滤某一个 IP 地址，“IP 地址策略”选择“IP 地址”并输入 IP 地址；如果需要过滤一个或几个 IP 地址段，“IP 地址策略”选择“IP 地址组”并选择对应的 IP 组策略即可。 IP 地址组策略应事先在「审计」>「分组策略」>「IP 组」页面配置好。
时间组	选择时间组策略，指定网址过滤策略生效的时间。 时间组策略应事先在「审计」>「分组策略」>「时间组」页面配置好。
URL 关键词	禁止/允许访问的网址关键词。
备注	网址过滤策略的备注信息。
状态	网址过滤策略的状态。
允许列表外的主机或设备访问互联网	- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问指定网址。 - 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都不能访问指定网址。 注意 只有配置了白名单后才能取消勾选。

9.2.6 用户过滤

登录到路由器 Web 管理页面后，点击「审计」>「上网过滤」>「用户过滤」。

您可以通过配置用户过滤规则来允许和禁止局域网内的认证用户连接到本路由器上网。

用户过滤配置举例

组网需求

某企业使用路由器进行网络搭建，且已在路由器中配置账号密码认证，账号密码认证时使用的账号已加入“研发部”认证用户组中。认证具体配置可参考认证管理。

要求：上班时间（星期一到星期五的 8:00~18:00），仅允许通过账号密码认证的研发部员工访问互联网，其他员工禁止访问互联网。

方案设计

可以采用路由器的用户过滤功能实现上述需求。

配置步骤

配置时间组 > 配置用户过滤策略

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置时间组。

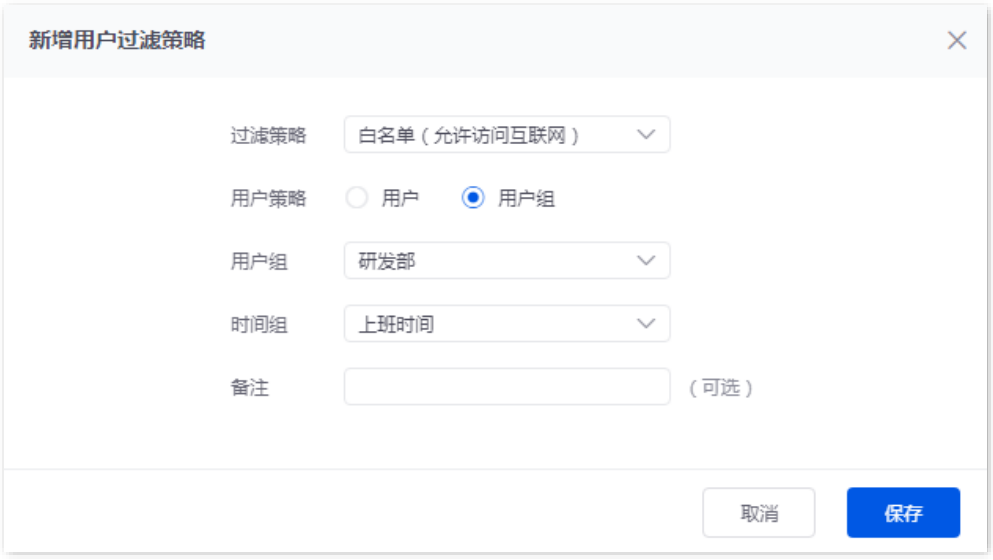
进入「审计」>「分组策略」>「时间组」页面，点击 新增，配置如下时间组。

步骤 3 配置用户过滤策略。

用户过滤策略参数示例如下表所示。

过滤策略	用户策略	用户或用户组（已预先配置）	时间组
白名单（允许访问互联网）	用户组	研发部	上班时间

1 进入「审计」>「上网过滤」>「用户过滤」页面，点击 新增，配置用户过滤策略相关参数，点击 保存。



2 取消勾选“允许列表外的主机或设备访问互联网”，确认提示信息后，点击 确定。

----完成

验证配置

上班时间（星期一到星期五的 8:00~18:00），仅通过账号密码认证的研发部员工可以访问互联网，其他员工无法访问互联网。

参数说明

标题项	说明
过滤策略	用户过滤有以下两种方式： - 黑名单（禁止访问互联网）：指定认证用户或者用户组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。 - 白名单（允许访问互联网）：指定认证用户或者用户组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。

标题项	说明
用户策略	选择用户策略，指定用户策略生效的认证用户或者用户组。 认证用户应提前在「认证」>「账号管理」>「账号管理」页面配置好；认证用户组应提前在「审计」>「分组策略」>「用户组」页面配置好。
用户名或用户组	需要过滤的认证用户账号或用户组。
时间组	选择时间组策略，指定用户过滤策略生效的时间。 时间组策略应事先在「审计」>「分组策略」>「时间组」页面配置好。
允许列表外的主机或设备访问互联网	- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问互联网。 - 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都无法访问互联网。 注意 只有配置了白名单后才能取消勾选。

9.2.7 VPN 访问权限

登录到路由器 Web 管理页面后，点击「审计」>「上网过滤」>「VPN 访问权限」。

您可以通过配置 VPN 访问权限策略来允许和禁止 VPN 用户访问局域网的服务器。

VPN 访问权限配置举例

组网需求

某企业使用路由器进行网络搭建，已通过路由器在该企业总部和分公司 1 之间建立 PPTP VPN。总部已在路由器上创建 VPN 用户组“分公司 1 员工”，且已将分公司 1 员工的账号与密码添加到该 VPN 用户组中。如果要查看 VPN 具体配置，可参考 VPN 服务。

要求：仅允许分公司 1 员工通过 PPTP VPN 访问企业总部 FTP 服务器，其他员工无法访问。

方案设计

可以采用路由器的 VPN 访问权限功能实现上述需求。假设企业总部 FTP 服务器 IP 地址为 192.168.0.104。

配置步骤

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置 VPN 访问权限策略。

VPN 访问权限策略参数示例如下表所示。

过滤策略	用户组（已预先配置）	内网服务器 IP 地址
白名单（允许访问）	分公司 1 员工	192.168.0.104

1 进入「审计」>「上网过滤」>「VPN 访问权限」页面，点击 新增 ，配置 VPN 访问权限策略相关参数，点击 保存 。

2 取消勾选“允许列表外的主机或设备访问互联网”，确认提示信息后，点击 确定 。

----完成

验证配置

仅分公司 1 员工通过 PPTP VPN 可以访问企业总部 IP 地址为 192.168.0.104 的 FTP 服务器，其他员工无法访问。

参数说明

标题项	说明
过滤策略	VPN 访问权限策略有以下两种方式： - 黑名单（禁止访问）：指定 VPN 用户组禁止访问局域网的指定服务器。 - 白名单（允许访问）：指定 VPN 用户组允许访问局域网的指定服务器。
用户组	指定 VPN 访问权限策略生效的 VPN 用户组。
内网服务器 IP 地址	指定 VPN 访问权限策略生效的内网服务器 IP 地址。

标题项	说明
允许列表外的主机或设备访问内网	- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问指定的内网服务器。 - 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都无法访问指定的内网服务器。 注意 只有配置了白名单后才能取消勾选。

9.3 日志审计

9.3.1 审计设置

登录到路由器 Web 管理页面后，点击「审计」>「日志审计」>「审计设置」。

您可以根据实际需要采集指定类型的日志信息。

日志审计默认关闭，开启后如下所示。

参数说明

标题项	说明
日志审计	开启/关闭日志审计功能。
用户访问 URL 日志审计	记录用户访问网页的信息。
用户进出网时间记录	记录用户从用户 DHCP 服务器获取 IP 地址的时间。
用户停留时间记录	记录用户在线时长。
无线用户 AP 的记录	记录无线用户连到的 AP 的信息。
无线用户连接的 SSID 记录	记录无线用户连接到的 Wi-Fi 名称。

9.3.2 日志存储

登录到路由器 Web 管理页面后，点击「审计」>「日志审计」>「日志存储」。

您可以设置日志审计结果的存储位置。开启日志审计后，日志审计结果只能存在本地电脑或 USB 存储。存储在本地电脑时，需要安装日志工具如：syslog。

系统默认为 USB 存储，如下图所示。

参数说明

标题项	说明
存储方式	支持两种存储方式。 - USB 存储：将日志审计结果通过 USB 接口存储到其他 USB 存储设备上。 - 本地电脑存储：将日志审计结果存储在本地电脑上。
USB 存储信息	USB 存储设备的基本信息。存储方式为 USB 存储时，系统会自动获取该信息。
USB 存储可用空间	当前 USB 存储设备可用的存储空间大小。存储方式为 USB 存储，系统会自动扫描。
本地电脑 IP 地址	本地存储审计结果的电脑的 IP 地址。存储方式为本地电脑存储时需填入。

10 更多功能

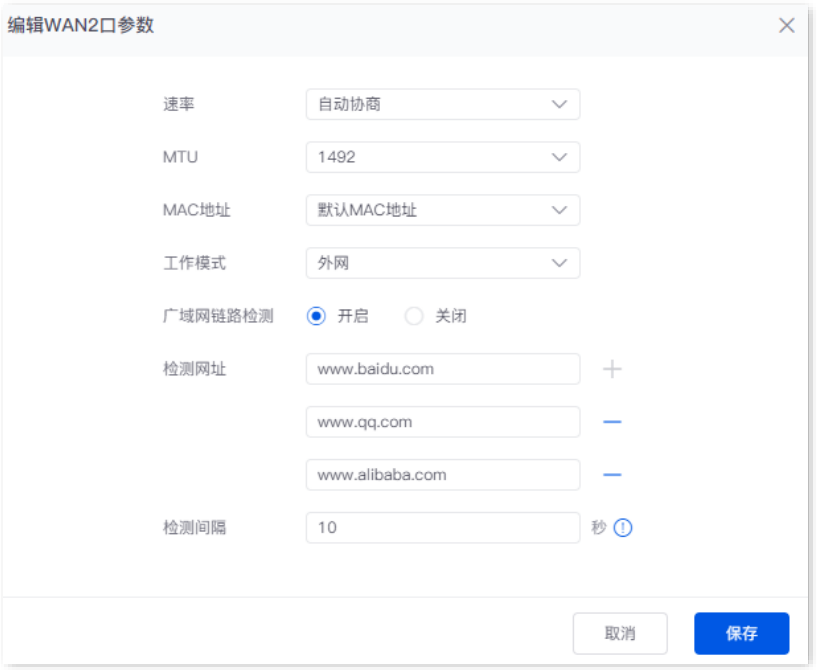
本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

10.1 高级路由

10.1.1 WAN 口参数

登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「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，可以尝试点击 编辑 修改 WAN 口参数解决。



参数说明

标题项	说明
WAN 口	当前路由器的 WAN 口。
速率	WAN 口的速率与双工模式，它必须与对端端口的速率与双工模式保持一致。 一般情况下，建议保持默认设置“自动协商”。如果路由器 WAN 口连接正常，但对应接口灯不亮；或者插上网线后接口灯要等待一会儿（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。
MTU	MTU（Maximum Transmission Unit，最大传输单元）是网络设备传输的最大数据包。取值范围与 WAN 口联网方式有关。 一般情况下，建议保持默认设置。如果您无法访问某些网站、或打不开安全网站（如网银、支付宝登录页面）、或无法收发邮件、或无法访问 FTP 和 POP 服务器等，可以尝试修改 MTU 值，建议修改范围是 1400~1500，下面是常用的 MTU 值适用的场景： - 1500：一般用于非宽带拨号、非 VPN 拨号环境下最常用的设置。 - 1492：一般用于宽带拨号环境。 - 1472：是使用 ping 的最大值（大于此值的包会被分解）。 - 1468：一般用于一些 DHCP（动态 IP）环境。 - 1436：一般用于 VPN 或 PPTP 环境。
MAC 地址	WAN 口的 MAC 地址。 正确完成联网设置后，如果路由器还是无法联网，有可能是宽带服务商将上网账号信息与某一 MAC 地址（物理地址）绑定了。此时，您可以尝试通过修改 WAN 口 MAC 地址解决该问题。
工作模式	WAN 口的工作模式。 - 内网：WAN 口不能访问互联网，一般用于连接企业内网。 - 外网：WAN 口可以访问互联网，一般用于连接互联网。
广域网线路检测	开启后，路由器会周期性地检测 WAN 口与“检测网址”的连通情况，然后根据检测结果选择最佳的 WAN 口链路做为主要出口链路。
检测网址	需要检测的域名。
检查间隔	路由器执行广域网线路检测的时间间隔。

10.1.2 多 WAN 策略

登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「多 WAN 策略」。

您可以设置多 WAN 策略和网银数据源进源出。

- **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。

- 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。
- 基于连接数均衡：根据 LAN 口的连接数，系统自动按照权重分配给 WAN 口，适用多用户并发访问场景。
- 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。
- 关闭：关闭多 WAN 策略。

- **网银数据源进源出**

启用“网银数据源进源出”功能后，用户访问同一银行网站时，数据从同一 WAN 口转发。避免因数据通过多个 WAN 转发导致访问失败的现象。仅多 WAN 策略为“智能负载均衡”时可见。

自定义多 WAN 策略配置举例

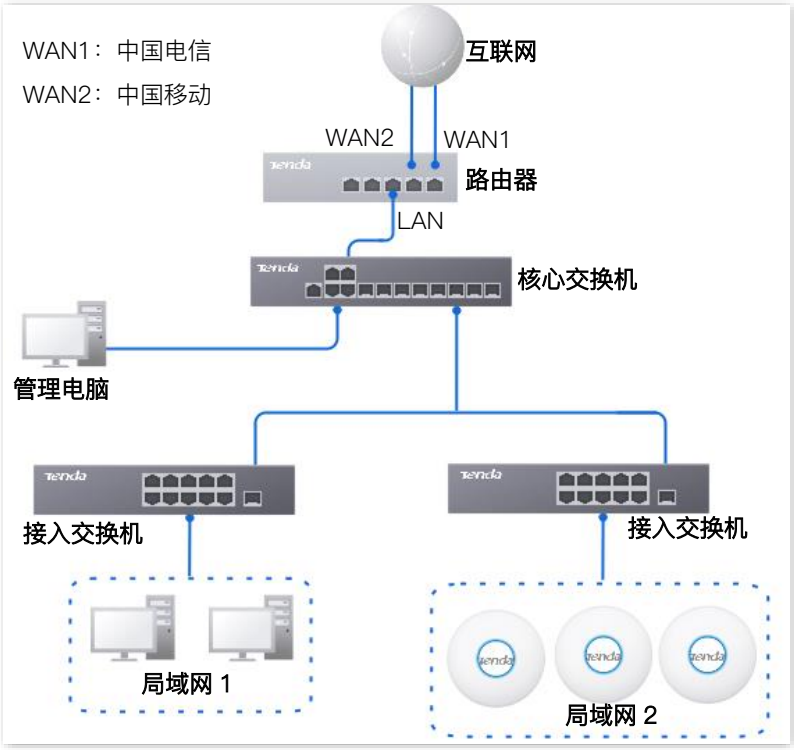
组网需求

某企业使用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：

- IP 地址为 192.168.0.2~192.168.0.100 的终端设备通过电信宽带访问互联网。
- IP 地址为 192.168.0.101~192.168.0.250 的终端设备通过移动宽带访问互联网。

方案设计

可以采用路由器的多 WAN 策略功能实现上述需求。



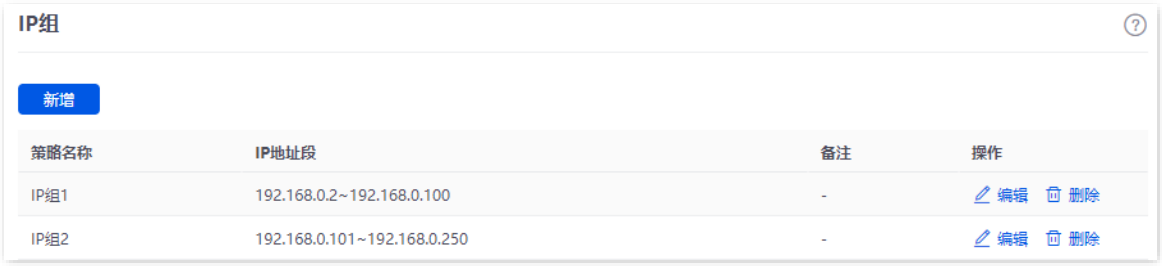
配置步骤

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 登录到路由器 Web 管理页面。

步骤 2 配置 IP 组。

进入「审计」>「分组策略」>「IP 组」页面，点击 新增，配置如下 IP 组。



步骤 3 开启自定义多 WAN 策略功能。

1 点击「更多」>「高级路由」>「多 WAN 策略」。

2 选择“多 WAN 策略”为“自定义”。

3 确认提示信息后，点击 确定。

步骤 4 自定义多 WAN 策略规则。

进入「更多」>「高级路由」>「多 WAN 策略」页面，点击 新增，配置如下多 WAN 策略规则。

----完成

验证配置

局域网中 IP 组 1（IP 地址在 192.168.0.2~192.168.0.100 范围内）的设备访问外网时，数据流量由 WAN1 口转发；局域网中 IP 组 2（IP 地址在 192.168.0.101~192.168.0.250 范围内）的设备访问外网时，数据流

量由 WAN2 口转发。

参数说明

标题项	说明
IP 组	自定义多 WAN 策略引用的 IP 组，以指定规则对应的用户。IP 组应事先在「审计」>「分组策略」>「IP 组」页面配置好。
WAN 口	选择对应 IP 组数据流量使用的 WAN 接口。

10.1.3 静态路由

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。
- 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。

登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「静态路由」。

您可以根据实际网络情况配置相应的静态路由。

静态路由配置举例

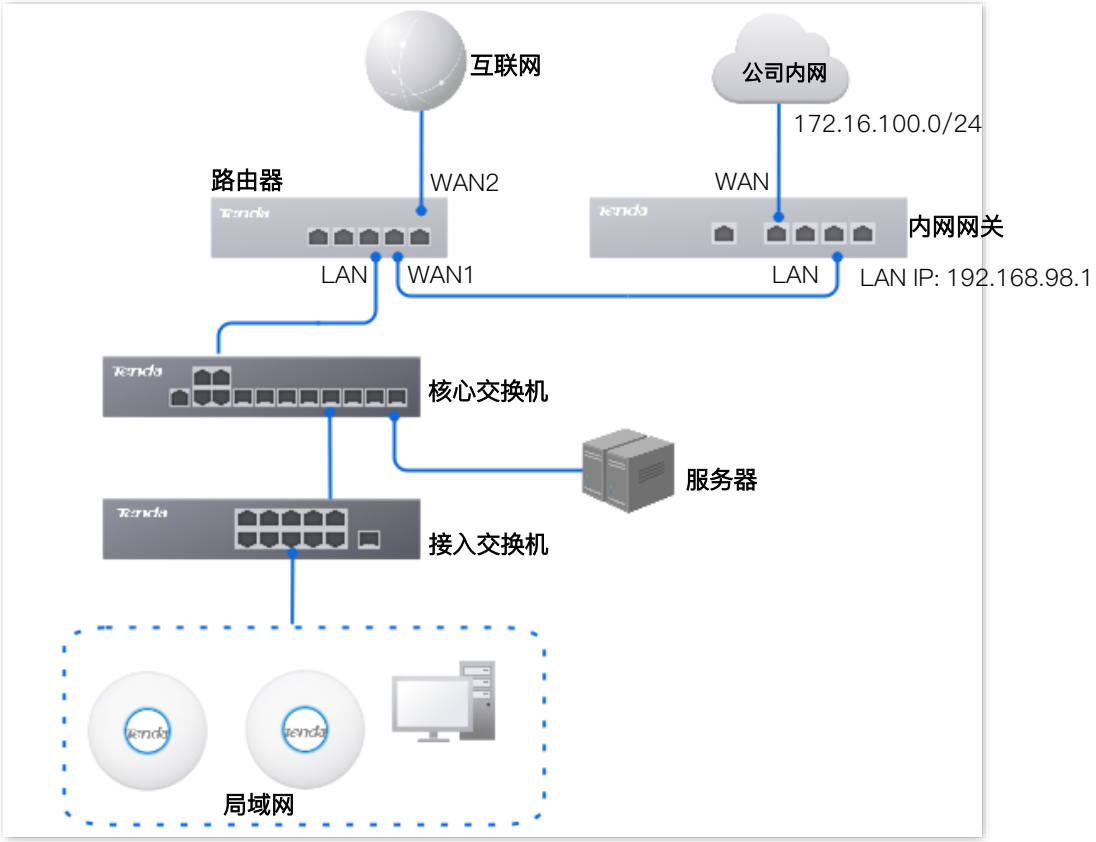
组网需求

某企业使用路由器进行网络搭建。路由器的 WAN2 已通过宽带拨号接入互联网。现企业内部搭建了一个公司内网，与互联网处在不同网络，路由器的 WAN1 口通过自动获取 IP 地址接入公司内网。

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

可以采用路由器的静态路由功能实现上述需求。



配置步骤

配置 WAN 口联网 > 配置静态路由

步骤 1 登录到路由器 Web 管理页面。

步骤 2 启用 2 个 WAN 口，并设置 WAN1 联网。

1 点击「网络」>「联网设置」。

2 设置“LAN1”为“WAN1”，并确认提示信息。

3 在 WAN1 处选择“联网方式”为“动态 IP”，点击 连接 。

稍等片刻，当联网状态显示“已联网”时，WAN1 口联网成功。

步骤 3 配置静态路由。

1 获取 WAN1 口的 IP 地址信息。

进入「网络」>「联网设置」页面，查看 WAN1 获取的 IP 地址信息，本例中相关信息如下。

WAN1 IP 地址	子网掩码	默认网关	首选 DNS
192.168.98.190	255.255.255.0	192.168.98.1	192.168.98.1

2 配置静态路由。

静态路由参数示例如下表所示。

策略名称	目标网络	子网掩码	默认网关	接口
内网访问	172.16.100.0	255.255.255.0	192.168.98.1	WAN2

进入「更多」>「高级路由」>「静态路由」页面，点击 新增，配置静态路由参数，点击 保存。

----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。

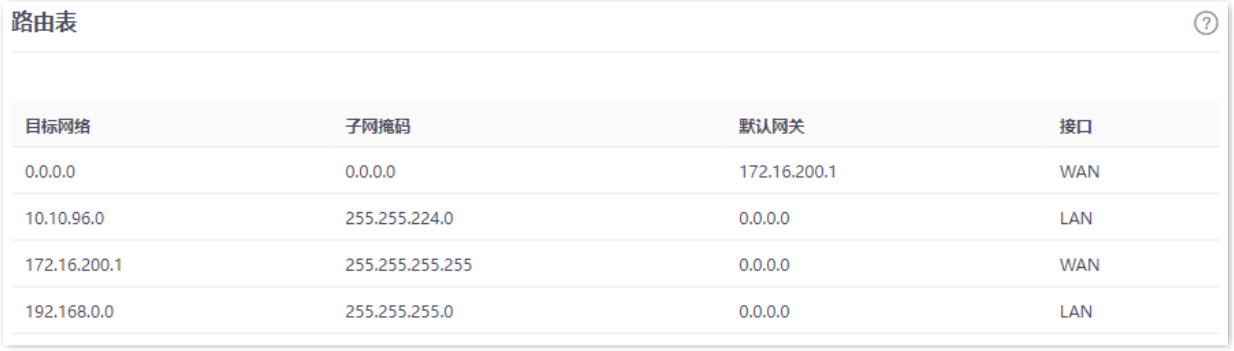
参数说明

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。

10.1.4 路由表

登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「路由表」。

您可以查看路由器的详细路由信息。


路由表

目标网络	子网掩码	默认网关	接口
0.0.0.0	0.0.0.0	172.16.200.1	WAN
10.10.96.0	255.255.224.0	0.0.0.0	LAN
172.16.200.1	255.255.255.255	0.0.0.0	WAN
192.168.0.0	255.255.255.0	0.0.0.0	LAN

参数说明可参考静态路由的参数说明。

10.1.5 策略路由

策略路由，也叫做基于策略的路由，是指在决定一个 IP 包的下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。本路由器的策略路由通过对源网络、目的网络、目的端口、协议和 WAN 口的设置，更加精确的控制路由器进行选路。

策略路由设置完成后，路由器将满足该策略条件的数据包通过指定的 WAN 口转发。

登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「策略路由」。您可以配置策略路由。

策略路由配置举例

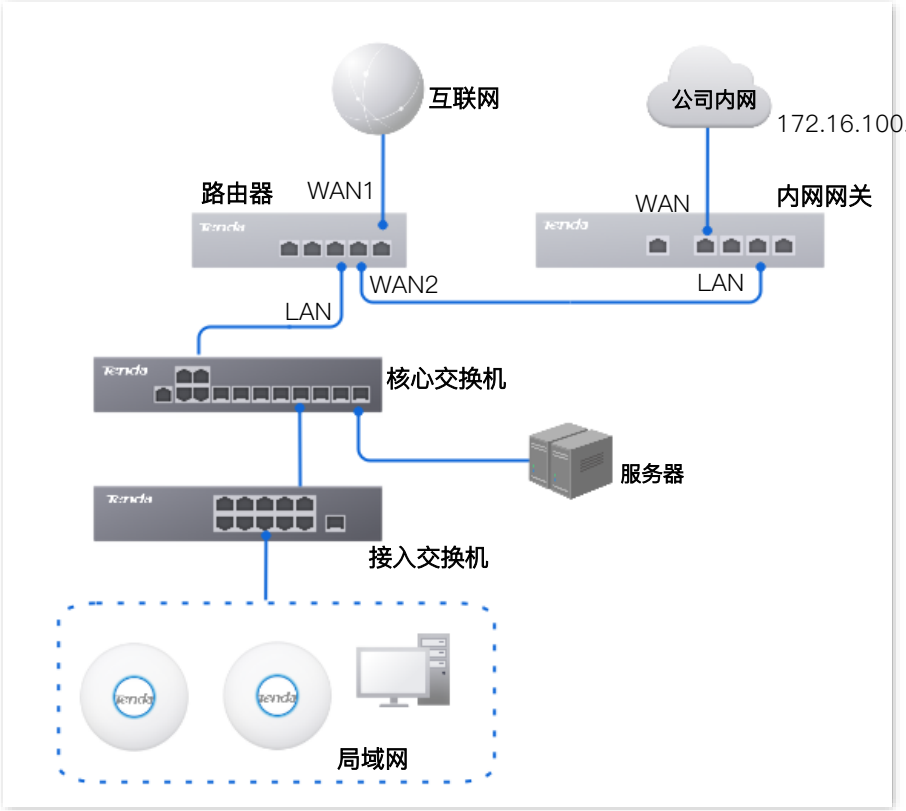
组网需求

某企业使用路由器进行网络搭建，路由器已通过宽带拨号接入互联网。现企业内网搭建了一个 Web 服务器，与互联网在不同的网络。企业内网的接入方式为动态 IP。

要求：局域网地址为 192.168.0.2~192.168.0.254 的用户能同时访问互联网和公司内网的 Web 服务器。

方案设计

可以采用路由器的策略路由功能实现上述需求。



配置步骤

配置 WAN1 口联网 > 配置策略路由

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置 WAN1 口联网。

1 点击「网络」>「联网设置」。

2 设置“LAN1”为“WAN1”，并确认提示信息。

3 在 WAN1 处选择“联网方式”为“动态 IP”，点击 连接 。

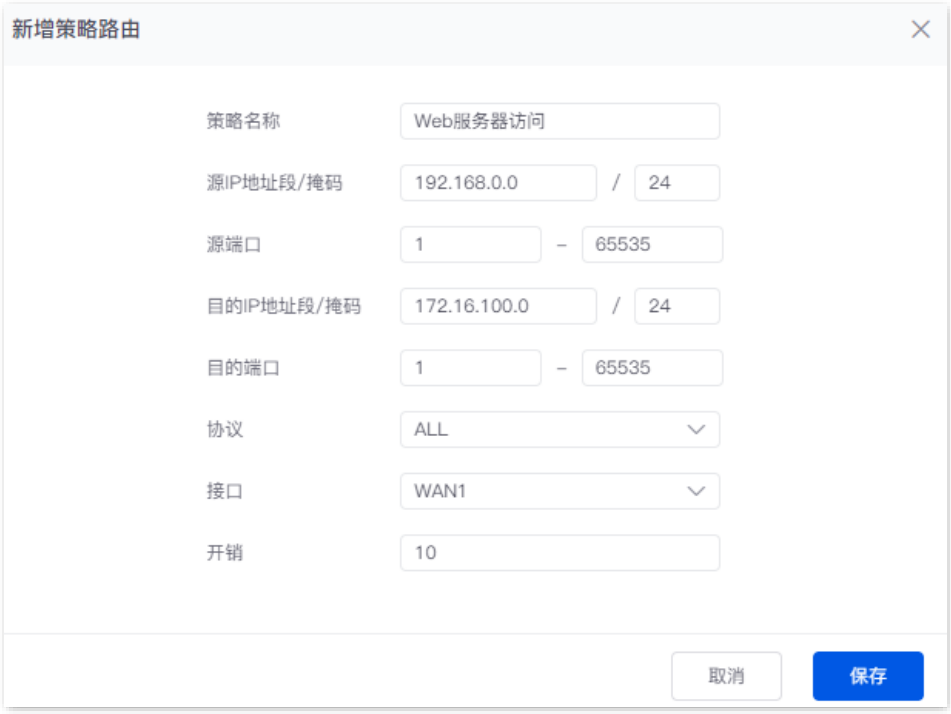
稍等片刻，当联网状态显示“已联网”时，WAN1 口联网成功。

步骤 3 配置策略路由。

策略路由参数示例如下表所示。

策略名称	源 IP 地址段/掩码	源端口	目的 IP 地址段/掩码	目的端口	协议	接口	开销
Web 服务器访问	192.168.0.0/24	1~65535	172.16.100.0/24	1~65535	ALL	WAN1	10

进入「更多」>「高级路由」>「策略路由」页面，点击 新增 ，配置策略路由参数，点击 保存 。



----完成

验证配置

局域网地址为 192.168.0.2~192.168.0.254 的用户能同时访问互联网和公司内网的 Web 服务器。

参数说明

标题项	说明
源 IP 地址段/掩码	要进行精确路由转发的源 IP 地址段。
源端口	要进行精确路由转发的源端口号。
目的 IP 地址段/掩码	数据包被转发到的目的 IP 地址段。
目的端口	数据包被转发到的目标网络的端口号。
协议	数据包的协议类型。
接口	策略生效的物理接口，满足策略路由条件的数据包将由该接口转发出去。
开销	策略的优先级，值越小，策略路由优先级越高。

10.1.6 自定义 NAT

NAT（Network Address Translation，网络地址转换）可以实现局域网内的多台设备共享一个或多个公网 IP 地址接入互联网，同时隐藏了局域网的设备，使广域网无法直接访问到局域网设备，为局域网提供一定的安全保障。

本路由器支持 NAT 功能，具体工作机制如下：

- 当路由器局域网 IP 地址范围内的设备需要通过该路由器上网时，路由器自动将其 IP 地址转换为合法的公网 IP 地址进行上网。
- 当不在路由器局域网 IP 地址范围内的设备需要通过该路由器进行代理上网时，您可以通过自定义 NAT 功能，让路由器将其 IP 地址转换为合法的公网 IP 地址进行上网。

登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「自定义 NAT」。您可以自定义 NAT 策略。

非局域网 IP 的设备通过路由器上网

组网需求

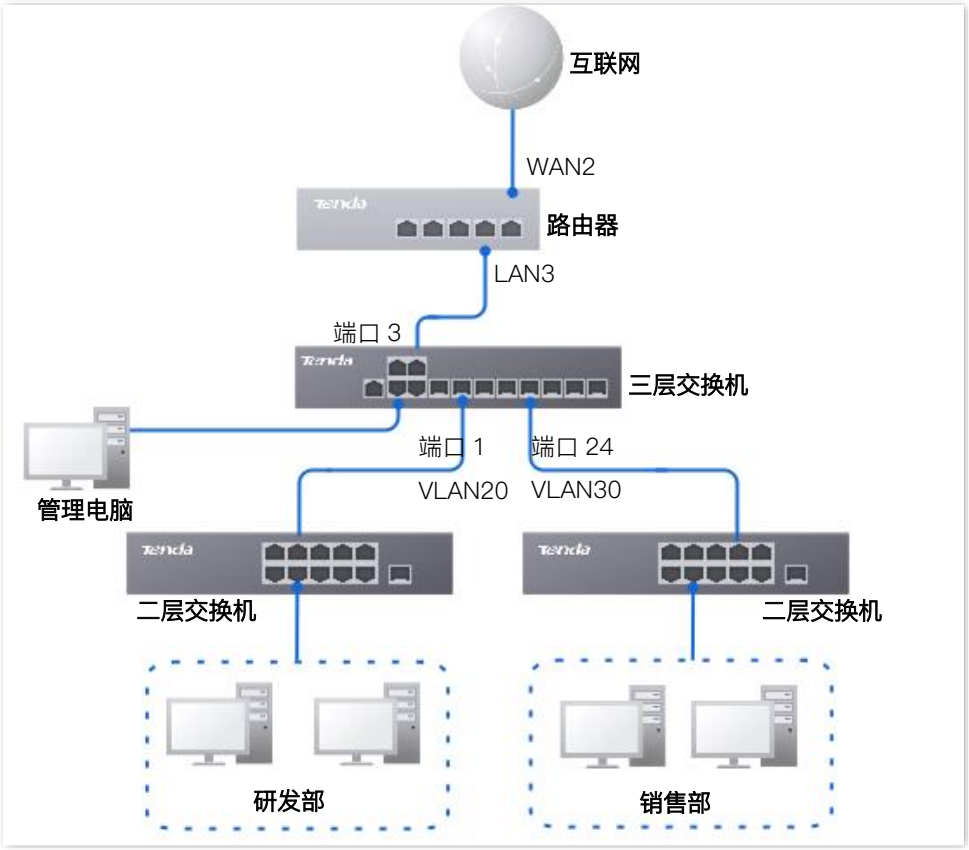
某企业使用路由器和三层交换机 TEG5328XP-24-410W 进行网络搭建，路由器的 LAN3 口连接三层交换机的端口 3，公司内部网络使用三层交换机将研发部和销售部划分到不同的 VLAN 中，具体组网如下描述。

