IP-COM

Web 配置指南

企业级路由器

www.ip-com.com.cn

声明

由于产品版本升级或其它原因，本文档内容会不定期更新。除非另有约定，本文档仅作为使用指导，文中的所有陈述、信息和建议均不构成任何形式的担保。

前言

感谢选择 IP-COM 产品。开始使用本产品前，请先阅读本手册。

适用型号

本手册适用于 IP-COM 企业级路由器系列产品。文中涉及到的“路由器”、“产品”均指 IP-COM 企业级路由器系列产品，如无特殊说明，下文均以型号 M30 为例。

不同型号产品的 Web 页面可能存在差异，请以实际产品的 Web 页面为准。

约定

本文用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
按钮	边框+底纹	点击 确定 。

本文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。

相关资料获取方式

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

产品资料一览表

文档名称	概述
产品彩页	帮助您了解路由器的基本参数。包括产品概述、产品特性、产品规格等。
用户手册	帮助您快速设置路由器联网。包括路由器的外观、安装、连线、上网设置指导、安全注意事项、保修政策等。
快速安装指南	帮助您快速使用路由器。包括包装清单、产品外观、安装方式及注意事项、连线、上网设置指导、常见问题等。
Web 配置指南	帮助您了解路由器的更多功能配置。包括路由器管理页面上的所有功能介绍。

技术支持

如需了解更多信息，请通过以下方式与我们联系。

40066-50066	ip-com@ip-com.com.cn	www.ip-com.com.cn

修订记录

版本号	修订内容	发布日期
V1.0	首次发行	2022-12-28

目录

1 工作模式

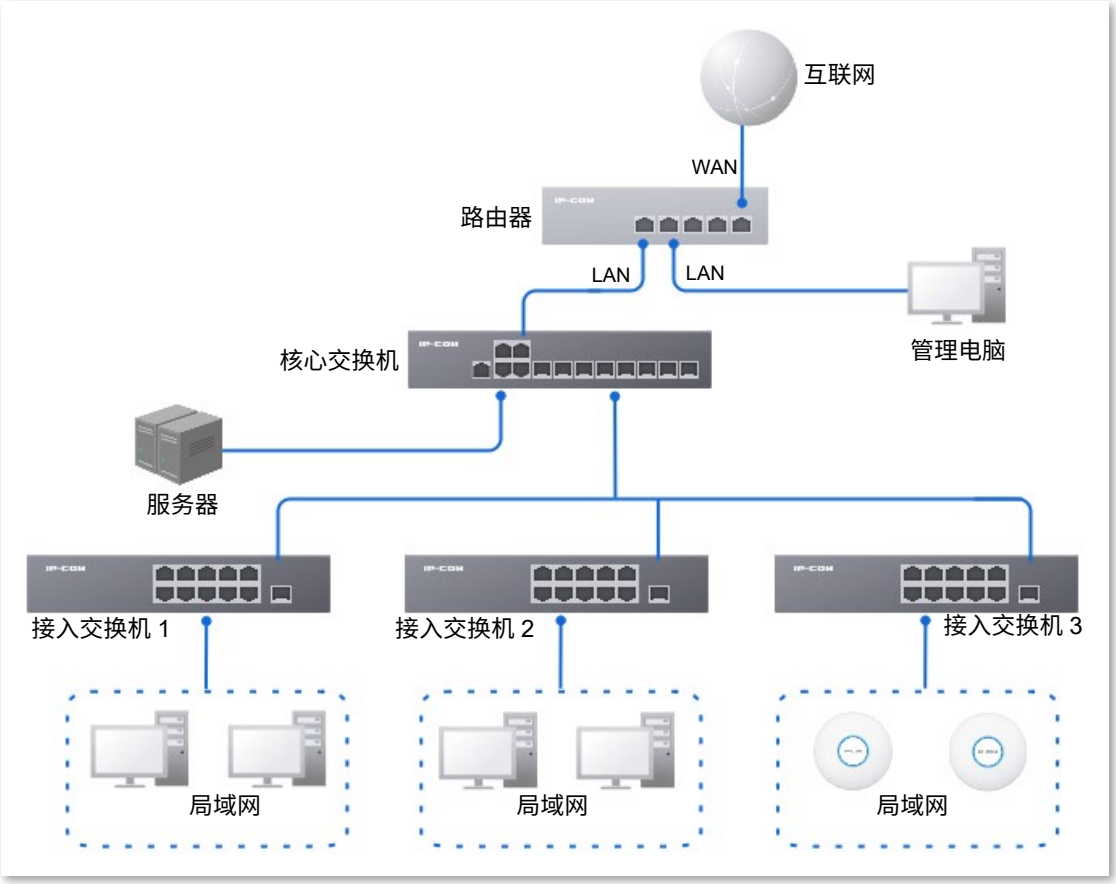
本路由器支持多种工作模式，请根据实际情况选择。正文说明以路由模式为例。

- 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

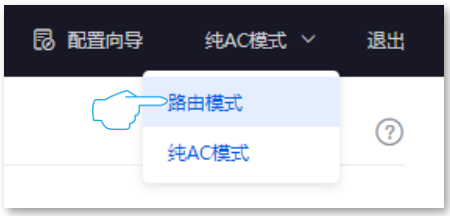
1.1.1 概述

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。

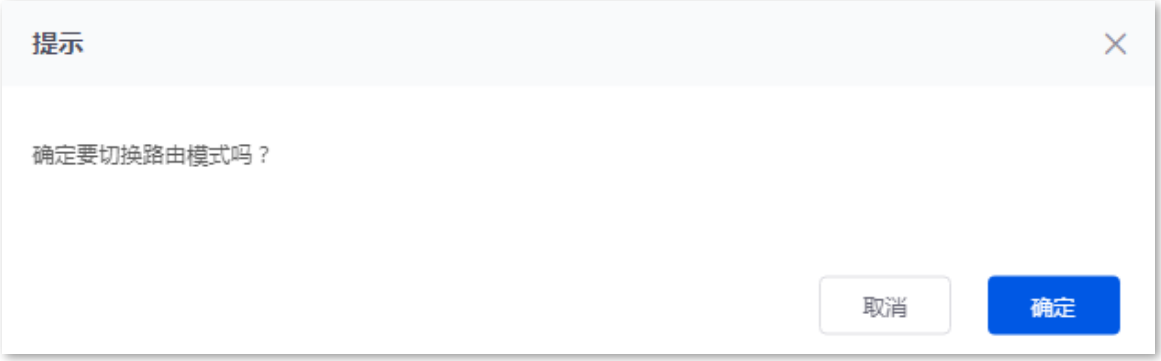


1.1.2 设置路由器工作在路由模式

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“路由模式”。下图仅供参考。



2. 确认提示信息后，点击 确定 。



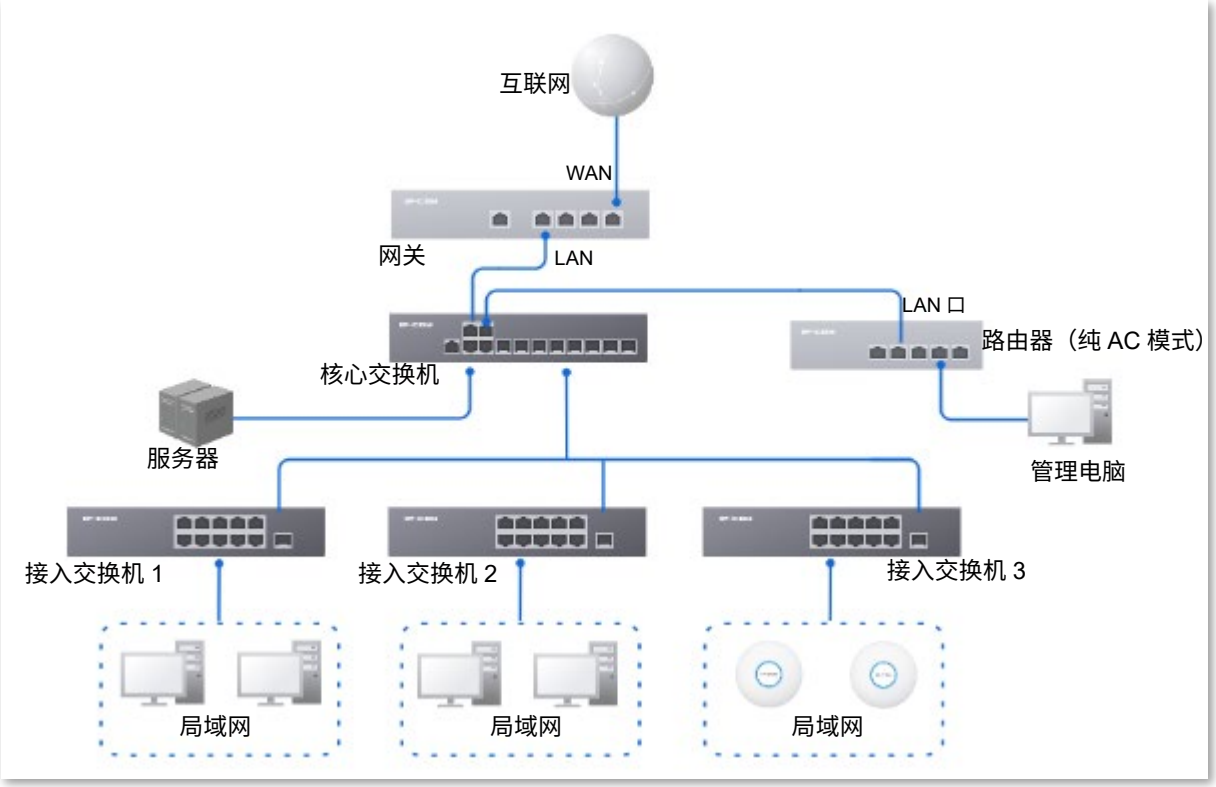
---完成

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。



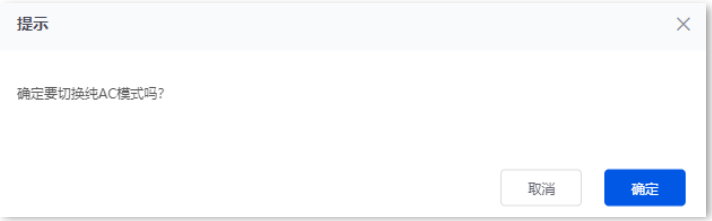
提示

纯 AC 模式下，如果您要使用路由器的远程 WEB 管理、云维护、远程调试功能，请另外将路由器通过WAN口连接至其他互联网，并通过动态 IP 或静态 IP 方式设置路由器成功联网，否则配置无效。

1.2.2 设置路由器工作在纯 AC 模式

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”。

2. 确认提示信息后，点击 确定 。



---完成

2 登录 Web 管理界面

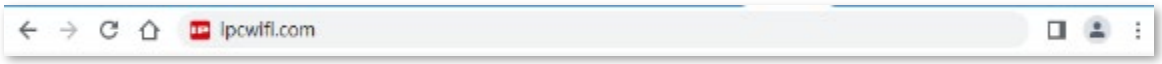
2.1 登录

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（前往 www.ip-com.com.cn 可下载安装指南）。否则，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

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



3. 输入登录密码，点击 登录 。

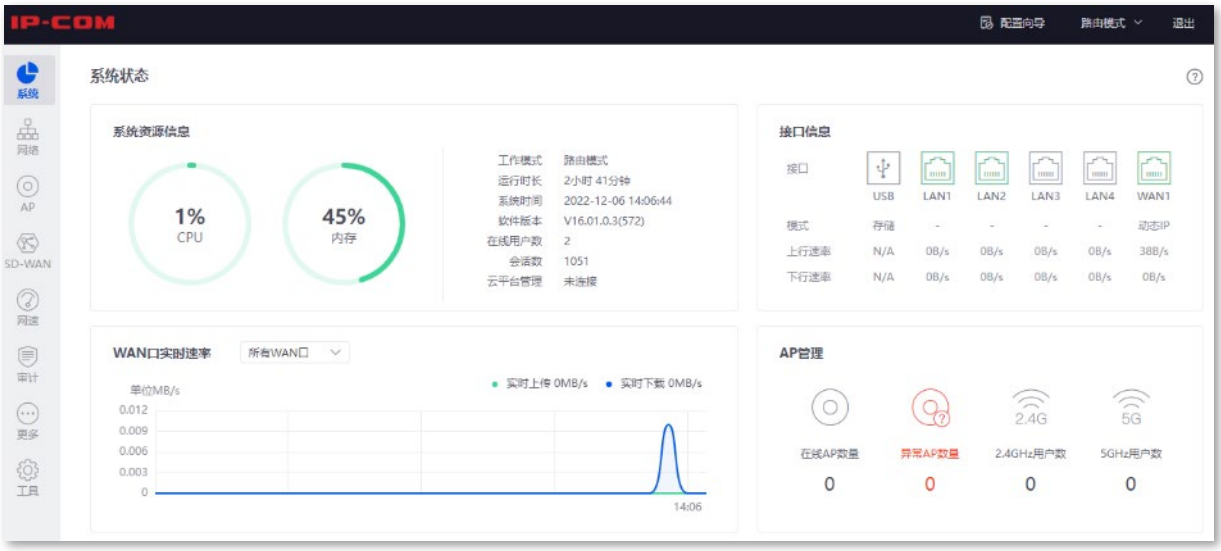
---完成

提示

如果未出现上述页面，请尝试使用以下办法解决：

- 确保管理电脑连接正常，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”。
- 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将路由器联网。

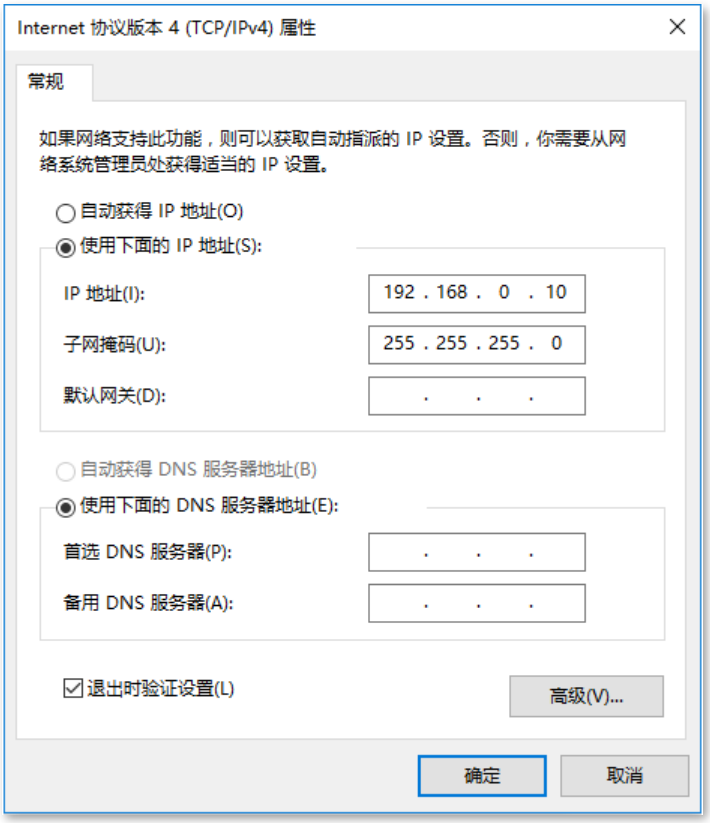
成功登录路由器管理页面。



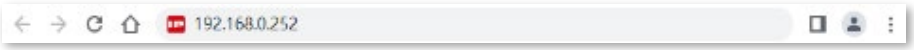
纯 AC 模式下登录设备管理页面

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。
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”。