- 研发部处于 VLAN20，连接在三层交换机的端口 1。
- 销售部处于 VLAN30，连接在三层交换机的端口 24。
- 三层交换机端口 3 在交换机的默认 VLAN1 中，路由器 LAN3 口在路由器的默认 VLAN 中，设置三层交换机端口 3 与路由器 LAN3 口的 IP 地址在同一网段。假设路由器 LAN3 口 IP 地址保持默认值为 192.168.0.252，三层交换机端口 3 的 IP 地址设置为 192.168.0.2。

要求：研发部和销售部都能访问互联网。

方案设计

可以采用路由器的策略路由功能实现上述需求。



配置步骤

步骤 1 配置三层交换机。

1 为交换机的端口 1、24 分别设置 VLAN，并设置 DHCP 服务器。

VLAN 的参数示例如下表所示。

交换机端口	IP 地址	子网掩码	VLAN ID（允许通过的 VLAN）	端口属性	PVID
1	192.168.20.1	255.255.255.0	20	Access	20
24	192.168.30.1	255.255.255.0	30	Access	30

VLAN 的 DHCP 服务器参数示例如下表所示，配置后并启用 DHCP 使能。

VLAN ID	DHCP 服务器地址池	子网掩码	默认网关	DNS
20	192.168.20.2~192.168.20.250	255.255.255.0	192.168.20.1	223.5.5.5
30	192.168.30.2~192.168.30.250	255.255.255.0	192.168.30.1	223.5.5.5

2 在交换机上配置端口 3 的 IP 地址（交换机默认 VLAN 的 IP 地址），如下表所示。

交换机端口	IP 地址	VLAN ID（允许通过的 VLAN）	端口属性	PVID
3	192.168.0.2	1	Access	1

其他未提到的端口保持默认设置即可。

3 在交换机上配置如下一条默认路由。

目的地址	子网掩码	下一跳（默认网关）
0.0.0.0	0.0.0.0	192.168.0.252

具体配置方法请参考交换机的使用说明书。

步骤 2 配置路由器。

1 登录到路由器 Web 管理页面。

2 配置如下静态路由规则。

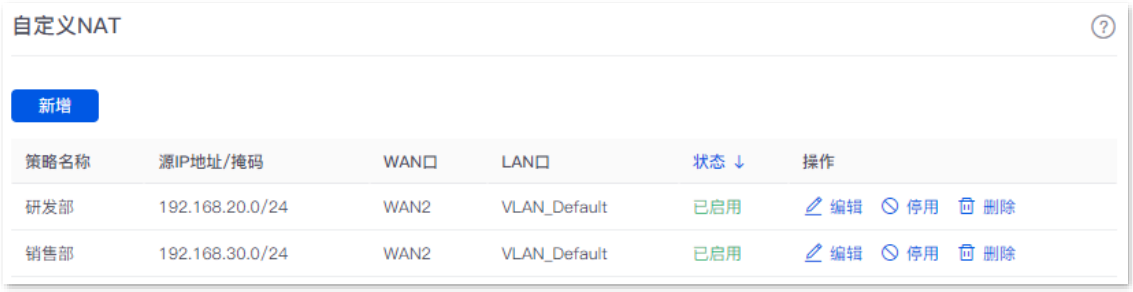
策略名称	目标网络	子网掩码	默认网关	接口
研发部	192.168.20.0	255.255.255.0	192.168.0.2	VLAN_Default
销售部	192.168.30.0	255.255.255.0	192.168.0.2	VLAN_Default

进入「更多」>「高级路由」>「静态路由」页面，点击 新增，配置如下静态路由。

3 配置如下自定义 NAT 规则。

策略名称	源 IP 地址段/掩码	WAN 口	LAN 口
研发部	192.168.20.0/24	WAN2	VLAN_Default
销售部	192.168.30.0/24	WAN2	VLAN_Default

进入「更多」>「高级路由」>「自定义 NAT」页面，点击 新增，自定义如下 NAT 规则。



----完成

验证配置

研发部和销售部的员工都可以访问互联网。

参数说明

标题项	说明
源 IP 地址/掩码	要进行网络地址转换的源 IP 地址段。
WAN 口	进行网络地址转换的互联网口。
LAN 口	“源 IP 地址/掩码”接到的 LAN 口。
添加到 SD-WAN 路由	开启后 SD-WAN 网络中的 IP 也适用该 NAT 规则。

10.2 虚拟服务

10.2.1 DMZ

将局域网中某台设备设置为 DMZ 主机后，该设备与互联网通信时将不受限制。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 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 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。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「DMZ」。

路由器默认已为各 WAN 接口创建了相应的 DMZ 策略，状态为“已停用”，您根据实际需要修改相应的 DMZ 策略。

DMZ 配置举例

组网需求

某企业使用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

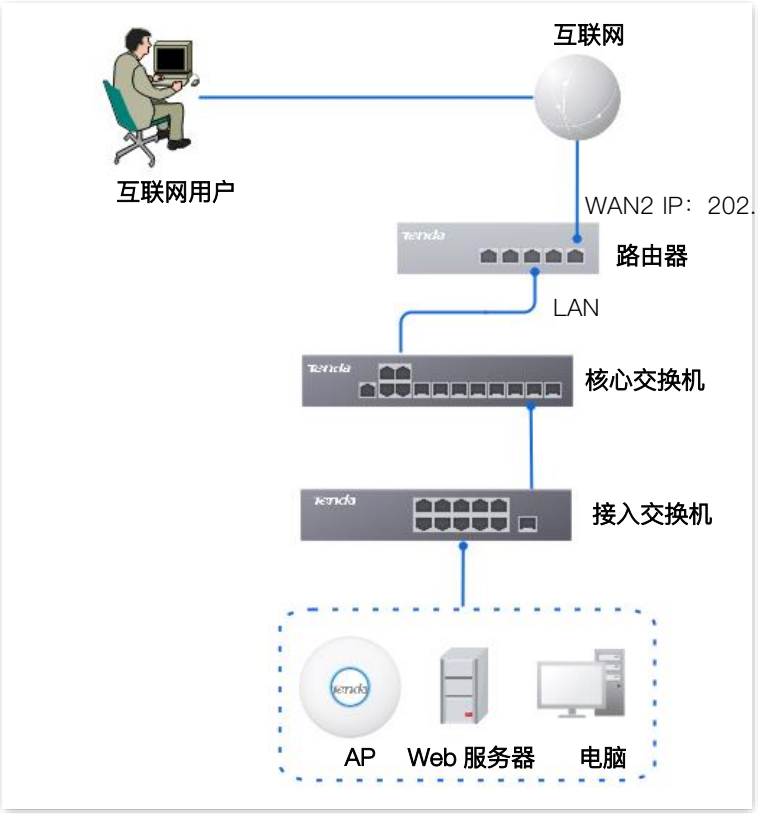
- 采用路由器的 DMZ 功能实现互联网用户访问企业内部 Web 服务器的需求。
- 采用路由器的静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

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访问未经报备使用默认端口号 80 的 Web 服务。因此，在使用 DMZ 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 DMZ 主机 > 给 DMZ 主机分配固定 IP 地址

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置 DMZ 主机。

1 点击「更多」>「虚拟服务」>「DMZ」。

2 找到相应的 WAN 口，点击编辑。

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 保存 。

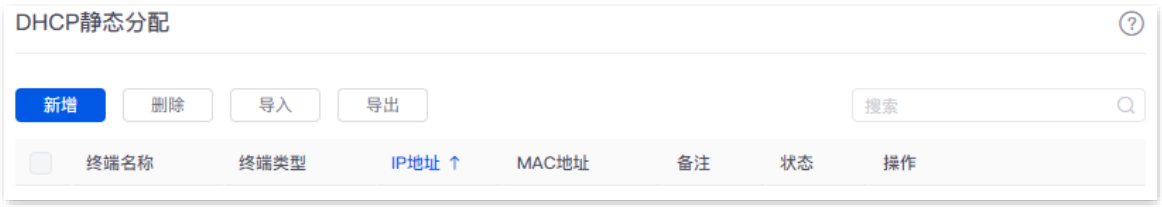
5 点击启用。

步骤 3 给 DMZ 主机分配固定 IP 地址。

DHCP 静态分配规则参数示例如下所示。

终端名称：Web 服务器	固定分配给服务器主机的 IP 地址：192.168.0.250
服务器主机的 MAC 地址：C8:9C:DC:60:54:69	规则备注信息：Web 服务器地址

1 点击「网络」>「DHCP 设置」>「DHCP 静态分配」，然后点击 新增 。



2 配置 DHCP 静态分配规则的相关参数后，点击 保存 。

---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”。您可以在连接状态找到路由器 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:内网服务端口”访问。

参数说明

标题项	说明
接口	DMZ 策略生效的 WAN 接口。
DMZ 主机 IP 地址	要设置为 DMZ 主机的局域网设备的 IP 地址。

10.2.2 DDNS

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 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。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「DDNS」。

路由器默认已为各 WAN 接口创建了相应的 DDNS 策略，状态为“已停用”。您根据实际情况修改相应的 DDNS 策略。

DDNS 配置举例

组网需求

某企业使用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

- 采用路由器的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。
- 采用路由器的 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。
- 采用路由器的静态 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。

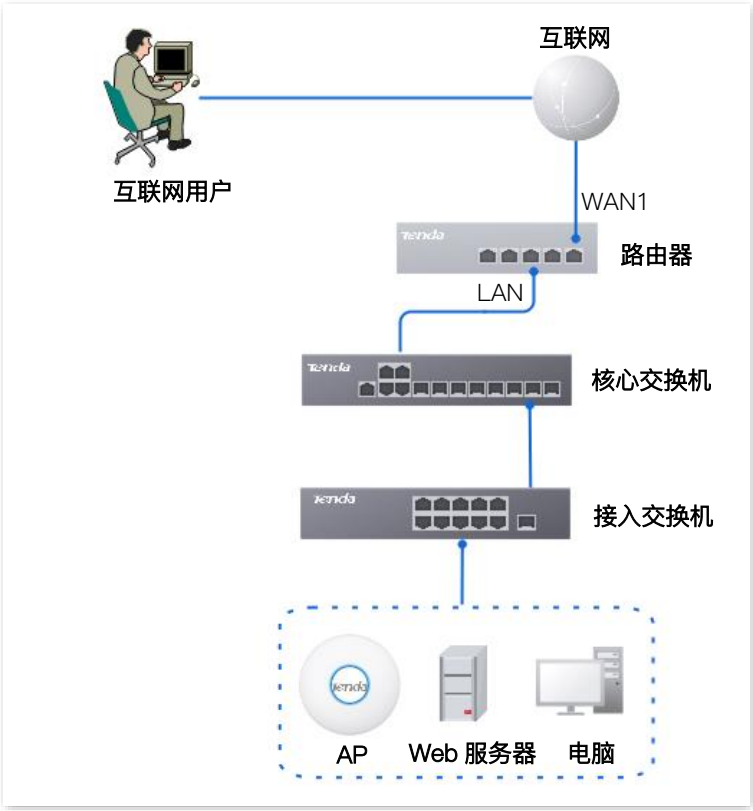
假设 Web 服务器信息如下：

- 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，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访问未经报备使用默认端口号 80 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

配置端口映射 > 给服务器主机分配固定 IP 地址 > 配置 DDNS

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置端口映射。

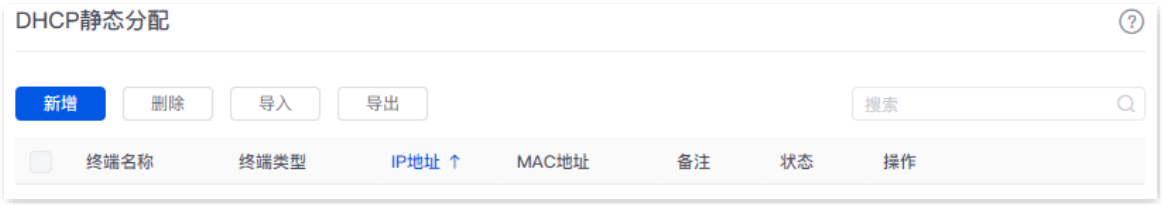
点击「更多」>「虚拟服务」>「端口映射」，配置如下规则。若有需要，可参考端口映射。

步骤 3 给服务器主机分配固定 IP 地址。

DHCP 静态分配规则参数示例如下所示。

终端名称：Web 服务器	固定分配给服务器主机的 IP 地址：192.168.0.250
服务器主机的 MAC 地址：C8:9C:DC:60:54:69	规则备注信息：Web 服务器地址

1 点击「网络」>「DHCP 设置」>「DHCP 静态分配」，然后点击 **新增**。



2 配置 DHCP 静态分配规则的相关参数后，点击 **保存**。

步骤 4 注册域名。

登录到 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 zhangsan123456，申请到的域名为 zhangsan.3322.org。

步骤 5 配置 DDNS。

1 点击「更多」>「虚拟服务」>「DDNS」，点击对应 WAN 口规则后的编辑，本例为“WAN1”。

2 选择您申请域名的 DDNS 服务提供商，本例为“3322.org”。

3 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“zhangsan123456”。

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

5 点击 保存 。

6 点击启用。

----完成

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

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。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。

参数说明

标题项	说明
接口	DDNS 策略生效的 WAN 接口。
连接状态	DDNS 服务的运行状态。
服务提供商	DDNS 的服务提供商。
用户名	登录 DDNS 服务的用户名。
域名	在 DDNS 服务商处申请的域名信息。服务提供商设置为除 oray 外的其他提供商时，需要手动输入在对应网站上申请的域名。

10.2.3 DNS 劫持

DNS，Domain Name Server，域名服务器。用于管理域名与 IP 地址之间的关系，将域名和 IP 地址相互映射。

启用 DNS 劫持后，可以设置域名与 IP 地址的对应规则。这样，当局域网用户访问规则中的域名时，直接解析为访问对应的映射 IP 地址。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「DNS 劫持」。您可以根据实际需要配置 DNS 劫持策略。

DNS 劫持配置举例

组网需求

某企业使用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。现要求局域网用户访问淘宝（taobao.com）、京东（jd.com）等网站时，访问的是路由器的 Web 管理页面。

方案设计

可以采用路由器的 DNS 劫持功能实现上述需求。假设路由器的 IP 地址为 192.168.0.252。

配置步骤

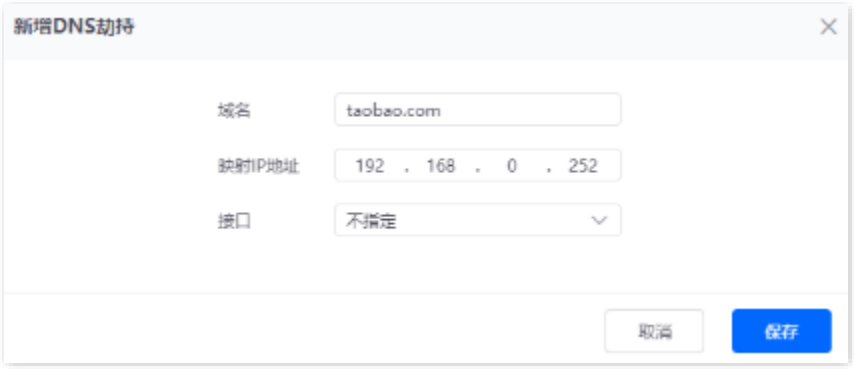
步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「更多」>「虚拟服务」>「DNS 劫持」，然后点击 新增 。

步骤 3 配置 DNS 劫持规则的各项参数后，点击 保存 。

1 输入淘宝的域名地址，本例为“taobao.com”。

2 输入映射的路由器 IP 地址，本例为“192.168.0.252”。



步骤 4 参考步骤 2~3 新增一条域名为京东（jd.com）的 DNS 劫持策略。

----完成

验证配置

局域网设备访问淘宝（taobao.com）、京东（jd.com）网站时，始终是访问到路由器 Web 管理页面。

参数说明

标题项	说明
域名	要解析为固定 IP 地址的域名。
映射 IP 地址	DNS 劫持后域名解析的 IP 地址，即用户访问指定域名时，会解析到该 IP 地址。
接口	数据从路由器出去的的接口。

10.2.4 IP 劫持

启用 IP 劫持后，局域网内的用户访问指定 IP 地址和端口时，直接劫持到映射 IP 地址对应端口服务。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「IP 劫持」。您可以根据实际需要配置 IP 劫持策略。

IP 劫持配置举例

组网需求

某企业使用路由器进行网络搭建，且已接入互联网，可以为局域网用户提供上网服务。现要求局域网用户访问 1.1.1.1 网址时，访问的是路由器的 Web 管理页面。

方案设计

可以采用路由器的 IP 劫持功能实现上述需求。假设路由器的管理 IP 地址为 192.168. 0.252，对应的端口号为 443。

配置步骤

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「更多」>「虚拟服务」>「IP 劫持」，然后点击 新增 。

步骤 3 输入目的 IP 地址，本例为“1.1.1.1”。

步骤 4 输入映射的路由器 IP 地址，本例为“192.168.0.252”。

步骤 5 输入端口号，本例为“443”。

步骤 6 点击 保存 。

----完成

验证配置

局域网设备访问 1.1.1.1:443 网址时，可以访问到路由器的 Web 管理页面。

参数说明

标题项	说明
目的 IP 地址	需要劫持访问的 IP 地址。
映射 IP 地址	劫持后访问的 IP 地址，即用户访问“目的 IP 地址:端口”时，都会解析到该 IP 地址。
端口	“映射 IP 地址”指定服务对应的端口号。访问指定服务端口时，才会劫持到“映射 IP 地址”。 提示 0 表示所有的端口。
接口	数据从路由器出去的接口。

10.2.5 UPnP

开启 UPnP（Universal Plug and Play，通用即插即用）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。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「UPnP」。

UPnP 功能默认关闭，您可以开启 UPnP 功能。

当 UPnP 功能已开启且局域网中运行支持 UPnP 的程序（如迅雷等）时，您可以查看应用程序发出请求时提供的端口转换信息。下图仅供参考。

10.2.6 端口镜像

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。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「端口镜像」。您可以根据实际需要配置端口镜像。端口镜像默认关闭。

端口镜像配置举例

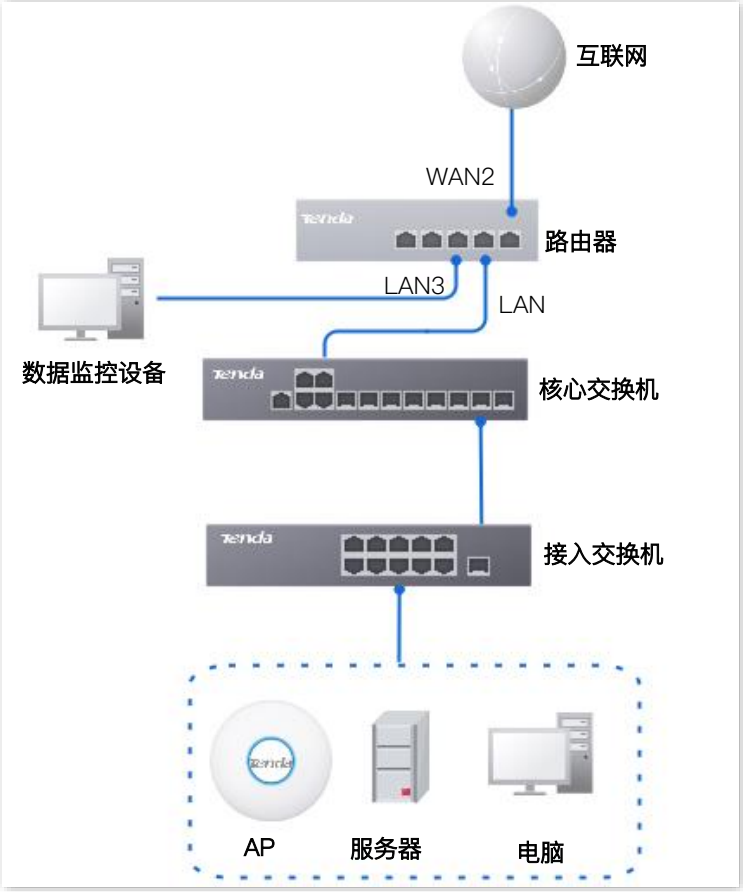
组网需求

某企业使用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

可以采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 登录到路由器 Web 管理页面。

步骤 2 点击「更多」>「虚拟服务」>「端口镜像」。

步骤 3 开启“镜像端口”功能。

步骤 4 选择“镜像端口”，本例为“LAN3”。

步骤 5 选择“被镜像端口”，本例为“LAN1、WAN2、LAN4、LAN5、LAN6”。

步骤 6 点击 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。

参数说明

标题项	说明
镜像端口	选择镜像的端口，被镜像端口的数据都会复制到该端口上。一般此接口下的设备会安装监控软件。
被镜像端口	选择被镜像端口。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。

10.2.7 端口映射

默认情况下，广域网中的用户不能访问局域网内的设备。端口映射开放了一个或多个服务端口，并以 IP 地址和内网端口来指定其对应的局域网服务器，之后，路由器将广域网中对此服务端口的请求定位到该局域网服务器上，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。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「端口映射」。

您可以根据实际情况配置端口映射策略。端口映射功能默认关闭。

端口映射配置举例

组网需求

某企业使用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

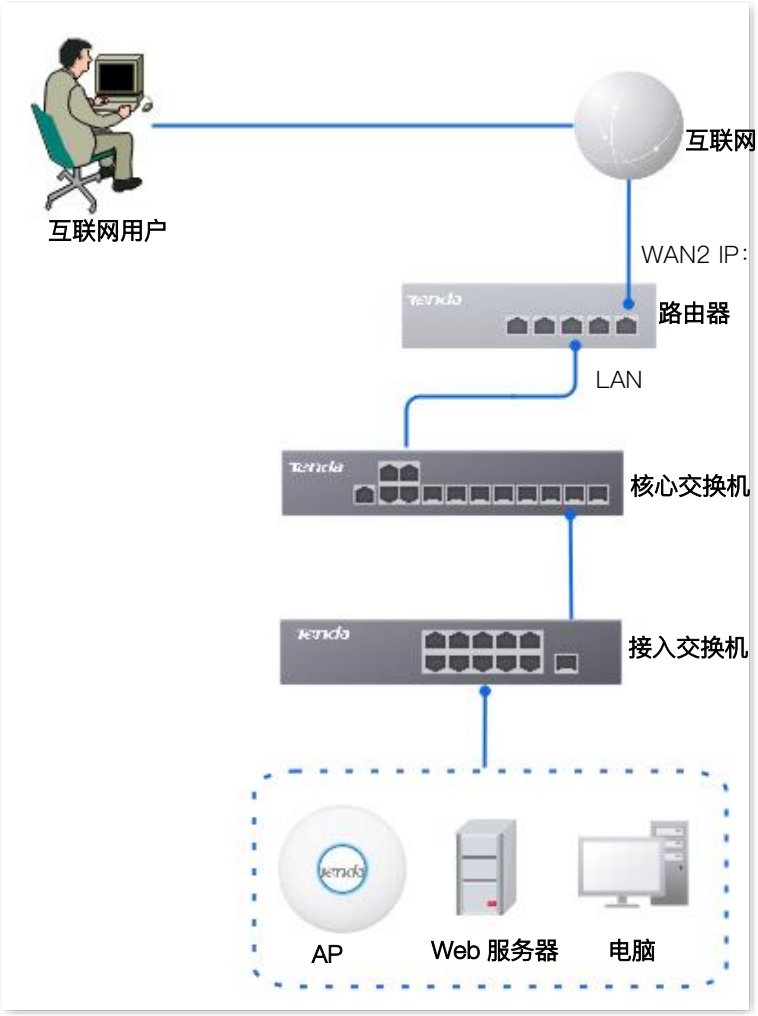
- 采用路由器的端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。假设路由器开放的外网端口为 9999。
- 采用路由器的 DHCP 静态分配功能，防止因 Web 服务器 IP 地址改变导致互联网用户访问企业内部 Web 服务器失败。

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，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访问未经报备使用默认端口号 80 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

配置端口映射 > 给服务器主机分配固定 IP 地址

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置端口映射。

端口映射规则参数示例如下所示。

内网 IP 地址：192.168.0.250	内网端口（Web 服务端口）：9999
外网端口：9999	协议：TCP
接口：WAN2	

1 点击「更多」>「虚拟服务」>「端口映射」。

2 开启“端口映射”功能后，点击 新增 。

3 配置端口映射规则的相关参数后，点击 保存 。

端口映射规则配置完成，如下图示。

步骤 3 给服务器主机分配固定 IP 地址。

DHCP 静态分配规则参数示例如下所示。

终端名称：Web 服务器	固定分配给服务器主机的 IP 地址：192.168.0.250
服务器主机的 MAC 地址：C8:9C:DC:60:54:69	规则备注信息：Web 服务器地址

1 点击「网络」>「DHCP 设置」>「DHCP 静态分配」，然后点击 新增 。

2 配置 DHCP 静态分配规则的相关参数后，点击 保存 。

----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://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”。

您可以在连接状态页面找到路由器当前的 WAN 口 IP 地址。

如果对应 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: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。

参数说明

标题项	说明
内网 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。

标题项	说明
协议	内网服务的协议类型。设置时，如果不确定服务的协议类型，可以选择“TCP&UDP”。
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。
备注	端口映射策略的备注信息。

10.2.8 DNS 缓存

DNS，Domain Name Server，域名服务器。用于管理域名与 IP 地址之间的关系，将域名和 IP 地址相互映射。用户在访问某域名时，实际上是通过 DNS 域名解析然后访问到了相应的 IP 地址。

开启 DNS 缓存功能后，系统在用户首次访问某域名时，在本地电脑缓存了域名和 IP 地址的映射关系。这样，用户再次访问该域名时，不用通过域名解析，直接访问到 IP 地址，加快了上网速度，提升上网体验。

登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「DNS 缓存」。

您可以开启/关闭 DNS 缓存功能。DNS 缓存功能默认开启，显示如下。

10.3 维护服务

10.3.1 远程 WEB 管理

一般情况下，只有接到路由器 LAN 口或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。

登录到路由器 Web 管理页面后，点击「更多」>「维护服务」>「远程 WEB 管理」。

您可以开启或关闭远程 WEB 管理，也可以限定能够远程登录到本路由器的主机。远程 Web 管理默认关闭。

远程 WEB 管理配置举例

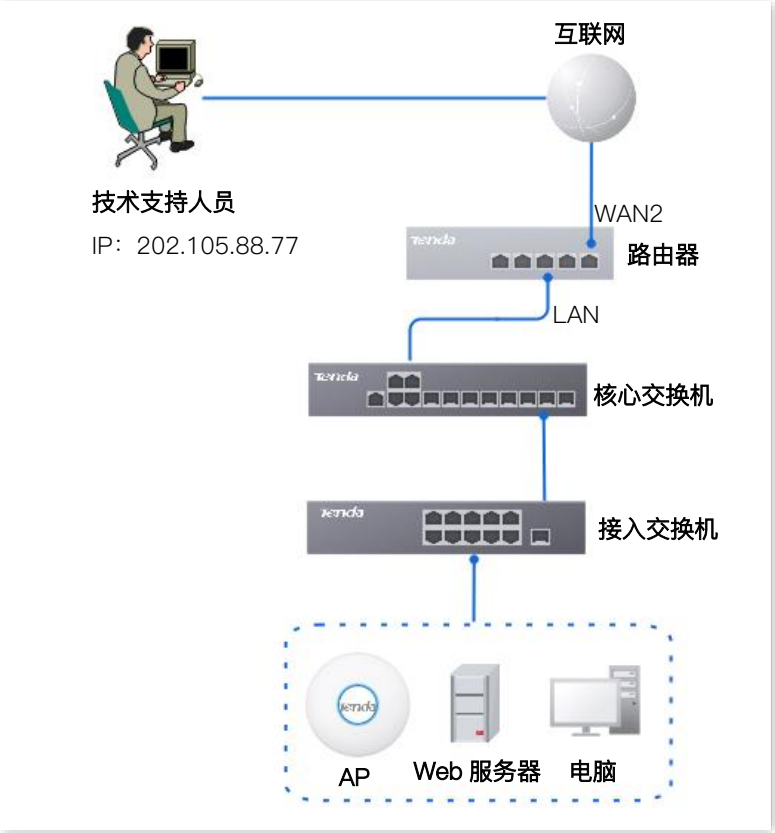
组网需求

某企业使用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

由器管理页面进行分析并解决。

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 登录到路由器 Web 管理页面。

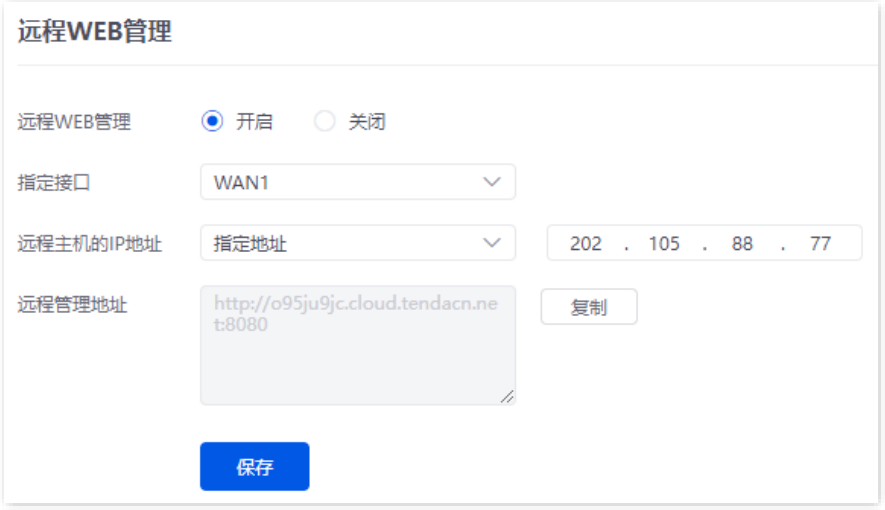
步骤 2 点击「更多」>「维护服务」>「远程 WEB 管理」。

步骤 3 开启“远程 WEB 管理”功能。

步骤 4 选择远程访问路由器时所使用的 WAN 口，本例为“WAN2”。

步骤 5 选择“指定地址”，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 6 点击 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“远程管理地址”，即可登录路由器管理页面并对其进行管理。

参数说明

标题项	说明
远程 WEB 管理	开启/关闭远程 WEB 管理功能。
指定接口	选择路由器的 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。 - 所有地址：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。 - 指定地址：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）。
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。

10.3.2 安全设置

登录到路由器 Web 管理页面后，点击「更多」>「维护服务」>「安全设置」。

您可以进行路由器安全设置。

参数说明

标题项	说明
防 WAN 口 Ping	开启/关闭防 WAN 口 Ping 功能。 开启后，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。
内网 DDoS 攻击防御	开启/关闭内网 DDoS 攻击防御功能。 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。
ARP 攻击防御	开启/关闭 ARP 攻击防御功能。 开启后，路由器可以识别局域网的 ARP 欺骗，并记录攻击者的 MAC 地址。
二元绑定	开启后，仅“DHCP 静态分配”列表中的设备才可以上网。
Web 页面登录方式	路由器 Web 管理页面登录方式。 - HTTPS，Hyper Text Transfer Protocol Secure，超文本传输安全协议。它在 HTTP 的基础上利用 SSL/TLS 加密数据包，建立全通道，从而保证了数据传输过程的安全性。通过 HTTPS 访问，可以保证数据传输的安全性和网站的真实性。 - HTTP，Hyper Text Transfer Protocol，超文本传输协议。一种浏览器和服务器之间进行沟通的规范。
Web 闲置超时时间	当您登录到路由器的管理页面后，如果在所设置的“WEB 闲置超时时间”内没有任何操作，系统将自动退出登录，保障网络安全。

10.3.3 云维护

概述

Tenda 掌中宝云管理系统是 Tenda 公司提供的一个云平台，可以统一管理支持云维护的 Tenda 设备。

路由器支持被该云平台管理。您可以通过 Tenda 掌中宝云平台 Web（https://cloudfi.tenda.com.cn）或 Tenda 掌中宝 App，将路由器加入云平台后进行远程管理。

登录到路由器 Web 管理页面后，点击「更多」>「维护服务」>「云维护」。

您可以配置路由器的云维护功能。云维护功能默认关闭，下图仅供参考。

参数说明

标题项	说明
管理模式	云维护的管理模式。 - 云托管：适用于集中统一管理项目并配置维护项目的场景。路由器可被 Tenda 掌中宝云管理系统管理，且相关功能的配置信息可由 Tenda 掌中宝云管理系统下发，登录路由器的 Web 管理页面时，也可以进行功能配置。 - 本地托管：适用于集中统一管理并查看项目的场景。路由器可被 Tenda 掌中宝云管理系统管理，但是功能不能修改，所有功能的配置需在路由器的 Web 管理页面完成。
云平台唯一码	用于指定设备关联的云平台账号。可以在 Tenda 掌中宝云平台 Web 管理页面（https://cloudfi.tenda.com.cn）或 Tenda 掌中宝 App 获取。
设备信息上报	开启后，路由器才能被云平台管理，路由器的配置信息将会上报到云平台。

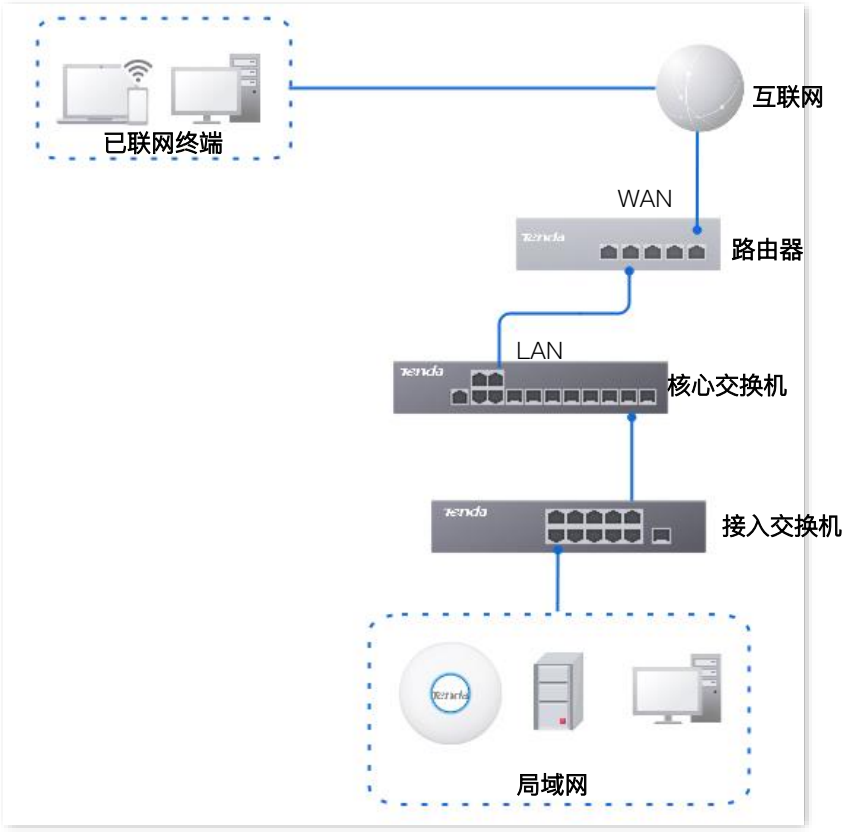
Tenda 掌中宝云平台 Web 配置举例

组网需求

某企业使用路由器进行网络搭建，已成功接入互联网。现在想要实现远程管理路由器并下发相关配置。

方案设计

可以采用路由器的云维护功能+Tenda 掌中宝云平台 Web（https://cloudfi.tenda.com.cn）实现上述需求。



配置步骤

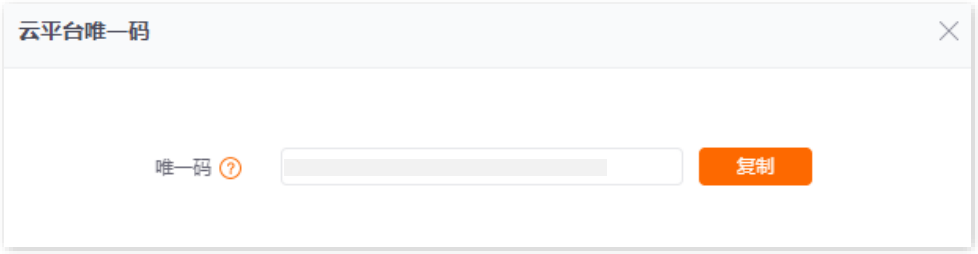
提示

配置路由器的云维护功能之前，请确保路由器已成功联网。

步骤 1 获取云平台唯一码。

1 在已联网的电脑上访问 https://cloudfi.tenda.com.cn，登录到 Tenda 掌中宝云平台 Web 管理页面。

2 点击 Tenda 掌中宝云平台 Web 管理页面右上角的“新建”>“云平台唯一码”，然后复制该云平台唯一码。



步骤 2 开启路由器的云维护功能。

1 登录到路由器 Web 管理页面，点击「更多」>「维护服务」>「云维护」。

2 开启云维护功能。

3 设置管理模式，输入云平台唯一码，开启“设备信息上报”功能，点击 保存 。如果弹出提示窗口，请确认提示信息后，点击 确定 。

步骤 3 在 Tenda 掌中宝云平台 Web 上将路由器添加到项目中。

1 登录 Tenda 掌中宝云平台 Web 管理页面，点击右上角的“新建”>“设备加入提醒”。

2 选择要加入项目的路由器，点击 添加设备到项目 。图示仅供参考。

3 选择要将路由器加入的项目。下图仅供参考。

- 如果已创建项目，选择“已有项目”，在“项目名称”下拉菜单选择相应的项目，然后点击 确认 。

- 如果要新建项目，选择“新建项目”，然后设置“项目名称”、“项目场景”与“项目位置”，然后点击 确认 。

加入成功。进入「项目列表」页面可查看相关项目信息，进入具体项目的页面即可查看已添加设备。下图仅供参考。

----完成

验证配置

路由器可以通过 Tenda 掌中宝云管理系统进行管理，相关配置信息可由云平台下发。

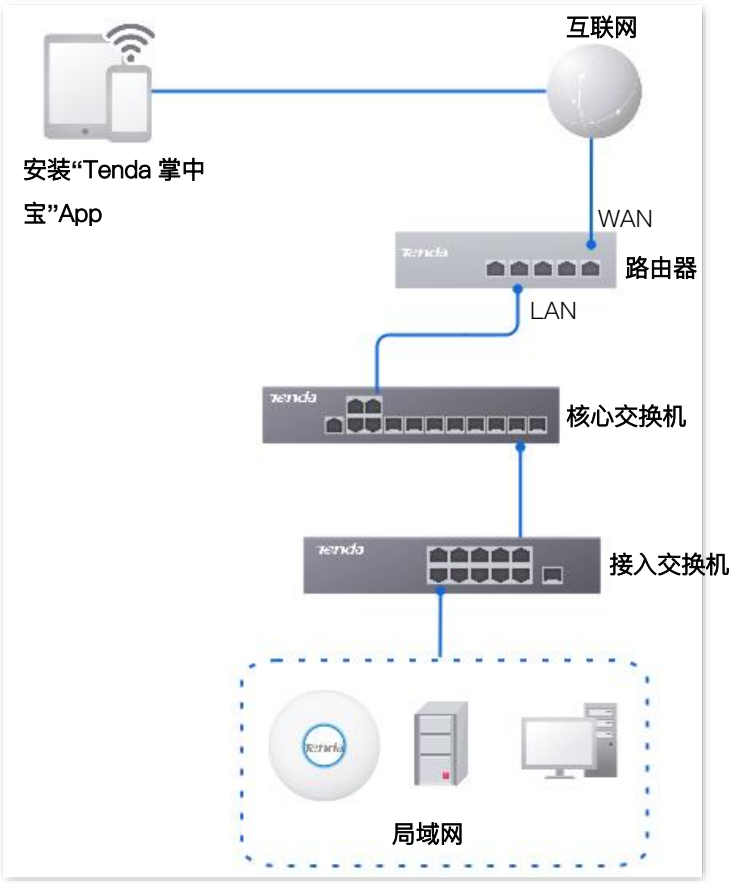
Tenda 掌中宝 App 配置举例

组网需求

某企业使用路由器进行网络搭建，已成功接入互联网。现在想要实现远程管理路由器并下发相关配置。

方案设计

可以采用路由器的云维护功能+Tenda 掌中宝 App 实现上述需求。



配置步骤（方法 1：推荐）

提示

配置路由器的云维护功能之前，请确保路由器已成功联网。

步骤 1 安装并登录 Tenda 掌中宝 App。

扫码下载“Tenda 掌中宝”App

步骤 2 手机等移动终端连接局域网内 AP 的 Wi-Fi。

步骤 3 运行 Tenda 掌中宝 App，将路由器添加至 Tenda 掌中宝 App。

1 新建项目。（如已创建，可跳过此步骤）

2 进入待添加路由器的项目，界面自动弹出发现路由器，然后根据提示将路由器添加至项目中。

具体方法可在 Tenda 掌中宝 App 的「帮助中心」页面查看 Tenda 掌中宝 App 的帮助文档。

配置步骤（方法 2）

提示

配置路由器的云维护功能之前，请确保路由器已成功联网。

步骤 1 登录 Tenda 掌中宝 App，获取云平台唯一码。

扫码下载“Tenda 掌中宝”App

步骤 2 开启路由器的云维护功能。

1 登录到路由器 Web 管理页面，点击「更多」>「维护服务」>「云维护」。

2 开启云维护功能。

3 设置管理模式，输入云平台唯一码，开启“设备信息上报”功能，点击 保存 。如果弹出提示窗口，请确认提示信息后，点击 确定 。

步骤 3 在 Tenda 掌中宝 App 上新建项目。（如已创建，可跳过此步骤）

步骤 4 在**设备加入提醒**页面，根据提示将路由器添加到项目中。

具体方法可在 Tenda 掌中宝 App 的「帮助中心」页面查看 Tenda 掌中宝 App 的帮助文档。

验证配置

路由器可以通过 Tenda 掌中宝云管理系统进行管理，相关配置信息可由云平台下发。

10.3.4 SSH 维护

本功能适用于专业人员需要远程维护网络时使用。开启后，专业人员可以通过 SSH 远程连接到本路由器，从而进行远程维护。

登录到路由器 Web 管理页面后，点击「更多」>「维护服务」>「SSH 维护」。

您可以配置远程调试功能。SSH 维护功能默认关闭。

通过 SSH 终端工具远程接入路由器

开启路由器远程调试功能

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「更多」>「维护服务」>「SSH 维护」。

步骤 3 开启 SSH 维护功能，其他参数保持默认，点击 保存 。

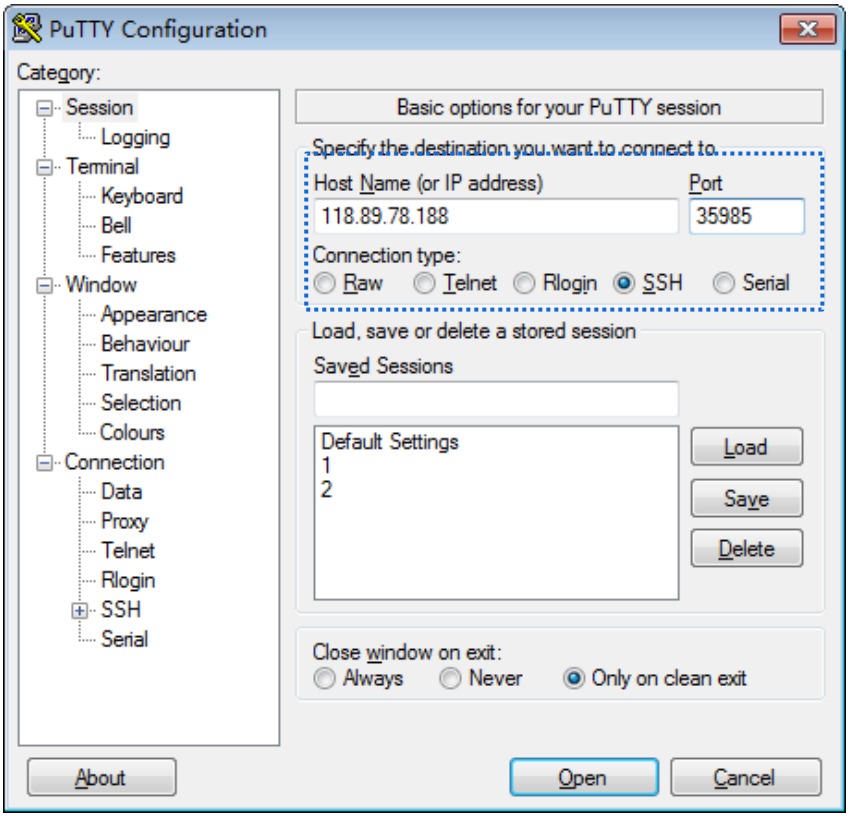
稍等片刻，当状态显示已连接时，您可以在 SSH 工具输入“SSH 维护地址”远程接入路由器了。

通过 SSH 终端工具远程接入路由器

步骤 1 在远端已联网的电脑上运行 SSH 终端工具，下文以 Putty 为例。

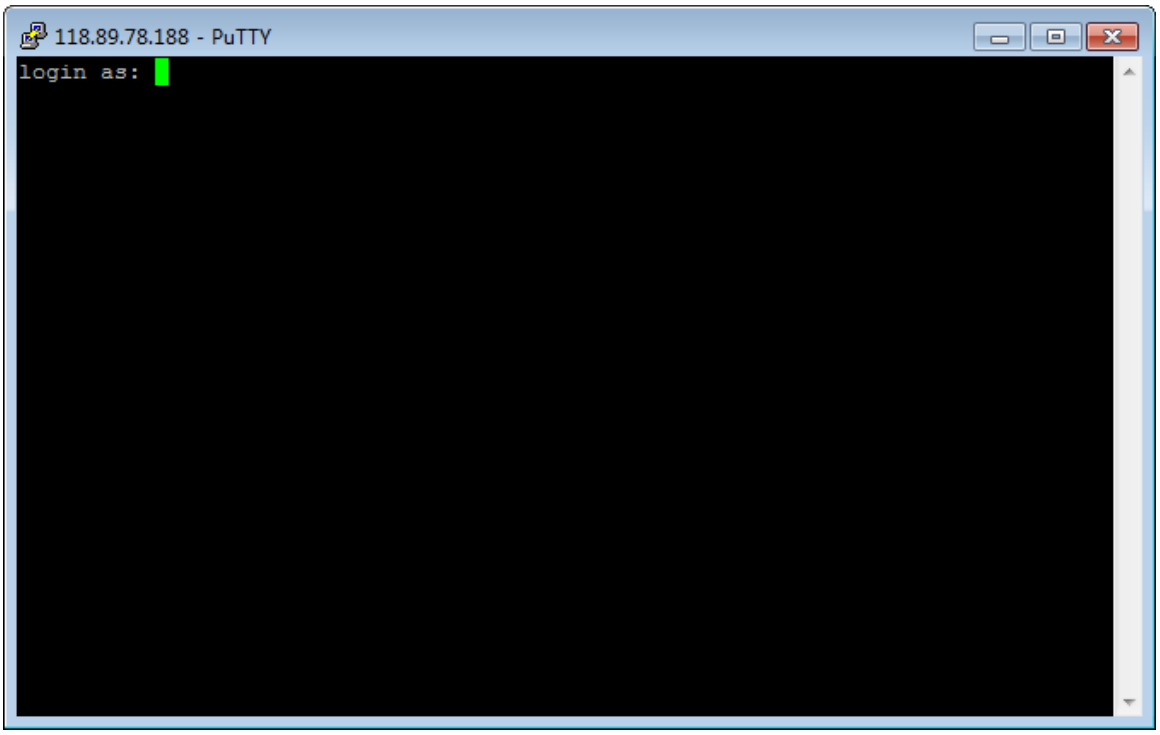
步骤 2 选择“Connection type”为“SSH”。

步骤 3 在远程调试地址 (Host Name or IP adress) 及端口输入路由器上的 SSH 维护地址，点击 Open 。下图仅供参考。



----完成

成功连接到路由器。



参数说明

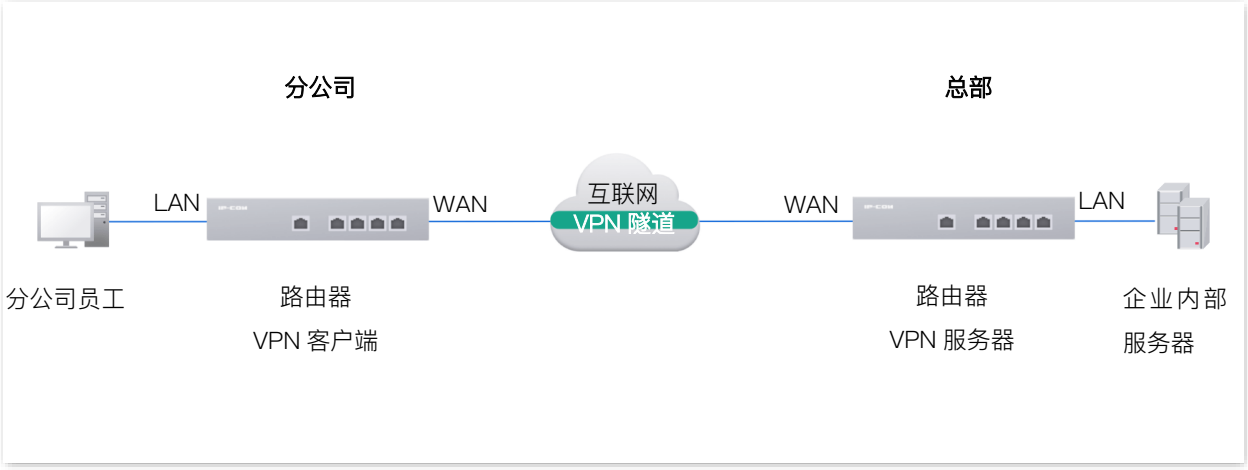
标题项	说明
SSH 维护	开启/关闭 SSH 维护功能。
设备公钥	本设备的 RSA 公钥。已预置到默认服务器的授权列表。如果不使用默认服务器，需要在自定义的服务器上添加设备公钥。
服务器 IP 地址	外网服务器的 IP 地址，必须是公网 IP 地址。留空表示使用默认的服务器。
服务器端口	外网服务器的服务端口。留空表示使用默认的服务器端口。
SSH 维护地址	远程 SSH 连接本设备的地址。

10.4 VPN

10.4.1 概述

VPN（Virtual Private Network，虚拟专用网），是一个建立在公用网（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。使用 VPN 技术，可以让企业的分公司员工在方便共享对方或公司总部局域网资源的同时，保证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。



常见的 VPN 服务有 PPTP (Point to Point Tunneling Protocol, 点到点隧道协议), L2TP (Layer 2 Tunneling Protocol，第二层隧道协议)、OpenVPN（开源 VPN 服务）和 IPSec（IP Security，IP 安全性）。

- **二层隧道协议：PPTP、L2TP**

二层隧道协议，用于传输二层（数据链路层）网络协议，此时在隧道内传输的是数据链路层的帧。

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

- **三层隧道协议：IPSec**

三层隧道协议，用于传输三层（网络层）网络协议，此时在隧道内传输的是网路层的分组。

IPSec 协议把数据封装在隧道协议中，依靠第三层进行传输只适用于 TCP/IP 网络。

三层隧道协议与二层隧道协议相比，具有更好的安全性和可靠性。第二层隧道一般中止在用户侧设备上，对用户端的安全及防火墙技术要求很高；而第三层隧道一般中止在 ISP(Internet Service Provider，互联网服务提供商）网关，不会对用户端的安全性有较高的需求。

- **OpenVPN**

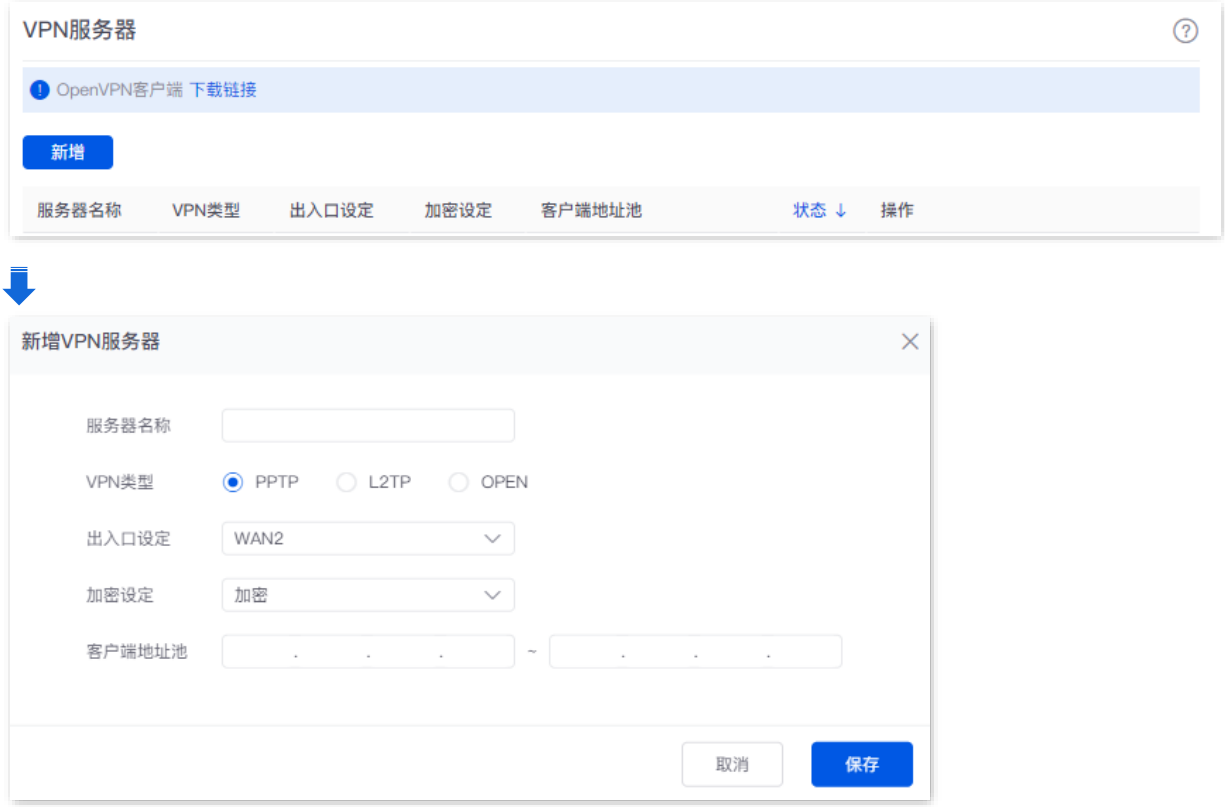
OpenVPN 基于 SSL/TLS（安全套接层/传输层安全）协议，工作在应用层和传输层之间。使用应用层的机制来建立和管理 VPN 连接，同时依赖传输层的 TCP（传输控制协议）或 UDP（用户数据报协议）进行数据传输。安全性在二层隧道协议（PPTP、L2TP）和三层隧道协议（IPSec）之间。

10.4.2 PPTP/L2TP/OpenVPN

配置 PPTP/L2TP/OpenVPN 服务器

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

登录到路由器 Web 管理页面，在「更多」>「VPN 服务」>「VPN 服务器」页面，点击 新增，配置各项参数，然后点击 保存。



参数说明

标题项	说明
服务器名称	VPN 服务器的名称。
VPN 类型	路由器使用的 VPN 协议类型。 - 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。 - OPEN：路由器作为 OpenVPN 服务器，接受 OpenVPN 客户端的连接。
出入口设定	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”。
加密设定	仅 PPTP 和 L2TP 服务器支持。 - PPTP：是否启用 128 位数据加密。PPTP 客户端与 PPTP 服务器双方的加密设置需保持一致，否则将不能正常通信。 - L2TP：是否启用 IPSec 对数据报文加密（L2TP over IPsec）。L2TP 客户端与 L2TP 服务器双方的配置应保持一致，否则将不能正常通信。
预共享密钥	启用 IPSec 对数据报文加密时，使用该预共享密钥来验证身份。L2TP 客户端与 L2TP 服务器双方的配置应保持一致，否则将不能正常通信。仅 L2TP 服务器支持。
IKE 策略	建立安全的管理通道，用于协商后续的 IPsec SA（安全关联）。这是 VPN 连接的第一阶段。仅 L2TP 服务器支持。
转换集	定义实际保护用户数据的加密参数。这是 VPN 连接的第二阶段，用于创建 IPsec SA。仅 L2TP 服务器支持。

标题项	说明
协商模式	协商模式必须与对端设置相同。仅 L2TP 服务器支持。 - 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。 - 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。
本地 ID 类型	本地网关标识。仅 L2TP 服务器支持。 - IP 地址：本地路由器使用对应 WAN 口 IP 地址与对端网关协商。 - NAME：选此项时，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。
客户端地址池	VPN 服务器可分配给 VPN 客户端的 IP 地址范围。仅 PPTP 和 L2TP 服务器支持。
服务器模式	OpenVPN 服务器的认证模式，仅 OpenVPN 服务器支持。 - 账号密码：OpenVPN 客户端需要使用 OpenVPN 服务器提供的账号和密码才能连接到 OpenVPN 服务器，服务器账号和密码在用户管理配置。 - 证书：基于公钥基础设施（PKI）体系。服务器和客户端都有自己的数字证书，数字证书包含了公钥、所有者信息等内容。服务器会验证客户端证书的有效性，包括检查证书是否由信任的证书颁发机构（CA）颁发、证书是否过期、证书的签名是否合法等。同样，客户端也可以验证服务器证书的合法性。只有双方证书验证通过后，才能建立 VPN 连接。 - 账号+证书：同时使用账号密码和证书 2 种认证模式。
协议	数据传输协议。仅 OpenVPN 服务器支持。 - TCP：数据传输具有可靠性保证，能够确保数据有序接收并且重传丢失的数据，传输速度相对较慢。适用于对数据准确性较高的场景。 - UDP：数据传输更加高效，适用于对实时性要求较高但对数据丢失不太敏感的场景，如视频通话等。
端口号	OpenVPN 服务使用的端口号，建议设为非熟知端口（1024~65535），以确保服务正常启动。
IP 地址	OpenVPN 地址池网段，地址池首个可用地址分配给服务器使用，其余地址分配给客户端，如设置地址范围为 10.10.99.0/24，则服务器端 VPN 虚拟地址为 10.10.99.1。注意不能与路由器本身 LAN 口网点地址重合。 仅 OpenVPN 服务器支持。
下发路由配置	VPN 服务器给 VPN 客户端下发的路由配置，指导客户端通过哪条路径发送数据包到目标网络。

点击--**展开高级设置**--显示 OpenVPN 的高级参数，下图仅供参考。

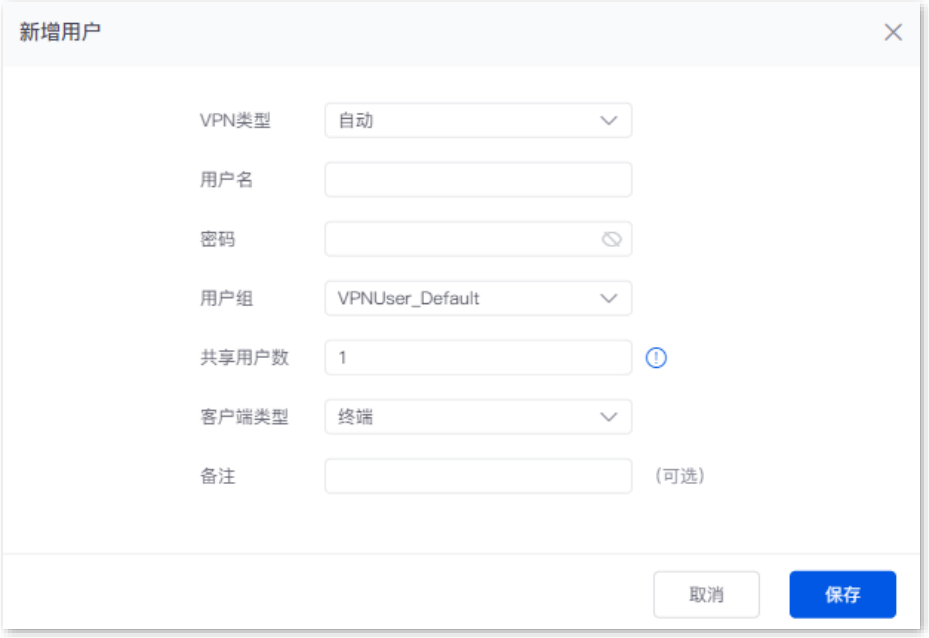
参数说明

标题项	说明
TLS 身份验证	开启后，TLS 身份验证工作在传输层上。在 OpenVPN 服务器和客户端建立安全传输通道（如 SSL/TLS 加密连接）过程中不仅进行身份验证，TLS 协议还确保了数据在传输过程的安全性。但也会占用较多系统资源和增加网络时延。（OpenVPN 客户端需 2.4.0 版本以上）
数据压缩	开启后，OpenVPN 服务器和客户端之间传输数据时，通过一定的算法将数据的大小进行缩减，从而占用更少的带宽，提高传输效率。服务器和客户端设置需保持一致。
流量全部走 VPN	开启后，OpenVPN 客户端将所有的流量（除了发往本地局域网的流量）都通过 VPN 隧道发送到 OpenVPN 服务器。
数据加密算法	数据加密的方式。 如果在服务器端将此参数设置为“Auto”，则可以在客户端将此参数设置为任何选项。如果服务器端配置了特定的加密算法，客户端必须选择相同的加密算法，否则将导致连接失败。
下发 DNS 配置	OpenVPN 服务器向 OpenVPN 客户端下发 DNS 配置，确保客户端在通过 VPN 访问网络资源时能够正确解析域名。
认证摘要算法	它是一种将任意长度的数据转换为固定长度哈希值（或称为消息摘要）的函数，也称为哈希函数（Hash Function）。这个哈希值就像是数据的“指纹”，用于验证数据的完整性和真实性。

用户管理

登录到路由器 Web 管理页面后，点击「更多」>「VPN 服务」>「用户管理」。

您可以配置 PPTP/L2TP/OpenVPN 用户账号，即，开启 PPTP/L2TP/OpenVPN 服务器时，VPN 用户拨入路由器的 VPN 时需要使用的账号。



参数说明

标题项	说明
VPN 类型	用户的服务类型。
用户名	VPN 客户端进行 VPN 连接时输入的用户名。
密码	VPN 客户端进行 VPN 连接时输入的密码。
用户组	将 VPN 账号加入到 VPN 用户组中。VPN 用户组需事先在「审计」>「分组策略」>「用户组」配置好。仅 PPTP 和 L2TP 服务器支持。
共享用户数	允许同时通过该 VPN 账号连接的最大用户数。
客户端类型	VPN 客户端类型，当 VPN 客户端为单个主机时，请选择客户端类型为终端；当 VPN 客户端为一个网络时，请选择客户端类型为网络设备。仅 PPTP 和 L2TP 服务器支持。
客户端网段/子网	客户端内网 IP 地址范围。客户端类型为网络设备时需要输入。仅 PPTP 和 L2TP 服务器支持。

用户列表

登录到路由器 Web 管理页面后，点击「更多」>「VPN 服务」>「用户列表」。

您可以查看拨入路由器 VPN 服务器的 VPN 客户端详细信息。

配置 PPTP/L2TP/OpenVPN 客户端

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

登录到路由器 Web 管理页面，在「更多」>「VPN 客户端」页面，打开“VPN 客户端”开关，配置各项参数，然后点击 保存 。

参数说明

标题项	说明
VPN 客户端	开启/关闭 VPN 客户端功能。 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：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。 - OPEN：要连接的 VPN 服务器是 OpenVPN 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	要连接的 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。“客户端类型”为“PPTP”或“L2TP”时支持。
用户名	VPN 服务器分配给 VPN 客户端的用户名和密码。

标题项	说明
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。“客户端类型”为“PPTP”或“L2TP”时支持。
预共享密钥	“客户端类型”为“L2TP”，且“加密”为“开启”时支持，和对端服务器的配置保持一致。
IKE 策略	
转换集	
协商模式	
本地 ID 类型	
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。“客户端类型”为“PPTP”或“L2TP”时支持。
服务器内网网段	VPN 服务器端局域网的网段和子网掩码。“客户端类型”为“PPTP”或“L2TP”时支持。
客户端配置	“客户端类型”为“OPEN”时支持。配置客户端的方式。 - 文件导入：导入 OpenVPN 服务器发来的配置文件，将自动填充所有参数。 - 界面配置：手动配置所有参数。
服务器模式	需和对端 OpenVPN 服务器的认证模式保持一致。
客户端配置	“客户端配置”为“文件导入”时，导入对端 OpenVPN 服务器的配置文件。