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”）。



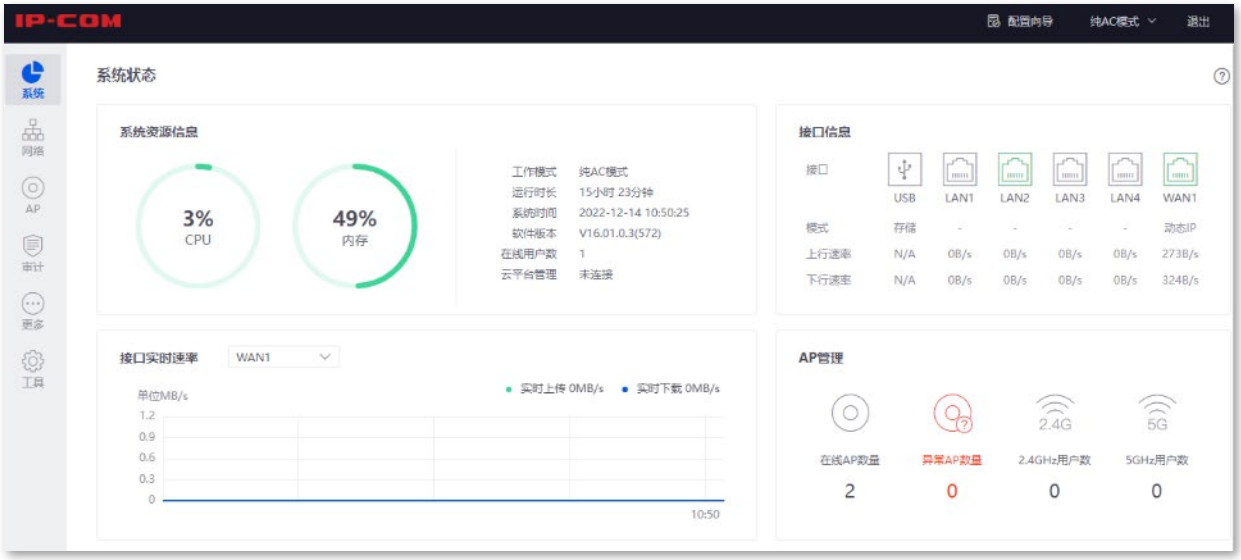
4. 输入登录密码，点击 登录 。

---完成

提示

若未出现上述页面，请确认网线是否连接正确，且网线无松动。

成功登录路由器管理页面。



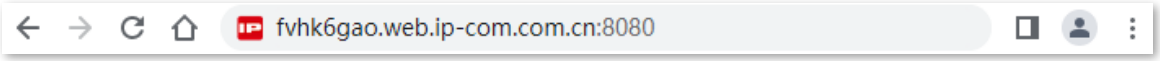
2.1.2 远程登录

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。

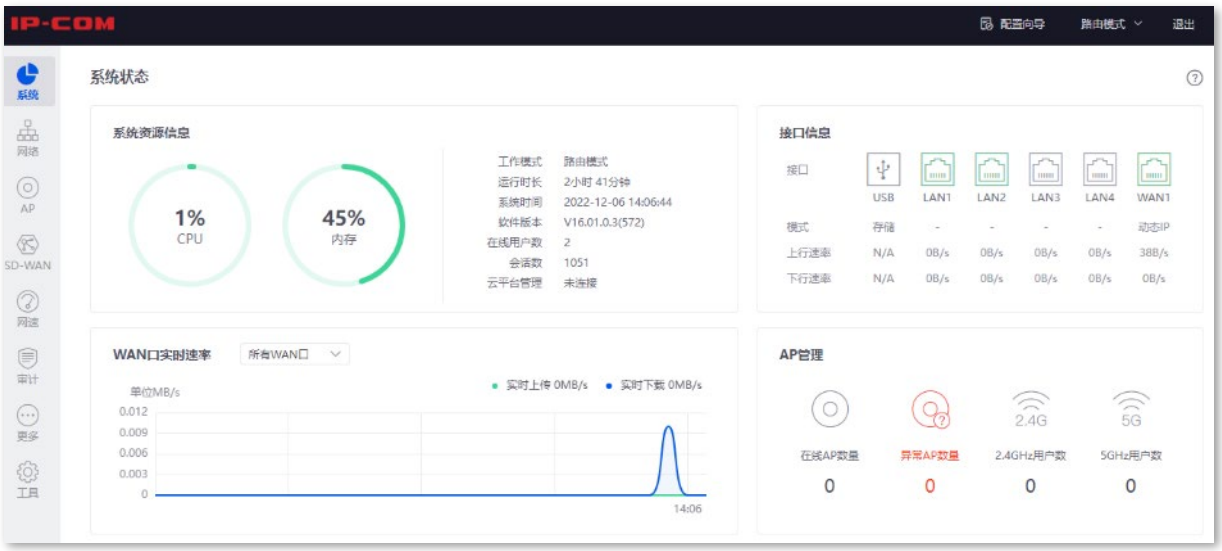
1. 在已接入互联网的终端上打开浏览器，访问路由器远程管理地址。下图仅供参考。



2. 输入登录密码，点击 登录 。

---完成

成功登录路由器管理页面。



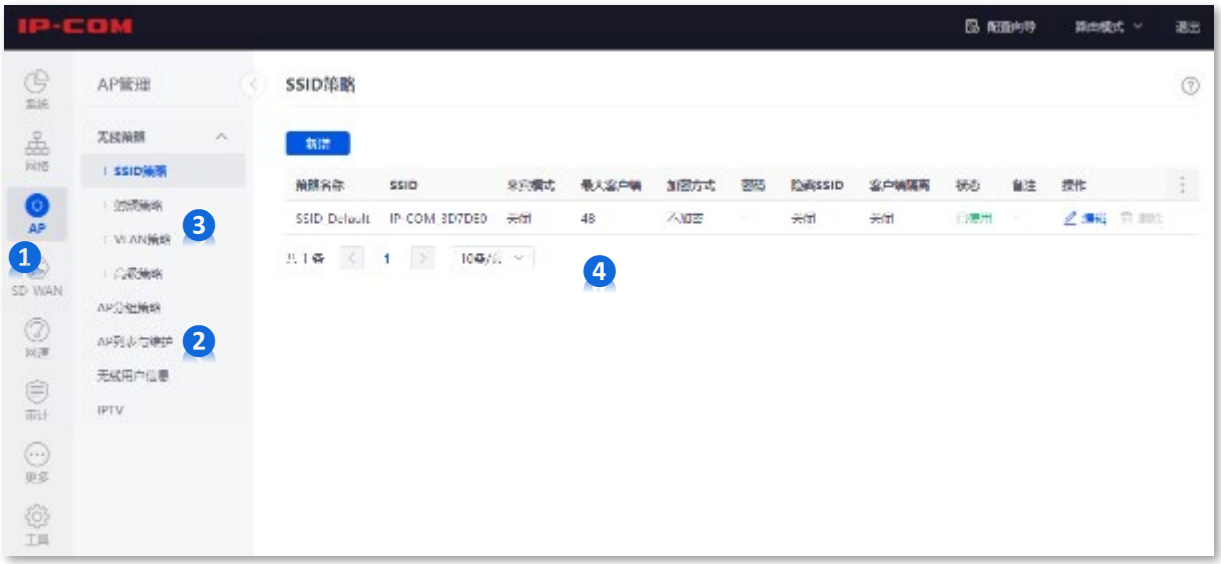
2.2 退出登录

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

4.1 系统资源信息

进入页面：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。

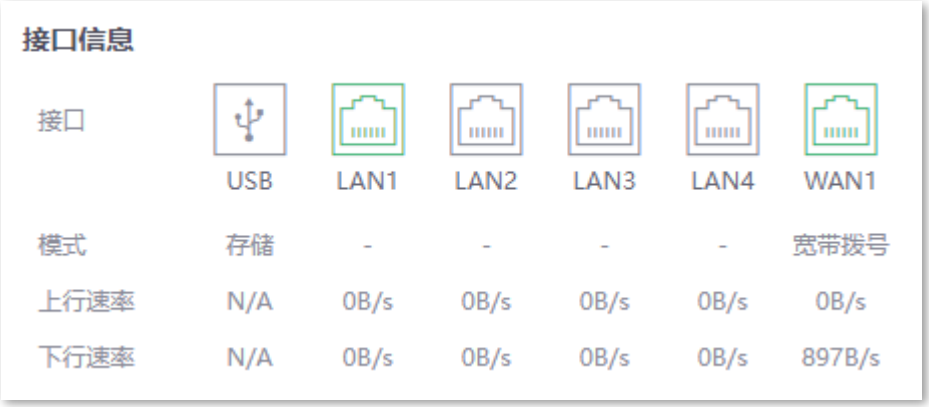
参数说明

标题项	说明
CPU	路由器的 CPU 使用率。
内存	路由器的内存使用率。
工作模式	路由器的工作模式。
运行时长	路由器最近一次启动后连续运行的时长。
系统时间	路由器的系统时间。
软件版本	路由器的系统软件版本号。
在线用户数	连接到路由器的用户设备数量。
会话数	路由器的并发连接数量。
云平台管理	路由器与云平台的连接状态。

4.2 接口信息

进入页面：登录到路由器 Web 管理页面后，点击「系统」。

在“接口信息”模块，您可以查看路由器各接口的基本状态信息。



参数说明

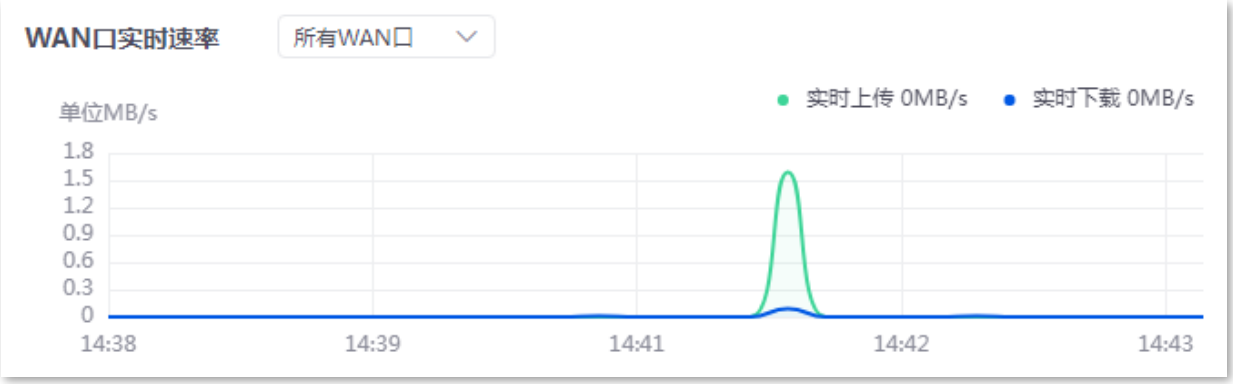
标题项	说明
接口	路由器各端口角色及物理连接状态。 – 绿色表示已连接。 – 灰色表示未连接。
模式	路由器各端口当前的工作模式。 支持显示 WAN 口的联网方式，某端口的镜像端口模式（端口镜像已开启的情况下）。部分路由器支持插入 USB 设备，显示工作模式为“存储”。
上行速率	路由器各端口当前的上传/下载速率。
下行速率	

4.3 WAN 口实时速率

进入页面：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”的下拉框可以选择查看某一个 WAN 口的实时速率。



4.4 AP 管理

进入页面：登录到路由器 Web 管理页面后，点击「系统」。

在“AP 管理”模块，您可以查看路由器已管理 AP 的基本信息。

参数说明

标题项	说明
在线 AP 数量	在线 AP 的数量。
异常 AP 数量	离线 AP 的数量。
2.4GHz 用户数	连接到 2.4GHz 网络的用户设备数。
5GHz 用户数	连接到 5GHz 网络的用户设备数。

5 网络设置

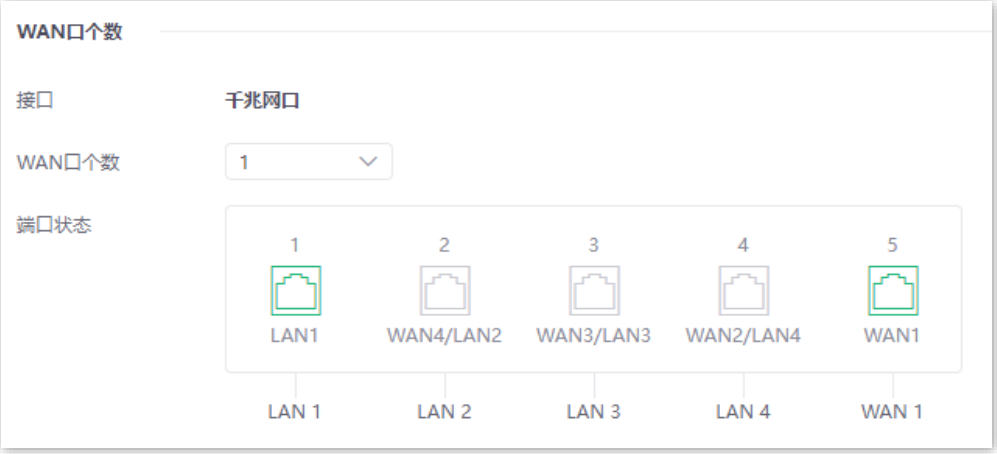
5.1 联网设置

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

进入页面：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。

在这里，您可以查看 WAN 口的速率类型，设置 WAN 口个数，查看各网口的连接状态及属性。下图以型号为“M30”的路由器为例。



参数说明

标题项	说明
接口	路由器的接口类型。
WAN 口个数	路由器 WAN 口的个数。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，也可以根据需要修改 WAN 口个数。
端口状态	路由器接口的类型及各接口连接状态。 绿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。

5.1.2 设置联网

进入页面：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。

在这里，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、静态 IP、动态 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 WAN1 口设置为例，其他 WAN 口的设置方法类似。
- 各上网参数均由网络运营商提供，如不清楚，请咨询您的网络运营商。

宽带拨号

路由器使用网络运营商提供的宽带账号和密码拨号上网。

设置步骤：

1. 登录到路由器 Web 管理页面，点击「网络」>「联网设置」。
2. 在“连接设置”模块，选择“联网方式”为“宽带拨号”。
3. 输入网络运营商提供的“宽带账号”和“宽带密码”。
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	网络运营商提供的宽带账号/密码。
宽带密码	
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 如果网络运营商未提供，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 如果网络运营商未提供，请勿填写，否则可能会导致拨号失败。
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	

动态 IP

路由器使用网络运营商动态分配的 IP 地址信息上网。

设置步骤：

1. 登录到路由器 Web 管理页面，点击「网络」>「联网设置」。
2. 在“连接设置”模块，选择“联网方式”为“动态 IP”。
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

路由器使用网络运营商提供的固定 IP 地址、子网掩码、默认网关、DNS 服务器信息上网。

设置步骤：

1. 登录到路由器 Web 管理页面，点击「网络」>「联网设置」。
2. 在“连接设置”模块，选择“联网方式”为“静态 IP”。
3. 输入网络运营商提供的“IP 地址”、“子网掩码”、“默认网关”和“首选/备用 DNS”。
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
IP 地址	网络运营商提供的“IP 地址”、“子网掩码”、“默认网关”和“首选/备用 DNS”。 提示 如果网络运营商只提供一个 DNS 服务器地址，“备用 DNS”可不填。
子网掩码	
默认网关	
首选 DNS	
备用 DNS	

5.1.3 查看连接状态

进入页面：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，包括网口连接速率及双工模式、联网状态、联网时长，以及 IP 地址等。如下图示仅供参考。

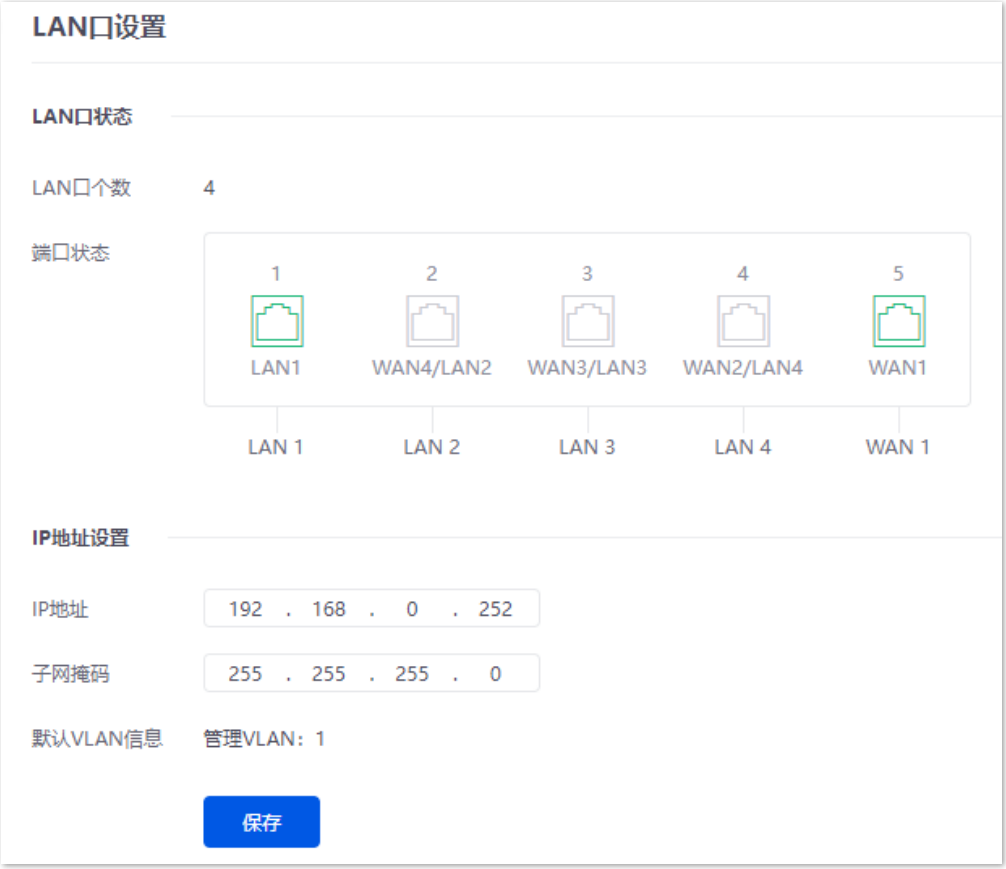
参数说明

标题项	说明
物理连接	对应 WAN 口的协商速率和双工模式。 如果显示异常，请根据页面信息及当前环境排障。
联网状态	显示路由器 WAN 口的连接状态。 – 已联网/认证成功：路由器 WAN 口已获得 IPv4 地址信息并联网正常。 – 连接中…：路由器正在连接到上级网络设备。 – 未联网/联网失败：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网络运营商。 如果显示其他状态信息，请根据联网状态提示信息采取相应措施。
联网时长	WAN 口最近一次成功接入 IPv4 网络的时长。
IP 地址	WAN 口的 IPv4 地址。
子网掩码	WAN 口的子网掩码。
默认网关	WAN 口的 IPv4 网关地址。
首选 DNS	WAN 口的首选/备用 IPv4 DNS 服务器地址。
备用 DNS	

5.2 LAN 口设置

进入页面：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。



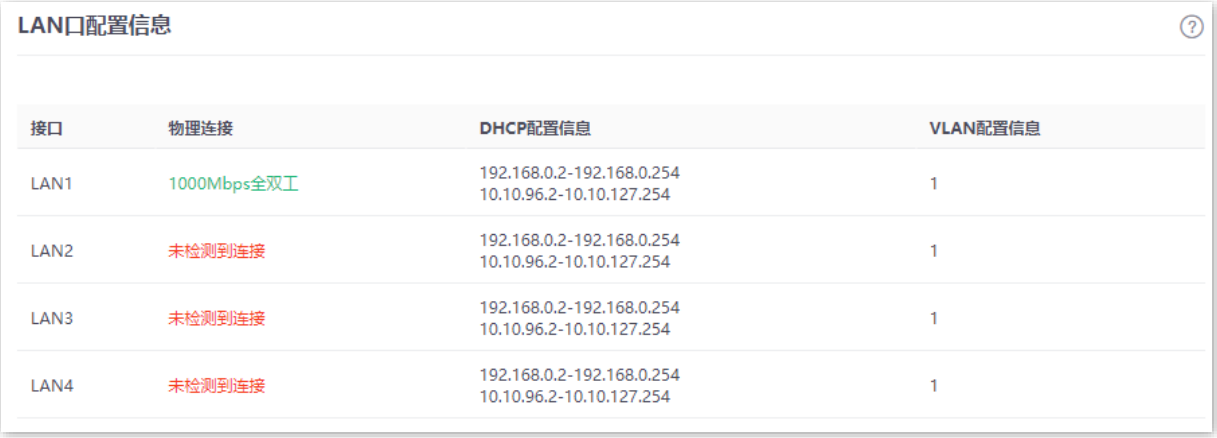
参数说明

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	路由器接口的类型及各接口连接状态。 绿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 VLAN_Default 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。
	默认 VLAN 信息	VLAN_Default 接口的 VLAN ID。

5.3 LAN 口配置信息

进入页面：登录到路由器 Web 管理页面后，点击「网络」>「LAN 口配置信息」。

在这里，您可以查看各 LAN 口的连接状态及相关配置信息。



LAN口配置信息

接口	物理连接	DHCP配置信息	VLAN配置信息
LAN1	1000Mbps全双工	192.168.0.2-192.168.0.254 10.10.96.2-10.10.127.254	1
LAN2	未检测到连接	192.168.0.2-192.168.0.254 10.10.96.2-10.10.127.254	1
LAN3	未检测到连接	192.168.0.2-192.168.0.254 10.10.96.2-10.10.127.254	1
LAN4	未检测到连接	192.168.0.2-192.168.0.254 10.10.96.2-10.10.127.254	1

参数说明

标题项	说明
接口	当前作为 LAN 口使用的端口。
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。 – 未连接：接口未连接或连接异常。
DHCP 配置信息	当前 LAN 口的 DHCP 地址池范围。 您可以在「网络」>「DHCP 设置」>「DHCP 服务器」页面修改地址池范围。
VLAN 配置信息	当前 LAN 口所属的 VLAN。

5.4 VLAN 设置

5.4.1 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。

进入页面：登录到路由器 Web 管理页面后，点击「网络」>「VLAN 设置」。

在这里，您可以配置 VLAN 规则。

以 M30 为例，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
VLAN 名称	VLAN 接口的名称。
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，只处理不带 Tag 的数据。

标题项	说明
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。
接口	该 VLAN 包含的物理接口。
备注	VLAN 的备注信息。
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。
状态	VLAN 策略的状态。 – 已启用：该策略生效。 – 已停用：该策略失效。