10.4.3 PPTP/L2TP VPN 配置举例

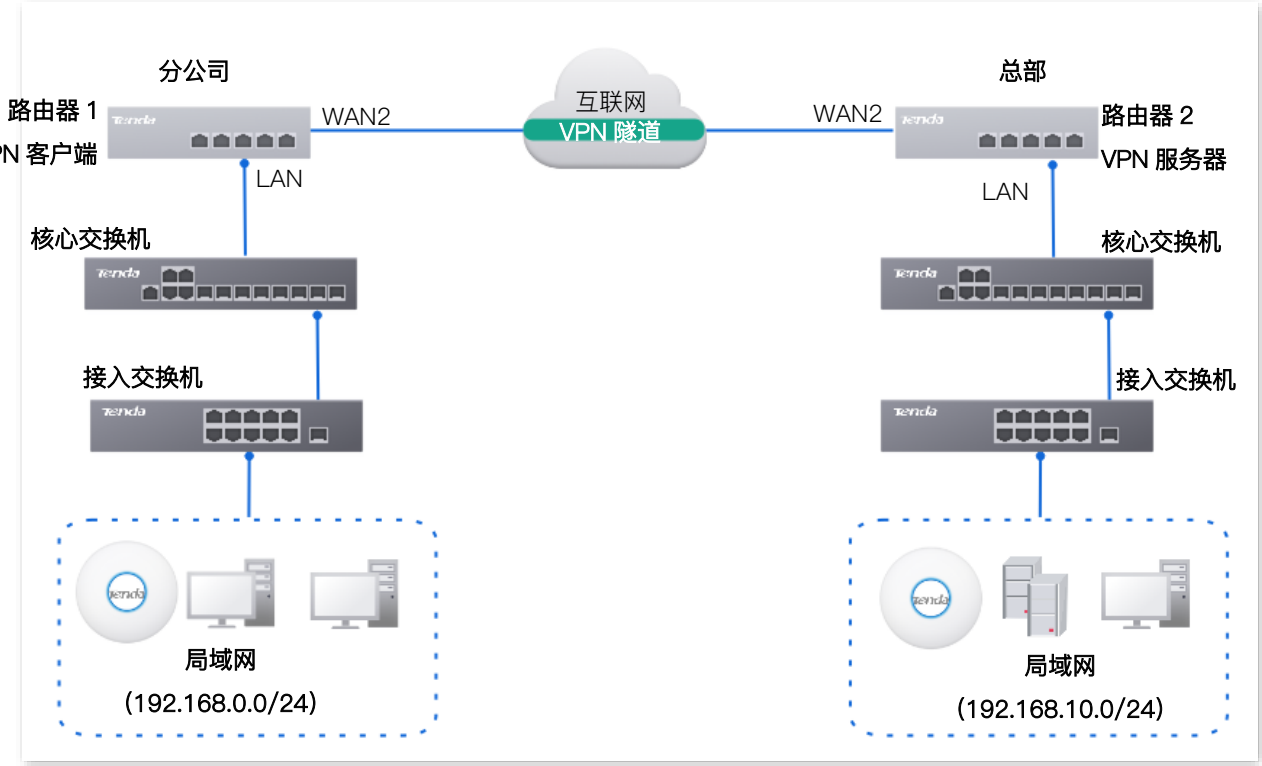
组网需求

某企业总部和分公司都使用路由器 M80–F 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

将总部路由器设置为 VPN 服务器，分公司路由器设置为 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。

假设总部路由器的 WAN2 IP 地址为 202.105.11.22。



配置步骤

配置总部路由器为 VPN 服务器 > 配置分公司路由器为 VPN 客户端

一、配置总公司路由器为 VPN 服务器

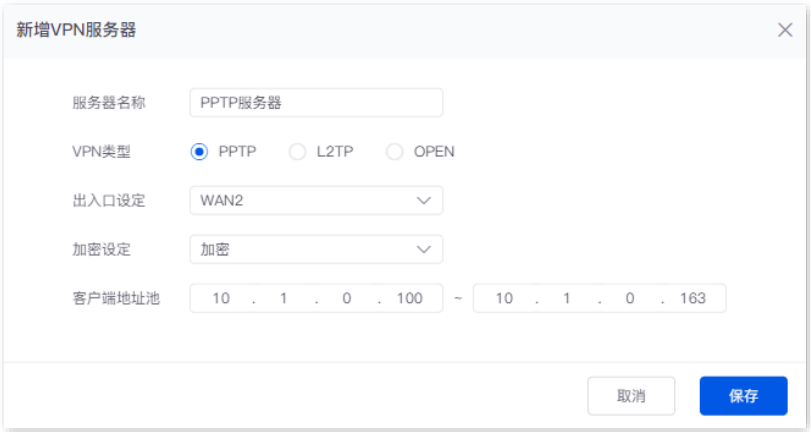
步骤 1 登录到总公司路由器的 Web 管理页面。

步骤 2 配置 PPTP 服务器。

PPTP 服务器参数示例如下表所示。

服务器名称	出入口设定	加密设定	客户端地址池
PPTP 服务器	WAN2	加密	10.1.0.100~10.1.0.163

进入「更多」>「VPN 服务」>「VPN 服务器」页面，点击 新增，配置 PPTP 服务器相关参数，点击 保存。



步骤 3 配置 PPTP 用户。

PPTP 用户参数示例如下表所示。

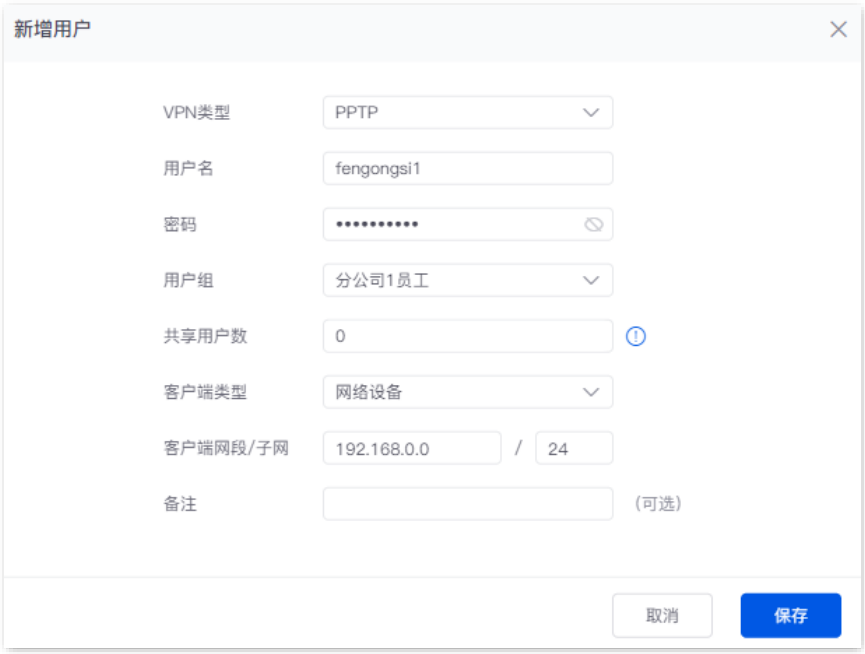
VPN 类型	用户名&密码	共享用户数	用户组	客户端类型	客户端网络
PPTP	fengongsi1	无限制	分公司 1 员工	网络设备	192.168.0.0/24

1 配置 VPN 用户组。

进入「审计」>「分组策略」>「用户组」页面，点击 新增 ，然后创建一个分公司的 VPN 用户组，点击 保存 。

2 配置 PPTP 用户账号。

进入「更多」>「VPN 服务」>「用户管理」页面，点击 新增 ，配置 PPTP 用户相关参数，然后点击 保存 。



二、配置分公司路由器为 VPN 客户端

步骤 1 登录到分公司路由器的 Web 管理页面。

步骤 2 配置 PPTP 客户端。

1 点击「更多」>「VPN 客户端」，打开 VPN 客户端开关。

2 选择“客户端类型”与 VPN 服务器侧一致，本例为“PPTP”。

3 指定 VPN 客户端与服务器建立隧道的 WAN 口，本例为“WAN2”。

4 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”。

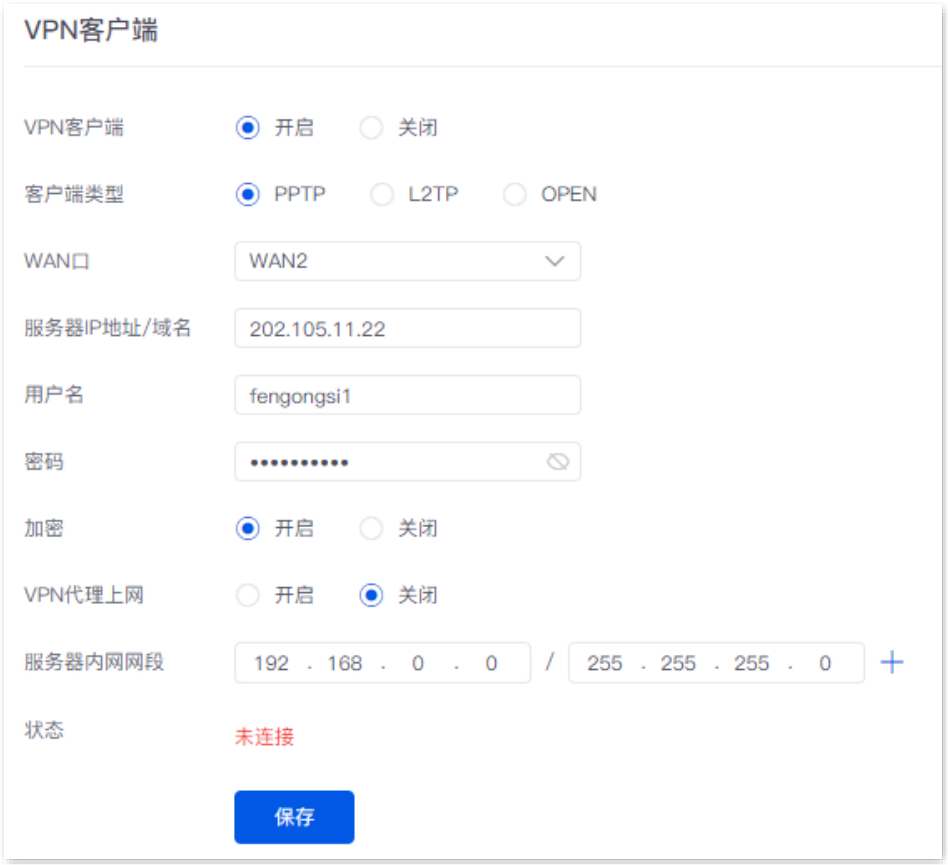
5 输入 VPN 服务器分配的用户名，本例为“fengongsi1”。

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

7 选择“加密”为“开启”，与 VPN 服务器侧配置保持一致。

8 输入 VPN 服务器内网的网段，本例为“192.168.0.0”/“255.255.255.0”。

9 点击 保存 。



---完成

当页面的状态显示为“已连接”时，VPN 连接成功。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。

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：

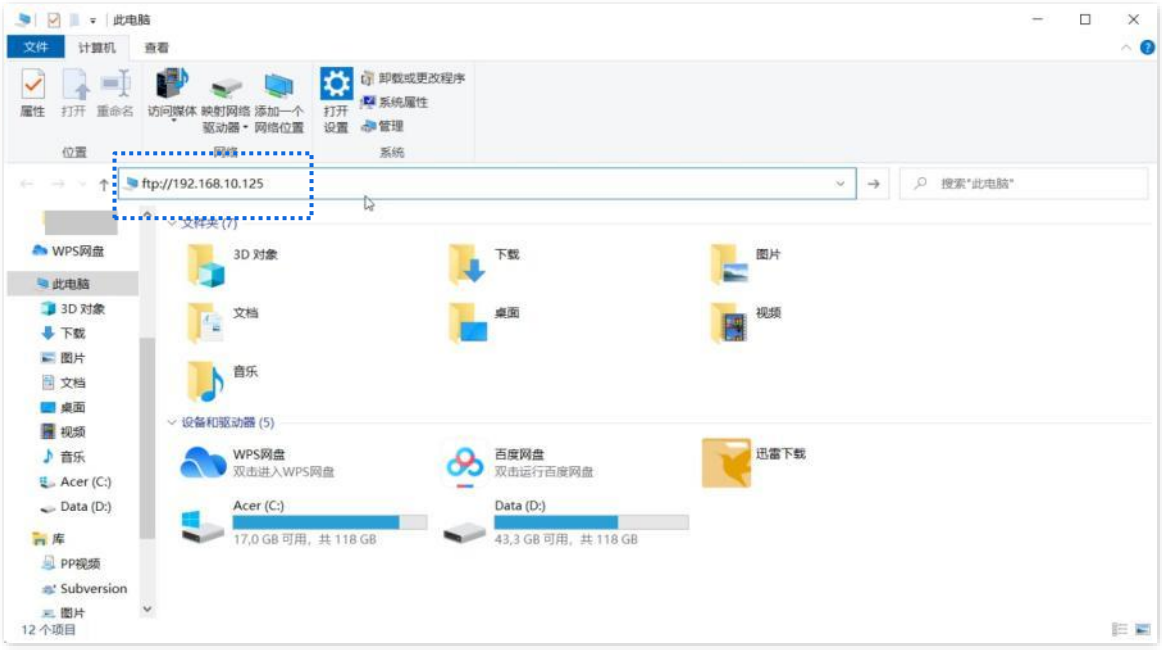
- FTP 服务器 IP 地址为 192.168.10.125
- FTP 服务端口为 21
- FTP 服务器登录用户名为 zhangsan，密码为 Zs123456@

当分公司员工访问总部项目资料时，步骤如下：

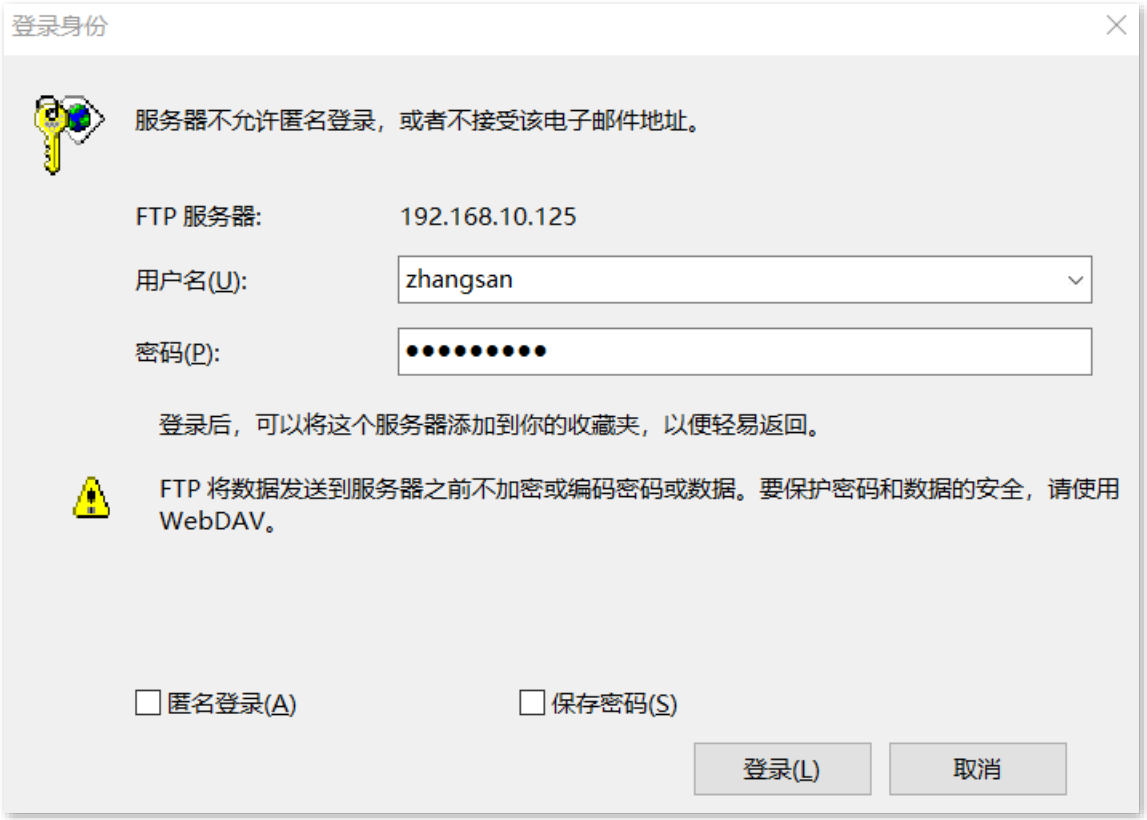
步骤 1 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 ftp://192.168.10.125。

提示

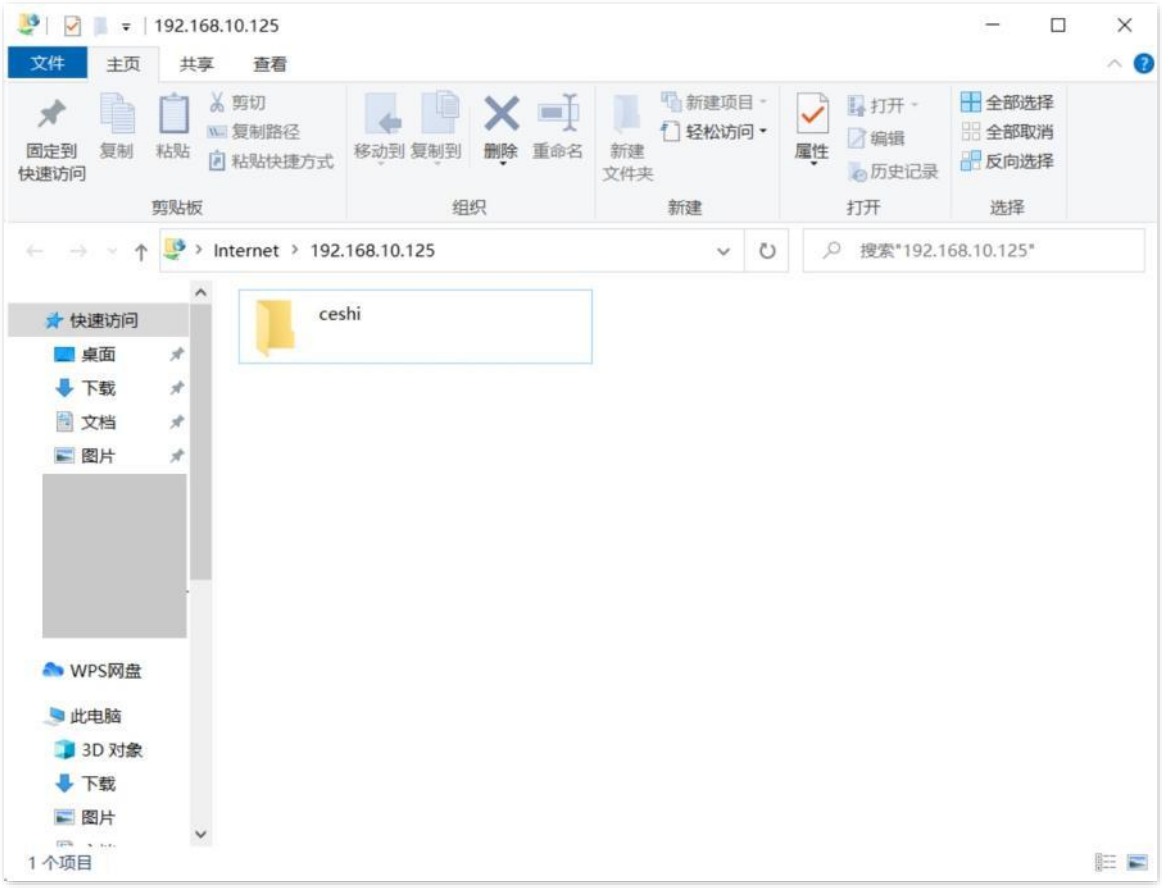
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



步骤 2 输入登录用户名与密码，本例用户名为“zhangsan”，密码为“Zs123456@”，然后点击 登录 。



访问成功。



10.4.4 L2TP over IPSec VPN 配置举例

组网需求

某公司使用路由器进行网络搭建，并成功接入互联网。出差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。

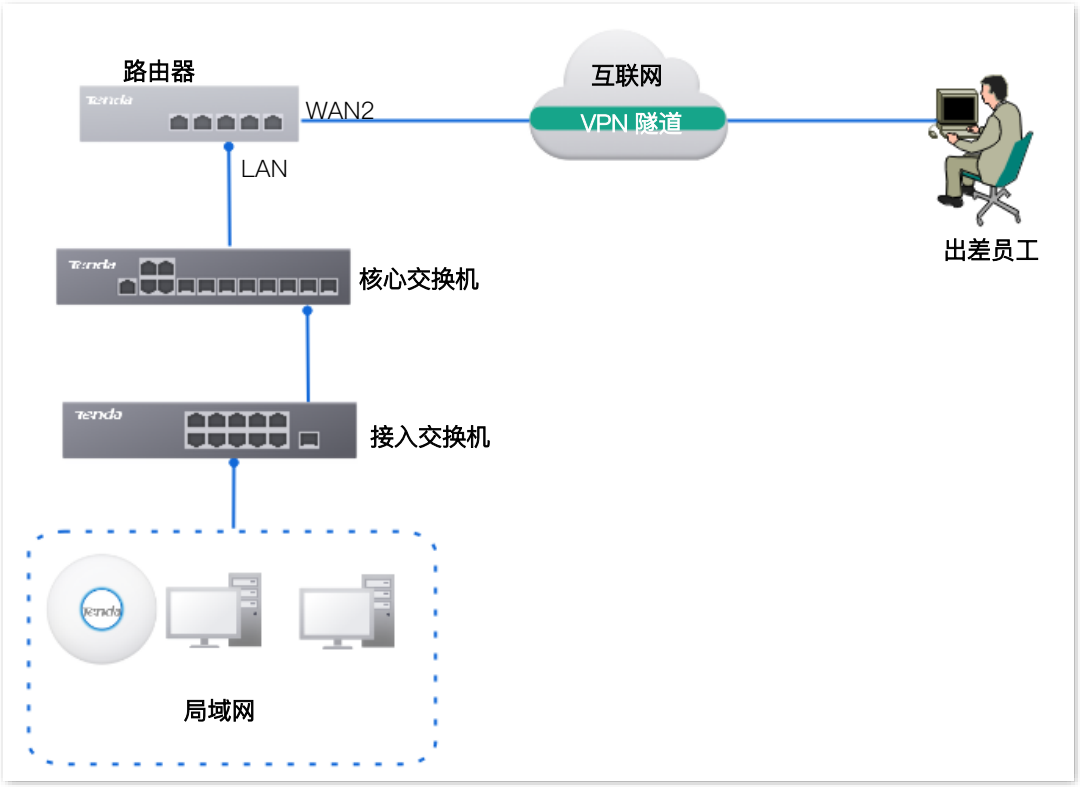
方案设计

在路由器上配置 L2TP 服务器，并开启 IPSec 对数据报文加密，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 L2TP 服务器基本信息如下：

- L2TP 服务器分配的用户名、密码均为 fengongsi1。
- L2TP 服务器 IP 地址为 202.105.11.22。
- L2TP 服务器对数据启用加密。
- L2TP 服务器内网为 192.168.10.0/24。
- L2TP 服务器建立 VPN 隧道的接口为 WAN2。

假设 L2TP 服务器与 L2TP 客户端建立连接时，用来验证身份的预共享密钥为 12345678。



配置步骤

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置 L2TP 服务器。

L2TP 服务器参数示例如下表所示，其他未提及的参数保持默认设置。

服务器名称	出入口设定	加密设定	共享秘钥	客户端地址池
L2TP 服务器	WAN2	加密	12345678	10.1.0.100~10.1.0.163

进入「更多」>「VPN 服务」>「VPN 服务器」页面，点击 新增，配置 L2TP 服务器相关参数，点击 保存。

提示

“加密设定”设置为“加密”表示 L2TP 服务器使用 IPSec 加密。

步骤 3 配置 L2TP 用户。

L2TP 用户参数示例如下表所示。

VPN 类型	用户名	密码	用户组	客户端类型
L2TP	fengongsi1	fengongsi1	分公司 1 员工	终端

1 配置 VPN 用户组。

进入「审计」>「分组策略」>「用户组」页面，点击 新增 ，然后创建一个移动端的 VPN 用户组，点击 保存 。

2 配置 L2TP 用户账号。

进入「更多」>「VPN 服务」>「用户管理」页面，点击 新增 ，配置 L2TP 用户相关参数，然后点击 保存 。

验证配置

出差员工进行 VPN 拨号访问总部资源。

场景 1：出差员工在电脑（以 Windows 10 为例）上访问总部资源

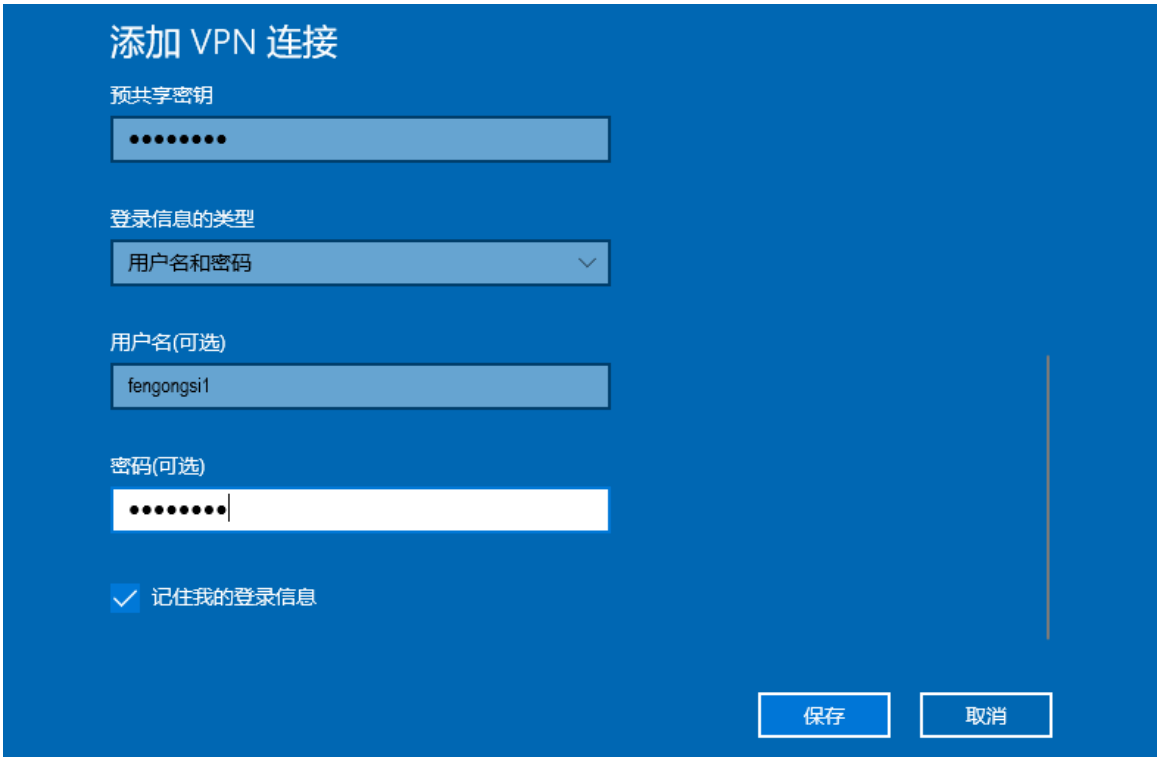
一、出差员工建立 VPN 连接

步骤 1 点击桌面右下角图标，选择“网络和 Internet 设置”。

步骤 2 点击“VPN”，然后点击“添加 VPN 连接”。

步骤 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“fengongsi1”。



步骤 4 点击“VPN 访问”，然后点击 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。

二、出差员工访问总部资源

假设出差员工要访问总部 FTP 服务器，且服务器信息如下：

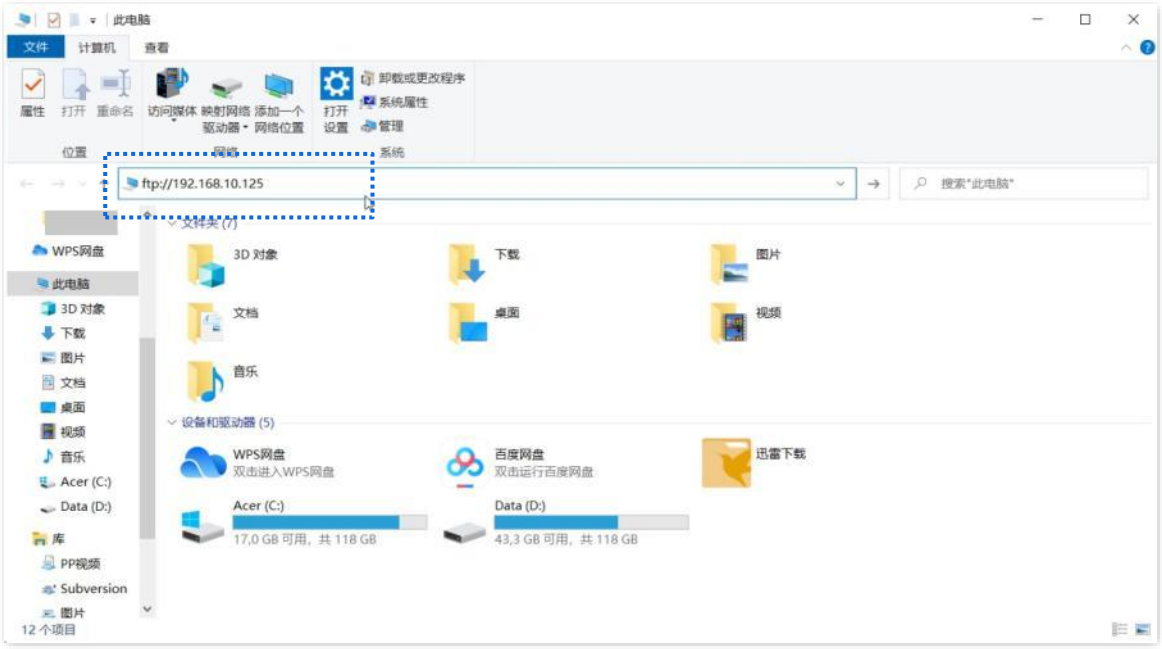
- FTP 服务器 IP 地址为 192.168.10.125
- FTP 服务端口为 21
- FTP 服务器登录用户名为 zhangsan，密码为 Zs123456@

当分公司员工访问总部项目资料时，步骤如下：

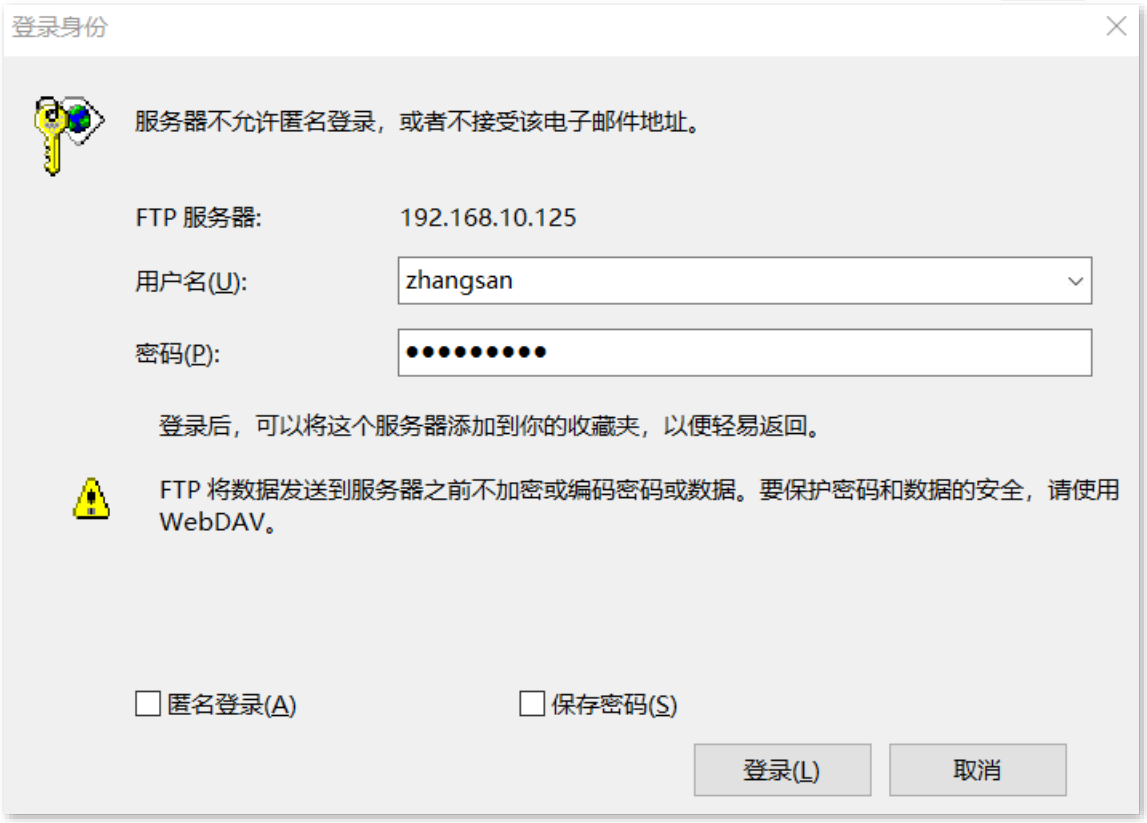
步骤 1 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 ftp://192.168.10.125。