5.4.2 VLAN 配置举例

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。

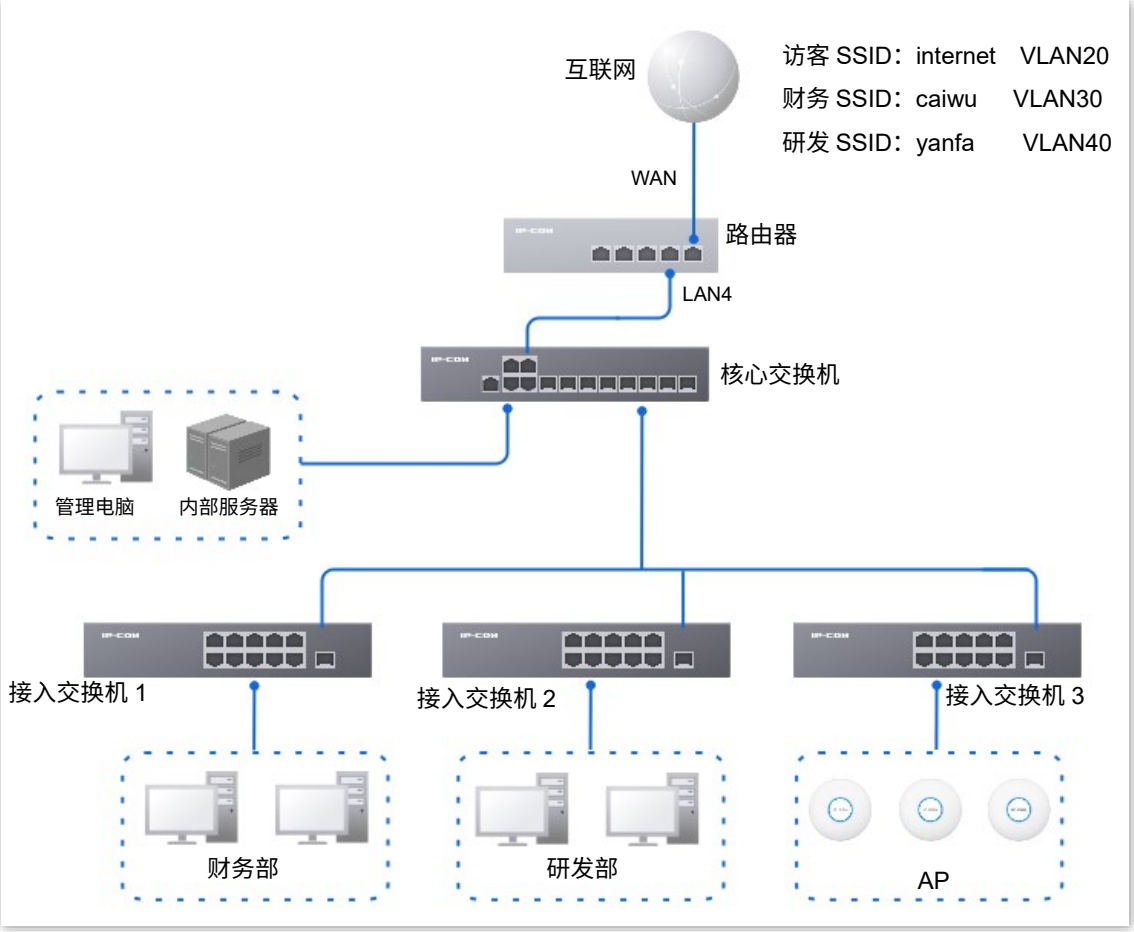
- 访客接入无线网络，只能访问互联网且与其他网络隔离。
- 财务部员工支持接入有线网络与无线网络，只能访问内网且与其他网络隔离。
- 研发部员工支持接入有线网络与无线网络，只能访问内网且与其他网络隔离。

方案设计

- 在路由器上成功管理 AP，并配置不同的无线策略下发给 AP。
- 配置访客连接的 SSID 策略，SSID 为 internet，无线密码为 UmXmL9UK，VLAN ID 为 20。
- 配置财务部员工连接的 SSID 策略，SSID 为 caiwu，无线密码为 CetTLb8T，VLAN ID 为 30。
- 配置研发部员工连接的 SSID 策略，SSID 为 yanfa，无线密码为 ZeFtub6m，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。



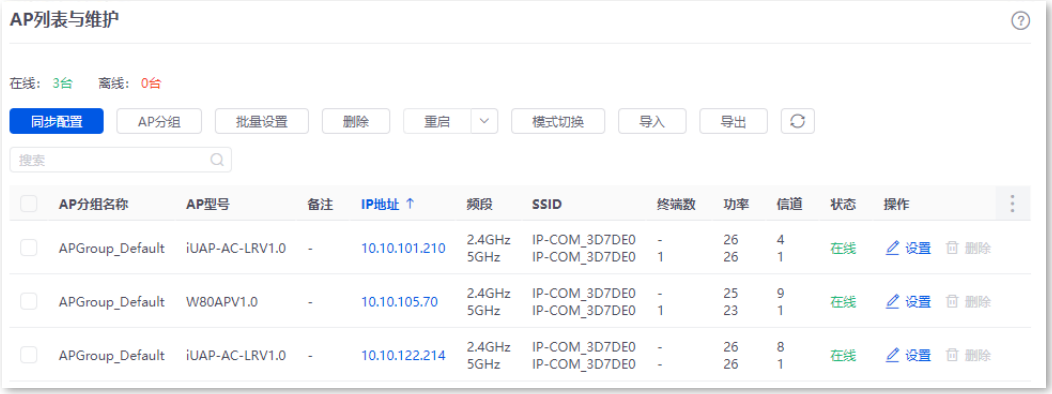
配置步骤

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

1. 登录到路由器 Web 管理页面。
2. 管理 AP。（如已管理上 AP，请跳过此步）
   1) 点击「更多」>「维护服务」>「AP 管理模式」。
   2) 确定“AP 管理模式”为“胖 AP 管理”。
   3) 点击 新增 ，然后为管理端口添加 DHCP 策略，下图仅供参考。

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。



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	LAN4

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
访客	访客	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 。

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 。

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。

SSID 策略	射频策略	VLAN 策略	AP 分组策略
策略名称：访客 SSID SSID：internet 加密方式/加密类型：WPA2-PSK/AES 密码：UmXmL9UK VLAN ID：20	RF_Default	策略名称：AP VLAN AP VLAN：开启 Trunk 口：LAN0	策略名称：企业 SSID 个数：3 2.4G/5G SSID1 策略：访客 SSID 2.4G/5G SSID2 策略：财务 SSID 2.4G/5G SSID3 策略：研发 SSID 射频策略：RF_Default VLAN 策略：AP VLAN
策略名称：财务 SSID SSID：caiwu 加密方式：WPA2-PSK/AES 密码：CetTLb8T VLAN ID：30			
策略名称：研发 SSID SSID：yanfa 加密方式：WPA2-PSK/AES 密码：ZeFtub6m VLAN ID：40			

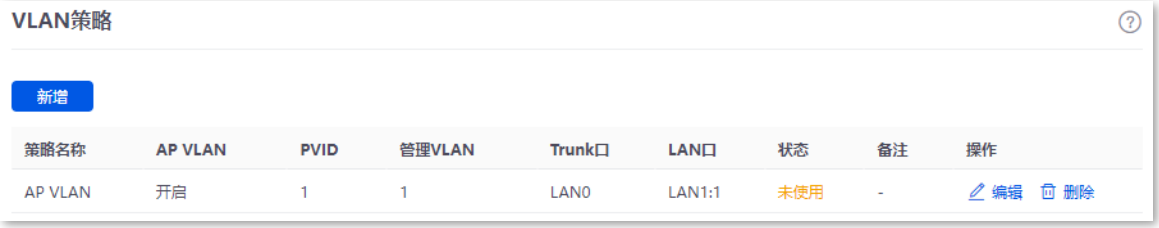
1） 配置 SSID 策略。

进入「AP」>「无线策略」>「SSID 策略」页面，点击 新增 ，然后配置 SSID 策略相关参数，点击 保存 。

2） 配置 VLAN 策略。

进入「AP」>「无线策略」>「VLAN 策略」页面，点击 新增 ，开启“AP VLAN”功能，设置 Trunk

口，点击 保存 。



3） 配置 AP 分组策略。

进入「AP」>「AP 分组策略」页面，点击 新增 ，配置 AP 分组策略相关参数，点击 保存 。

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“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
交换机 1（财务部）	30	Access	30
交换机 2（研发部）	40	Access	40
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

为连接到交换机的端口添加 VLAN 并配置 DHCP 服务器。

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

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

3. 设置连接到交换机的端口的 VLAN。

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

5.5 DHCP 设置

5.5.1 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。

提示

DHCP 静态分配功能主要针对用户，若将 AP 加入静态分配，可能导致 AP 获取 IP 地址异常，为保证 AP 正常工作，请勿将 AP 加入静态分配。

5.5.2 DHCP 服务器

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

在这里，您可以配置基于 VLAN 接口的 DHCP 服务器。

参数说明

标题项	说明
策略名称	DHCP 服务器策略名称。
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 IP-COM 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。
首选 DNS 备用 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。
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。
状态	– 已启用：该条 DHCP 服务器策略生效。 – 已停用：该条 DHCP 服务器策略失效。
备注	DHCP 服务器的备注信息。

5.5.3 DHCP 静态分配

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

在这里，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。添加“DHCP 静态分配”规则后，显示如下。

参数&按钮说明

标题项	说明
终端名称	设备的名称。
终端类型	设备的类型，如果识别不到，则显示“其他”。
IP 地址	需要给设备固定分配的 IP 地址。
MAC 地址	设备的 MAC 地址。MAC 地址格式示例：00:23:24:E8:14:5A、00-23-24-E8-14-5A 或 002324E8145A。
备注	DHCP 静态分配的备注信息。
状态	– 已启用：该条静态 IP 地址分配策略生效。 – 已停用：该条静态 IP 地址分配策略停用。 – 已失效：该条静态 IP 地址分配策略失效。
导入	将配置有 DHCP 静态分配策略的.csv 格式文件导入到路由器。
导出	将 DHCP 静态分配策略以.csv 文件格式导出到本地。 提示 如果您要修改导出的文件，需要将该文件以 txt 格式打开。

5.5.4 DHCP 列表

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

在这里，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。
- 回收 IP 地址到地址池，用于给其他设备分配。一般用于回收处于离线状态，且租约未到期的设备 IP 地址。

参数说明

标题项	说明
终端名称	设备的名称。
备注	设备的备注信息。
终端类型	设备的类型，如果识别不到，则显示“其他”。
IP 地址	设备的 IP 地址。
MAC 地址	设备的 MAC 地址。
状态	– 在线：该设备已连接到本路由器。 – 离线：该设备未连接到本路由器。
操作	可对设备进行如下操作。 – 加入静态分配：将当前的 IP 地址固定分配给该设备。加入成功后，该设备将出现在“DHCP 静态分配”列表。 – 回收：回收 IP 地址到地址池，用于给其他设备分配。

6 AP 管理

6.1 概述

路由器集成了无线控制器的功能，可以管理 IP-COM 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 要能被本路由器管理，首先需要发现并加入本路由器。本路由器作为主路由使用时，AP 加入路由器的步骤如下：

1. AP 获取到自身的 IP 地址。

   IP-COM 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。

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。

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。

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	设置 AP 管理模式	**可选。** 路由器已默认设置“AP 管理模式”为“胖 AP 管理”，且默认为 VLAN_Default 接口添加了 AP_DHCP_Default 策略。
2	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，开启了用户 DHCP 和 AP DHCP 服务。
3	配置无线策略	**可选。** 路由器默认已创建一条策略名称为“SSID_Default”的 SSID 策略，一条策略名称为“RF_Default”的射频策略。
4	配置 AP 分组策略	**可选。** 路由器默认已创建一条策略名称为“APGroup_Default”的 AP 分组策略。
5	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 无线策略

无线策略模块用于预置 AP 的配置信息，以便配置 AP 分组策略时引用，包括 SSID 策略、射频策略、VLAN 策略、高级策略。

6.3.1 SSID 策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线策略」>「SSID 策略」。

在这里，您可以配置 SSID 策略相关参数。系统默认已创建一条策略名称为“SSID_Default”的 SSID 策略，点击 新增 可以新建一条 SSID 策略。

参数说明

标题项	说明
策略名称	SSID 策略的名称。
SSID	无线网络的名称。
来宾模式	开启后，该 SSID 仅作为访客网络，连接到该 SSID 的用户仅可访问互联网，无法互相访问，也无法访问局域网。
最大客户端	该无线网络最多允许接入的客户端数量。 注意 一般情况下，IP-COM AP 的最大客户端数为 128，如需将多个 SSID 策略下发给同一台 AP 时，需确保这些 SSID 策略的最大客户端数之和不能大于 128。

标题项	说明
加密方式	SSID 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：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。 – 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。 – 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。
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 SSID 时需要输入无线密码。
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。
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 SSID	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。
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。
VLAN ID	对应 SSID 所属的 VLAN。默认为 1，表示不配置 VLAN。
状态	策略的使用状态。
备注	策略的备注信息。

6.3.2 射频策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线策略」>「射频策略」。

在这里，您可以配置射频策略相关参数。系统默认已创建一条策略名称为“RF_Default”的射频策略，点击 新增 可以新建一条射频策略。

参数说明

标题项	说明
策略名称	射频策略的名称。
2.4G	配置 2.4GHz Wi-Fi 和 5GHz Wi-Fi 的射频策略参数。
5G	

标题项	说明
射频状态	开启/关闭该频段的射频策略，“不配置”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。 2.4GHz 频段支持设置 11b、11g、11b/g、11b/g/n 和 11b/g/n/ax。 – 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。 5GHz 频段支持设置 11a、11ac、11a/n 和 11a/n/ac/ax。 – 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。
国家或区域代码	AP 当前所在的国家或地区，以适应不同国家或地区对信道及发射功率的管制要求。
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。
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。 – /（不配置）：路由器不会给 AP 下发信道配置，AP 使用其自身 Web 管理页面上配置的信道。信道的可选择范围由当前选择的国家或地区代码、无线工作频段及信道带宽来决定。
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。
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。

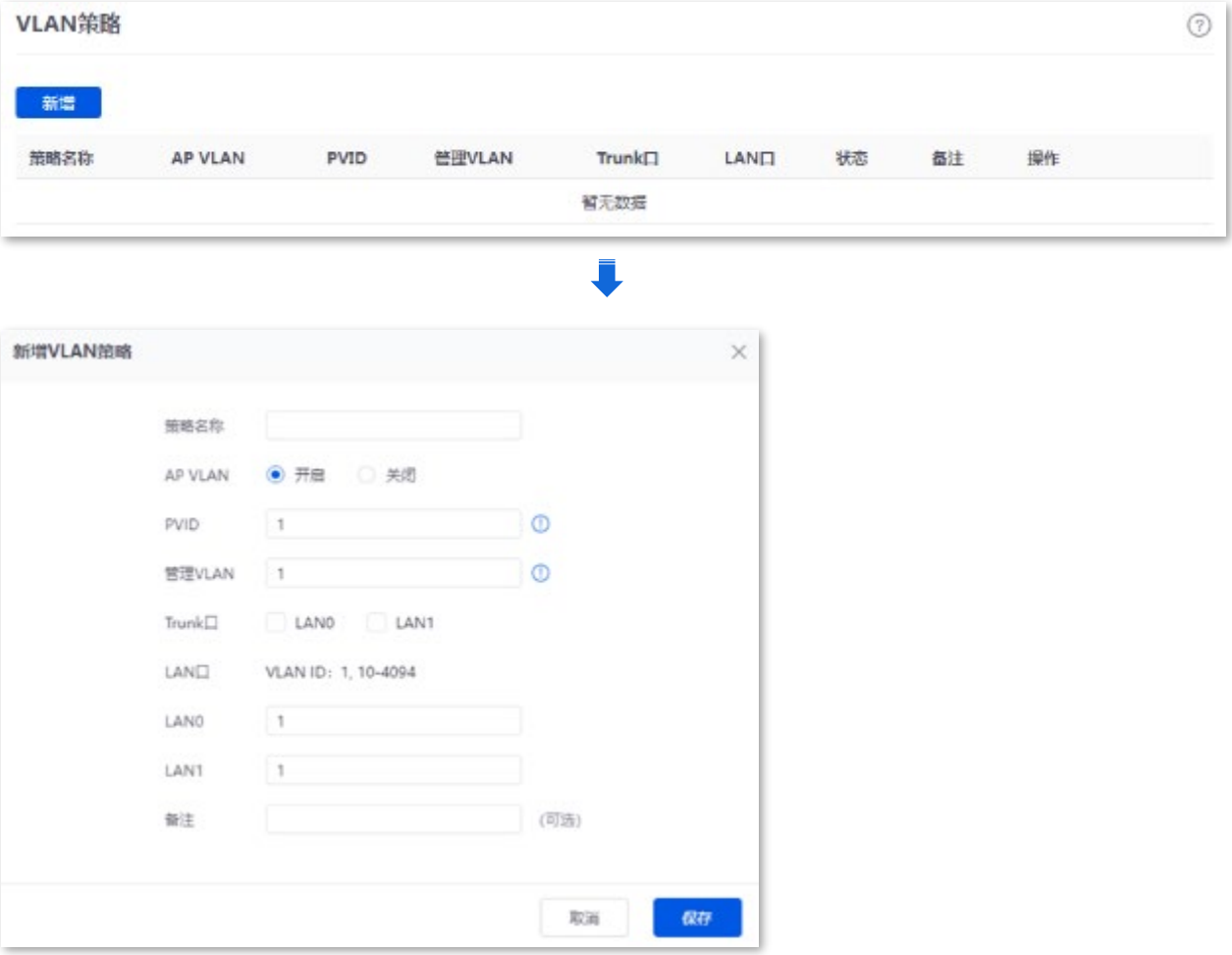
标题项	说明
抗干扰模式	选择设备的干扰抑制模式。仅 2.4GHz 支持。 – 0：禁用所有抗干扰。 – 1：启用同频段干扰抑制，如微波炉、手机、蓝牙设备造成的同频干扰，一般用于干扰较小的环境。 – 2：强制启用无线电干扰抑制，主要用在无线信号干扰源在 30 个以下的场景，一般用于干扰较大的环境。 – 3：自动启用无线电干扰抑制，一般用于干扰很大的环境。 – 4：自动启用无线电干扰抑制并降低噪声。一般用于无线信号干扰源超过 30 个的环境，如高密场景等。 – /（不配置）：路由器不会给 AP 下发抗干扰模式配置，AP 使用其自身 Web 管理页面上配置的抗干扰模式。
空口调度	启用后，可以让不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，如果 AP 接收到的终端 5GHz 信号强度不低于“5GHz 优先阈值”，则让双频用户优先连接到 AP 的 5GHz 网络。 提示 – 5GHz 优先的前提是 AP 的 2.4GHz 和 5GHz 射频都开启，且 2.4GHz 和 5GHz 的 SSID 相同，无线认证加密方式、密码也相同。 – 5GHz 优先阈值由 AP 自身 Web 管理页面配置。
状态	策略的使用状态。
备注	策略的备注信息。

6.3.3 VLAN 策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线策略」>「VLAN 策略」。

在这里，您可以配置 VLAN 策略，将 AP 的 VLAN 相关配置绑定在一起（如 AP VLAN 启用状态、管理 VLAN、Trunk 口等）。

点击 新增 可以新建一条 VLAN 策略。



参数说明

标题项	说明
策略名称	VLAN 策略的名称。
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，路由器需要重新连接到新的管理 VLAN，才能管理 AP。客户端（如管理电脑）需要重新连接到新的管理 VLAN，才能进入 AP 的 Web 管理页面。
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。

标题项	说明
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。
状态	策略的使用状态。
备注	策略的备注信息。

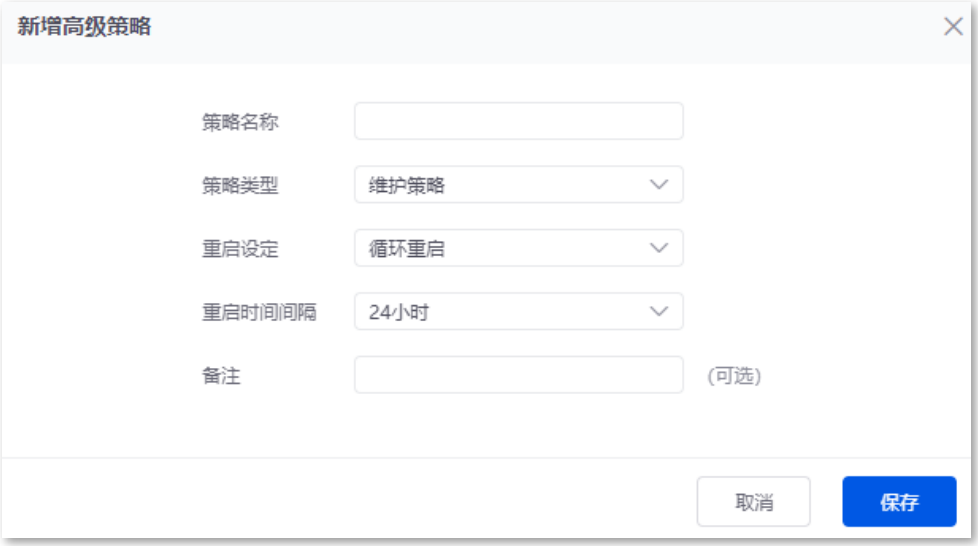
6.3.4 高级策略

维护策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线策略」>「高级策略」。

在这里，您可以配置 AP 维护策略，即，AP 的重启策略。重启可以使 AP 保持高性能运行状态，建议让 AP 在网络相对空闲的时候自动重启。

点击 新增 可以新建一条维护策略。



参数说明

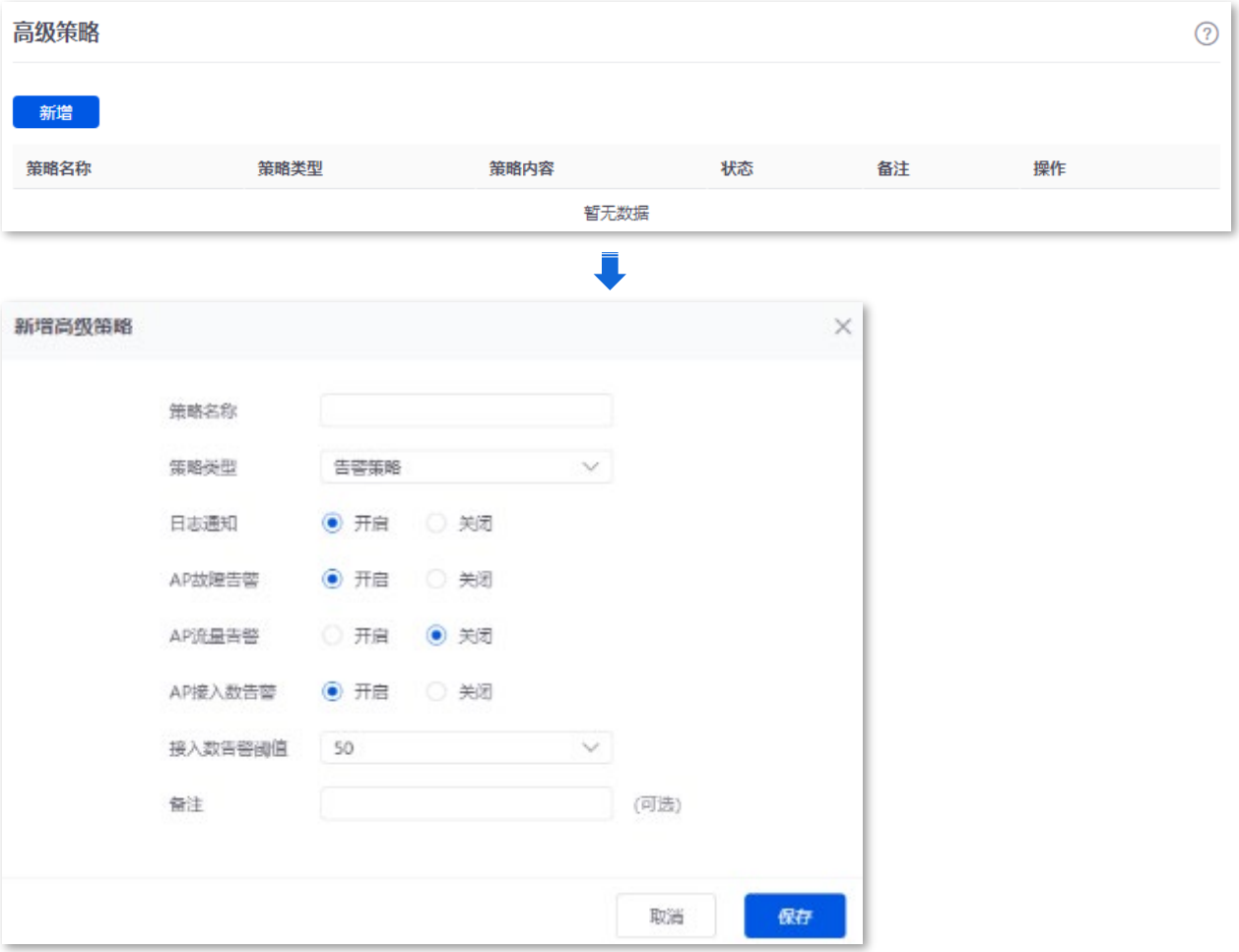
标题项	说明
策略名称	维护策略的名称。
策略类型	选择“维护策略”。
策略内容	策略的具体内容。
重启设定	自动重启类型。 – 定时重启：AP 在指定的日期的时间点自动重启一次。 – 循环重启：AP 每隔一个指定的“重启间隔时间”自动重启一次。
时间	AP 自动重启的时间点和日期。重启设定为“定时重启”时支持。
重复	
重启时间间隔	AP 自动重启的间隔时间。重启设定为“循环重启”时支持。
状态	策略的使用状态。
备注	策略的备注信息。

告警策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线策略」>「高级策略」。

在这里，您可以配置 AP 告警策略，即，AP 在发生相关告警事件后，路由器发出告警信息，网络管理员通过查看这些告警信息来实时监控网络状态。

点击 新增 可以新建一条告警策略。



参数说明

标题项	说明
策略名称	告警策略的名称。
策略类型	选择“告警策略”。
策略内容	策略的具体内容。
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“胖 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。
流量告警阈值	AP 发出流量告警的流量限定值。当 AP 的流量达到该值时，AP 发出流量告警。
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。

标题项	说明
接入数告警阈值	AP 发出接入数告警的无线客户端接入数限定值。当接入 AP 的无线客户端达到该限定值，AP 发出接入数告警。
状态	策略的使用状态。
备注	策略的备注信息。

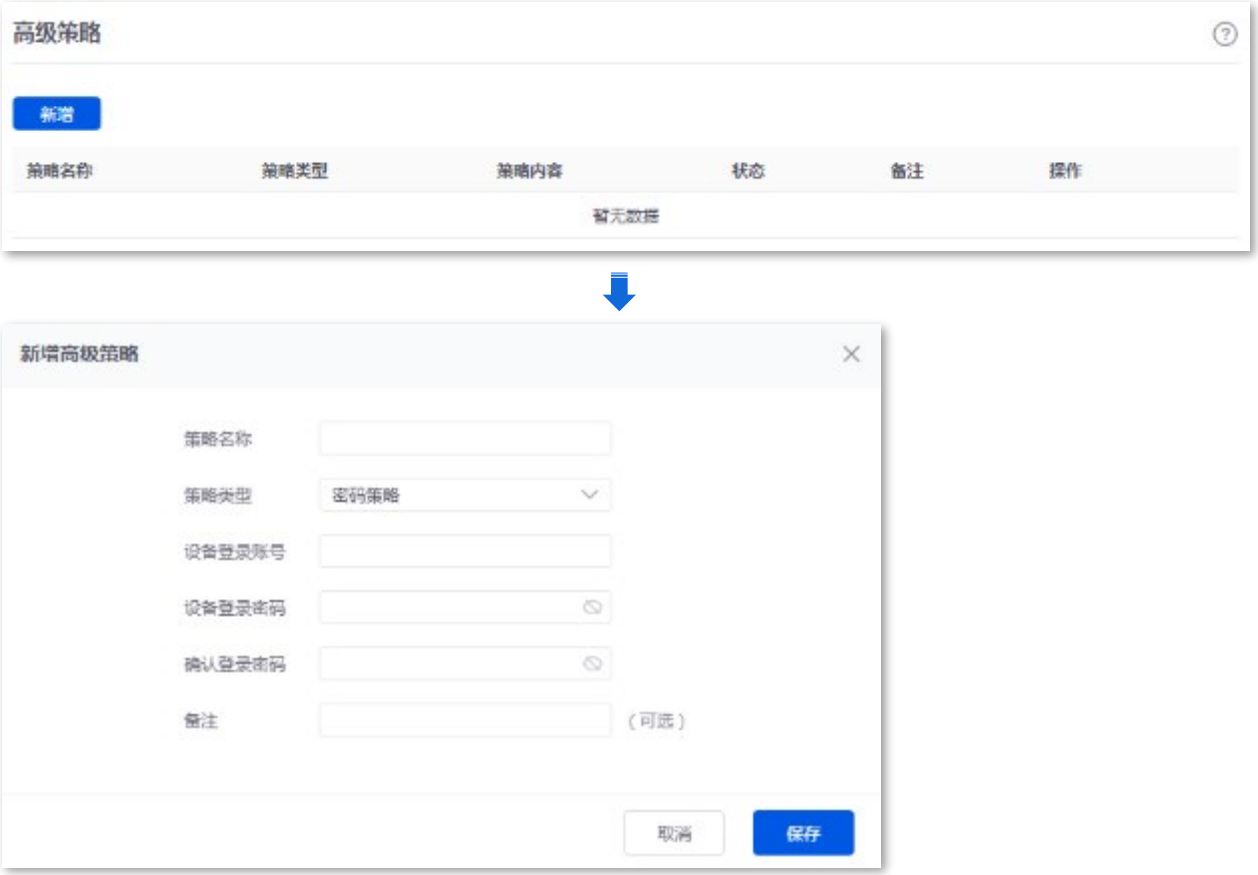
密码策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线策略」>「高级策略」。

在这里，您可以配置 AP 密码策略，即，预置 AP Web 管理页面的登录账号/密码。

AP Web 管理页面的登录账号/密码默认均为“admin”，为了防止非授权用户进入 AP 的 Web 管理页面更改设置，影响无线网络正常使用，管理员需要修改 AP 的登录账号与密码。

点击 新增 可以新建一条密码策略。



参数说明

标题项	说明
策略名称	密码策略的名称。

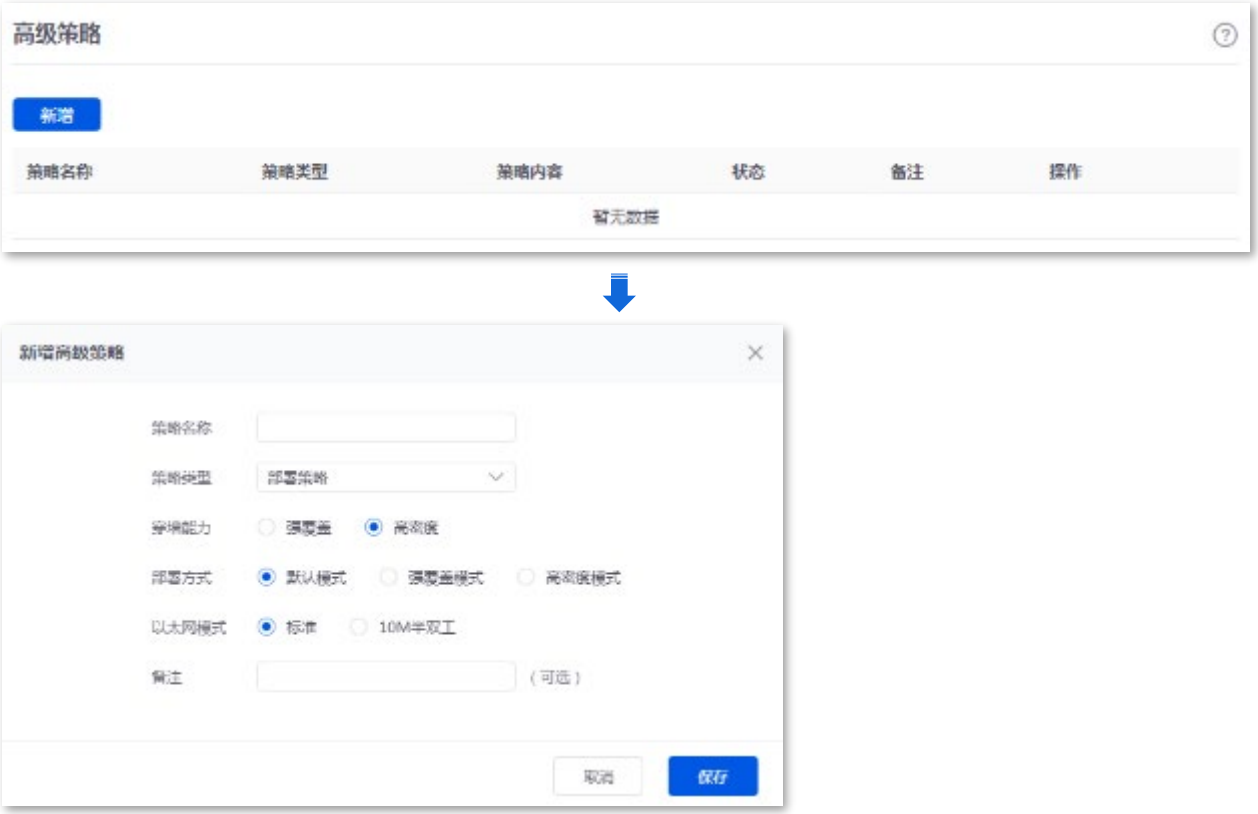
标题项	说明
策略类型	选择“密码策略”。
策略内容	策略的具体内容。
设备登录账号	AP Web 管理页面的登录用户名与密码。
设备登录密码	
确认登录密码	再一次输入 AP Web 管理页面的登录密码。
状态	策略的使用状态。
备注	策略的备注信息。

部署策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线策略」>「高级策略」。

在这里，您可以配置 AP 部署策略，以适应不同的无线覆盖场景。

点击 新增 可以新建一条部署策略。



参数说明

标题项	说明
策略名称	部署策略的名称。

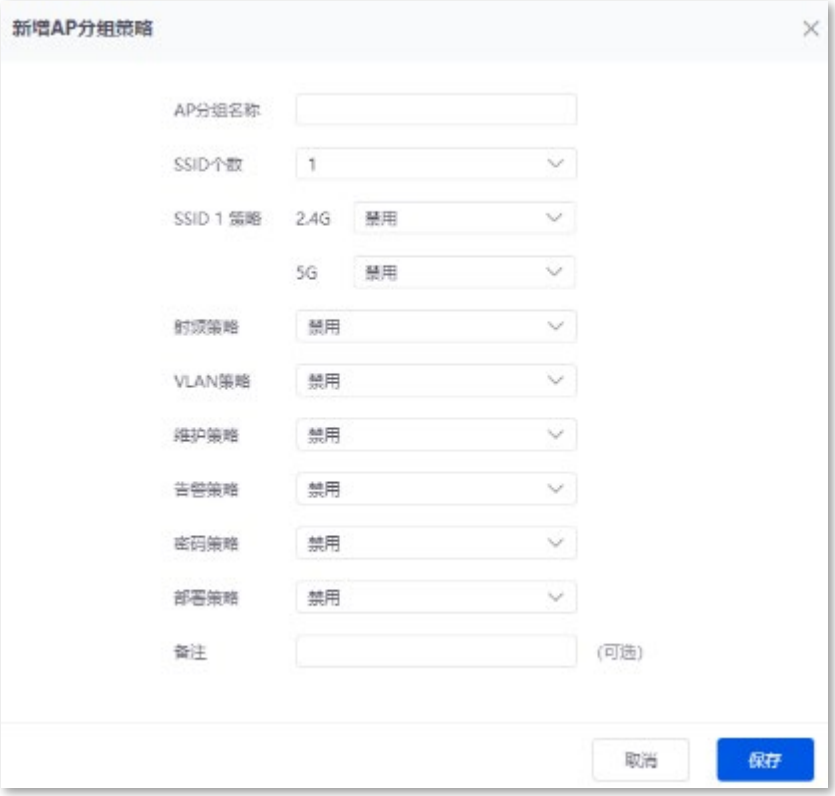
标题项	说明
策略类型	选择“部署策略”。
策略内容	策略的具体内容。
穿墙能力	AP 的穿墙能力，请根据实际应用场景选择。 – 强覆盖：常用于 AP 部署密度较低的场景，如办公室、仓库、医院等，使用此模式可以扩大 AP 的覆盖范围。 – 高密度：常用于 AP 部署密度较高的场景，如会场、展厅、宴会厅、体育场馆、高校教室、候机厅等，使用此模式可以有效减少 AP 相互之间的干扰。
部署方式	AP 的部署方式，请根据实际应用场景选择。 – 强覆盖模式：常用于 AP 部署密度较低的场景，此模式可以尽可能地确保客户端成功接入 AP。 – 高密度模式：常用于 AP 部署密度较高的场景，此模式可以确保客户端连接到信号好的 AP。 – 默认模式：介于“强覆盖”和“高密度”之间。
以太网模式	AP PoE 口的驱动模式。 – 标准：速率高，驱动距离较短。一般情况下，建议选择此模式。 – 10M 半双工：驱动距离远，但速率较低，协商速率为 10Mbps。 当连接 AP PoE 口与对端设备的网线超过 100 米时，才建议尝试改为“10M 半双工”模式以提高网线驱动距离。同时，必须确保对端端口工作模式为“自协商”，否则可能导致 AP PoE 口无法正常收发数据。
状态	策略的使用状态。
备注	策略的备注信息。

6.4 AP 分组策略

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「AP 分组策略」。

在这里，您可以配置 AP 分组策略，即，将无线策略组合起来，便于统一下发给相应的 AP。

系统默认已创建一条策略名称为“APGroup_Default”的 AP 分组策略，点击 新增 可以新建一条 AP 分组策略。



参数说明

标题项	说明
AP 分组名称	AP 分组策略的名称。
SSID 个数	SSID 的个数。
SSID 策略	分组策略引用的 SSID 策略，需先在 SSID 策略页面配置好。 若配置多个 SSID，每个 SSID 都要引用一个 SSID 策略，策略不能相同。
2.4G	SSID 策略生效频段。