提示

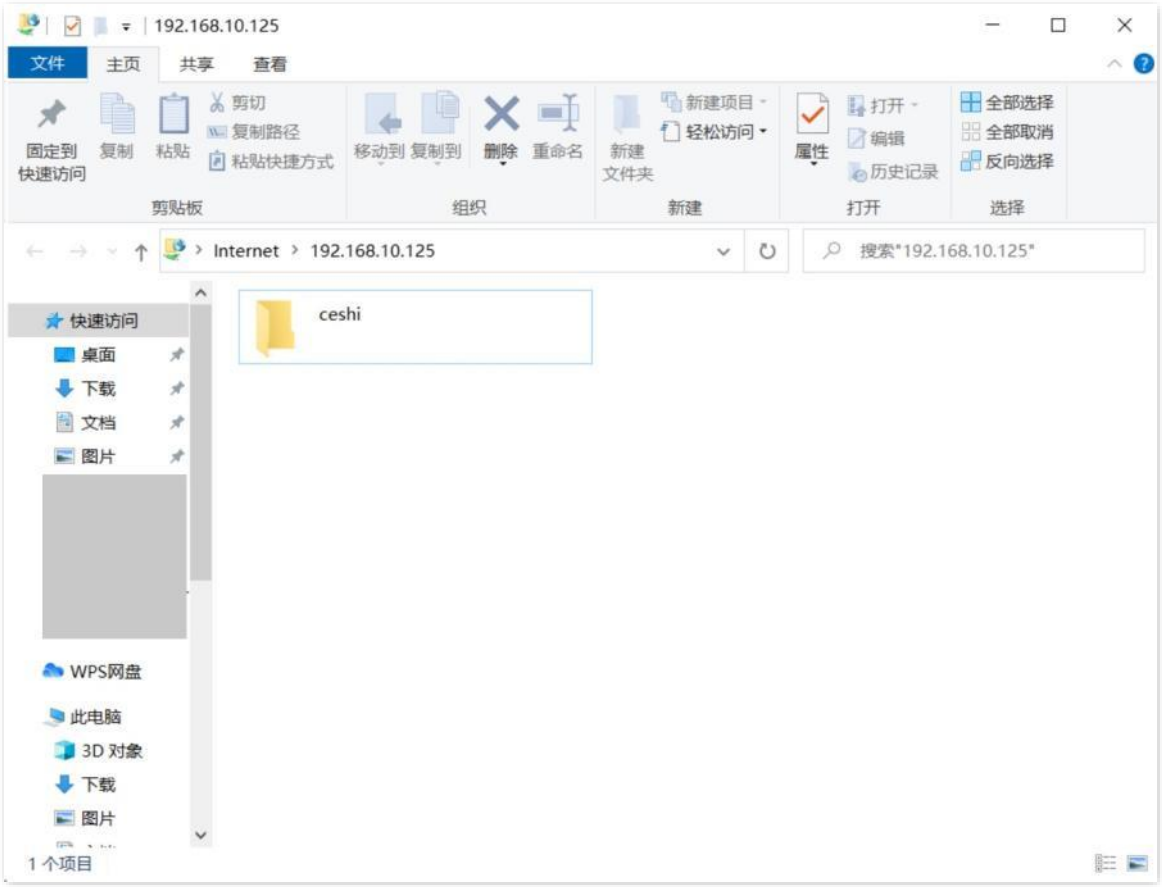
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



步骤 2 输入登录用户名和密码，本例均为“zhangsan”，密码为“Zs123456@”，然后点击 登录 。



访问成功。



场景 2：出差员工在移动设备（以 IOS 系统为例）上访问总部资源

一、出差员工建立 VPN 连接

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 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“fengongsi1”。
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。

二、出差员工访问总部资源

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

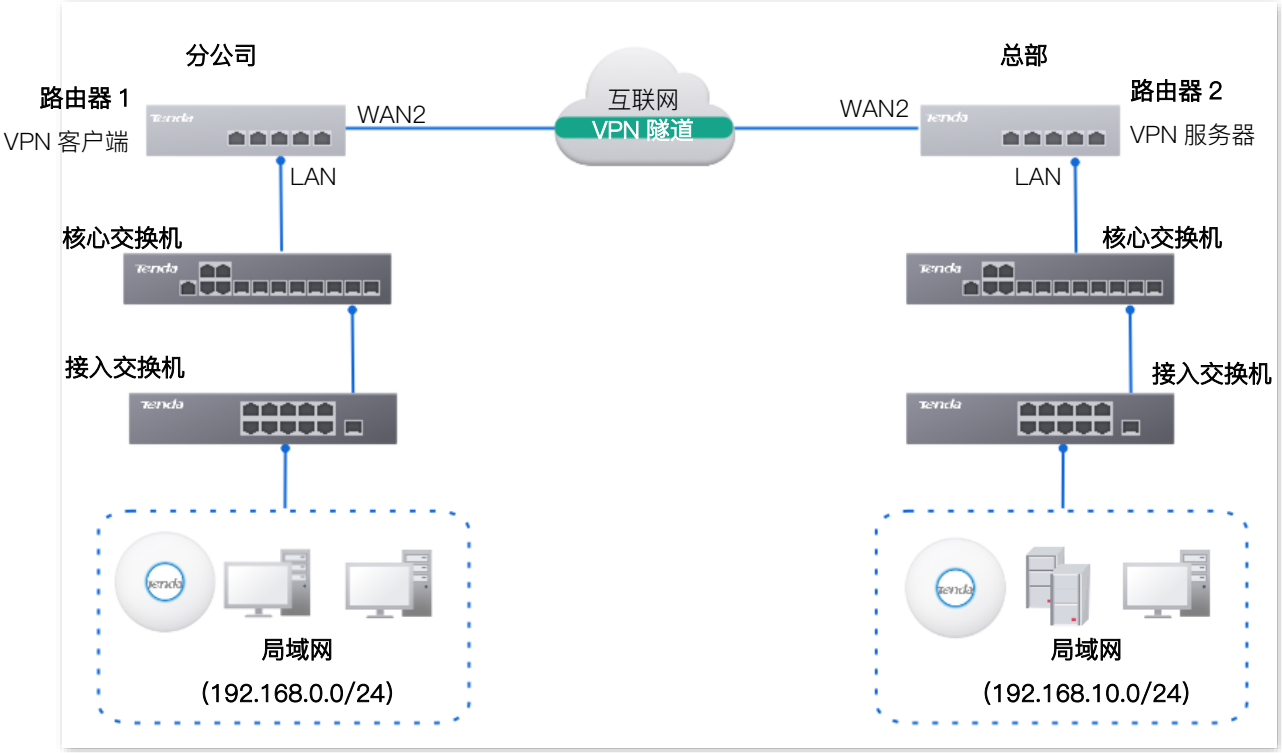
10.4.5 OpenVPN 配置举例一（VPN 客户端为路由器）

组网需求

某企业总部和分公司都使用路由器 G500-F 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

将总部路由器设置为 VPN 服务器，分公司路由器设置为 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 OpenVPN 为例说明。



配置步骤

配置总部路由器为 VPN 服务器 > 配置分公司路由器为 VPN 客户端

一、配置总公司路由器为 VPN 服务器

步骤 1 登录到总公司路由器的 Web 管理页面。

步骤 2 配置 OpenVPN 服务器。

OpenVPN 服务器参数示例如下表所示。其他未提及的参数保持默认设置。

服务器名称：OpenVPN 服务器

VPN 类型：OPEN

出入口设定：WAN2

服务器模式：账号密码

IP 地址：10.10.1.0/24

下发路由配置：192.168.10.0/255.255.255.0

进入「更多」>「VPN 服务」>「VPN 服务器」页面，点击 新增，配置 OpenVPN 服务器相关参数，点击 保存。

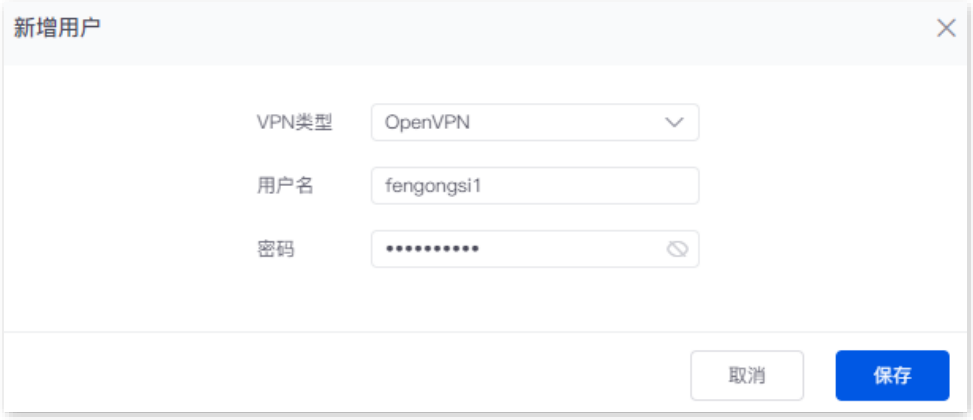
配置完成，点击 导出 ，并将下载的 xxxxxxxx_openvpn-client-cfg.tar 发送给 OpenVPN 客户端的管理电脑。

步骤 3 配置 OpenVPN 用户。

OpenVPN 用户参数示例如下表所示。

VPN 类型	用户名	密码
OpenVPN	fengongsi1	fengongsi1

进入「更多」>「VPN 服务」>「用户管理」页面，点击 新增 ，配置 OpenVPN 用户相关参数，然后点击 保存 。



二、配置分公司路由器为 VPN 客户端

步骤 1 将 OpenVPN 服务器发送的 xxxxxxxx_openvpn-client-cfg.tar 下载到 OpenVPN 客户端的管理电脑并解压，得到如下 3 个文件。

名称	大小	压缩后大小
ca.crt	1 151	1 536
ca.key	1 704	2 048
client.ovpn	1 397	1 536

步骤 2 登录到分公司路由器的 Web 管理页面。

步骤 3 配置 OpenVPN 客户端。

1. 点击「更多」>「VPN 客户端」，打开 VPN 客户端开关。
2. 选择“客户端类型”与 VPN 服务器侧一致，本例为“OPEN”。
3. 选择配置客户端的方式，本例为“文件导入”。
4. 选择服务器的认证模式，本例为“账号密码”。
5. 输入 VPN 服务器分配的用户名，本例为“fengongsi1”。
6. 输入 VPN 服务器分配的用户名对应的密码，本例为“fengongsi1”。
7. 点击 浏览 ，导入 client.ovpn 文件。
8. 点击 保存 。

---完成

当页面的状态显示为“已连接”时，VPN 连接成功。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。

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：

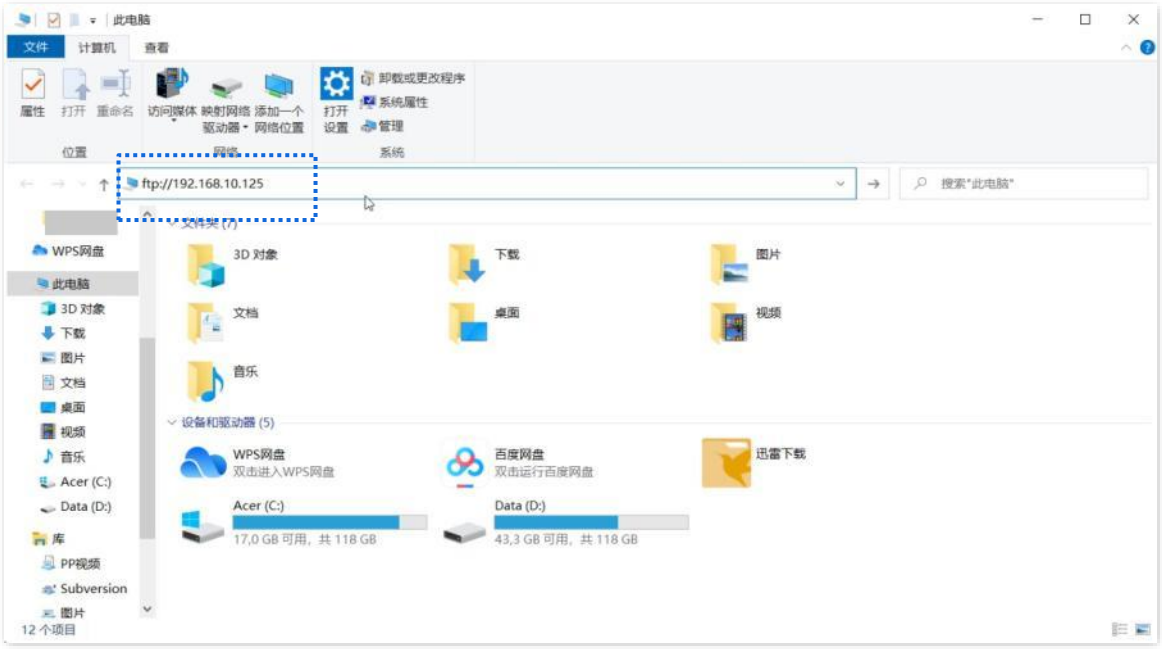
- FTP 服务器 IP 地址为 192.168.10.125
- FTP 服务端口为 21
- FTP 服务器登录用户名为 zhangsan，密码为 Zs123456@

当分公司员工访问总部项目资料时，步骤如下：

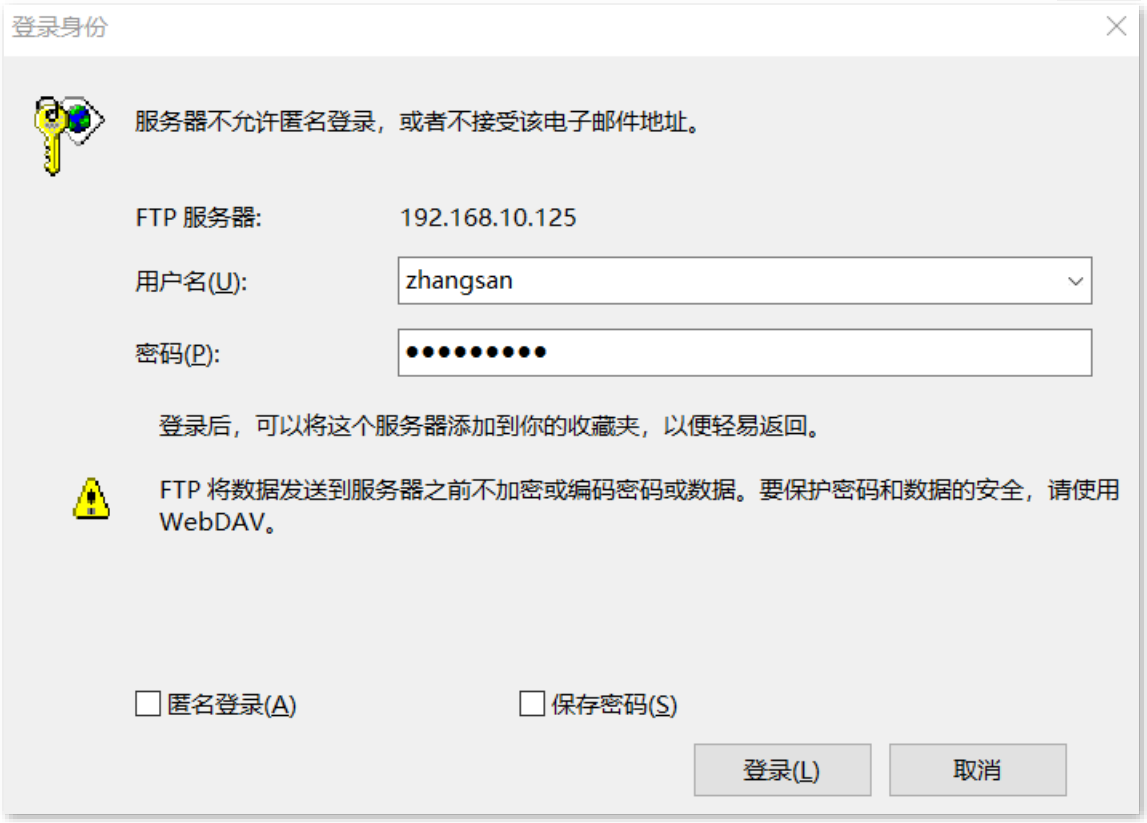
步骤 1 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 ftp://192.168.10.125。

提示

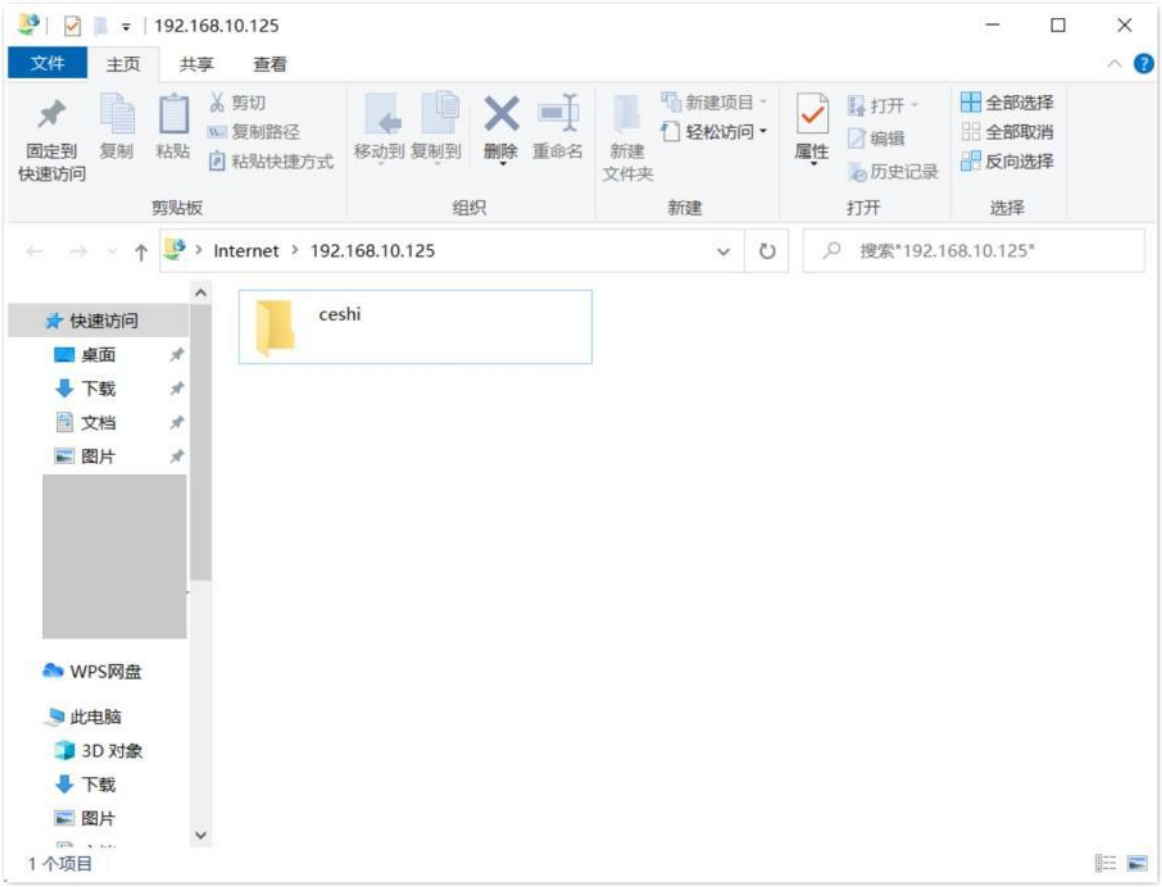
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



步骤 2 输入登录用户名与密码，本例用户名为“zhangsan”，密码为“Zs123456@”，然后点击 登录 。



访问成功。



10.4.6 OpenVPN 配置举例二（VPN 客户端为终端设备）

组网需求

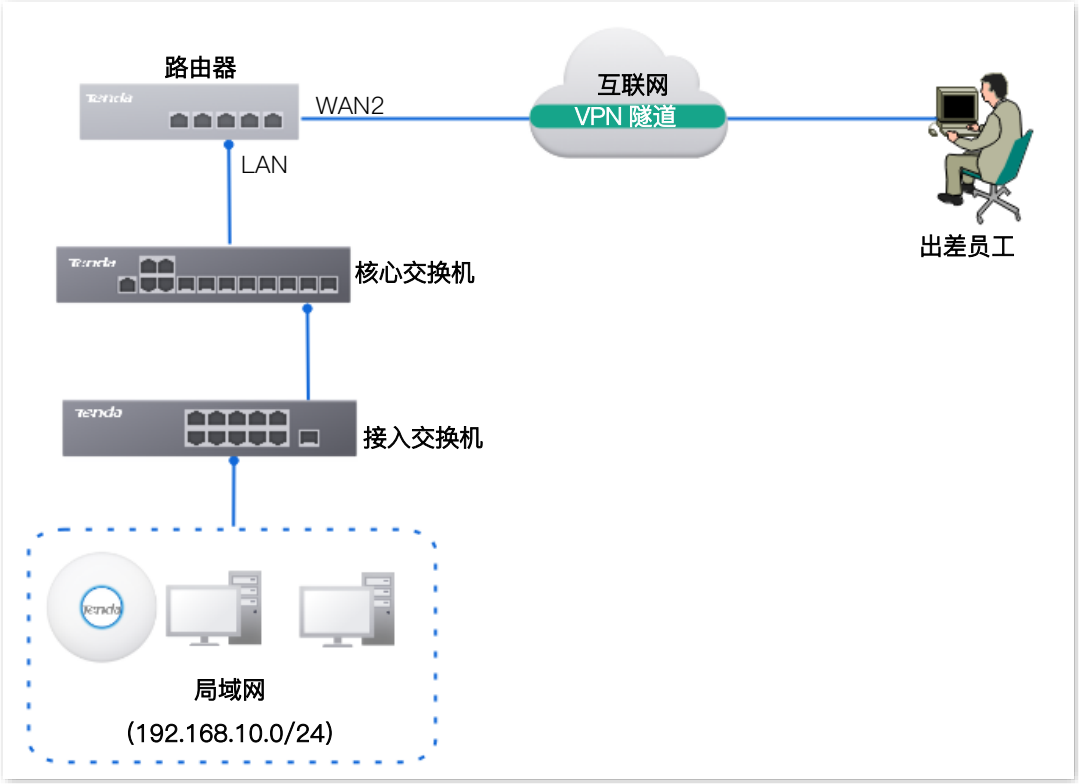
某公司使用路由器进行网络搭建，并成功接入互联网。出差员工需要经过互联网访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

方案设计

在路由器上配置 OpenVPN 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 OpenVPN 服务器基本信息如下：

- OpenVPN 服务器分配的用户名、密码均为 yuangong。
- OpenVPN 服务器 IP 地址为 10.10.1.0/24。
- OpenVPN 服务器给客户端下发的路由配置为 192.168.10.0/255.255.254.0。
- OpenVPN 服务器建立 VPN 隧道的接口为 WAN2。



配置步骤

步骤 1 登录到路由器 Web 管理页面。

步骤 2 配置 OpenVPN 服务器。

OpenVPN 服务器参数示例如下表所示。其他未提及的参数保持默认设置。

服务器名称：OpenVPN 服务器

VPN 类型：OPEN

出入口设定：WAN2

服务器模式：账号密码

IP 地址：10.10.1.0/24

下发路由配置：192.168.10.0/255.255.255.0

进入「更多」>「VPN 服务」>「VPN 服务器」页面，点击 新增，配置 OpenVPN 服务器相关参数，点击 保存。

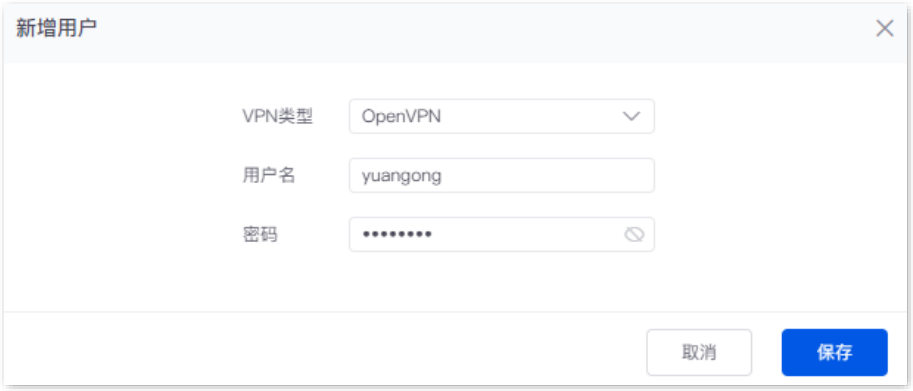
配置完成，点击 导出 ，并将下载的 xxxxxxxx_openvpn-client-cfg.tar 发送给出差员工。

步骤 3 配置 OpenVPN 用户。

OpenVPN 用户参数示例如下表所示。

VPN 类型	用户名	密码
OpenVPN	yuangong	yuangong

进入「更多」>「VPN 服务」>「用户管理」页面，点击 新增 ，配置 OpenVPN 用户相关参数，然后点击 保存 。



----完成

验证配置

出差员工进行 VPN 拨号访问总部资源。

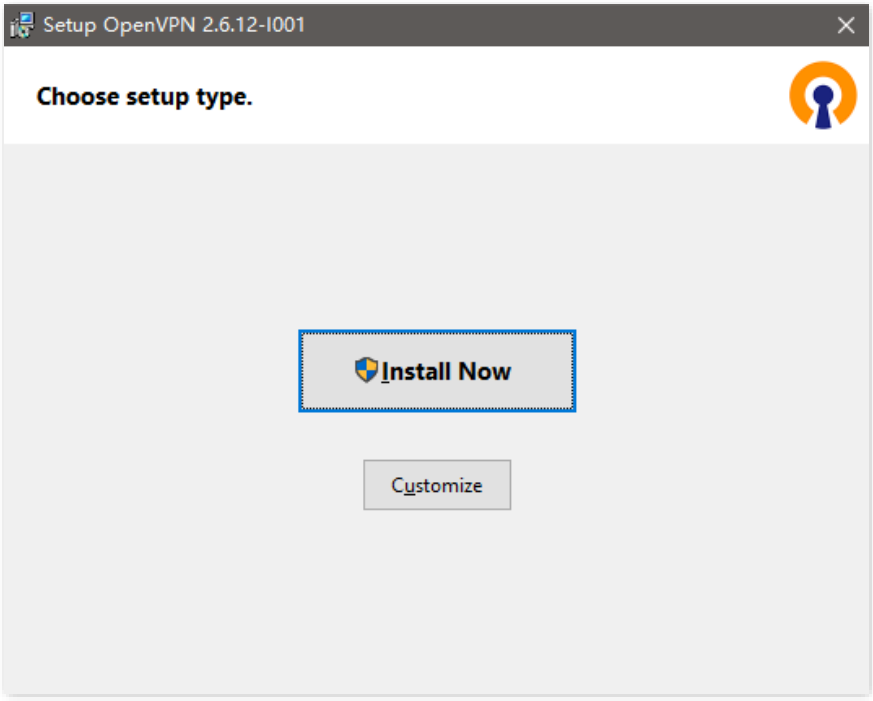
场景 1：出差员工在电脑（以 Windows 10 为例）上访问总部资源

一、出差员工下载 OpenVPN 客户端

步骤 1 访问 https://www.tenda.com.cn/openvpn/tdc/下载 OpenVPN 客户端安装包到员工电脑。

步骤 2 解压缩 OpenVPN_Client-Win.rar 得到 OpenVPN-x.x.x-lxxx-amd64.msi 安装程序。

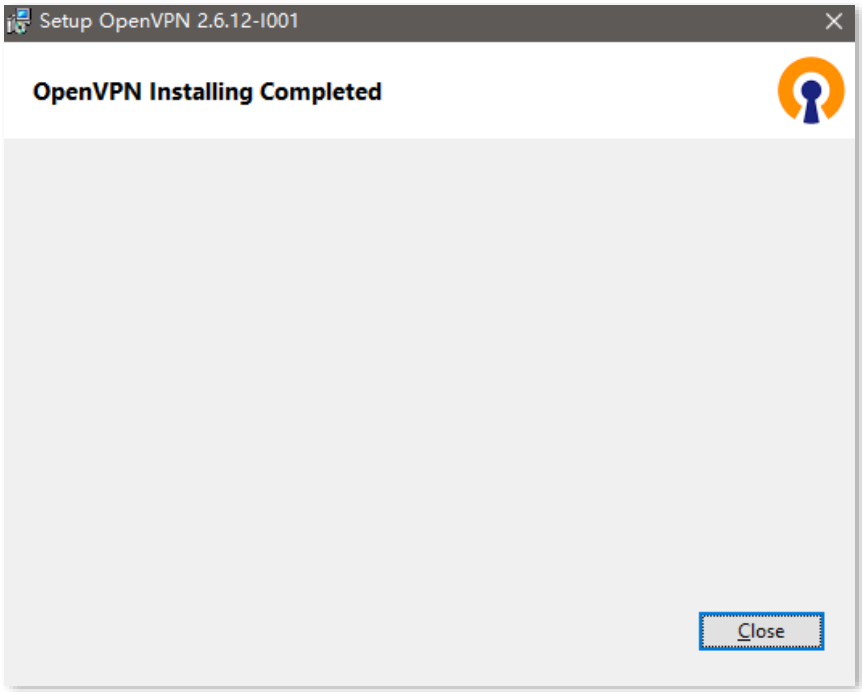
步骤 3 双击 OpenVPN-x.x.x-lxxx-amd64.msi 开始安装 OpenVPN 客户端。