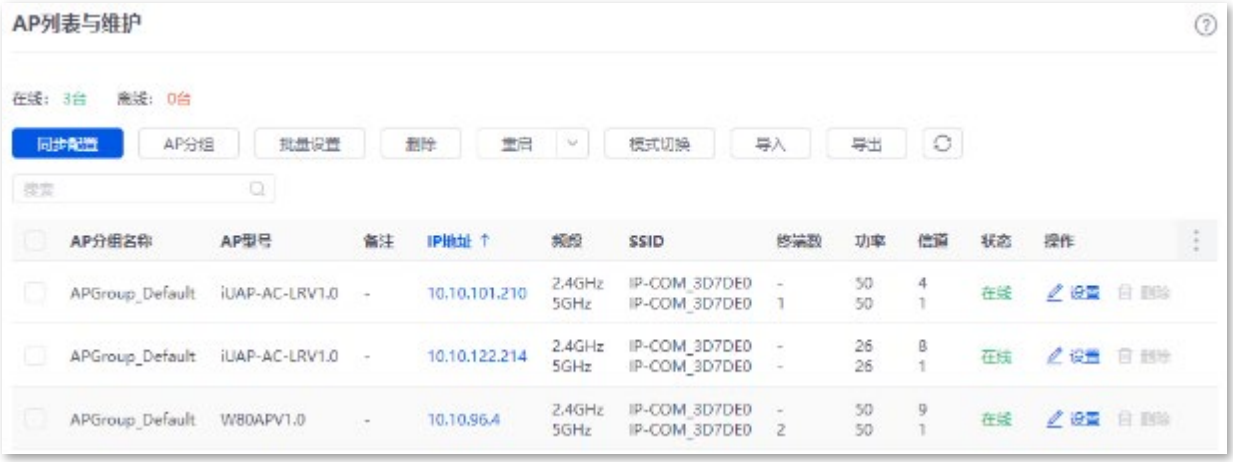
标题项	说明
5G	注意 如 AP 只支持 2.4GHz，则可以选择 2.4GHz 或 2.4GHz&5GHz；若选择 5GHz，则配置无效。
射频策略	分组策略引用的射频策略，需先在射频策略页面配置好。
VLAN 策略	分组策略引用的 VLAN 策略，需先在 VLAN 策略页面配置好。
维护策略	分组策略引用的维护策略，需先在高级策略页面配置好。
告警策略	分组策略引用的告警策略，需先在高级策略页面配置好。
密码策略	分组策略引用的密码策略，需先在高级策略页面配置好。
部署策略	分组策略引用的部署策略，需先在高级策略页面配置好。
备注	AP 分组策略的备注信息。

6.5 AP 列表与维护

6.5.1 概述

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「AP 列表与维护」。

在这里，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。

按钮	说明
AP 分组	AP 引用的 AP 分组策略，需先在 AP 分组策略页面配置好。
批量设置	批量对 AP 进行统一详细配置。
删除	删除离线 AP 的信息。
重启	重启 AP。
升级	升级 AP 的系统软件。
复位	将 AP 恢复出厂设置。
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。
导入	导入之前导出的 AP 配置信息。
导出	导出 AP 的配置信息。

参数说明

标题项	说明
AP 分组名称	AP 分组策略的名称。
AP 型号	AP 的型号。
备注	AP 的备注信息
IP 地址	AP 从路由器 AP DHCP 服务器获取到的 IP 地址，即 AP 的登录地址。
MAC 地址	AP 的 LAN 口 MAC 地址。
软件版本	AP 的系统软件版本号。
频段	AP 的工作频段。
SSID	AP 当前的 SSID。
终端数	当前连接到 AP 的无线终端数量。
功率	AP 的无线发射功率。
信道	AP 的工作信道。
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 WiFi 时，客户端优先从 5GHz 频段接入 AP 无线网络。

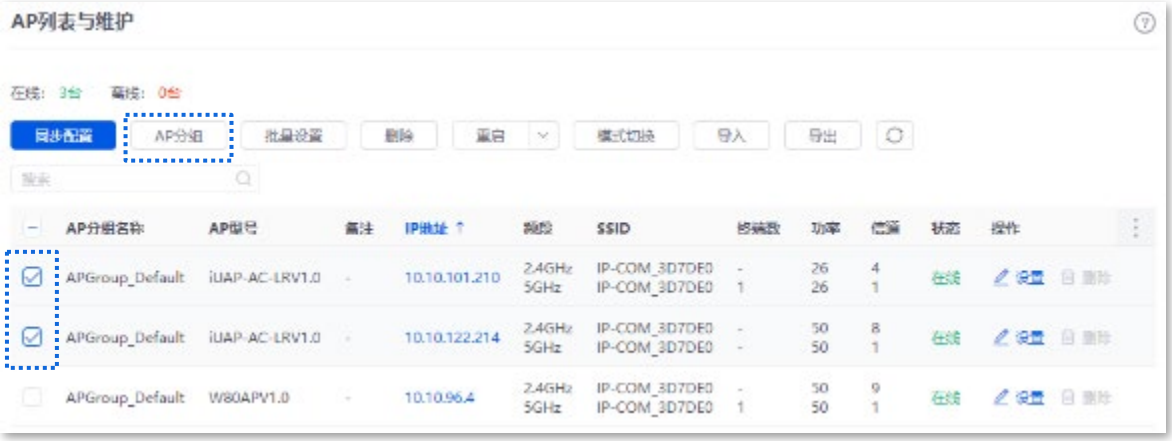
标题项	说明
管理模式	AP 的云维护状态。如果要设置 AP 的云维护功能，可参考设置 AP 云维护功能。 提示 部分 AP 不支持云维护功能，请以实际为准。
管理 VLAN	AP 的管理 VLAN ID，与数据 VLAN 做区分，未设置时默认显示“-”。
有线口 VLAN	AP 有线口默认所属的 VLAN ID。
射频开关	开启或关闭 AP 的无线射频。
在线时长	AP 在线的时长。
离线时长	AP 离线的时长。
状态	AP 的状态。

6.5.2 下发策略给 AP

提示

AP 上线时默认加入 APGroup_Default 分组。

1. 登录到路由器 Web 管理页面。
2. （若已配置，跳过）配置要下发给 AP 的无线策略，详情可参考无线策略。
3. （若已配置，跳过）设置 AP 分组策略，将已配置的无线策略添加到一个 AP 组，详情可参考 AP 分组策略。
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。

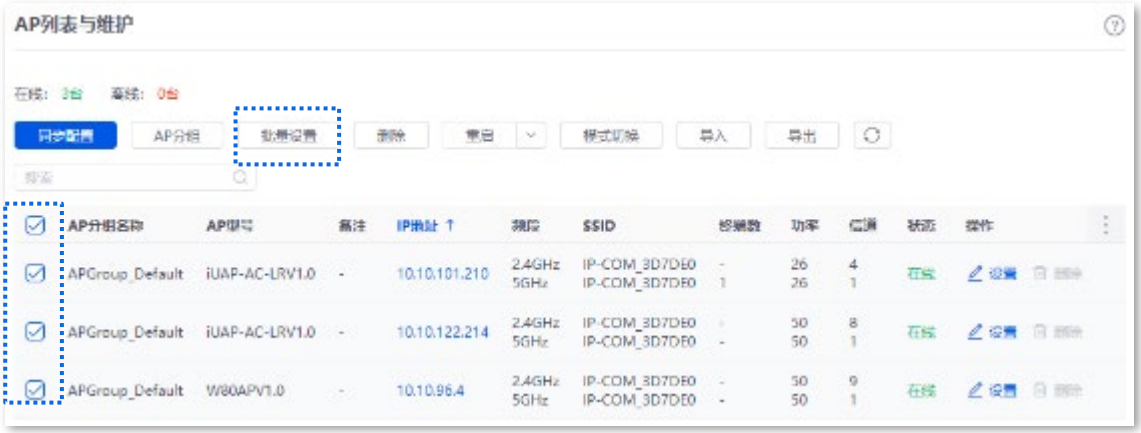
---完成

将 AP 加入某一 AP 组后，AP 将应用该 AP 组内关联的相关策略。

6.5.3 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。

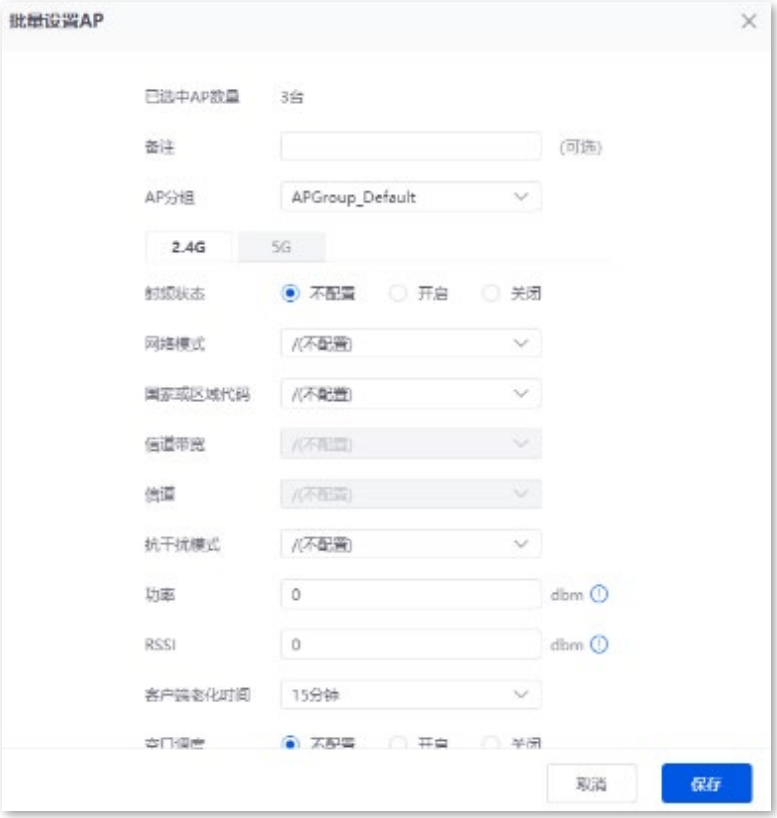
1. 登录到路由器 Web 管理页面。
2. 点击「AP」>「AP 列表与维护」。
3. 选择要进行详细配置的在线 AP，点击 批量设置 。下图仅供参考。



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

不配置表示不修改所属 AP 分组的配置。



---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
已选中 AP 数量	当前已选中 AP 的数量，不支持编辑。
备注	AP 的备注信息。
AP 分组	AP 引用的 AP 分组策略，需先在 AP 分组策略页面配置好。
2.4G	配置 2.4GHz Wi-Fi 和 5GHz Wi-Fi 的相关参数。请参考射频策略参数说明。
5G	

6.5.4 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。

如果要将 AP 和路由器添加到同一个项目，开启云维护功能时，请保持“云平台唯一码”相同。

开启 AP 云维护功能

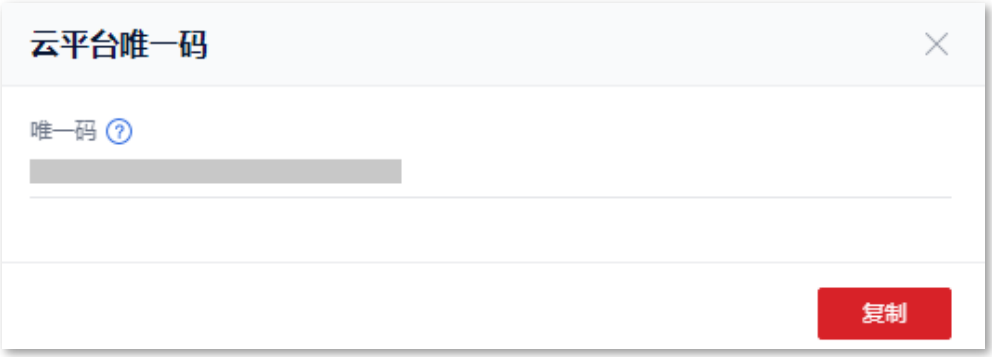
1. 获取云台唯一码。

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。
- 开启 AP 的云维护功能前，请确保 AP 已联网。

1) 访问 https://ims.ip-com.com.cn，进入 IP-COM 工程宝云管理系统。

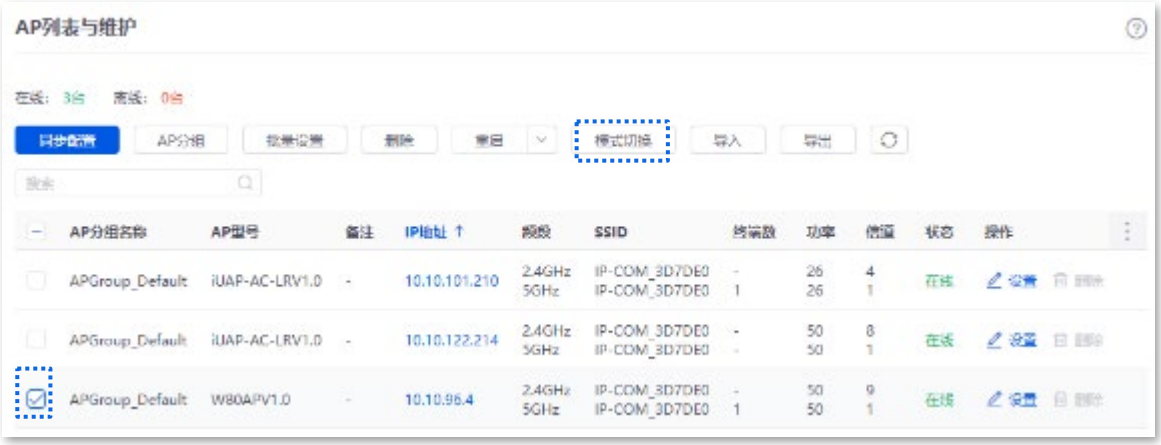
2) 点击 IP-COM 工程宝云管理系统页面右上角的“账号管理”>“云平台唯一码”，然后复制该云平台唯一码。



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。



1) 开启“云维护”功能，根据实际需要选择管理模式，如“云托管”。

2） 输入已获取的云台唯一码，开启“设备信息上报”功能。

3） 点击 确定 。

---完成

AP 开启“云维护”功能后，可以通过 IP-COM 工程宝云管理系统（https://ims.ip-com.com.cn）或“工程宝”App 添加并管理 AP。

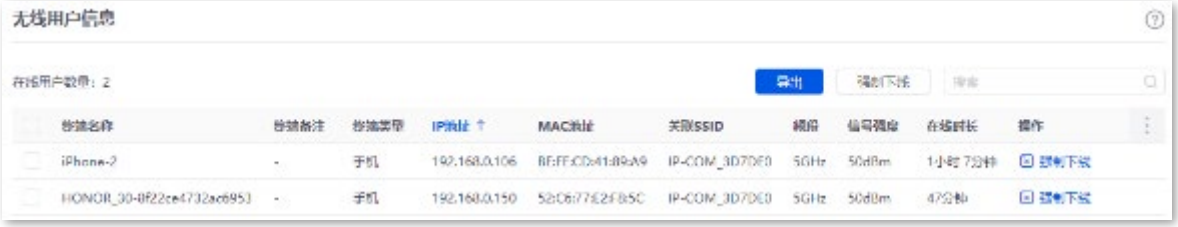
参数说明

标题项	说明
云维护	开启/关闭 AP 云维护功能。
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 IP-COM 工程宝云管理系统（工程宝云管理系统 Web 或工程宝 App）管理，且相关功能的配置信息由工程宝云管理系统下发，本地登录 AP 的 Web 管理页面时，可以查看相关配置。 – 本地托管：适用于集中统一管理并查看项目的场景。AP 可被工程宝云管理系统（工程宝云管理系统 Web 或工程宝 App）管理，本地登录 AP 的 Web 管理页面时，可配置 AP 的所有功能。
云平台唯一码	用于指定设备关联的云平台账号。获取方式如下。 – 在 IP-COM 工程宝云管理系统 Web 界面，点击右上角账户，即可在下拉菜单中获取。 – 在 IP-COM 工程宝 App 中，可以在个人中心中获取。
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。

6.6 无线用户信息

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「无线用户信息」。

在这里，您可以查看连接到 AP 的终端设备的基本信息。



按钮&参数说明

标题项	说明
导出	导出已选择的终端信息到本地电脑。
强制下线	强制指定终端设备下线。
在线用户数量	当前接入 AP 无线网络的终端数量。
终端名称	终端设备的名称。
终端备注	终端设备的备注信息。点击备注信息显示区域即可自定义。
终端类型	终端设备的类型，如果系统识别不出来，则显示“其他”。
IP 地址	终端设备的 IP 地址。
MAC 地址	终端设备的 MAC 地址。
关联设备	终端设备连接的无线网络所属的 AP。
关联设备备注	终端设备连接的无线网络所属 AP 的备注信息。
关联设备 IP	终端设备连接的无线网络所属 AP 的 IP 地址。
关联设备 MAC	终端设备连接的无线网络的 MAC 地址。
关联 SSID	终端设备连接的无线网络名称。
实时上传	终端设备的实时上传速率。
实时下载	终端设备的实时下载速率。
总流量	终端设备总使用流量。
频段	终端设备连接的无线网络所在频段。
信号强度	终端设备连接的无线网络的信号强度。
在线时长	终端设备当次连接无线网络后的在线时长。

6.7 胖 AP 管理配置举例

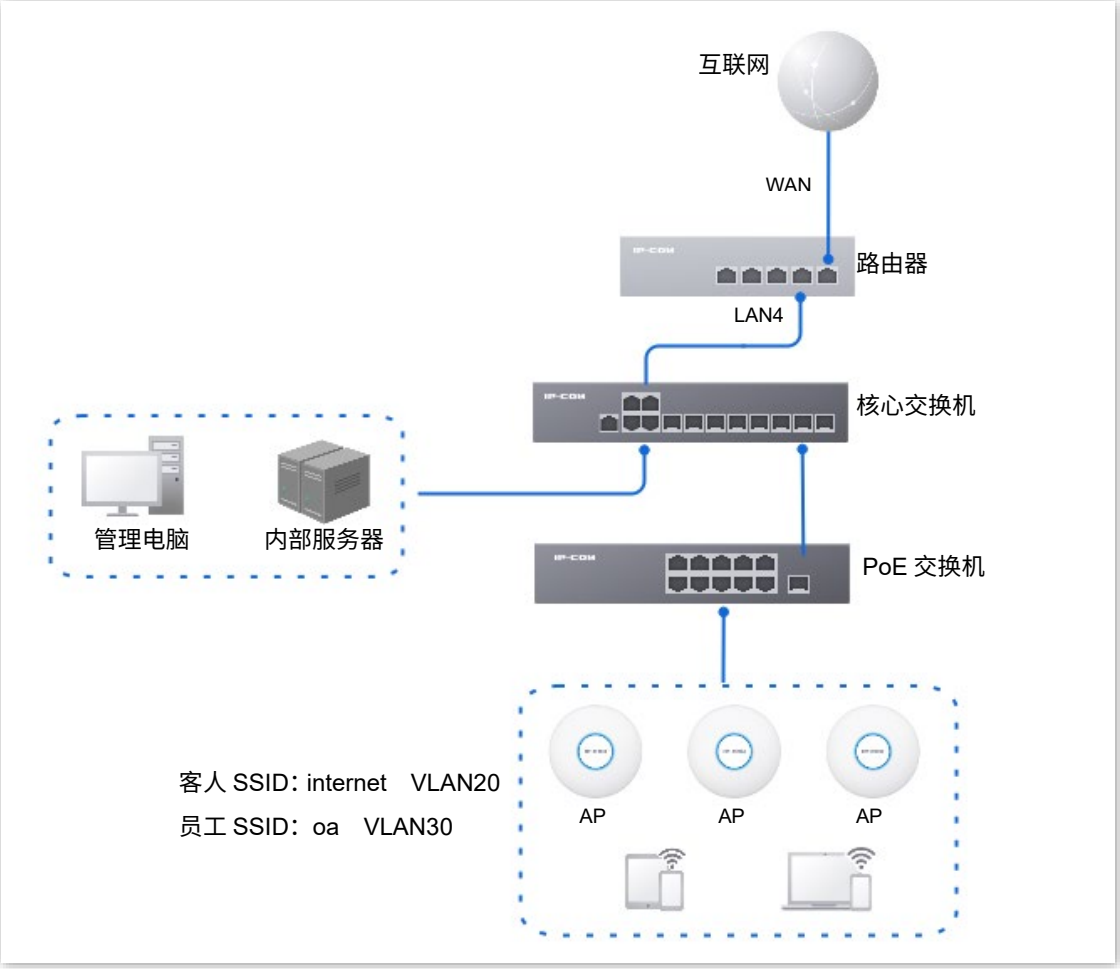
组网需求

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，并配置不同的无线策略下发给 AP。
- 配置客人连接的 SSID 策略，SSID 为 internet，无线密码为 UmXmL9UK，VLAN ID 为 20。
- 配置员工连接的 SSID 策略，SSID 为 oa，无线密码为 CetTLb8T，VLAN ID 为 30。
- 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。

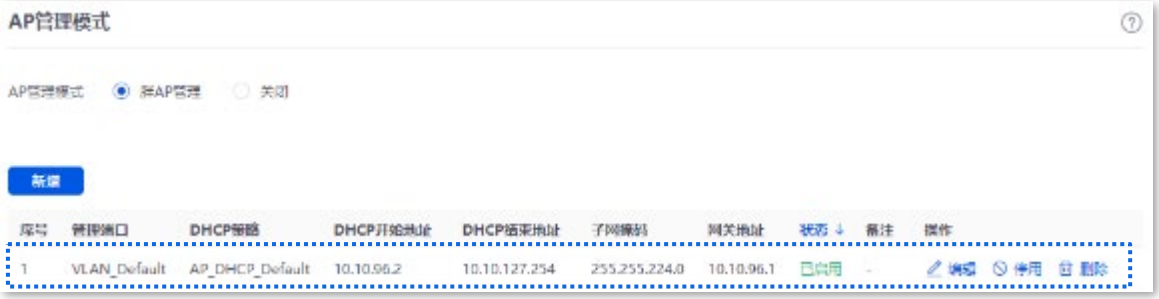


配置步骤

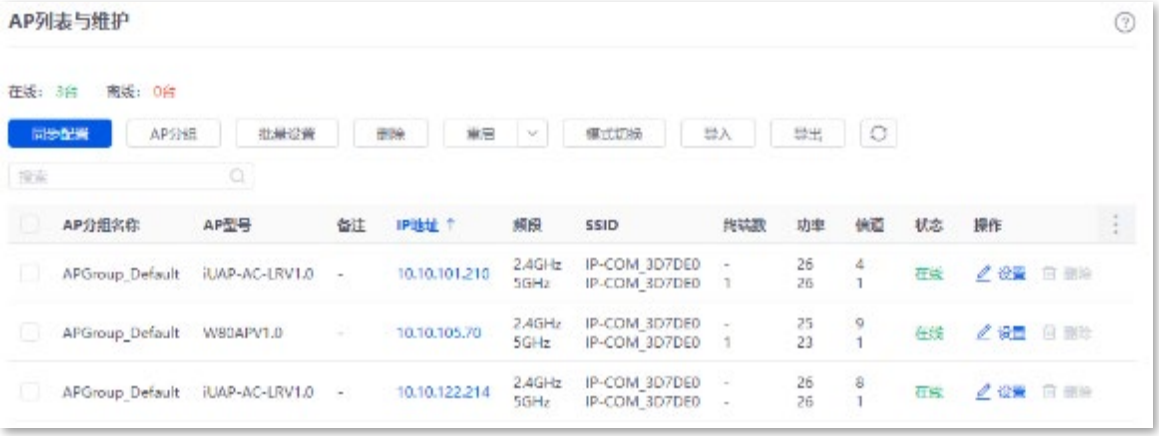
配置路由器 → 配置核心交换机 → 配置内部服务器

一、配置路由器

1. 登录到路由器 Web 管理页面。
2. 管理 AP。（如已管理 AP，请跳过此步）
   1) 点击「更多」>「维护服务」>「AP 管理模式」。
   2) 设置“AP 管理模式”为“胖 AP 管理”，确认提示信息后点击 确定 。
   3) 点击 新增 ，然后为管理端口添加 DHCP 策略。下图仅供参考。



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。



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	LAN4

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
客人	客人	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 。

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 。

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。

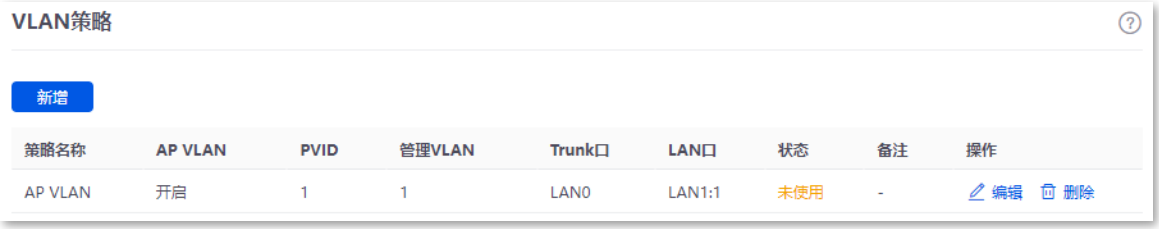
SSID 策略	射频策略	VLAN 策略	AP 分组策略
策略名称：客人 SSID SSID：internet 加密方式/加密类型：WPA2-PSK/AES 密码：UmXmL9UK VLAN ID：20	RF_Default	策略名称：AP VLAN AP VLAN：开启 Trunk 口：LAN0	AP 分组名称：酒店 SSID 个数：2 2.4G/5G SSID1 策略：客人 SSID 2.4G/5G SSID2 策略：员工 SSID 射频策略：RF_Defaul VLAN 策略：AP VLAN
策略名称：员工 SSID SSID：oa 加密方式：WPA2-PSK/AES 密码：CetTLb8T VLAN ID：30			

1） 配置 SSID 策略。

进入「AP」>「无线策略」>「SSID 策略」页面，点击 新增 ，然后配置 SSID 策略相关参数，点击 保存

2） 配置 VLAN 策略。

进入「AP」>「无线策略」>「VLAN 策略」页面，点击 新增 ，开启“AP VLAN”功能，设置 Trunk 口，点击 保存 。



3） 配置 AP 分组策略。

进入「AP」>「AP 分组策略」页面，点击 新增 ，AP 分组策略相关参数，点击 保存 。

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“AP 分组策略”，本例为“酒店”，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

为连接到交换机的端口添加 VLAN 并配置 DHCP 服务器。

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

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

3. 设置连接到交换机的端口的 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。

6.8 IPTV

6.8.1 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。

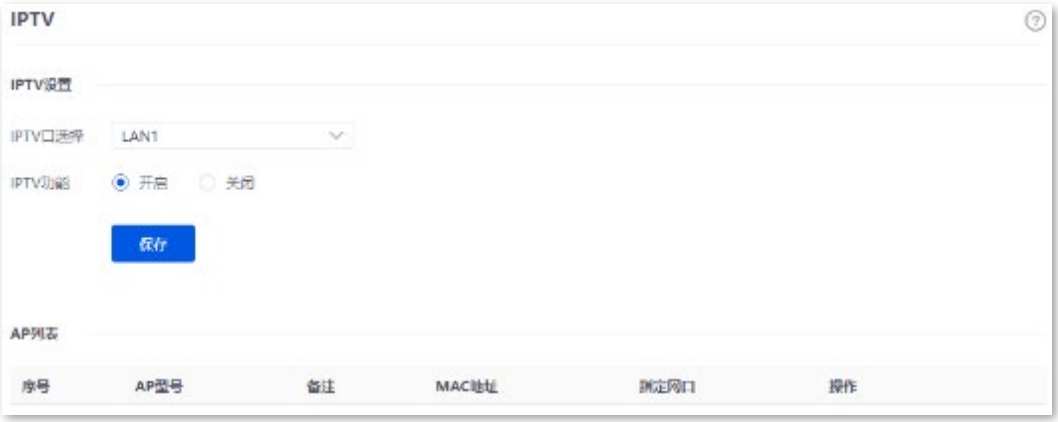
如果您办理的宽带含有 IPTV 业务，则可以启用路由器的 IPTV 功能，使您在通过路由器上网的同时，也可以通过网络机顶盒和电视机观看丰富的 IPTV 节目。

提示

此功能需配合支持 IPTV 功能的 IP-COM AP 使用。

进入页面：登录到路由器 Web 管理页面后，点击「AP」>「IPTV」。

IPTV 功能默认关闭，开启后，页面显示如下。



参数说明

标题项		说明
IPTV 设置	IPTV 口选择	指定路由器的一个 LAN 口作为 IPTV 口，用于连接光猫的 IPTV 口。LAN 端口号查看“系统”页面的“接口信息”。
	IPTV 功能	开启或关闭路由器的 IPTV 功能。
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。
	备注	AP 的备注信息。
	MAC 地址	AP 的 MAC 地址。

标题项	说明
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 LAN0。

6.8.2 观看 IPTV 节目（情景 1）

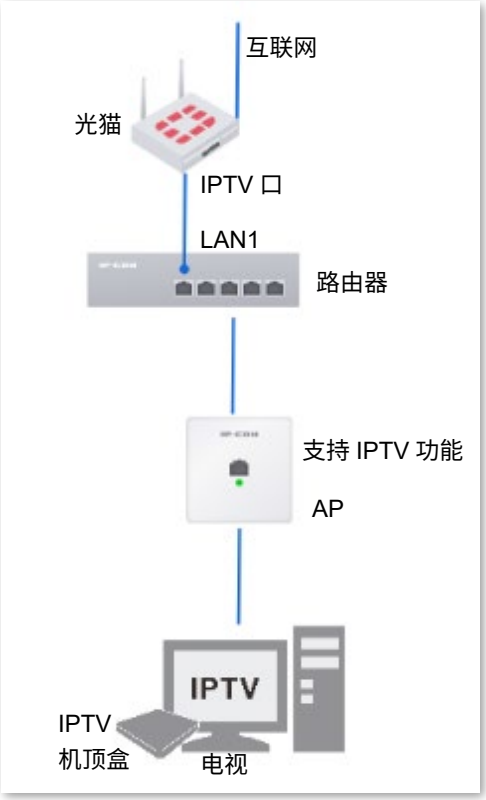
组网需求

某旅馆的宽带业务中包含 IPTV 业务。网络运营商提供了 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

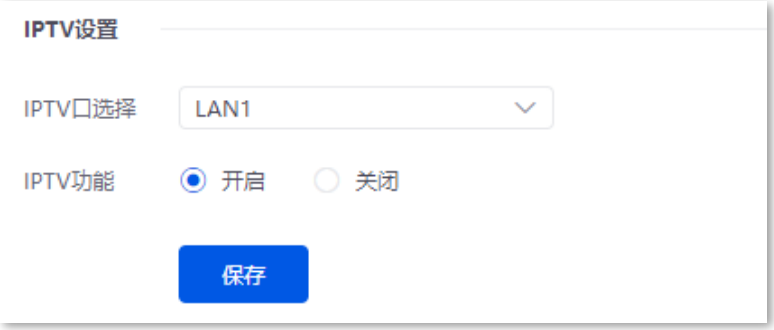
1. 配置路由器。

   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“LAN1”。
   - 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。

2. 设置您的 IPTV 机顶盒。

   使用网络运营商提供的 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。

6.8.3 观看 IPTV 节目（情景 2）

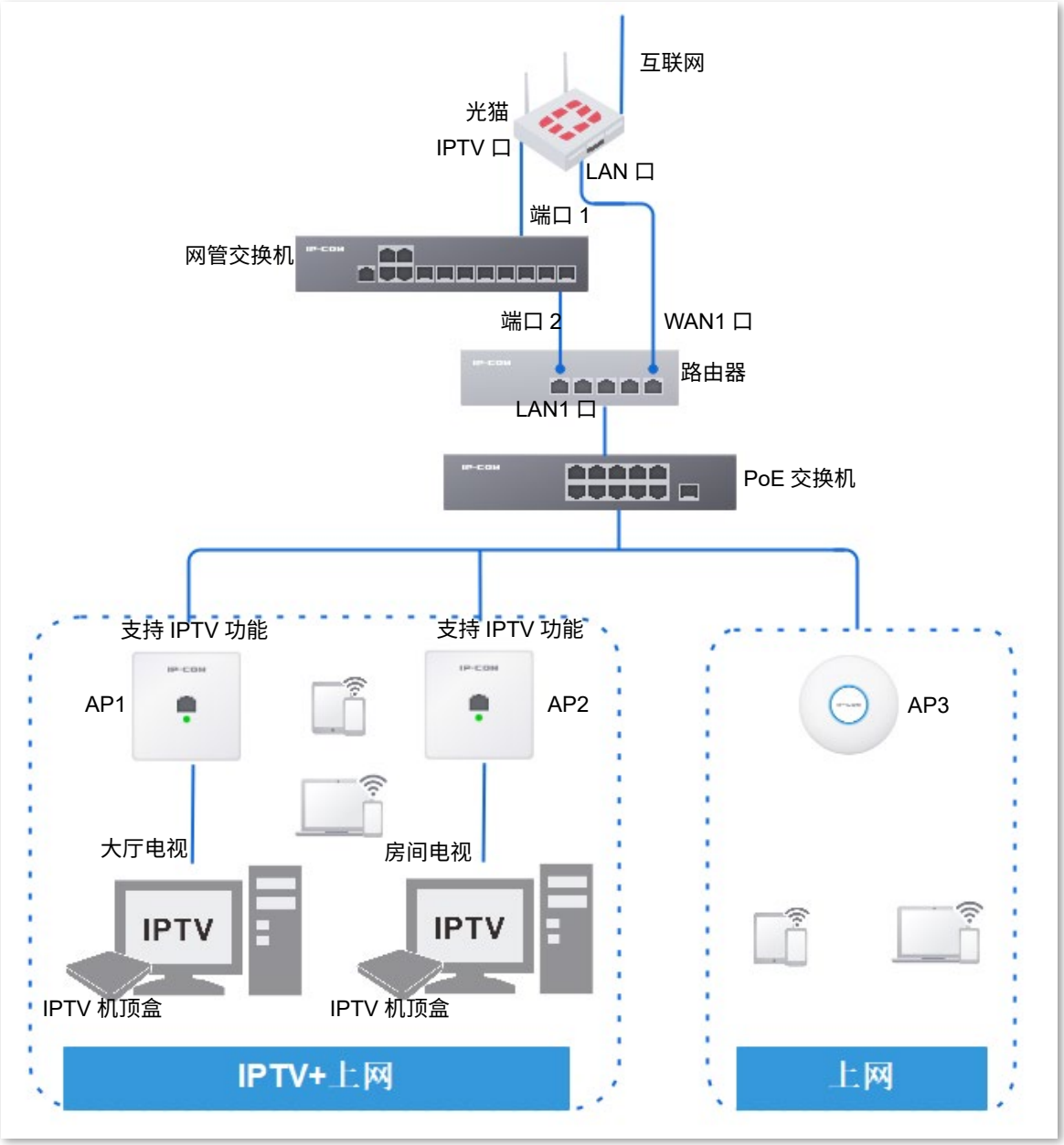
组网需求

某酒店的宽带业务中包含 IPTV 业务。网络运营商提供了 IPTV 账号和密码，且提供了 IPTV 业务的 VLAN ID（此处以 VLAN ID 为 2 为例）。

需求：能够同时观看 IPTV 节目和上网。

方案设计

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



配置步骤

配置 IPTV 业务

1. 配置交换机（此处以 IP-COM 二层网管型交换机 G3328FV1.0 为例）。

   1) 添加 VLAN。

   - 点击「常用功能」>「VLAN 划分」>「802.1Q VLAN」。
   - 点击 + 添加 。
   - 在弹出的窗口中设置“VLAN ID”为“2”，“VLAN 描述”为“IPTV”，点击 确认 。

   2) 配置端口属性。

   - 点击「常用功能」>「VLAN 划分」>「端口成员」。
   - 点击端口 1 后面的 按钮，设置“PVID”为“2”。
   - 点击端口 2 后面的 按钮，设置“PVID”为“2”。

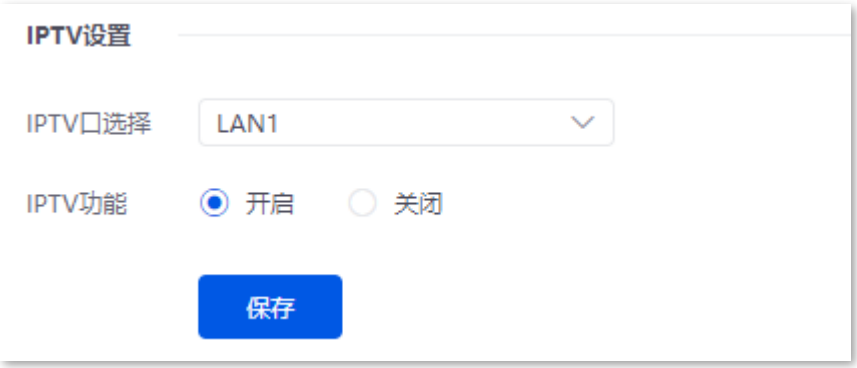
2. 配置路由器。

   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 端口。

   - 选择路由器作为 IPTV 的 LAN 口，本例为“LAN1”。
   - 选择“IPTV 功能”为“开启”。
   - 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 2 的（4），指定其他 AP2（支持 IPTV 功能）的有线网口。

3. 光猫下来的 IPTV 线接到交换机的端口 1。

4. 用网线将交换机的端口 2 连接至路由器的 IPTV 口。

5. IPTV 机顶盒连接至指定的 AP 有线网口。

6. 设置您的 IPTV 机顶盒。

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

   ----完成

验证配置

完成配置后，您可以同时观看 IPTV 节目和上网。

7 SD-WAN

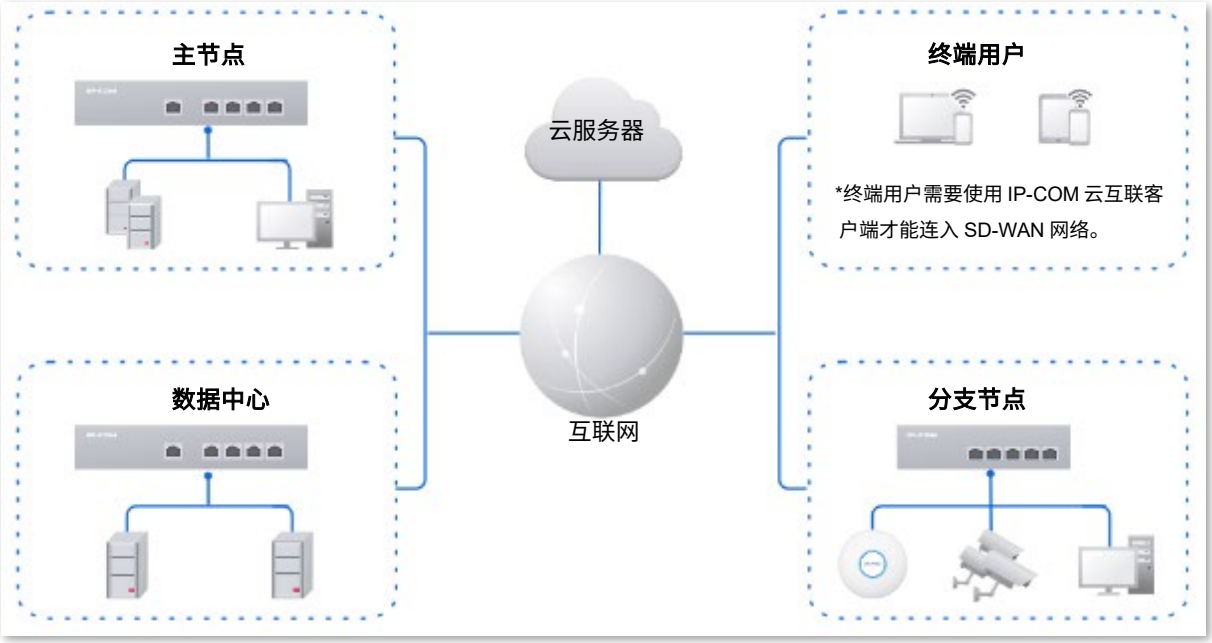
7.1 概述

SD-WAN，即软件定义广域网络，是将 SDN（Software Defined Network，软件定义网络）技术应用到广域网场景中所形成的一种服务。可以为企业提供出差员工、分公司、总部及数据中心的广域互联。