步骤 4 点击 Install Now，稍等片刻，便安装成功，点击 Close。

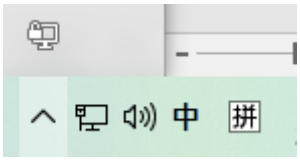
提示

点击 Customize 可以自定义安装路径，否则自动安装在电脑 C 盘。



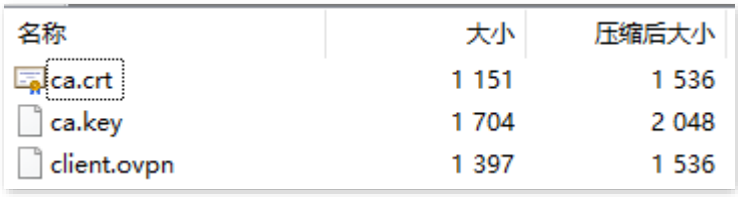
步骤 5 系统弹出如下提示，点击确定。

可以在电脑右下角任务栏看到 图标。

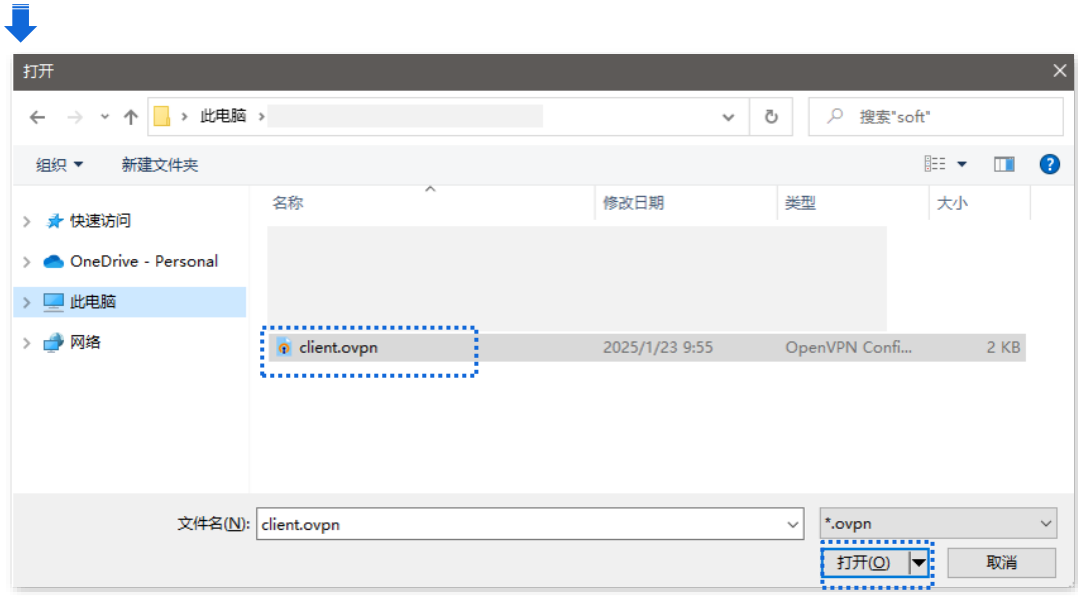


二、出差员工建立 VPN 连接

步骤 1 将 OpenVPN 服务器发送的 xxxxxxxx_openvpn-client-cfg.tar 下载到员工电脑并解压，得到如下 3 个文件。

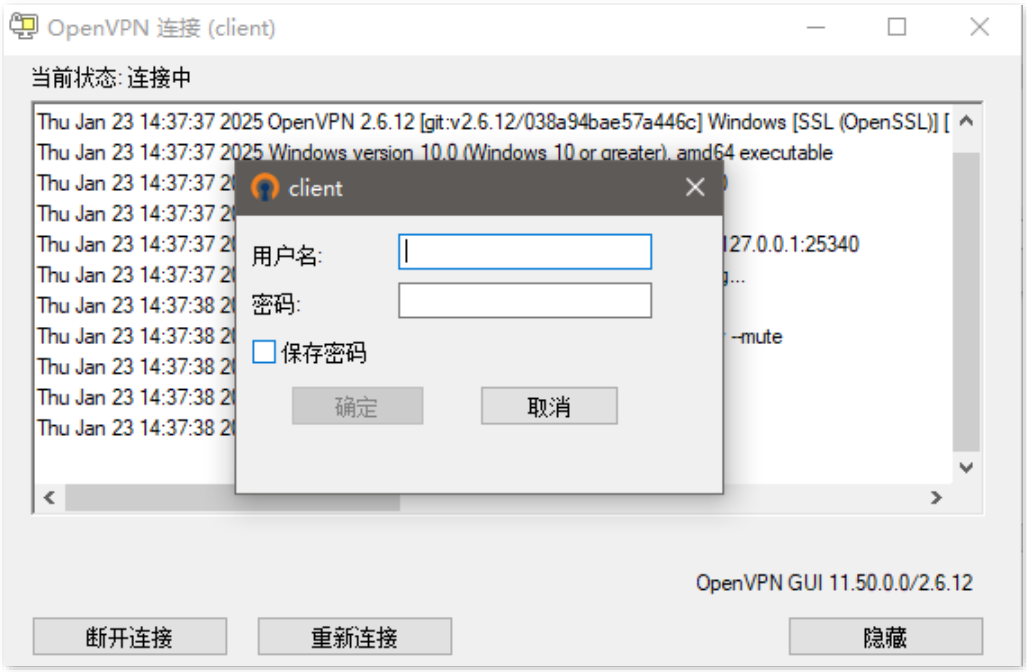


步骤 2 鼠标右击 图标，然后点击**导入** > **导入配置文件**，找到并导入 client.ovpn 文件。



导入成功。

步骤 3 双击 图标，并输入 VPN 服务器分配的用户名与密码，点击**确定**。



连接成功。

三、出差员工访问总部资源

假设出差员工要访问总部 FTP 服务器，且服务器信息如下：

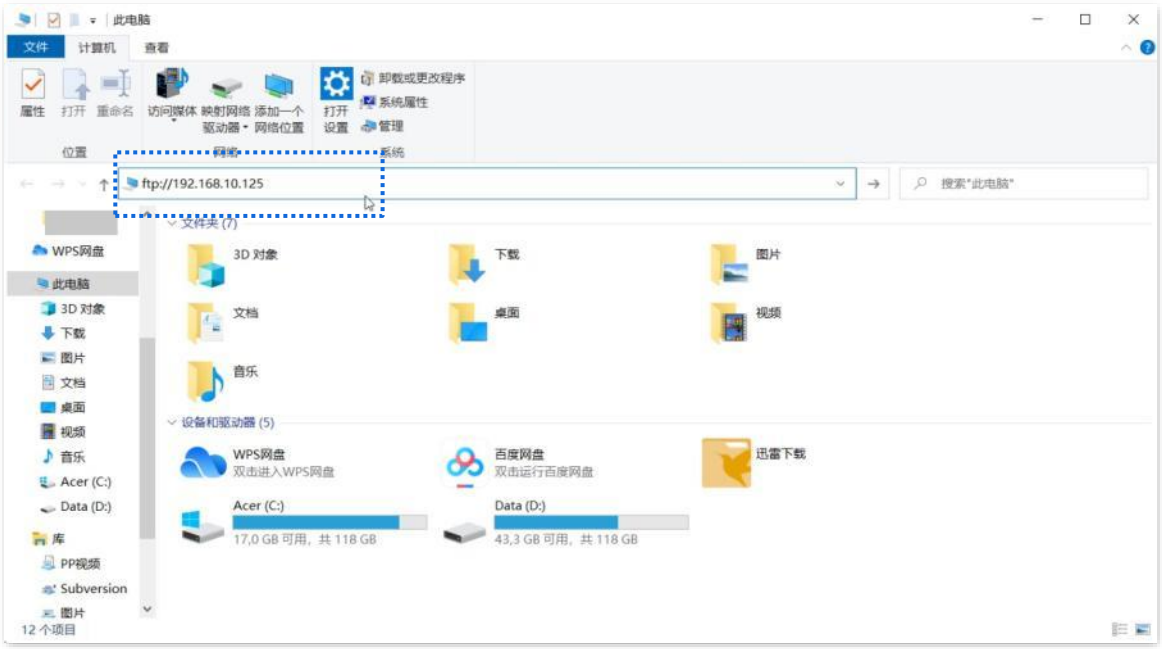
- FTP 服务器 IP 地址为 192.168.10.125
- FTP 服务端口为 21
- FTP 服务器登录用户名为 zhangsan，密码为 Zs123456@

当分公司员工访问总部项目资料时，步骤如下：

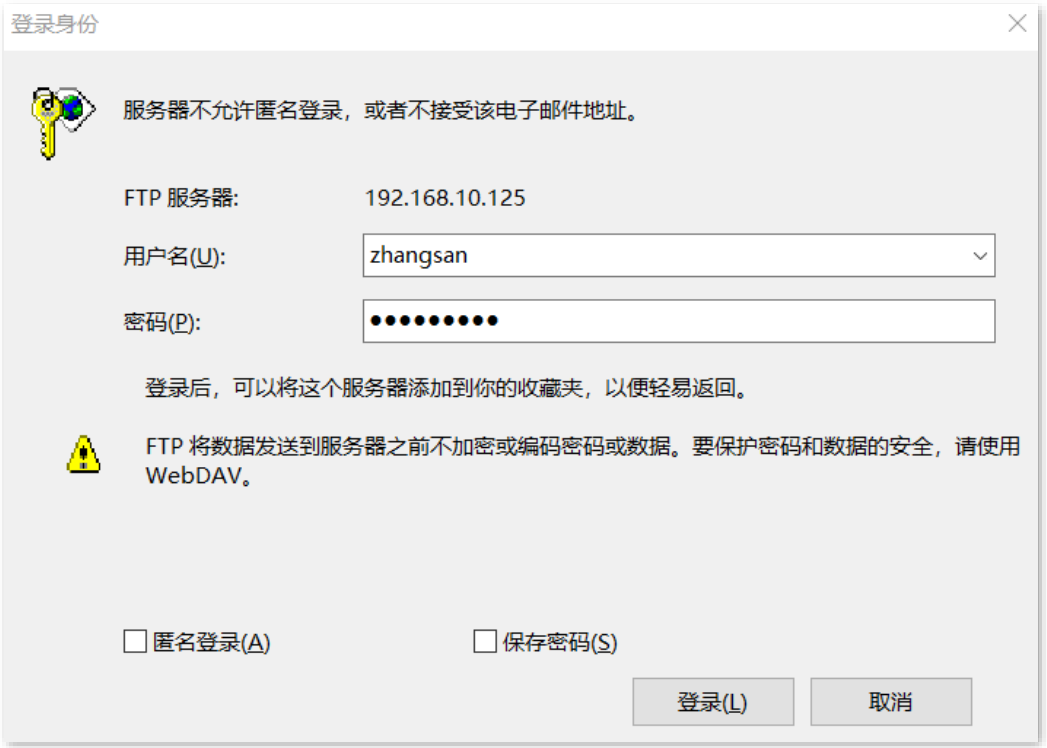
步骤 1 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 ftp://192.168.10.125。

提示

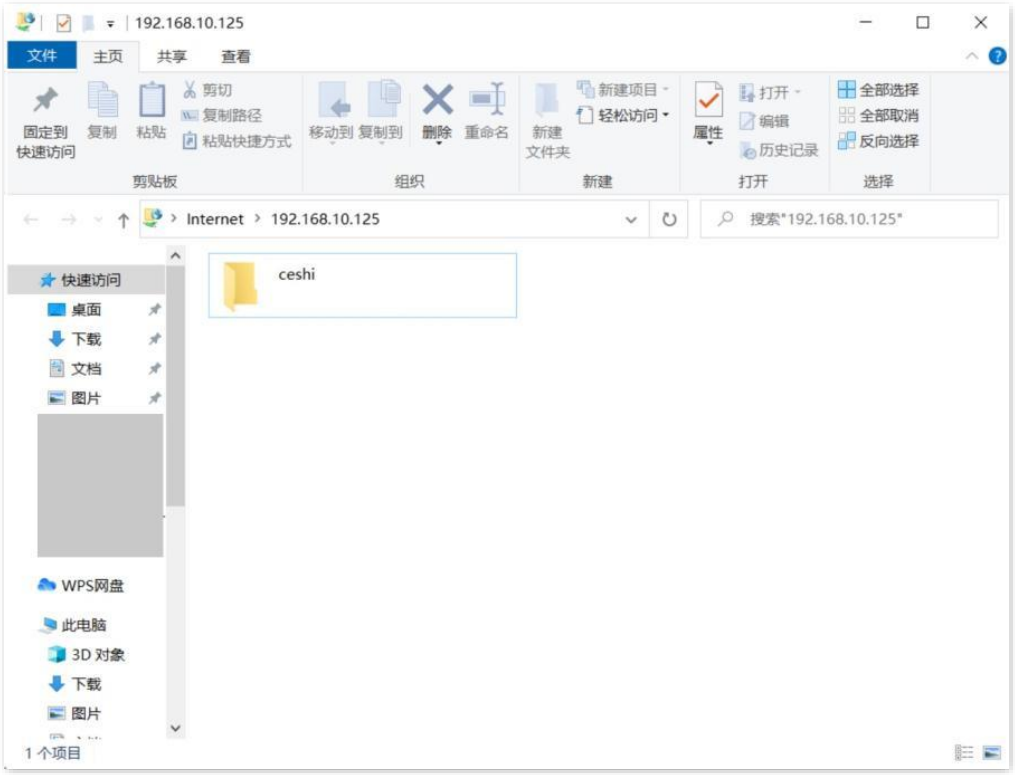
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



步骤 2 输入登录用户名和密码，本例均为“zhangsan”，密码为“Zs123456@”，然后点击 登录 。



访问成功。

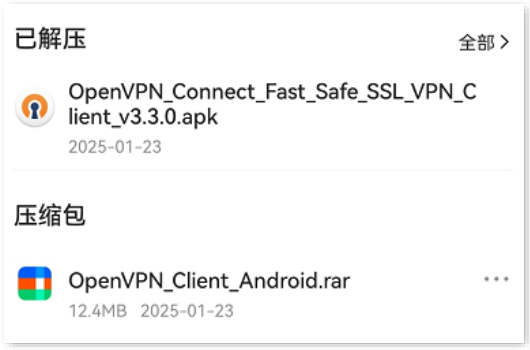


场景 2：出差员工在移动设备（以 Android 系统为例）上访问总部资源

一、出差员工下载 OpenVPN 客户端

步骤 1 访问 https://www.tenda.com.cn/openvpn/tdc/下载 OpenVPN 客户端安装包到员工手机。

步骤 2 解压缩 OpenVPN_Client-Android.rar 得到后缀为.apk 的安装程序。下图仅供参考。



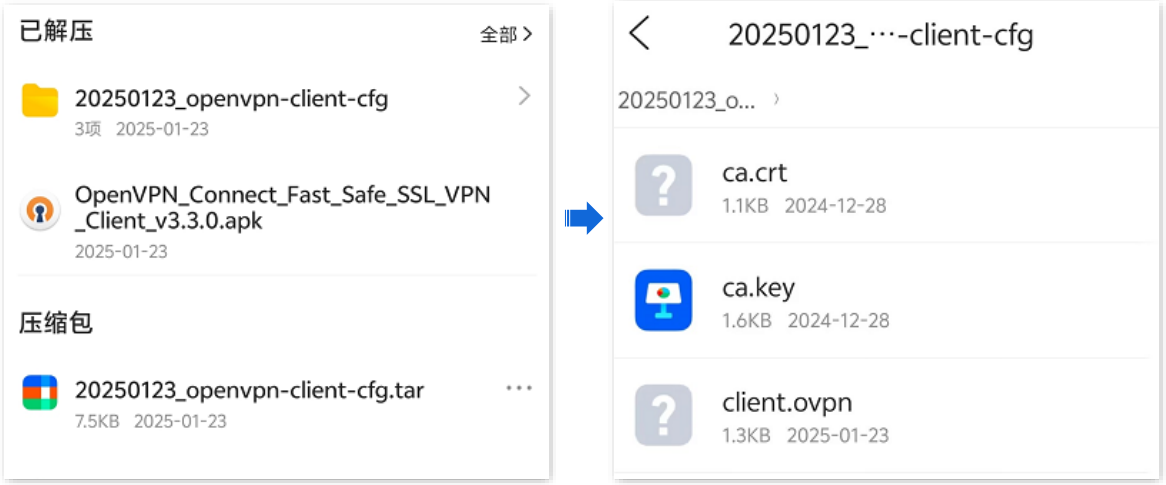
步骤 3 点击后缀为.apk 的安装程序开始安装 OpenVPN 客户端。稍等片刻，安装成功。

提示

如果安装过程中出现“此应用存在风险”相关提示，请继续安装。

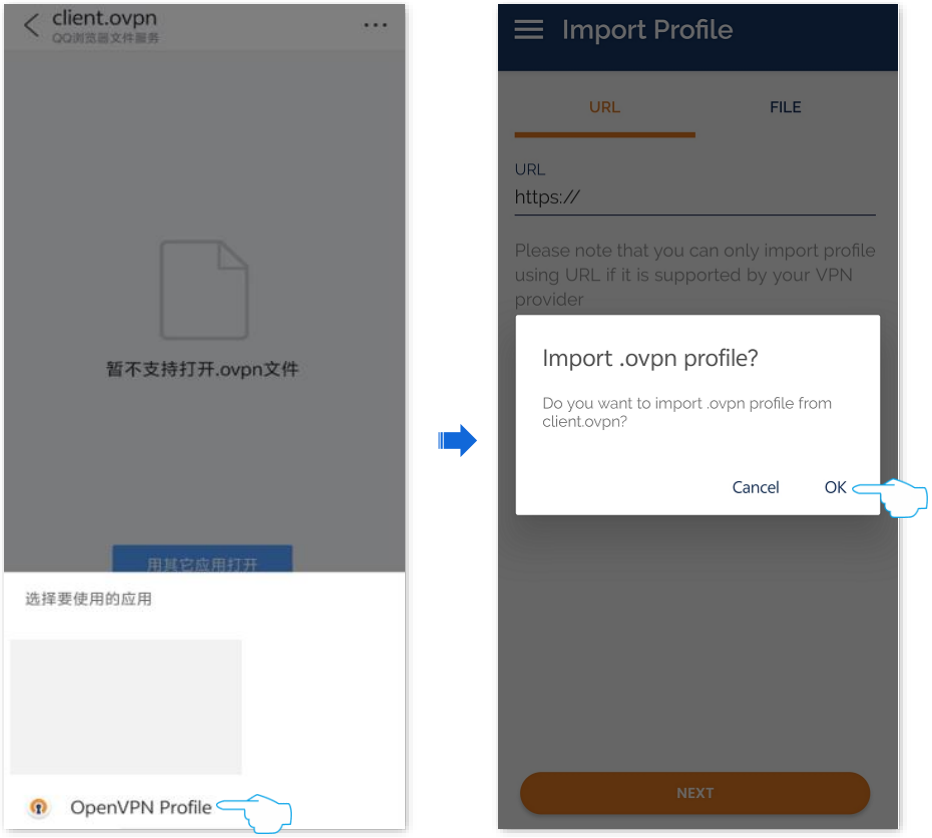
二、出差员工建立 VPN 连接

步骤 1 将 OpenVPN 服务器发送的 xxxxxxxx_openvpn-client-cfg.tar 下载到员工手机并解压，得到 3 个文件。下图仅供参考。



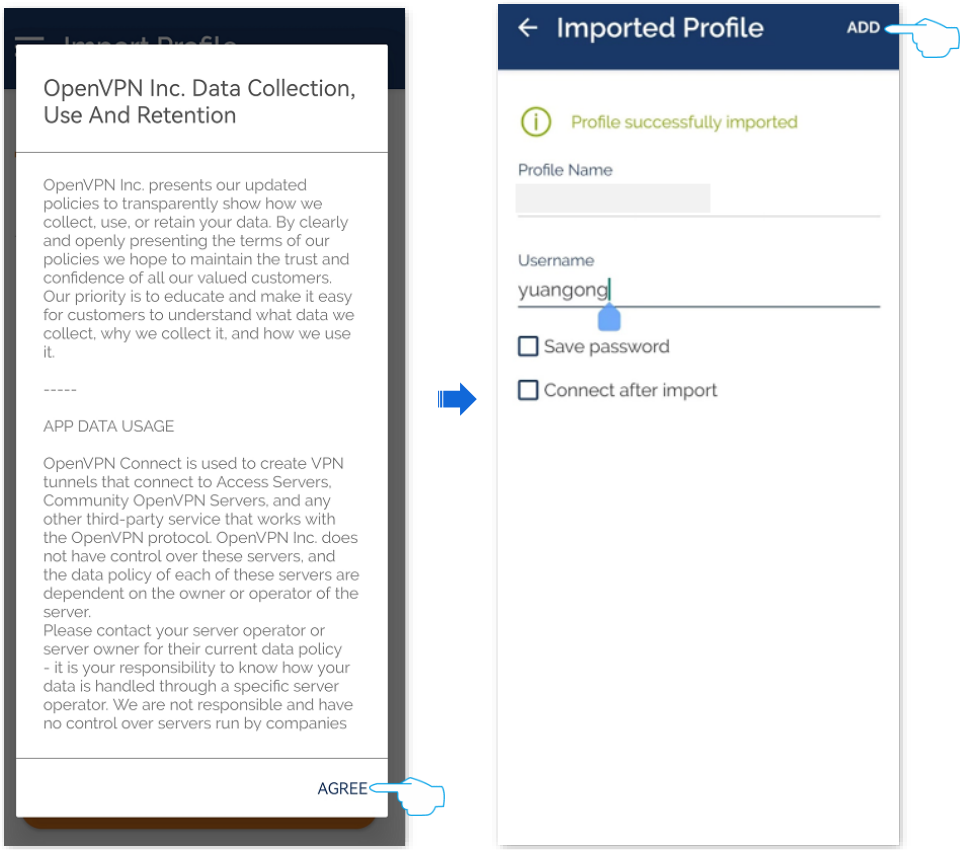
步骤 2 点击 client.ovpn，并选择要使用的应用“OpenVPN Profile”。

步骤 3 点击 OK。

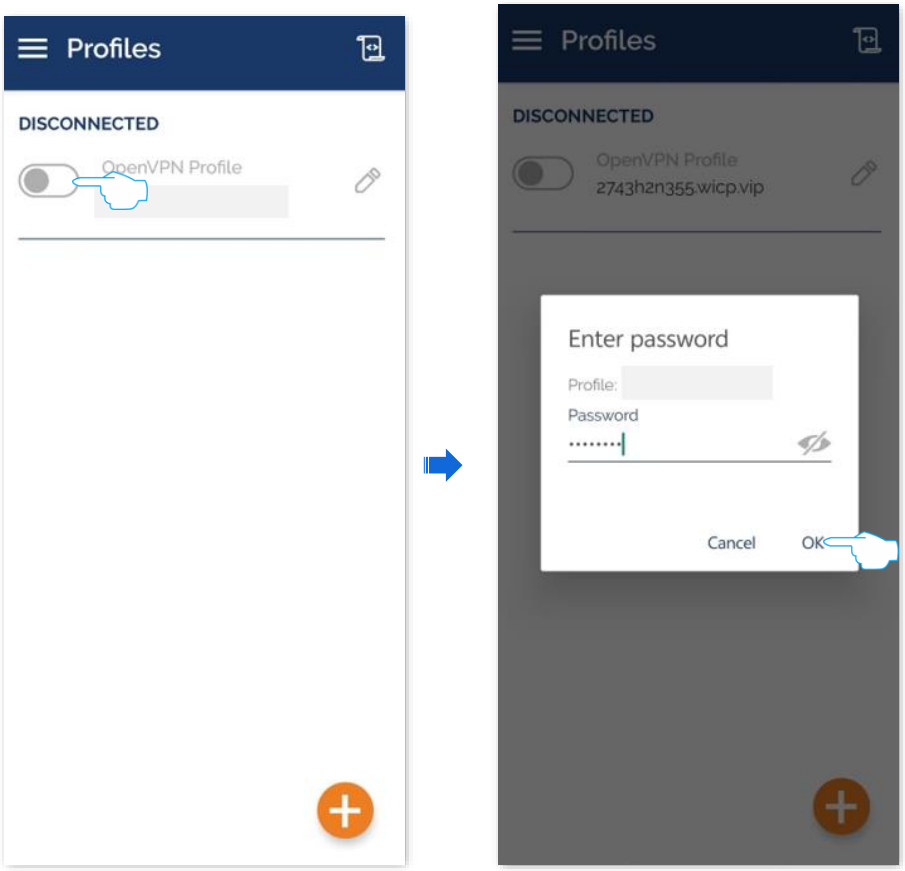


步骤 4　手机自动运行 OpenVPN 客户端，点击 **AGREE**。

步骤 5　在 Username 栏输入 VPN 服务器提供的用户名，本例为“yuangong”。点击 **ADD**。

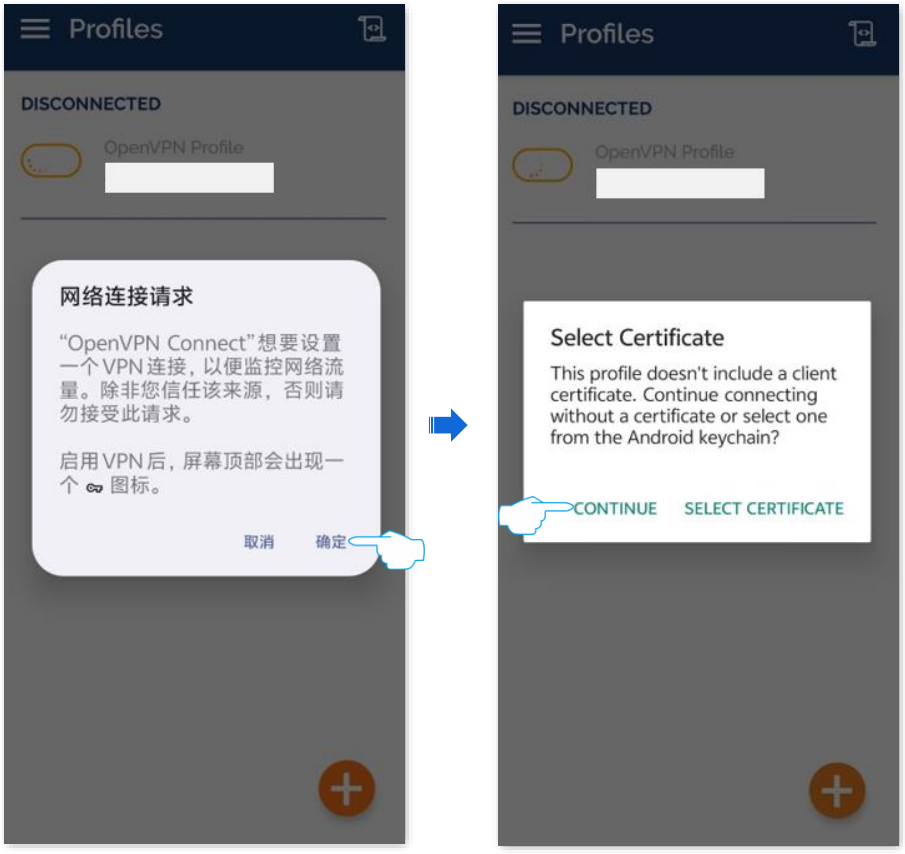


步骤 6　点击  ，然后输入 VPN 服务器提供的密码，本例为“yuangong”。点击 **OK**。

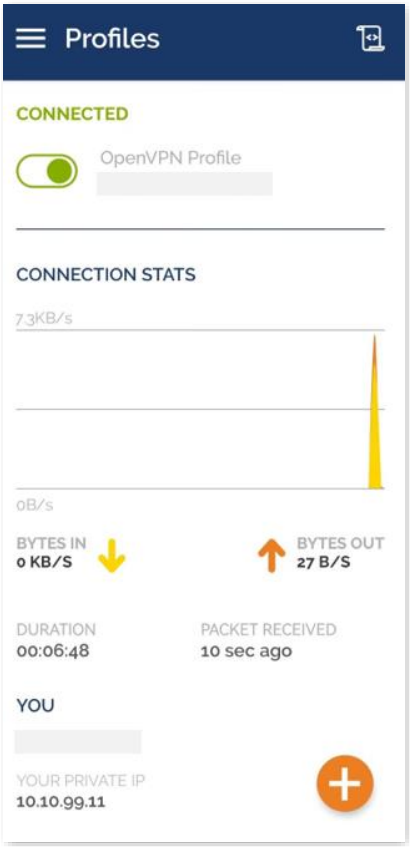


步骤 7 点击**确定**。

步骤 8 点击 CONTINUE。



稍等片刻，当 变为 时，拨号成功。



三、出差员工访问总部资源

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

10.4.7 IPSec

概述

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。

其相关概念如下：

- **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”两种封装模式。

  - 隧道（Tunnel）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（Authentication Header，鉴别首部）或 ESP（Encapsulating Security Payload，封装安全载荷）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（Transport）模式：不改变原有的 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。

协议 \ 封装模式	隧道模式	传输模式
AH	IP AH Data	IP AH IP Data
ESP	IP ESP Data ESP-T	IP ESP IP Data ESP-T
AH +ESP	IP AH ESP Data ESP-T	IP AH ESP IP Data ESP-T

- **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 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（Security Parameter Index，安全参数索引），目的 IP 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。
- SA 是单向的，在两个对等体之间的双向通信，最少需要两个 SA 来分别对两个方向的数据流进行安全保护。另外，如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的 SA。
- SA 可以手动建立或由 IKE（Internet Key Exchange，互联网密钥交换）协商生成。
  - 手动建立：配置复杂，创建 SA 所需的全部信息必须手动配置，且不支持一些高级特性（如：定时更新秘钥）。此时，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。一般用于小型静态环境中，或通信的对等体设备数量较少的情况。
  - IKE 自动协商：配置简单，只需要配置 IKE 协商安全策略的信息，即可由 IKE 自动协商来创建和维护 SA。此时，SA 有生命周期，会定时更新，增强了安全性。一般用于中、大型动态网络环境。

- **建立 SA 的方式**

手动建立

手动配置 SA 所需的全部信息，包括认证算法、认证秘钥、加密算法、加密秘钥、SPI 值等。

IKE 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。

具体完成过程如下：

1. 协商确认一系列算法等安全提议，确保对等体双方使用相同的安全提议。
2. 根据预共享密钥和协商的安全提议计算出 DH（Diffie-Hellman）公共值，用于密钥交换。
3. 对等体验证，路由器通过预共享密钥方式来验证对等体合法性。

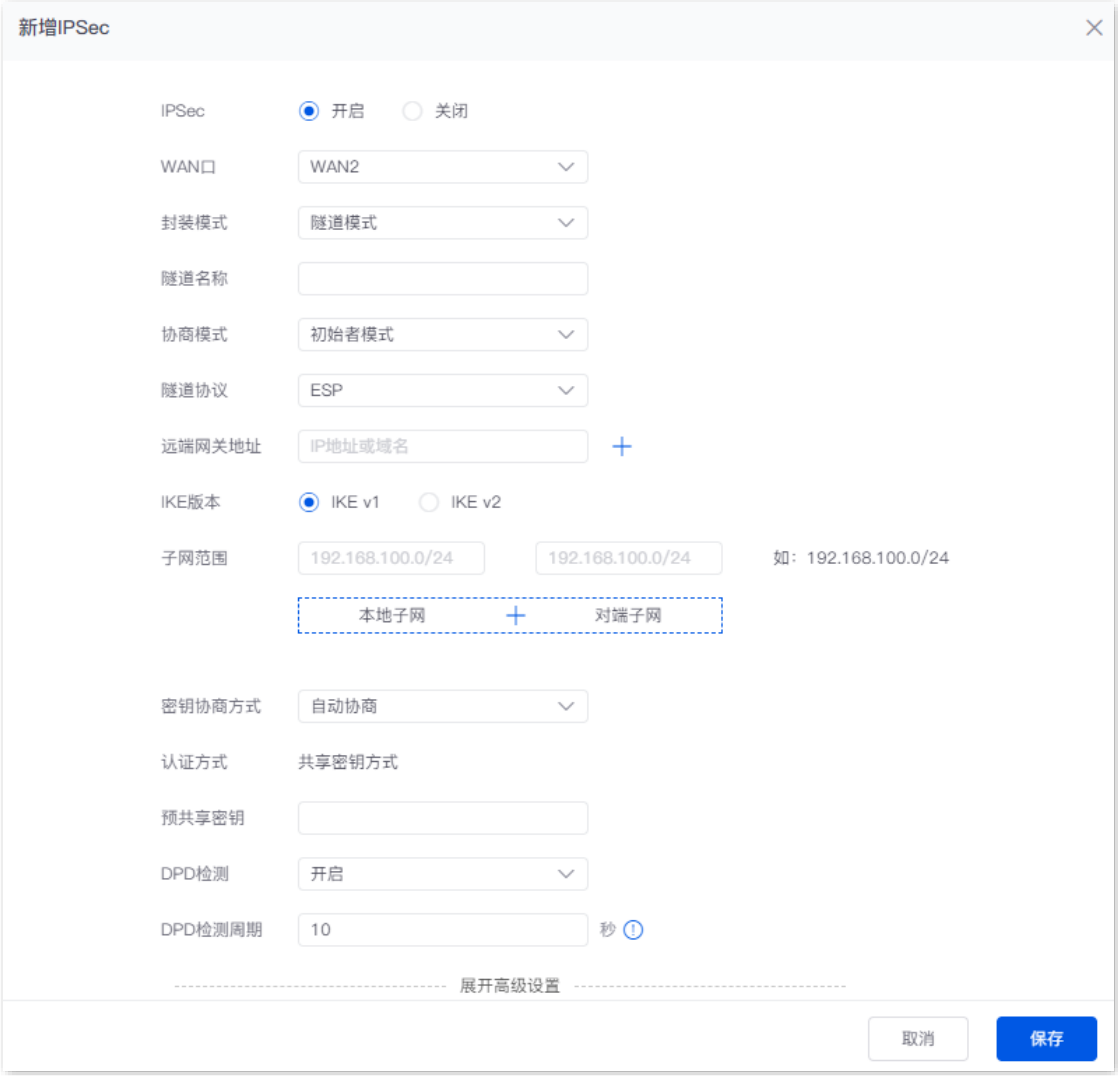
- 阶段 2

在阶段 1 建立的 ISAKMP SA 上为 IPSec 协商具体的 SA，建立一条用于 IP 数据安全传输的 IPSec SA。

新增 IPSec 连接---隧道模式

登录到路由器 Web 管理页面后，进入「更多」>「VPN 服务」>「IPSec」页面，点击 新增，然后在出现的页面配置各项参数，点击 保存。

IPSec 数据封装模式分为“隧道模式”和“传输模式”两种封装模式，默认为“隧道模式”，如下所示。



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。 - 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。 注意 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。

标题项	说明
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 WAN 口 IP 地址或域名。 注意 设置为域名时，需要在对端网关上设置 DDNS 功能，确保对端网关 WAN 口 IP 地址发生变化时，也不影响 IPSec 隧道的使用。
IKE 版本	- IKE v1：功能基础，易受攻击，但兼容性广。在配置子网范围时，要手动配置每个子网对，子网不匹配会导致 SA 建立失败。 - IKE v2：优化了流程并增强安全性和灵活性。在配置子网范围时，支持多子网和动态调整，子网不匹配会自动协商交集。
子网范围	- 本地子网：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，则本地子网可填为 192.168.0.0/24。 - 对端子网：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。 自动协商：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。