SD-WAN 组网优势：

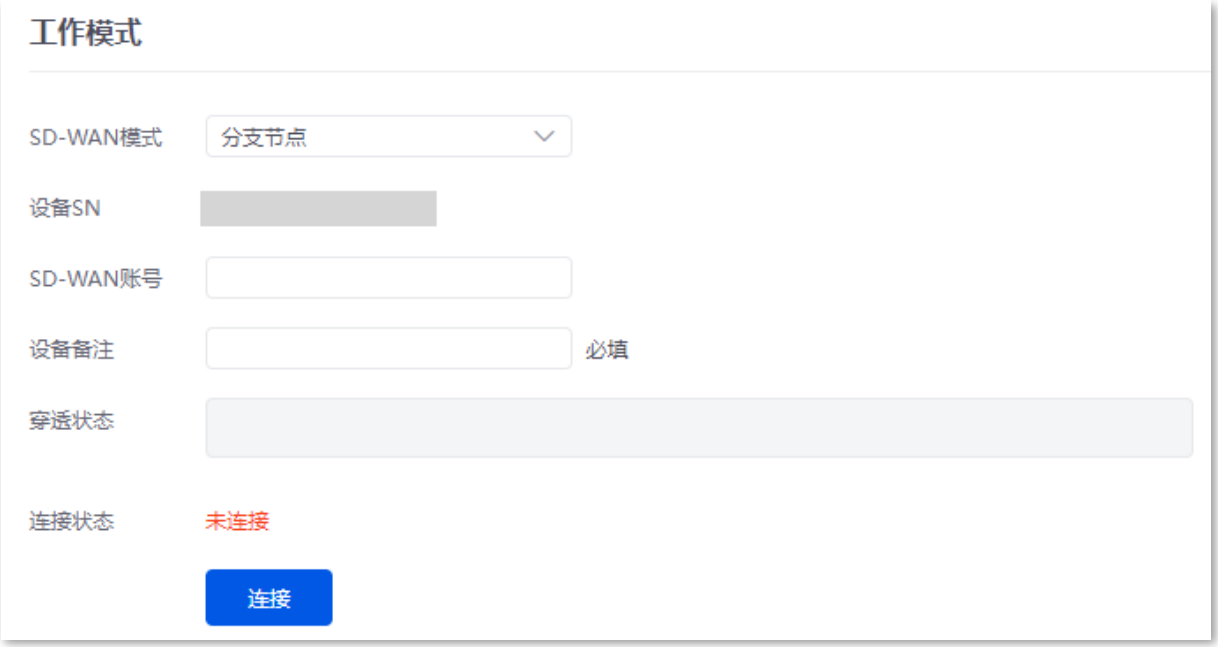
- 组网简单，通过云服务器实现一键互联。
- 权限管理，主节点可以给各个分支节点、终端账号和数据中心配置不同的访问策略。
- 统一管理，主节点可以对各分支节点的 WiFi 和视频监控进行统一管理。

SD-WAN 解决方案典型组网拓扑如下。



进入页面：登录到路由器 Web 管理页面后，点击「SD-WAN」。

在这里，您可以配置路由器的 SD-WAN 模式及相关信息，仅支持“分支节点”模式。本路由器 SD-WAN 功能默认关闭，设置为“分支节点”模式时显示如下。

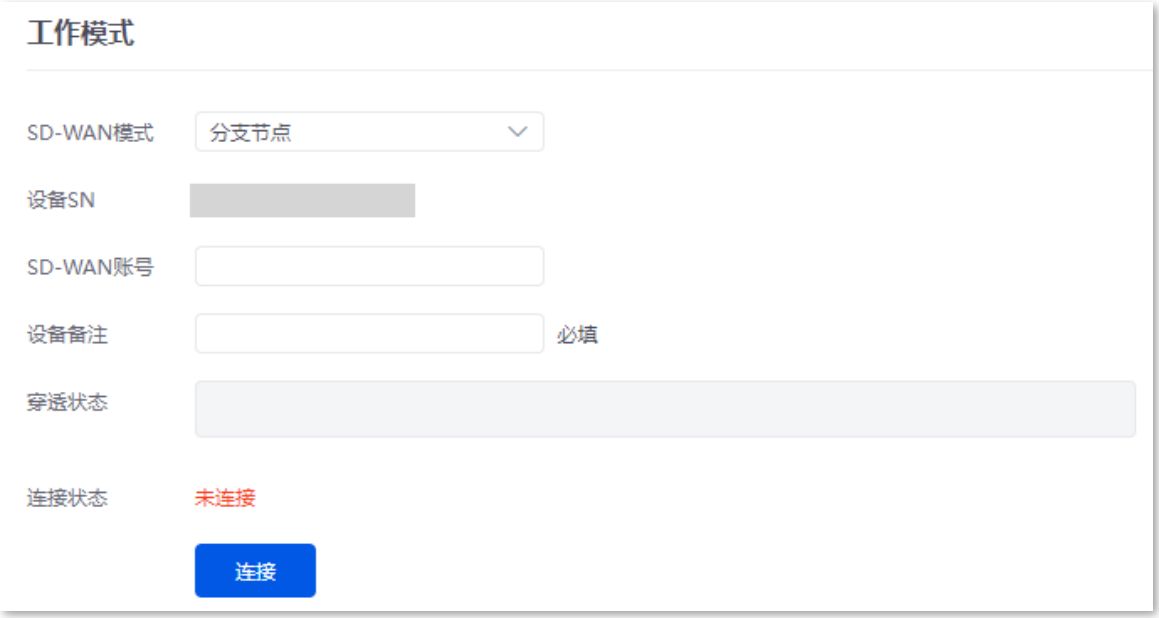


参数/按钮说明

标题项	说明
SD-WAN 模式	路由器的 SD-WAN 模式，仅支持“分支节点”模式。 – 分支节点：路由器在 SD-WAN 网络中为分支节点，可以接收主节点和数据中心下发的访问策略。 – 关闭：路由器不开启 SD-WAN 功能。
设备 SN	路由器的 SN 信息。
SD-WAN 账号	连接 SD-WAN 云服务的账号，即，主节点的 SD-WAN 账号。
设备备注	路由器的备注信息，方便主节点进行识别。
穿透状态	显示当前节点与 SD-WAN 网络中其他节点之间的穿透连接状态。
连接状态	路由器与主节点的连接状态，有已连接、未连接、连接中三种状态。
连接	用于连接/断开主节点。
断开	

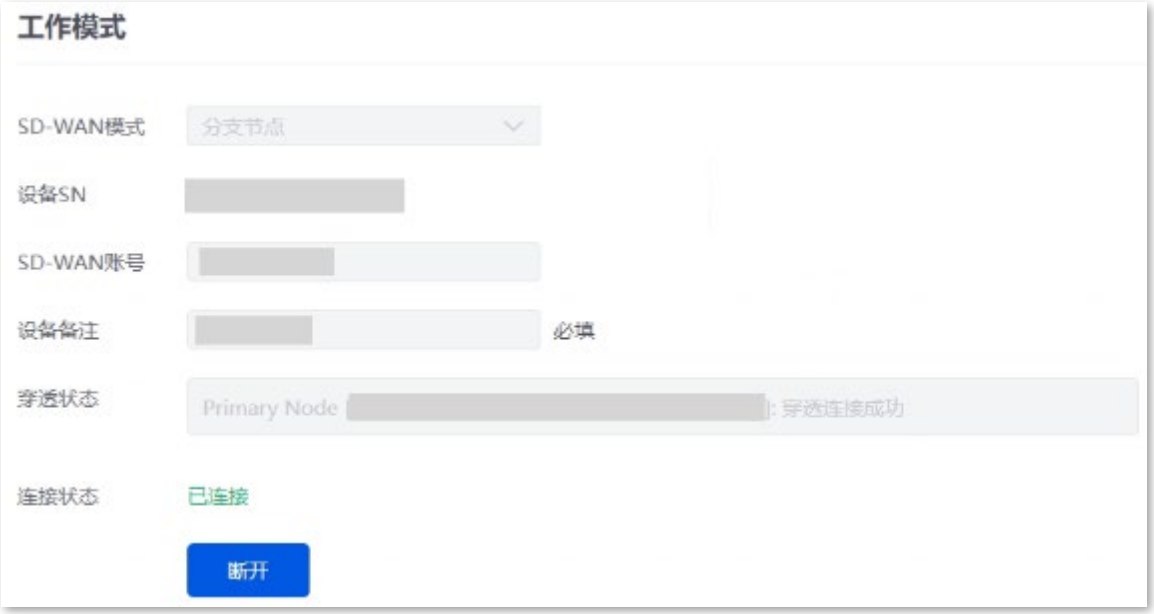
7.2 配置 SD-WAN 工作模式

1. 登录到路由器 Web 管理页面后，点击「SD-WAN」。
2. 选择“SD-WAN 模式”为“分支节点”。
3. 输入主节点的 SD-WAN 云服务账号。
4. 设置易识别的路由器备注信息。
5. 点击 连接 。



----完成

主节点将会收到本路由器的加入请求。主节点将本路由器加入到 SD-WAN 网络后，“连接状态”将显示已连接，下图供参考。



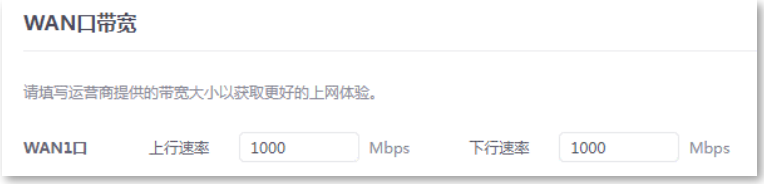
8 网速控制

8.1 WAN 口带宽

进入页面：登录到路由器 Web 管理页面后，点击「网速」>「WAN 口带宽」。

在这里，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，可以让智能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
上传速率	填入所办理的宽带的带宽值。不清楚时，可以咨询您的网络运营商。
下载速率	

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。

进入页面：登录到路由器 Web 管理页面后，点击「网速」>「分组限速」。

在这里，您可以配置路由器的分组限速策略。

参数说明

标题项	说明
序号	分组限速策略的名称。
备注	分组限速策略的备注。
限速方式	本路由器支两种分组限速策略。 – 智能限速：路由器根据 WAN 口带宽页面设置的 WAN 口上传/下载速率，在对应时间内平均地给 IP 组用户分配带宽。使用智能限速前，管理员需在「WAN 口带宽」页面正确输入办理的宽带带宽。 – 自定义限速：您可以根据实际环境需要，给 IP 用户在对应时间内单独设置最大上传/下载速率，或统一设置最大上传/下载速率。
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。
带宽共享策略	限速模式有共享和独享模式，智能限速模式只能选择共享模式。 – 共享：受限范围内的所有用户共享您设置的上传/下载速率。此模式下，每个受控用户所获得的带宽可能不一样。 – 独享：受限范围内的每个用户独享您设置的上传/下载速率。此模式下，每个受控用户所获得的带宽都是一样的。
并发连接数	受控 IP 地址范围中，每台用户设备所能使用的最大连接数。 提示 0 表示不限制。
上传速率	受控用户的最大上传/下载速率。

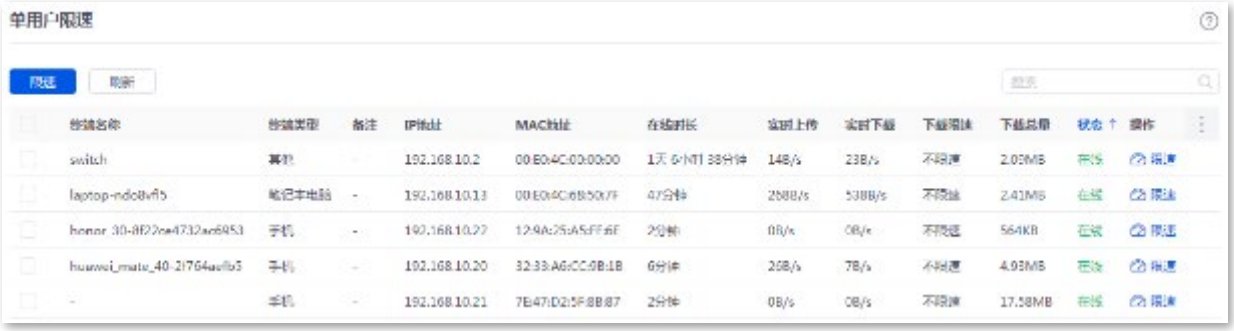
标题项	说明
下载速率	提示 0 表示不限速。

8.3 单用户限速

8.3.1 概述

进入页面：登录到路由器 Web 管理页面后，点击「网速」>「单用户限速」。

在这里，您可以根据实际需要，为连接到路由器的用户单独设置最大上传/下载速率，或统一设置最大上传/下载速率。



参数说明

标题项	说明
终端名称	终端设备的名称。
终端类型	终端设备的类型。
备注	终端设备的备注信息。
IP 地址	终端设备的 IP 地址。
MAC 地址	终端设备的 MAC 地址。
在线时长	终端设备本次接入路由器网络的时长。
实时上传	终端设备的实时上传/下载速率。
实时下载	
上传限速	终端设备的最大上传/下载速率。
下载限速	
上传总量	终端设备的总上传/下载流量。
下载总量	
状态	终端设备的状态。
操作	对单台终端设备进行限速管理。

8.3.2 限速终端设备

1. 登录到路由器 Web 管理页面，点击「网速」>「单用户限速」。
2. 找到要限速的终端设备，点击限速。

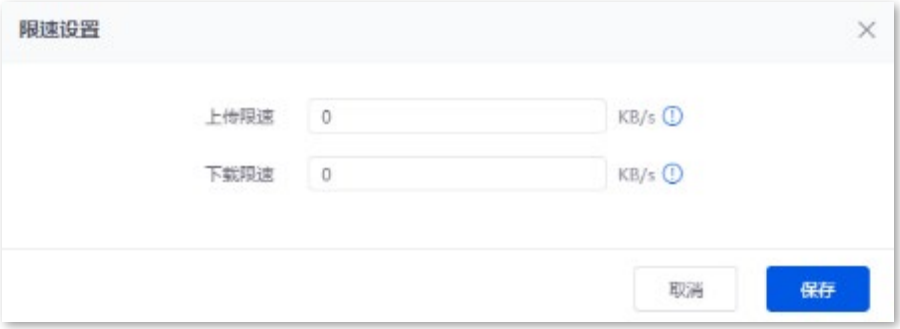
提示

如果您要同时对多台终端设备进行限速，可以选择多台终端设备后，点击 限速 ，然后根据页面提示操作。

3. 为终端设备设置最大上传速率和下载速率，点击 保存 。下图仅供参考。

提示

“0”表示不限速。



---完成

8.4 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。

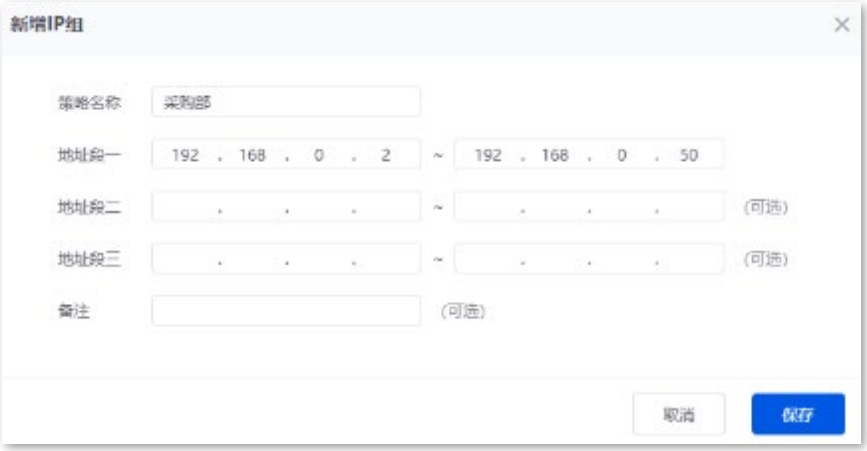
配置步骤

1. 登录到路由器 Web 管理页面。
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。

3. 配置 IP 组。

   点击「审计」>「分组策略」>「IP 组」，配置如下 IP 组。



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	限速方式：独享
限速方式：自定义限速	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。

9 行为与审计

9.1 分组策略

在配置上网过滤、分组限速和自定义多 WAN 策略等基于 IP 组、时间组生效的功能前，您需要先配置相应的 IP 组策略、时间组策略。

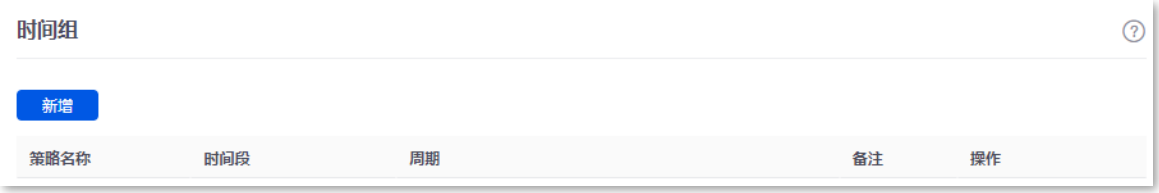
9.1.1 时间组

进入页面：登录到路由器 Web 管理页面后，点击「审计」>「分组策略」>「时间组」。

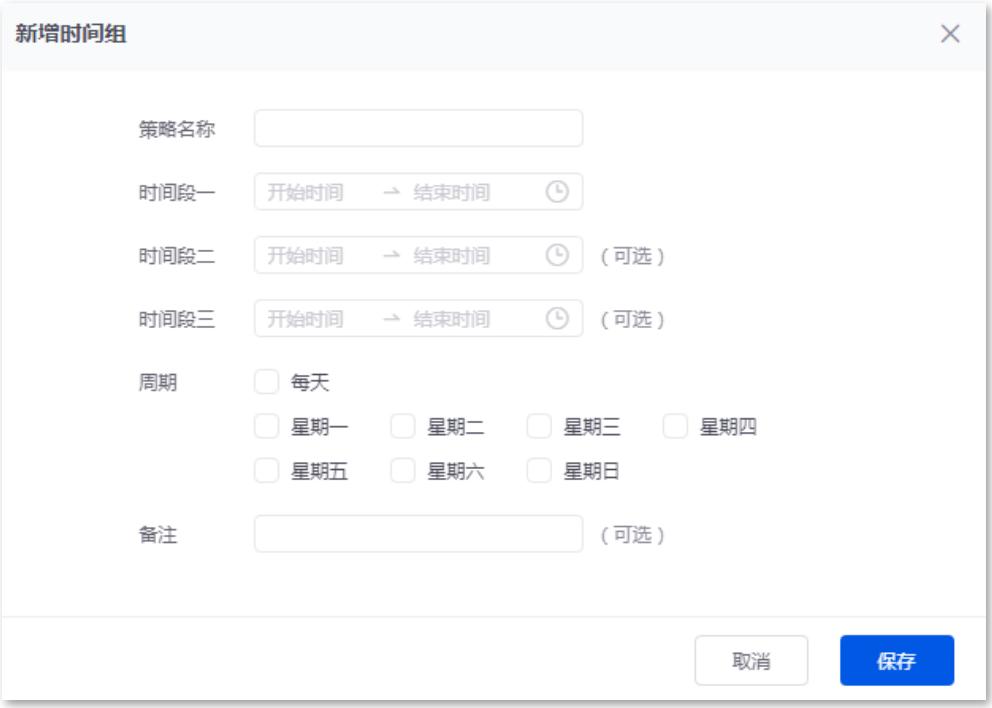
在这里，您可以根据实际需要配置相应的时间组策略。

设置步骤：

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



3. 配置时间组相关参数，点击 保存 。



---完成

参数说明

标题项	说明
策略名称	时间组策略的名称。
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。
备注	时间组策略的备注信息。