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。

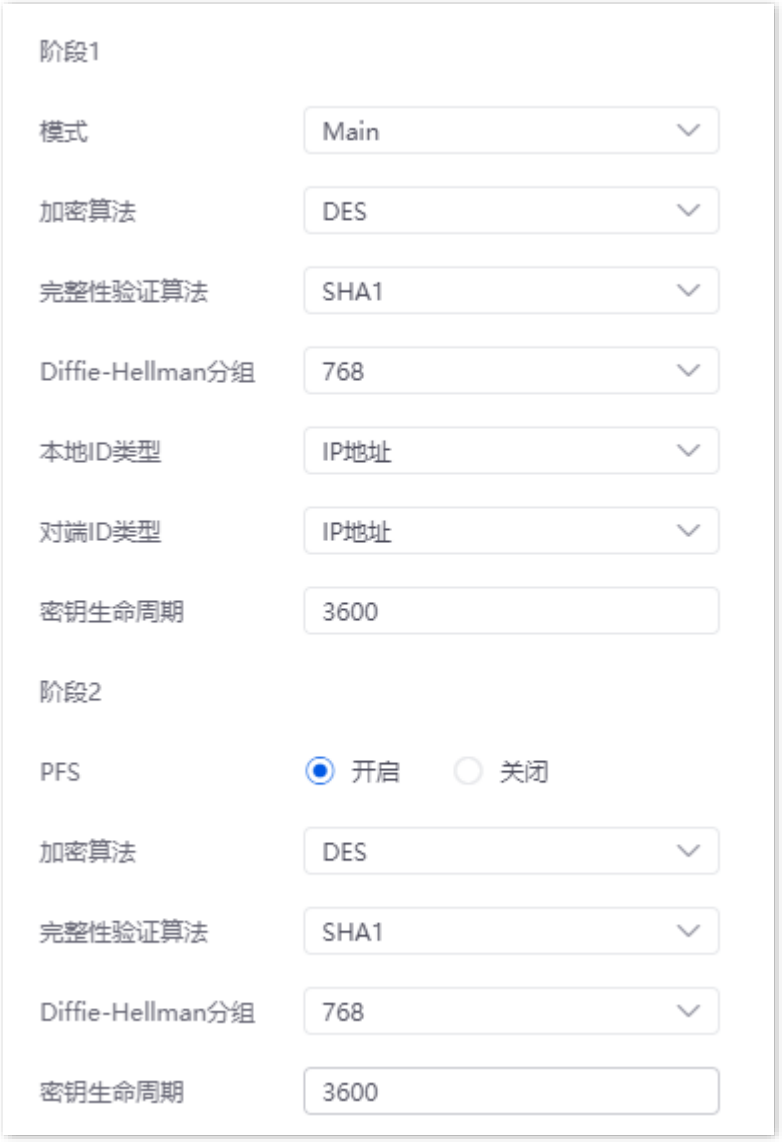
阶段 2：使用阶段 1 中建立的 ISAKMP SA 为 IPSec 的安全性协议协商参数，创建 IPSec SA，用于对双方的通信数据进行保护。

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**--展开高级设置--**可显示自动协商的高级参数。点击后，页面如下图示。



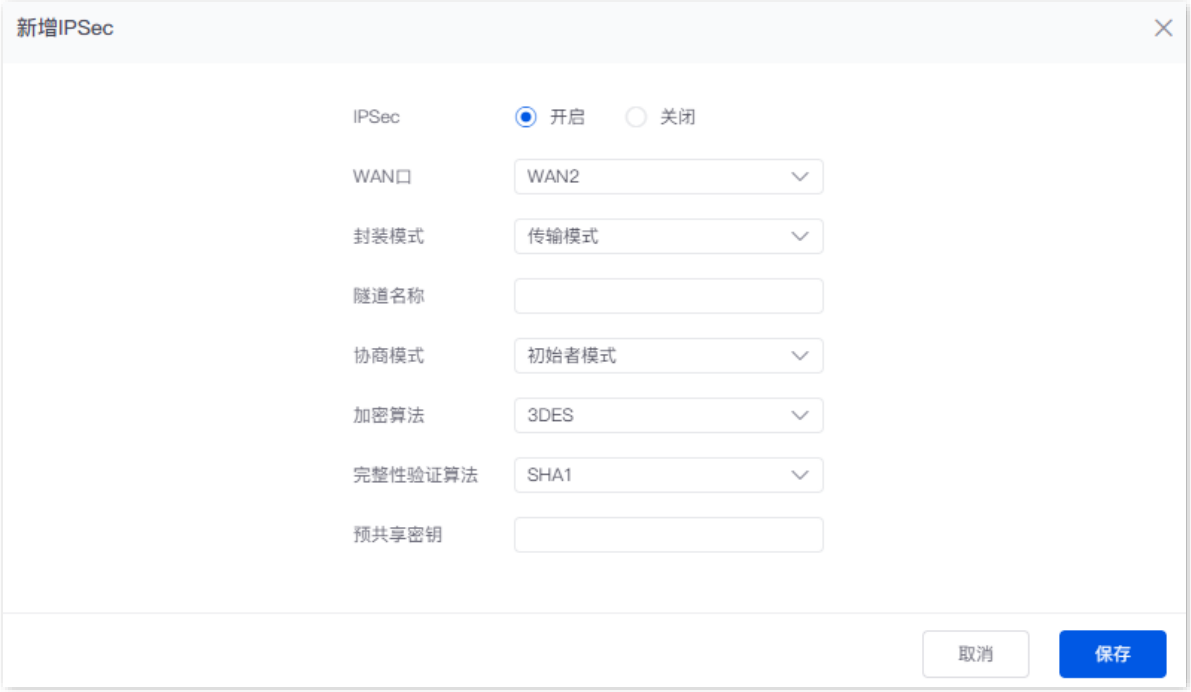
参数说明

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。

标题项	说明
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。
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。
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。

新增 IPSec 连接---传输模式

登录到路由器 Web 管理页面后，在「更多」>「VPN 服务」>「IPSec」页面，点击 新增 ，然后在出现的页面封装模式选择“传输模式”，并配置其他各项参数，点击 保存 。如下所示。



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。 - 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。 注意 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。
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。

标题项	说明
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。
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。

查看 IPSec SA

登录到路由器 Web 管理页面后，点击「更多」>「VPN 服务」>「IPSec 列表」。

IPSec 隧道两端设备完成配置后，您可以在 IPSec 列表中查看 IPSec SA。

参数说明

标题项	说明
名称	IPSec 隧道名称。
SPI	IPSec 隧道的 SPI（Security Parameter Index，安全参数索引），由 IKE 自动协商得出。
方向	SA 的方向（in：流入；out：流出）。 由于 IPSec SA 是单向的，所以当 IPSec 隧道成功建立后，每条隧道会产生一对名称相同 in 和 out 的 IPSec SA。
隧道两端	IPSec 隧道两端的网关地址。
数据流	IPSec 隧道两端的内网范围。
安全协议	当前隧道使用的安全协议。 - ESP(Encapsulating Security Payload，封装安全载荷)：在端对端的隧道通信中该协议会对整个数据包进行加密，用户可选使用带密钥的哈希算法保证报文的完整性和真实性（该协议在各网关产品中使用较广泛，兼容性较好）。 - AH(Authentication Header，鉴别首部)：该协议会对整个数据包完整性检查，包括外部 IP 报头，不对数据进行加密，若数据包在传输过程中数据被修改，则该数据包会被丢弃。
AH 验证算法	安全协议为 AH 时，当前隧道使用的验证算法。
ESP 验证算法	安全协议为 ESP 时，当前隧道使用的验证算法。
ESP 加密算法	安全协议为 ESP 时，当前隧道使用的加密算法。

10.4.8 IPSec VPN 配置举例

组网需求

某企业总部和分公司都使用路由器 M80–F 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

2 台路由器均建立 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。

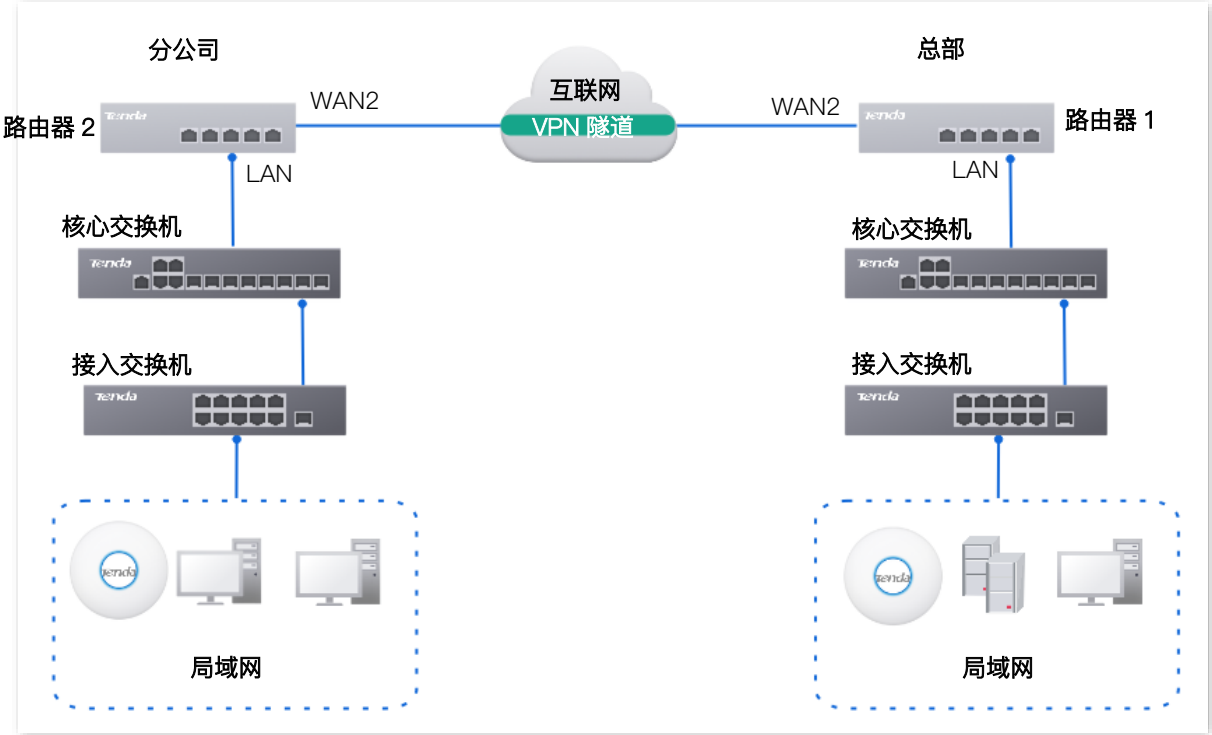
假设将路由器 1 部署在总部，基本信息如下：

- 建立 IPSec 隧道的接口为 WAN1。
- WAN2 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 2 台路由器进行 IPSec 连接时，用来验证身份的预共享密钥为 UmXmL9UK。



配置步骤

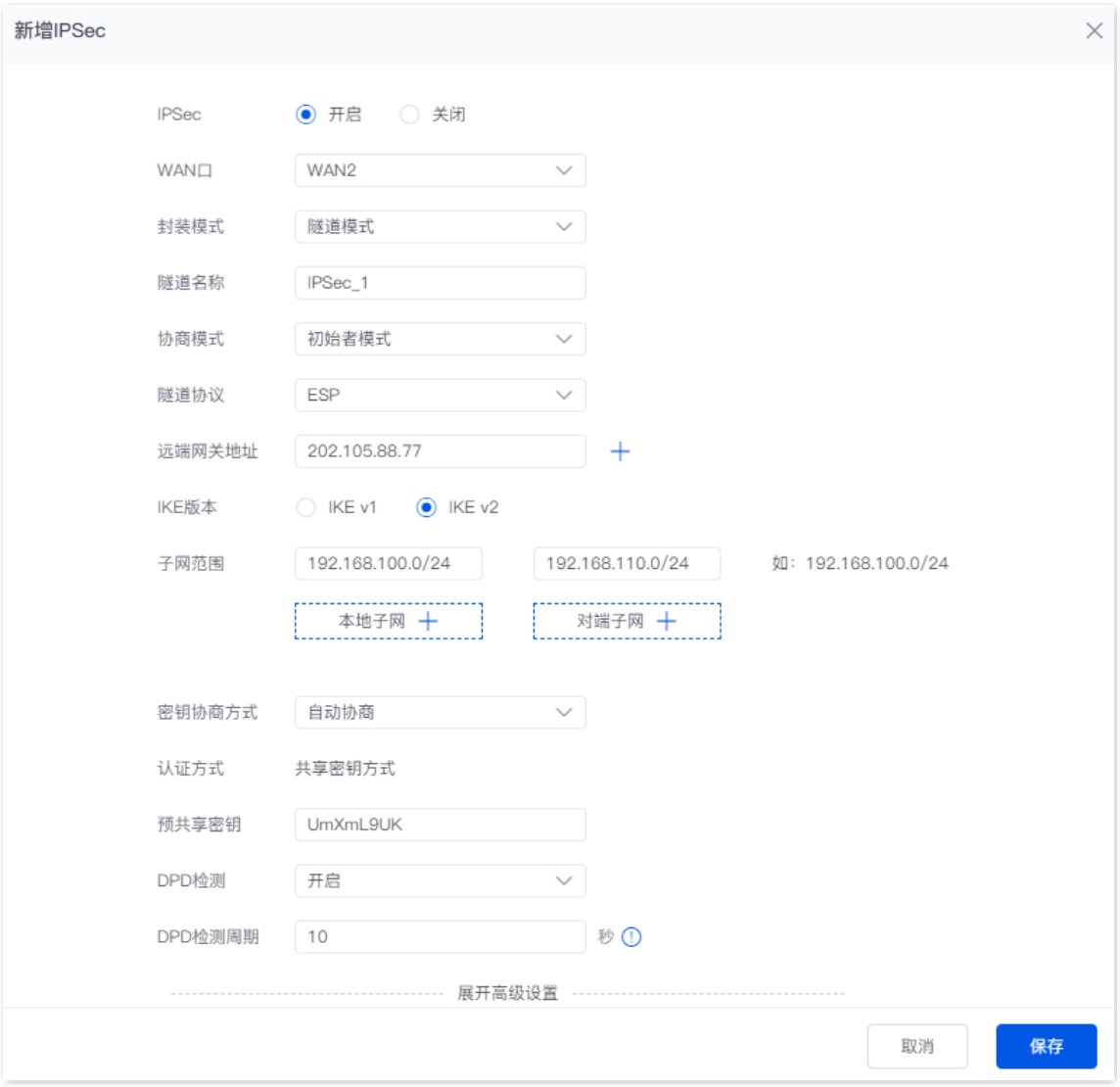
配置路由器 1　配置路由器 2

注意

配置过程中，如果需要设置 IPSec 连接的高级选项，请保持 2 台路由器的设置参数一致。

一、配置路由器 1

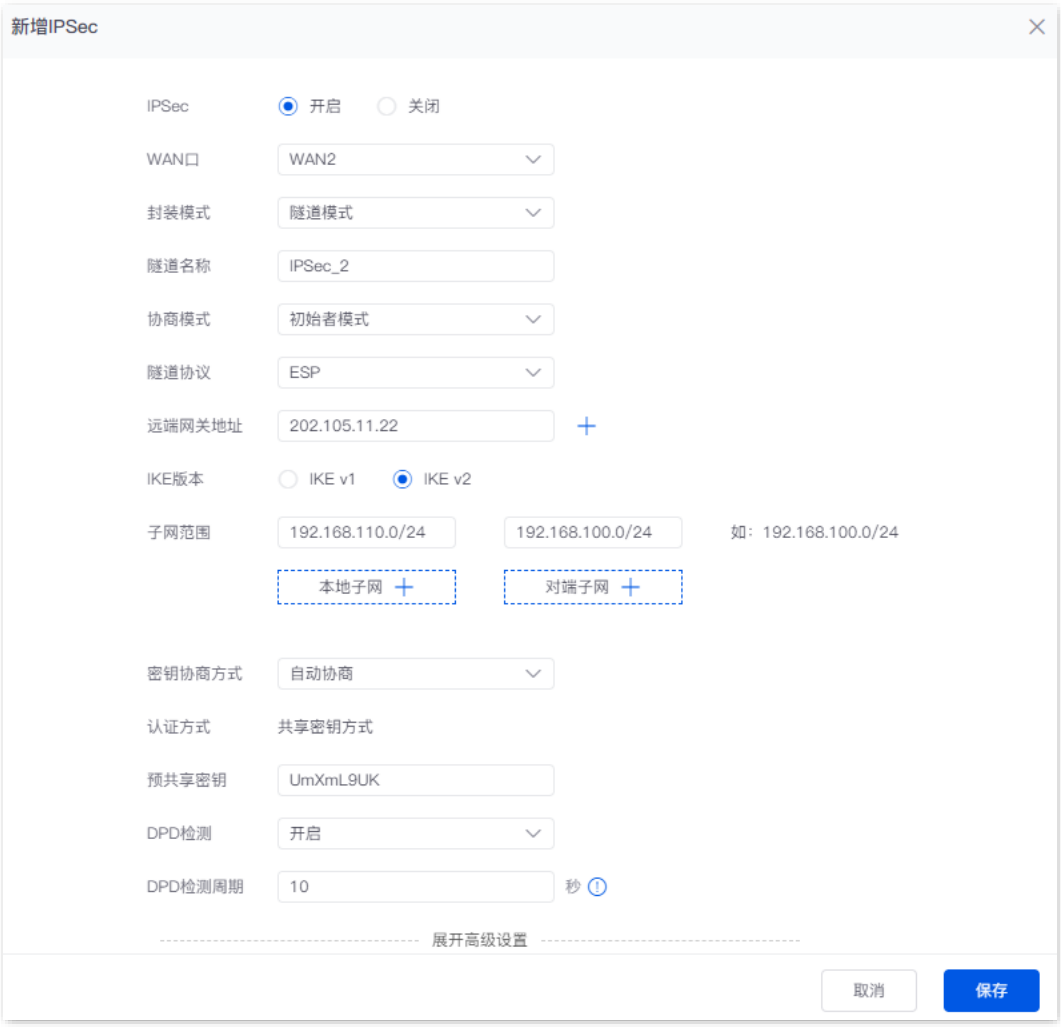
登录到路由器 1 的 Web 管理页面，进入「更多」>「VPN 服务」>「IPSec」页面，点击 新增，配置如下 IPSec。参数设置仅供参考。



路由器 1 的 IPSec 添加完成，如下图示。

二、配置路由器 2

登录到路由器 2 的 Web 管理页面，进入「更多」>「VPN 服务」>「IPSec」页面，点击 新增，配置如下 IPSec。参数设置仅供参考。

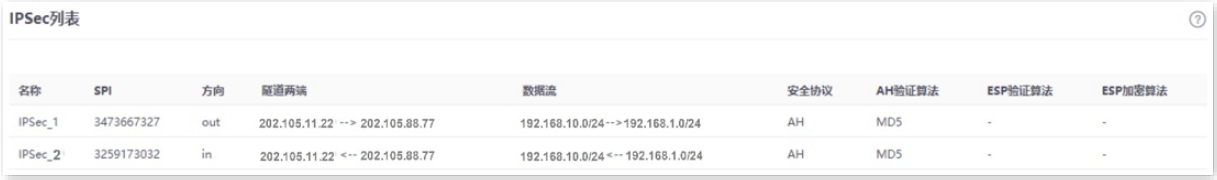


路由器 2 的 IPSec 添加完成，如下图示。

---完成

验证配置

进入 IPSec 列表中，若出现以下两条 IPSec SA，表示 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。


IPSec列表

名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
IPSec_1	3473667327	out	202.105.11.22 --> 202.105.88.77	192.168.10.0/24-->192.168.1.0/24	AH	MD5	-	-
IPSec_2	3259173032	in	202.105.11.22 <-- 202.105.88.77	192.168.10.0/24<-- 192.168.1.0/24	AH	MD5	-	-

10.5 IPv6

10.5.1 概述

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

IPv6 地址

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。

基本概念

- **DHCPv6**

IPv6 动态主机配置协议 DHCPv6（Dynamic Host Configuration Protocol for IPv6），属于有状态 IPv6 地址自动配置协议。DHCPv6 服务器可以给主机分配 IPv6 地址/前缀和其他网络配置参数。

- **SLAAC**

IPv6 的另一种动态主机配置协议 SLAAC（Stateless address autoconfiguration），属于无状态地址自动配置协议。主机通过路由通告（RA）方式自动生成 IPv6 地址/前缀和其他网络配置参数。

10.5.2 外网

登录到路由器 Web 管理页面后，点击「更多」>「IPv6」>「外网」。

您可以配置对应 WAN 口的 IPv6 地址信息。路由器 WAN 口支持两种 IPv6 地址获取方式，请根据上级设备的配置选择地址获取方式。

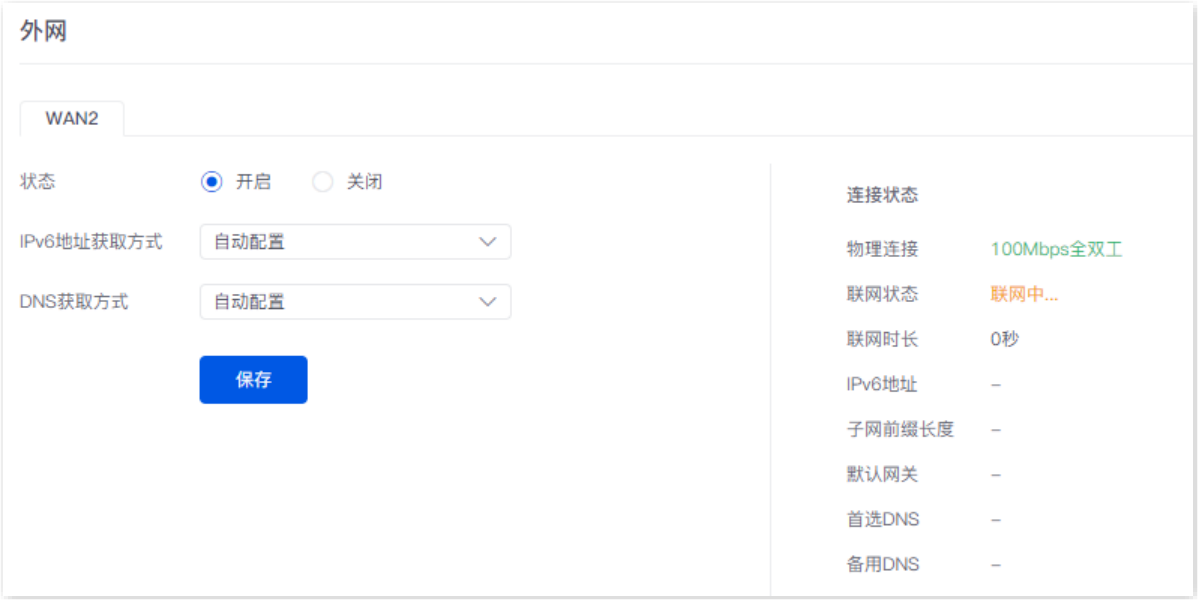
如果	请选择
上级设备的 LAN 口配置的 IP 地址分配方式为 DHCPv6、SLAAC 或 DHCPv6+SLAAC	
上级设备为宽带服务商设备，且运营商提供支持 IPv6 业务的宽带账号和宽带密码	自动配置
上级设备为宽带服务商设备，且运营商未提供具体上网参数	
上级设备不分配 IP 地址	
上级设备为宽带服务商设备，且运营商提供了一组用于上网的固定 IPv6 地址，包括 IP 地址、子网掩码、默认网关、DNS 服务器信息	手动设定

注意

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

自动配置

自动配置，即 WAN 口通过 DHCPv6 或 SLAAC 方式自动获取 IPv6 地址上网信息。WAN 口 IPv6 参数配置完成后，您可以在右侧“连接状态”模块查看 IPv6 联网状态。下图仅供参考。

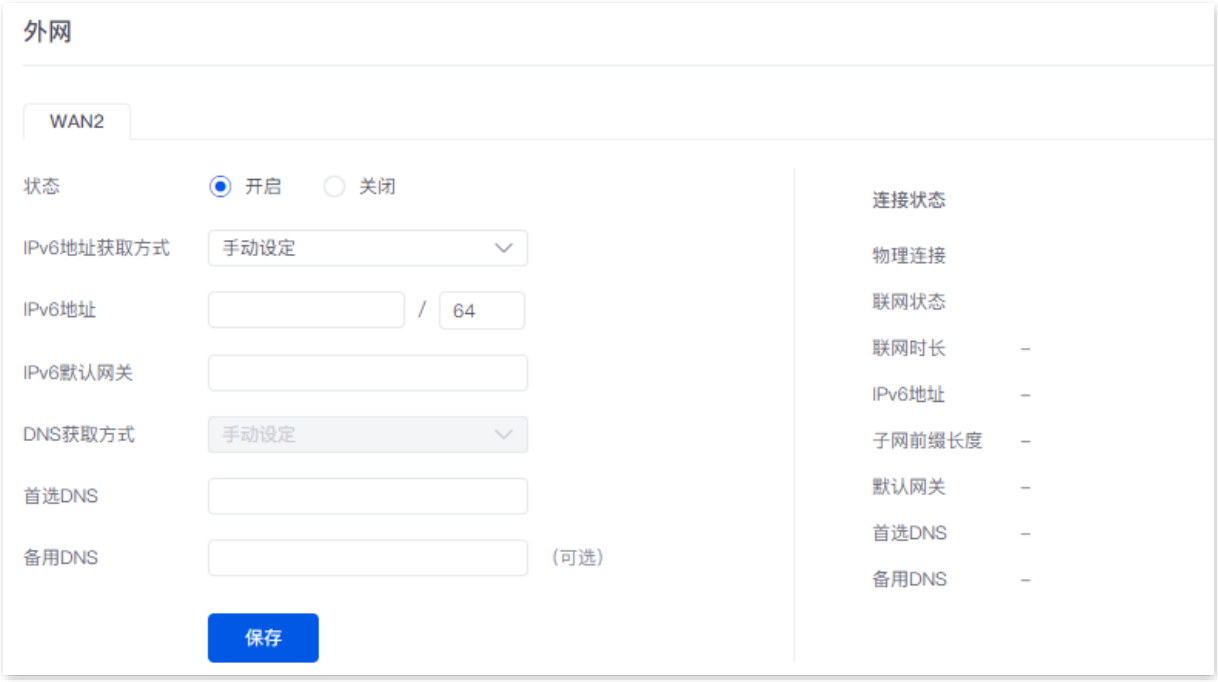


参数说明

标题项		说明
模式设定	状态	开启/关闭对应 WAN 口的 IPv6 功能。
	IPv6 地址获取方式	请选择自动配置。
	DNS 获取方式	对应 WAN 口获取 DNS 服务器地址的方式。 - 自动配置：通过 DHCPv6 或 SLAAC 方式自动获取 DNS 服务器地址。 - 手动设定：手动输入 DNS 服务器地址。
	首选 DNS	请输入正确的 IPv6 DNS 服务器地址。  如果只有一个 DNS 地址，“备用 DNS”可以不填。
	备用 DNS	
连接状态	物理连接	对应 WAN 口当前的速率和双工模式。
	联网状态	对应 WAN 口的连接状态。 - 已联网：路由器 WAN 口已插网线，并已经获得 IPv6 地址信息。 - 联网中...：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宽带服务商。
	联网时长	对应 WAN 口最近一次成功接入 IPv6 网络的时长。
	IPv6 地址	对应 WAN 口的 IPv6 全球单播地址。
	子网前缀长度	IPv6 地址的网络前缀位数。
	默认网关	对应 WAN 口的 IPv6 网关地址。
	首选 DNS	对应 WAN 口的首选/备用 IPv6 DNS 服务器地址。
	备用 DNS	

手动设定

手动设定，即手动输入宽带服务商提供的 IPv6 地址信息上网。



参数说明

标题项		说明
模式设定	状态	开启/关闭对应 WAN 口的 IPv6 功能。
	IPv6 地址获取方式	请选择手动设定。
	IPv6 地址	请输入宽带服务商提供的 IPv6 全球单播地址。
	IPv6 默认网关	请输入宽带服务商提供的 IPv6 网关地址。
	DNS 获取方式	对应 WAN 口获取 IPv6 DNS 服务器地址的方式。 仅支持“手动设定”，即，手动输入 IPv6 DNS 服务器地址。
	首选 DNS	请输入正确的 IPv6 DNS 服务器地址。 提示 如果只有一个 DNS 地址，“备用 DNS”可以不填。
	备用 DNS	
连接状态	物理连接	对应 WAN 口当前的速率和双工模式。
	联网状态	路由器对应 WAN 口的连接状态。 - 已联网：路由器 WAN 口已插网线，并已经获得 IPv6 地址信息。 - 联网中...：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宽带服务商。

标题项		说明
	联网时长	对应 WAN 口最近一次成功接入 IPv6 网络的时长。
	IPv6 地址	对应 WAN 口的 IPv6 全球单播地址。
	子网前缀长度	IPv6 地址的网络前缀位数。
	默认网关	对应 WAN 口的 IPv6 网关地址。
	首选 DNS	对应 WAN 口的首选/备用 IPv6 DNS 服务器地址。
	备用 DNS	

10.5.3 局域网

登录到路由器 Web 管理页面后，点击「更多」>「IPv6」>「局域网」。

您可以配置对应 VLAN 接口的 IPv6 地址信息，实现局域网内多台共享您办理的宽带服务上网。

VLAN 接口默认关闭 IPv6 功能，开启后，如下图所示。

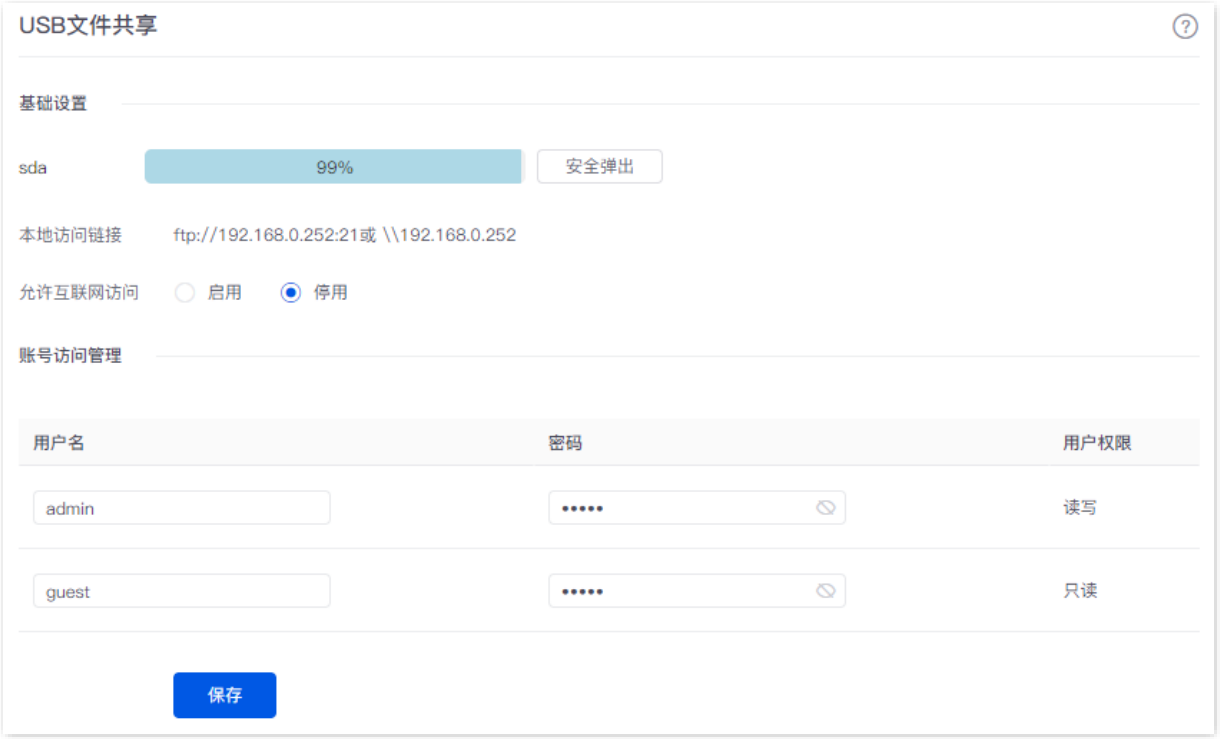
参数说明

标题项	说明
VLAN 接口	需配置 IPv6 功能的 VLAN 接口。
状态	开启/关闭该 VLAN 接口的 IPv6 功能
IPv6 地址获取方式	VLAN 接口获取 IP 地址的方式。 - 自动配置：VLAN 接口的 IPv6 地址前缀为“前缀代理接口”所选择的 WAN 口自动获取，IPv6 地址则由路由器根据标准自动生成。 - 手动配置：手动设置 VLAN 接口的 IP 地址前缀、完整的 IPv6 地址及地址分配方式。
前缀代理接口	VLAN 接口的 IPv6 地址前缀由该 WAN 口从上级设备处获取。“IPv6 地址获取方式”为“自动配置”时需要选择此项。
IPv6 地址前缀	VLAN 接口的 IPv6 地址前缀。
IPv6 地址	VLAN 接口完整的 IPv6 地址。
地址分配方式	路由器给局域网客户端分配 IPv6 地址的方式。 - DHCPv6：客户端直接从 DHCPv6 服务器获取全部的 IPv6 地址信息，包括 DNS 服务器等。 - SLAAC：客户端通过路由通告（RA）方式自动生成 IPv6 地址信息，包括 IPv6 地址、DNS 服务器等。 - SLAAC+DHCPv6：客户端通过路由通告（RA）方式自动生成 IPv6 地址，从 DHCPv6 服务器获取其他地址信息，如 DNS 服务器等。
开始地址	DHCPv6 服务器可分配的 IPv6 地址地址范围。 地址分配方式为 DHCPv6 时需要配置此项。
结束地址	
首选寿命	IPv6 地址租借期限的首选生命期。如果客户端在首选生命周期时间内未收到路由通告（RA），则会将该 IPv6 地址废止，不再使用该 IPv6 地址建立新的连接，但接收目的地址为该 IPv6 地址的报文。
有效寿命	IPv6 地址租借期限的有效生命期。到期后该 IPv6 地址将被删除，变成无效地址，断开所有会话。
首选 DNS	分配给客户端的首选/备用 DNS 服务器 IP 地址。 注意 为了使局域网设备能够正常上网，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。
备用 DNS	

10.6 USB 应用

登录到路由器 Web 管理页面后，点击「更多」>「USB 应用」。

当路由器的 USB 口插入 U 盘等 USB 存储设备时，您可以允许局域网用户或互联网用户通过账号和密码访问 USB 设备内容。



10.7 局域网 IP 扫描

通过局域网 IP 扫描功能，您可以扫描并查看路由器 LAN 口下指定 IP 网段内的所有设备，包括从路由器 DHCP 服务器获取 IP（打开“展示 DHCP 用户“开关后可扫描）的设备和您在设备端手动设置静态 IP 的设备。

设置步骤：

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「更多」>「局域网 IP 扫描」。

步骤 3 选择需要扫描的路由器接口，如“LAN3”、“LAN4”、“LAN5”、“LAN6”。

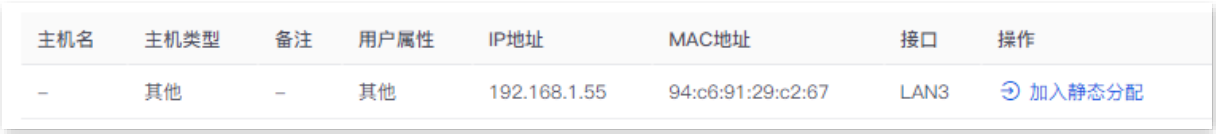
步骤 4 设置扫描的“开始 IP”和“结束 IP”，如“192.168.0.1”~“192.168.1.255”。

步骤 5 （可选）若要扫描从路由器 DHCP 服务器获得 IP 地址的设备信息，打开“展示 DHCP 用户”开关。

步骤 6 点击 开始扫描 。下图仅供参考。

----结束

稍等片刻，页面将显示连接在路由器 LAN 口但手动设置静态 IP 的设备的信息。下图仅供参考。点击加入静态分配，设备将显示在 DHCP 静态分配页面，由路由器分配该 IP 地址给设备，分配结果见 DHCP 静态分配页面的状态栏。



主机名	主机类型	备注	用户属性	IP地址	MAC地址	接口	操作
-	其他	-	其他	192.168.1.55	94:c6:91:29:c2:67	LAN3	加入静态分配

11 系统工具

本指南仅作为功能配置参考，不代表产品支持本指南内提及的全部功能。不同型号、不同版本产品的功能支持情况也可能存在差异，请以实际产品的 Web 管理页面为准。

11.1 系统时间

登录到路由器 Web 管理页面后，点击「工具」>「系统时间」。

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。路由器支持与网络时间同步和手动设置系统时间两种时间设置方式，默认为“与网络时间同步”。

11.1.1 与网络时间同步

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。

设置完成后刷新一下页面，您可以查看路由器的当前时间是否校对准确。

11.1.2 手动设置系统时间

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“手动设置系统时间”时，页面展开的相关参数如下图所示。

设置完成后刷新一下页面，您可以查看路由器的当前时间是否校对准确。

11.2 排障工具

11.2.1 Ping

Ping 用于检测网络的连通性和连通质量。

假设要检测路由器到 QQ 官网（www.qq.com）的链路是否畅通。

步骤 1 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。

步骤 2 选择“工具”为“Ping”。

步骤 3 选择数据出去的接口，本例为“WAN1”。

步骤 4 输入目的 IP 地址或域名，本例为“www.qq.com”。

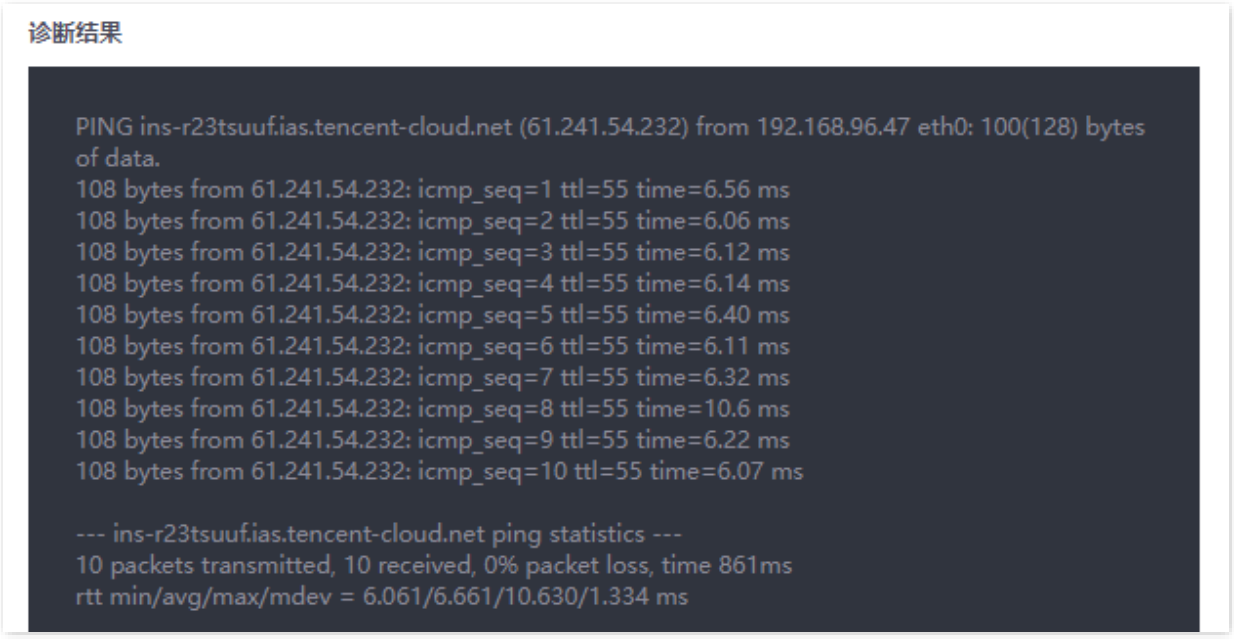
步骤 5 设置 ping 发送的数据包的个数，如“10”。

步骤 6 设置 ping 发送的数据包的大小，如“100”。

步骤 7 点击 开始 。

----完成

稍后，诊断结果将显示在页面下方。如下图示。



11.2.2 Tracert

Tracert 用于检测数据包从路由器到目标主机所经过的路由。

假设要检测路由器到 QQ 官网（www.qq.com）所经过的路由。

步骤 1 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。

步骤 2 选择“工具”为“Tracert”。

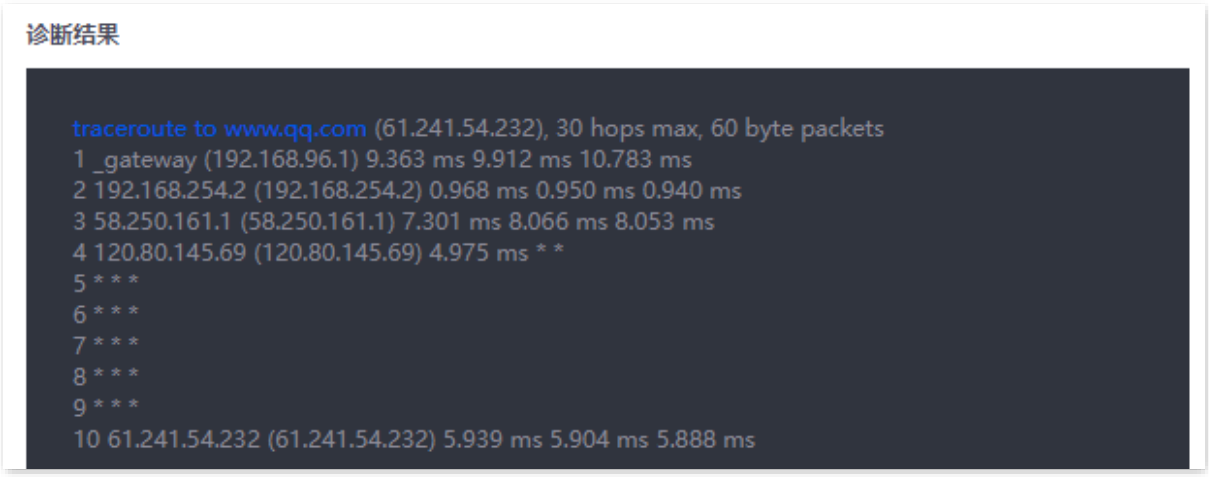
步骤 3 选择数据出去的接口，本例为“WAN1”。

步骤 4 输入目的 IP 地址或域名，本例为“www.qq.com”。

步骤 5 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。



11.2.3 抓包工具

抓包工具，可以将网络中传送的数据包完全截获下来，方便分析。

假设要截获路由器 LAN4 口的所有类型数据包，LAN4 口 IP 地址为 192.168.0.250，属于 VLAN_Default。

步骤 1 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。

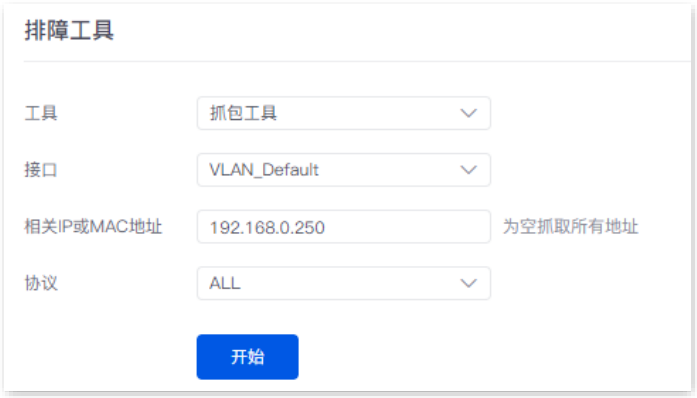
步骤 2 选择“工具”为“抓包工具”。

步骤 3 选择要截获数据的 VLAN 接口，本例为“VLAN_Default”。

步骤 4 输入 LAN4 口 IP 地址，本例为“192.168.0.250”。

步骤 5 选择数据协议类型，本例为“ALL”。

步骤 6 点击 开始 。



步骤 7 抓包过程中，可根据需要点击 结束 。

步骤 8 点击 下载 。pcap 类型的文件将下载到本地电脑，可以用抓包软件（WireShark）打开查看。

----完成

参数说明

标题项	说明
接口	要截获数据的 VLAN 接口。
相关 IP 地址或 MAC 地址	接口连接的设备的 IP 或 MAC 地址。为空表示抓取 VLAN 下所有接口的数据报文。 提示 如果所填的 IP 地址或 MAC 地址在网络中不存在，或不在所设置的 VLAN 接口下，则不会截获到报文。

标题项	说明
协议	数据协议类型。ALL 表示包括 ICMP、TCP、UDP 和 ARP 四种协议。 - ICMP：Internet Control Message Protocol，即 Internet 控制报文协议。用于在 IP 主机、路由器之间传递控制消息，包括网络通不通、主机是否可达、路由是否可用等。 - TCP：Transmission Control Protocol，即面向连接的通信协议。通过三次握手建立连接，通讯完成时要拆除连接，只能用于端到端的通讯，如 Telnet、FTP。 - UDP：User Datagram Protocol，即用户数据报协议。UDP 数据包括目的端口和源端口信息，通讯不需要连接，可以实现广播发送。使用 UDP 的服务包括 DNS、SNMP 等。 - ARP：Address Resolution Protocol，即地址解析协议，是根据 IP 地址获取物理地址的一个 TCP/IP 协议。

11.2.4 AP 故障诊断

AP 故障诊断：根据 AP 的 MAC 地址查看 AP 的情况，包括在线情况、IP 地址、所属 AP 分组。

假设要对网络中某一 AP（假设地址为 D8:38:0D:99:8B:B0）进行诊断。

步骤 1 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。

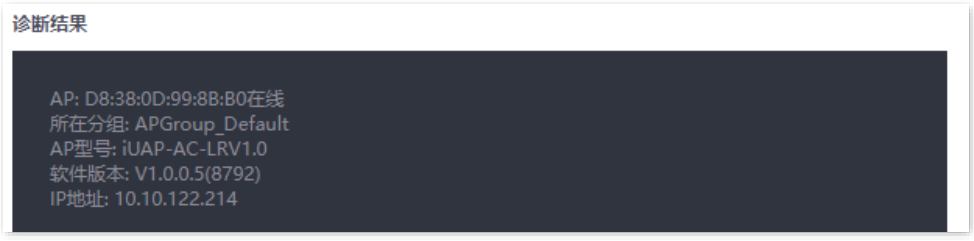
步骤 2 选择“工具”为“AP 故障诊断”。

步骤 3 输入要诊断的 AP 的 MAC 地址，本例为“D8:38:0D:99:8B:B0”。

步骤 4 点击 开始 。

----完成

稍等片刻，结果将会显示在下方区域，如下图示。



11.2.5 系统诊断

系统诊断，可以查看系统所有进程的状态信息。

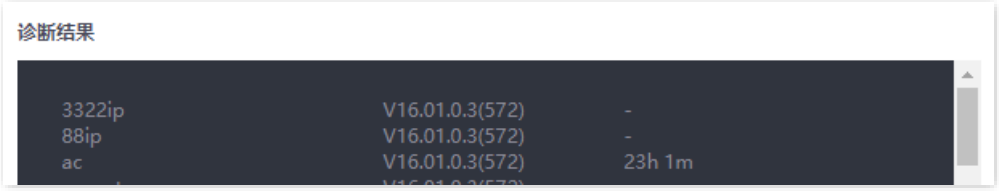
步骤 1 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。

步骤 2 选择“工具”为“系统诊断”。

步骤 3 点击 开始 。

----完成

稍等片刻，结果将会显示在下方区域，拉动滚动条可以查看更多信息，如下图示。



11.2.6 接口信息

您可以查看设备接口信息，包括物理接口、桥接口、隧道接口、VLAN 虚拟接口。桥接口和 VLAN 虚拟接口在创建 VLAN 接口时生成，但 VLAN 为 1 时不生成 VLAN 虚拟接口；隧道接口在创建 Wi-Fi 时生成。

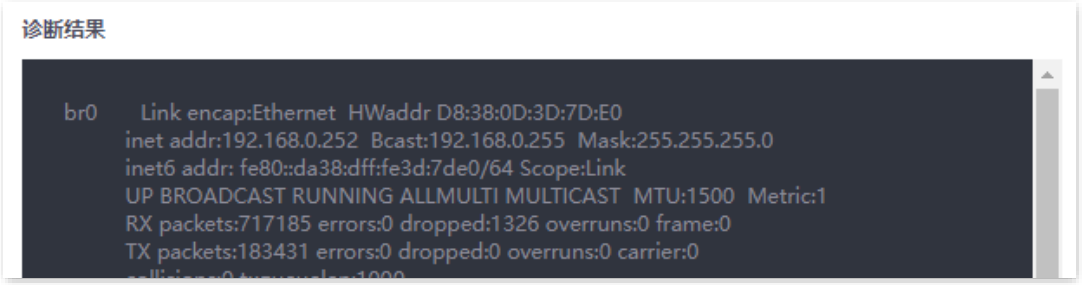
步骤 1 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。

步骤 2 选择“工具”为“接口信息”。

步骤 3 点击 开始 。

----完成

稍等片刻，结果将会显示在下方区域，拉动滚动条可以查看更多信息，如下图示。



11.3 日志中心

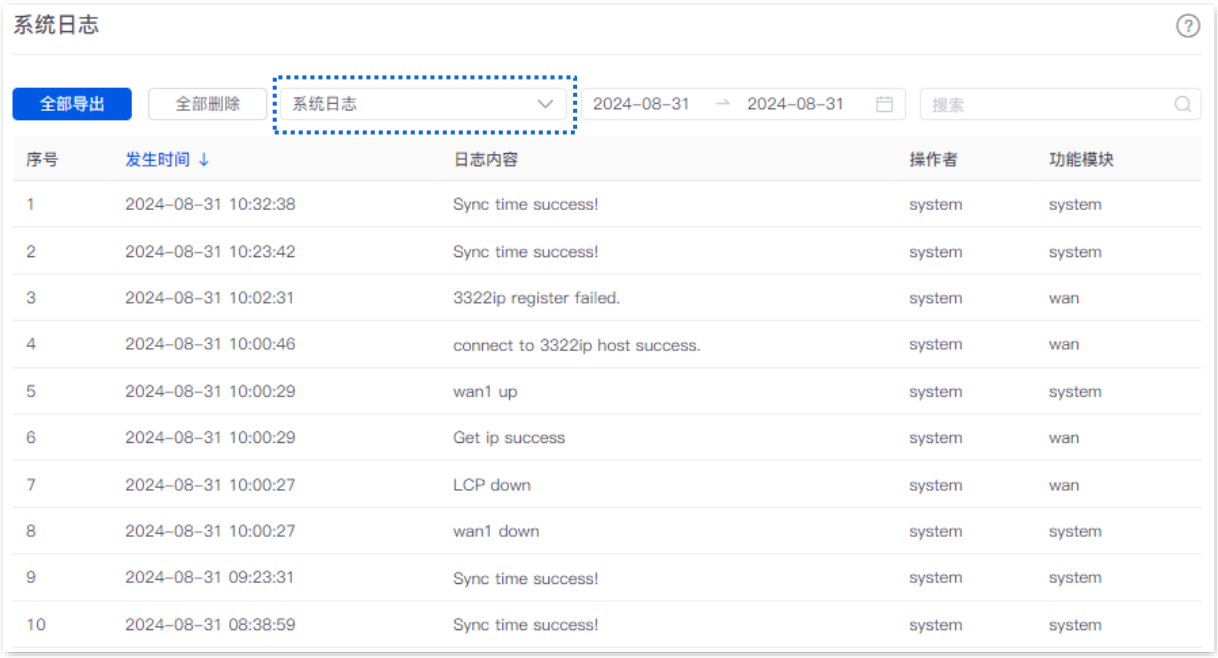
登录到路由器 Web 管理页面后，点击「工具」>「日志中心」。

您可以查看路由器记录的日志信息。日志中心记录了路由器的系统日志、操作日志和运行日志。如遇网络故障，可以利用路由器的日志信息进行问题排查。

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。

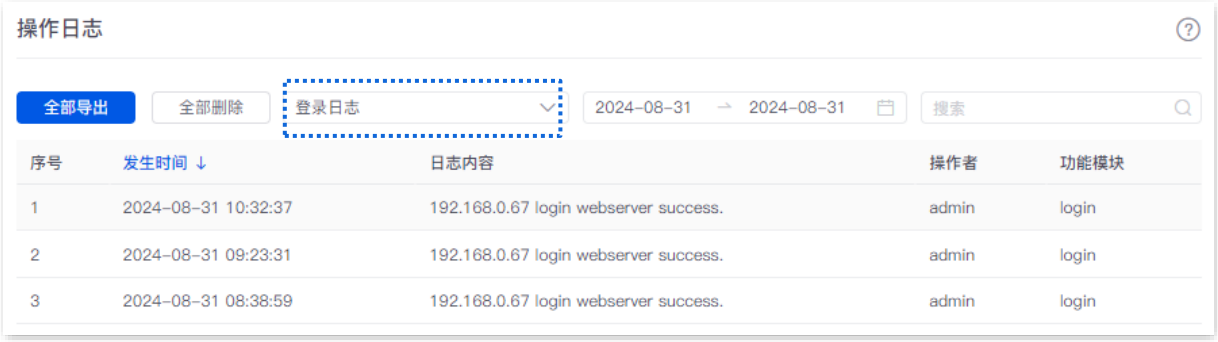
11.3.1 系统日志

系统日志记录系统运行相关日志信息，如 DHCP 日志、拨号日志等。点击下拉框选择相应日志类型即可查看。



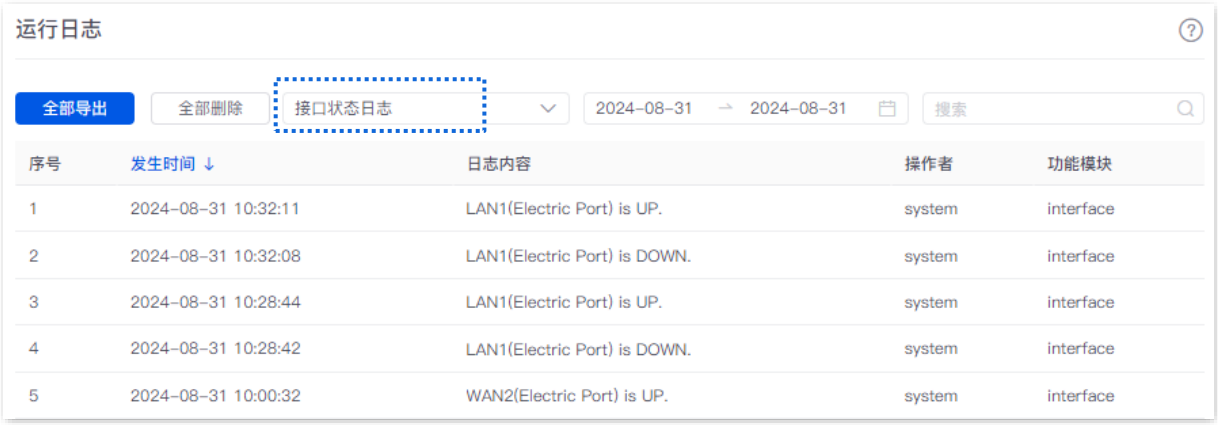
11.3.2 操作日志

操作日志记录用户对路由器进行的操作，如登录日志、配置变更。点击下拉框选择相应日志类型即可查看。



11.3.3 运行日志

运行日志记录系统进程运行、AP 上报等信息。点击下拉框选择相应日志类型即可查看。



11.4 系统维护

11.4.1 设备信息

登录到路由器 Web 管理页面后，点击「工具」>「系统维护」>「设备信息」。

您可以查看路由器的基本信息，包括 CPU 使用率、内存使用率、系统时间和系统运行时长。

11.4.2 配置备份与恢复

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。

备份配置

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「工具」>「系统维护」>「配置备份与恢复」。

步骤 3 点击 导出 。

----完成

浏览器将下载文件名为 RouterCfm.cfg 的配置文件。

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”。

恢复配置

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「工具」>「系统维护」>「配置备份与恢复」。

步骤 3 点击 浏览 ，选择并加载之前备份的配置文件。

步骤 4 点击 导入 。

步骤 5 确认提示信息后，点击 确定 。

----完成

将出现恢复进度提示，请耐心等待。进度条显示 100%时，路由器配置恢复完成。

11.4.3 恢复出厂设置

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，却忘记登录密码时，可以将路由器恢复出厂设置后重新设置。路由器支持软件恢复出厂设置和硬件恢复出厂设置两种方式。

恢复出厂设置后，路由器的 LAN 口 IP 地址为 192.168.0.252。

注意

- 恢复出厂设置后，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。请谨慎操作。
- 为避免损坏路由器，恢复出厂设置过程中，请确保路由器供电正常。

软件恢复出厂设置

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「工具」>「系统维护」>「恢复出厂设置」。

步骤 3 点击 恢复出厂 。

步骤 4 确认提示信息后，点击 确定 。

----完成

将出现恢复出厂进度提示，请耐心等待。进度条显示 100%时，路由器恢复出厂完成，请重新设置路由器。

硬件恢复出厂设置

使用此方式时，您无需进入路由器管理页面就可以将路由器恢复出厂设置。操作方法如下：

路由器系统灯闪烁状态下，用针状物按住机身前面板上的复位按钮约 8 秒，待指示灯全亮时松开。当系统灯重新闪烁时，路由器恢复出厂设置成功。

11.5 升级服务

登录到路由器 Web 管理页面后，点击「工具」>「升级服务」。

您可以对路由器进行软件升级和特征库升级。

- 系统软件升级：您可以通过升级路由器软件，体验更多功能，获得更好的用户体验。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：更新路由器的特征库。升级特征库不会对路由器系统软件产生影响。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	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 升级 ，系统将自动下载升级文件，并进行升级。

11.5.1 系统软件本地升级

注意

- 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 登录到路由器 Web 管理页面，点击「工具」>「升级服务」>「系统软件升级」。

步骤 3 选择“升级方式”为“本地升级”。

步骤 4 点击 浏览 ，找到并载入相应目录下的升级软件，然后点击 升级 。

步骤 5 确认提示信息后，点击 确定 。

----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「工具」>「升级服务」>「系统软件升级」页面，查看路由器当前的软件版本号来确认是否升级成功。

11.5.2 特征库本地升级

注意

- 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.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，下载对应型号的路由器最新的特征库文件并存放到本地电脑。

步骤 2 登录到路由器 Web 管理页面，点击「系统工具」>「升级服务」>「特征库升级」。

步骤 3 选择“升级方式”为“本地升级”。

步骤 4 点击 浏览 ，找到并载入相应目录下的特征库文件，然后点击 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「工具」>「升级服务」>「特征库升级」页面，查看当前的特征库版本号来确认是否升级成功。

11.6 重启

11.6.1 立即重启

重启路由器，可以提升路由器运行性能。重启过程中将断开当前网络连接，过程约 1 分钟。请在网络相对空闲时重启。

重启步骤：

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「系统工具」>「重启服务」>「重启」。

步骤 3 点击 重启设备 。确认提示信息后点击 确定 。

----完成

11.6.2 定时重启

定时重启，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。

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。

定时重启步骤：

步骤 1 登录到路由器 Web 管理页面。

步骤 2 点击「工具」>「重启服务」>「定时重启」。

步骤 3 开启定时重启功能。

步骤 4 选择路由器自动重启的时间点，如“03:00”。

步骤 5 设置重启日期，如“星期四”。

步骤 6 点击 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。

11.7 网络体检

11.7.1 网络诊断

登录到路由器 Web 管理页面后，点击「工具」>「网络体检」>「网络诊断」。

您可以检测路由器的网络状态，如果检测出网络异常，会上报到网络监控日志。

注意

点击 开始诊断 后，可能会持续一段时间，无法暂停或手动结束，请在相对空闲时操作。

11.7.2 终端检测

登录到路由器 Web 管理页面后，点击「工具」>「网络体检」>「终端检测」。

您可以通过设备 MAC 地址查询其 IP 地址。下图仅供参考。

11.7.3 WAN 口诊断

登录到路由器 Web 管理页面后，点击「工具」>「网络体检」>「WAN 口诊断」。

您可以点击 诊断 对路由器 WAN 口进行联网诊断。下图仅供参考。

参数说明

标题项	说明
网口选择	需要诊断的 WAN 口。
WAN 口诊断	检查 WAN 口的上网方式、接线情况及联网状态。
DNS 诊断	检查 WAN 口是否能够正常解析域名。
延时诊断	检查 WAN 口的网络延迟情况。

标题项	说明
HTTP 访问诊断	检查 WAN 口是否能够正常收到 HTTP 响应。

11.7.4 网络监控日志

登录到路由器 Web 管理页面后，点击「工具」>「网络体检」>「网络监控日志」。

您可以查看路由器的网络监控日志，如果碰到网络故障问题，可优先查看监控日志，方便快速定位问题。

参数说明

标题项	说明
发生时间	异常日志出现的时间。
日志内容	异常日志的内容。
厂商	局域网内检测到异常 DHCP 服务器设备的厂商信息。
MAC 地址	局域网内检测到异常 DHCP 服务器设备的 MAC 地址。
IP 地址	局域网内检测到异常 DHCP 服务器设备的 IP 地址。

11.8 系统账号

登录到路由器 Web 管理页面后，点击「工具」>「系统账号」。

您可以添加/修改/删除管理员账号和访客账号。

参数说明

标题项	说明
角色	登录路由器 Web 管理页面的账号类型。 - 管理员：使用此账号登录路由器后，您可以查看、配置路由器的所有功能。 - 访客：使用此账号登录路由器后，您仅可以查看路由器除系统账号信息之外的其他功能配置。
密码	设置账号对应的登录密码。
确认密码	
备注	账户的备注信息。
登录 IP 限制	设置后，只有该 IP 地址或 IP 地址段的用户可以使用该账号登录设备管理页面，不设置则不限制 IP 地址。

附录

A 纯 AC 模式下设置路由器联网

步骤 1 纯 AC 模式下登录路由器管理页面。

步骤 2 点击「网络」>「LAN 口设置」。在“IP 地址设置”模块，设置路由器的 LAN 口信息后，点击 保存 。下图仅供参考。

- 设置路由器 IP 地址，使其与上级网关的 LAN IP 地址在同一网段且未被其他设备占用。
- 子网掩码保持默认为 255.255.254.0。
- 设置默认网关为上级网关的 LAN IP 地址。
- 设置首选 DNS 为正确的 DNS 服务器或 DNS 代理的 IP 地址。

步骤 3 设置管理电脑为“自动获得 IP 地址”，“自动获得 DNS 服务器地址”。

----完成

在浏览器地址栏中输入新设置的路由器 IP 地址，可重新登录到路由器的管理页面。在「系统」的“联网信息”模块，可看到路由器已联网。

B 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）

缩略语	全称
CHAP	询问握手认证协议（Challenge Handshake Authentication Protocol）
CPU	中央处理器（Central Processing Unit）
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）
DMZ	非军事区（Demilitarized zone）
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）
FTP	文件传输协议（File Transfer Protocol）
GRE	通用路由封装（Generic Routing Encapsulation）
HTTP	超文本传送协议（Hyper Text Transfer Protocol）
HTTPS	超文本传输安全协议（Hyper Text Transfer Protocol Secure）
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）
IPSec	IP 安全性（IP Security）
ISAKMP	互联网安全性关联和密钥管理协议（Internet Security Association and Key Management Protocol）
ISP	互联网服务提供商（Internet Service Provider）
LAN	局域网（Local Area Network）
LCP	链路控制协议（Link Control Protocol）
LDAP	轻型目录访问协议（Lightweight Directory Access Protocol）
L2TP	二层隧道协议（Layer 2 Tunneling Protocol）
MAC	媒体接入控制（Medium Access Control）
MPDU	MAC 协议数据单元（MAC Protocol Data Unit）
MPPE	微软点对点加密（Microsoft Point-to-Point Encryption）

缩略语	全称
MSDU	MAC 服务数据单元（MAC Service Data Unit）
MTU	最大传输单元（Maximum Transmission Unit）
NAT	网络地址转换（Network Address Translation）
PAP	密码认证协议（Password Authentication Protocol）
PFS	完全前向保密（Perfect Forward Secrecy）
PPP	点对点协议（Point to Point Protocol）
PPPoE	基于以太网的点对点通讯协议（Point to Point Protocol over Ethernet）
PPTP	点对点隧道协议（Point to Point Tunneling Protocol）
RSSI	接收的信号强度指示（Received Signal Strength Indication）
SA	安全联盟（Security Association）
SDN	软件定义网络（Software Defined Network）
SLAAC	无状态地址自动配置协议（Stateless address autoconfiguration）
SMTP	简单邮件传输协议（Simple Mail Transfer Protocol）
SPI	安全参数索引（Security Parameter Index）
SSID	服务集标识符（Service Set Identifier）
TCP	传输控制协议（Transmission Control Protocol）
TKIP	临时密钥完整性协议（Temporal Key Integrity Protocol）
TLS	安全传输层协议（Transport Layer Security）
UDP	用户数据报协议（User Datagram Protocol）
UPnP	通用即插即用（Universal Plug and Play）
URL	统一资源定位符（Uniform Resource Locator）
USB	通用串行总线（Universal Serial Bus）
VLAN	虚拟局域网（Virtual Local Area Network）
VPN	虚拟专用网（Virtual Private Network）
WAN	广域网（Wide Area Network）
WMM	无线多媒体（Wi-Fi Multimedia）
WPA	Wi-Fi 网络安全接入（Wi-Fi Protected Access）
WPA-PSK	WPA 预共享密钥（WPA-Preshared Key）

深圳市和为顺网络技术有限公司

地址：深圳市南山区西丽中山园路 1001 号 TCL 高新科技园 E3 栋 1 层 A 单元 101 房

网址：www.Tenda.com.cn

技术支持邮箱：Tenda@Tenda.com.cn