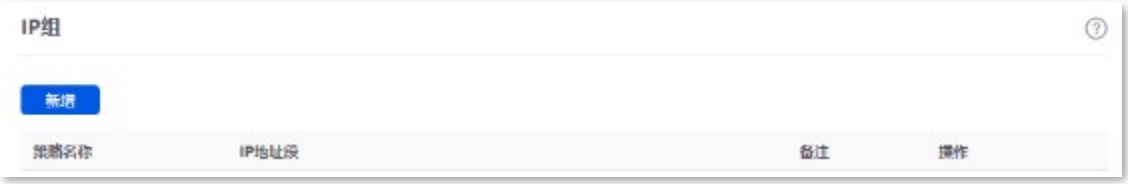
9.1.2 IP 组

进入页面：登录到路由器 Web 管理页面后，点击「审计」>「分组策略」>「IP 组」。

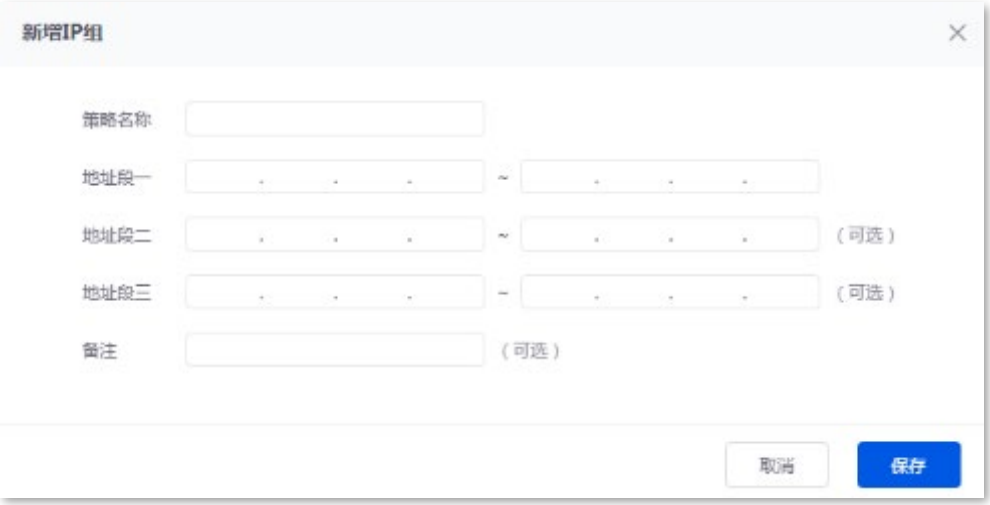
在这里，你可以根据实际需要配置相应的 IP 组策略。

设置步骤：

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



3. 配置 IP 组相关参数，点击 保存 。



---完成

参数说明

标题项	说明
策略名称	IP 组策略的名称。
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。
备注	IP 组策略的备注信息。

9.2 上网过滤

9.2.1 IP 过滤

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

在这里，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本路由器上网。

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 地址组策略应事先在「审计」>「分组策略」>「IP 组」页面配置好。
IP 地址或 IP 组	
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。
备注	IP 地址过滤策略的备注信息。
状态	IP 地址过滤策略的状态，包括已启用、已停用。
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。

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

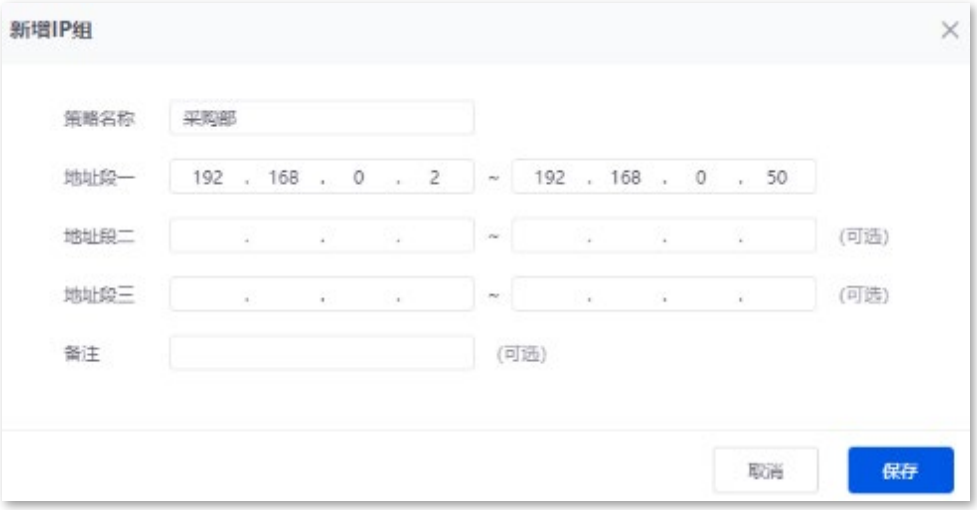
配置时间组 → 配置 IP 组 → 添加 IP 过滤策略

1. 登录到路由器 Web 管理页面。
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。

3. 配置 IP 组。

进入「审计」>「分组策略」>「IP 组」页面，配置如下 IP 组。



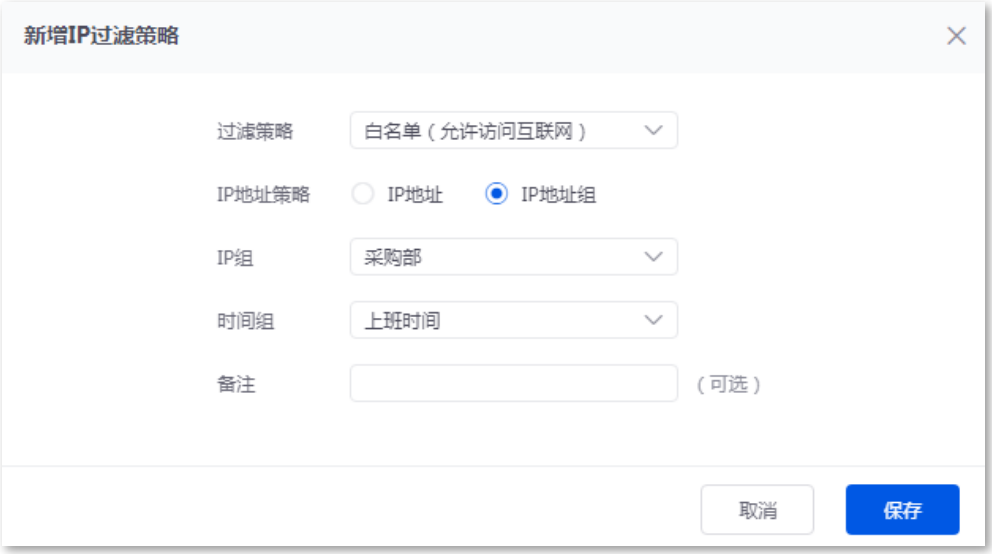
4. 添加 IP 过滤策略。

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 地址策略：IP 地址组	IP 组：采购部 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。

9.2.2 MAC 过滤

概述

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

在这里，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。

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。
状态	MAC 地址过滤策略的状态，包括已启用、已停用。
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。

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

1. 登录到路由器 Web 管理页面。
2. 配置时间组。

   点击「审计」>「分组策略」>「时间组」，配置如下时间组。

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。

9.2.3 端口过滤

概述

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

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

在这里，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。

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。
端口	禁止访问的服务的端口。
协议	禁止访问的服务的协议。
备注	端口过滤策略的备注信息。
状态	MAC 地址过滤策略的状态，包括已启用、已停用。

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

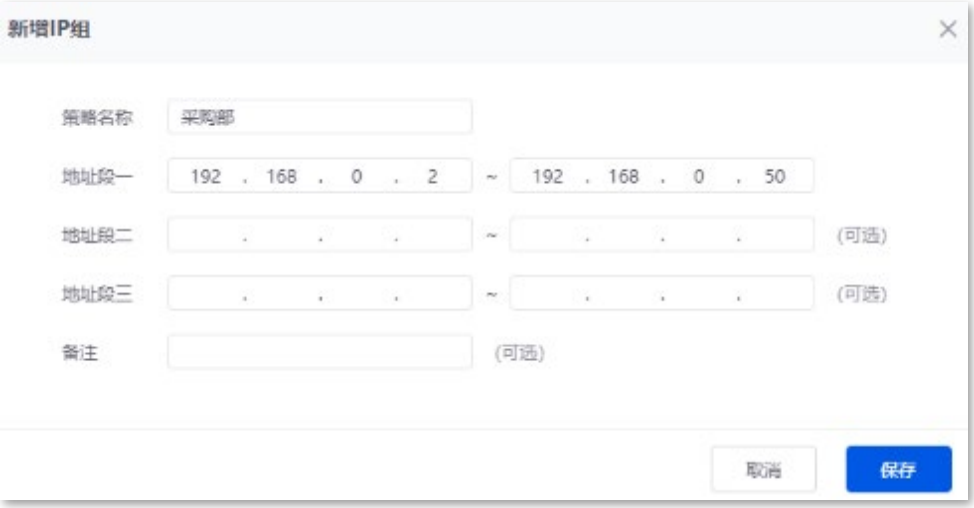
配置时间组 → 配置 IP 组 → 添加端口过滤策略

1. 登录到路由器 Web 管理页面。
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。

3. 配置 IP 组。

   进入「审计」>「分组策略」>「IP 组」页面，配置如下 IP 组。



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。

9.2.4 URL 过滤

概述

进入页面：登录到路由器 Web 管理页面后，点击「行为与审计」>「上网过滤」>「URL 过滤」。

在这里，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。

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，包括已启用、已停用。

标题项	说明
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。

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

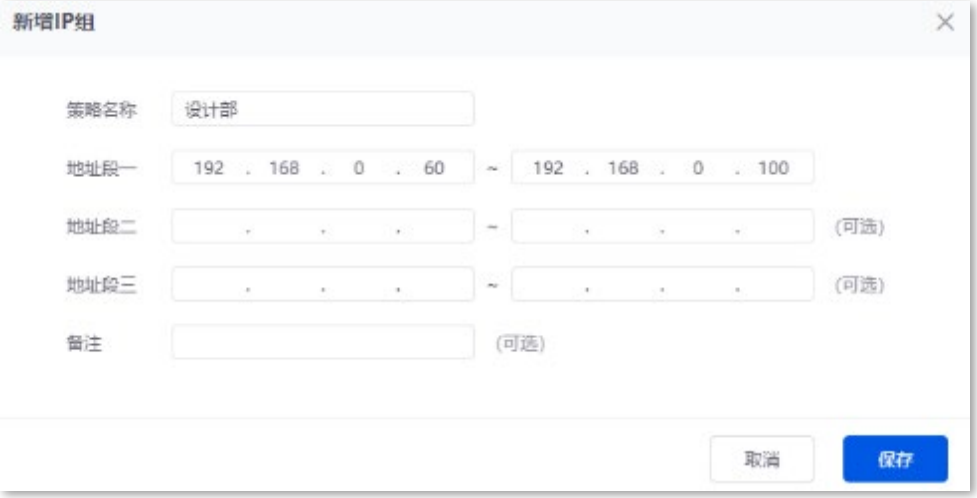
配置时间组 → 配置 IP 组 → 添加 URL 过滤策略

1. 登录到路由器 Web 管理页面。
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。

3. 配置 IP 组。

进入「审计」>「分组策略」>「IP 组」页面，配置如下 IP 组。



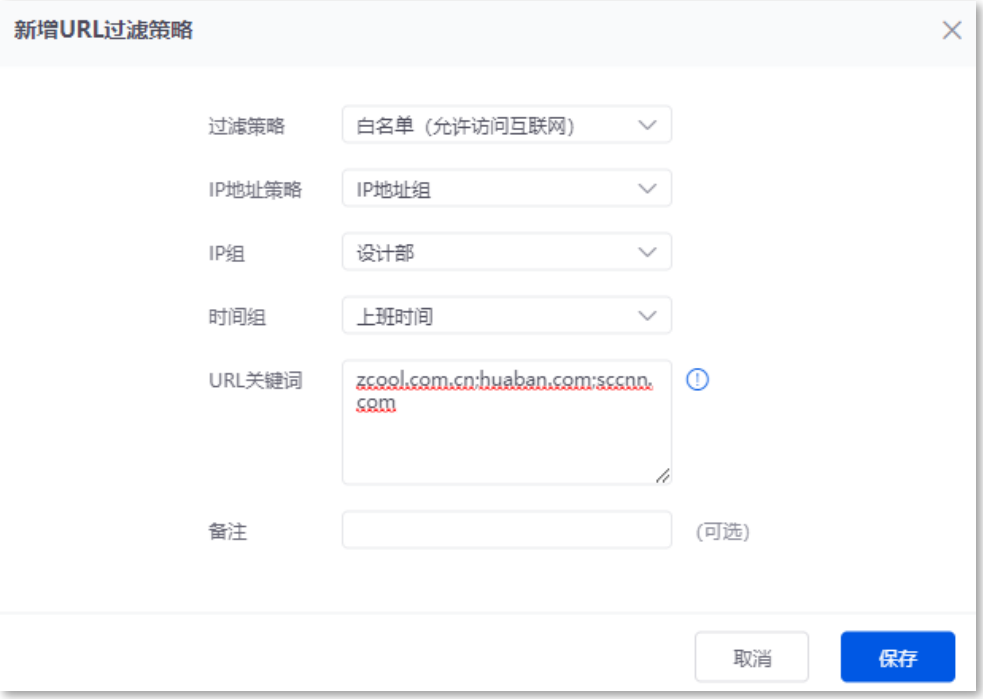
4. 添加 URL 过滤策略。

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。

9.3 日志审计

9.3.1 审计设置

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

在这里，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 SSID 名称。
审计接口范围	日志审计生效的接口。 – 所有用户：审计所有 VLAN 接口和无线接口的日志。 – 自定义：自定义选择审计 VLAN 接口或无线接口的日志。

9.3.2 日志存储

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

在这里，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。

仅部分路由器支持该功能，请以产品实际界面为准。

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。

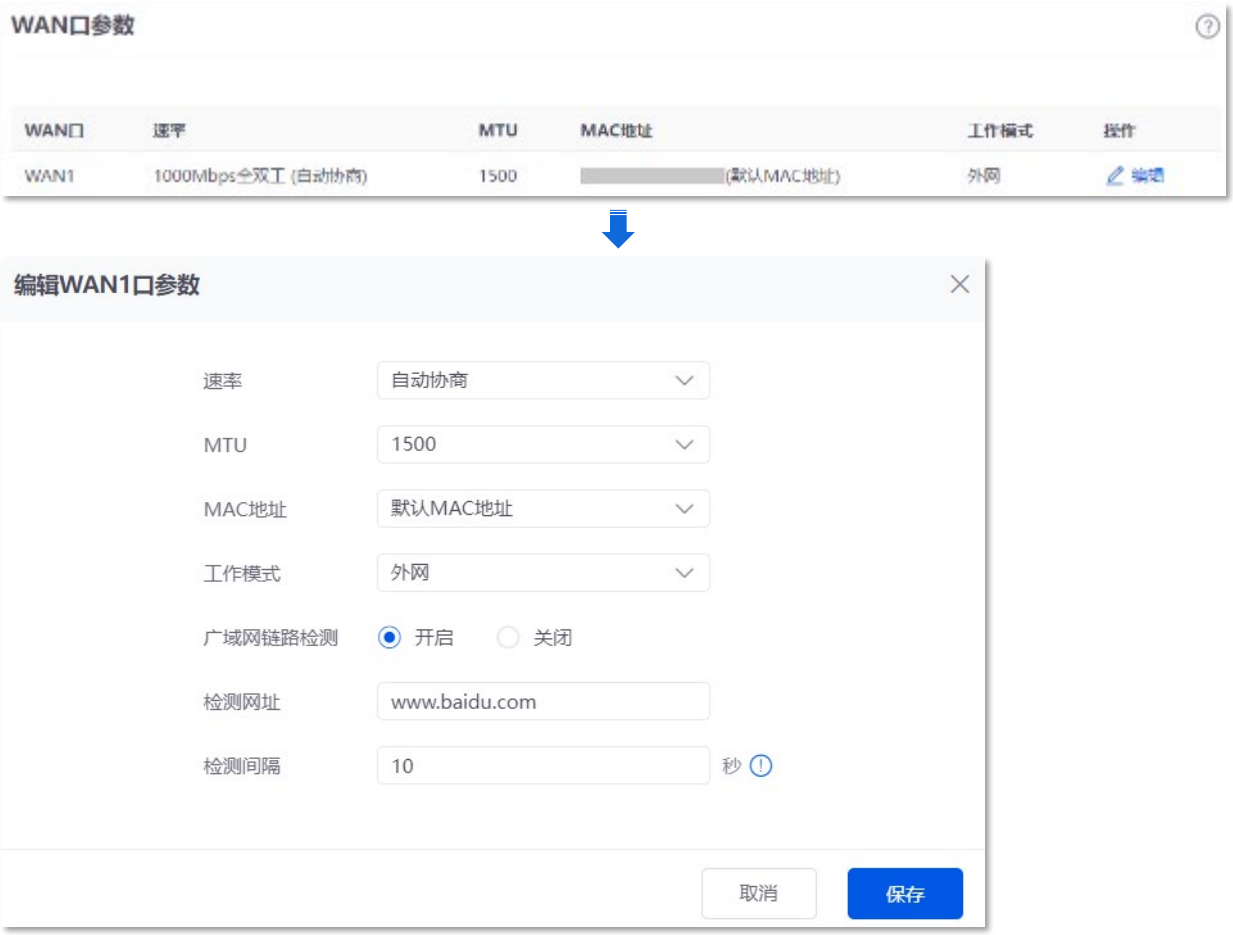
10 更多功能

10.1 高级路由

10.1.1 WAN 口参数

进入页面：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。

标题项	说明
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，有可能是网络运营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

概述

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

在这里，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，

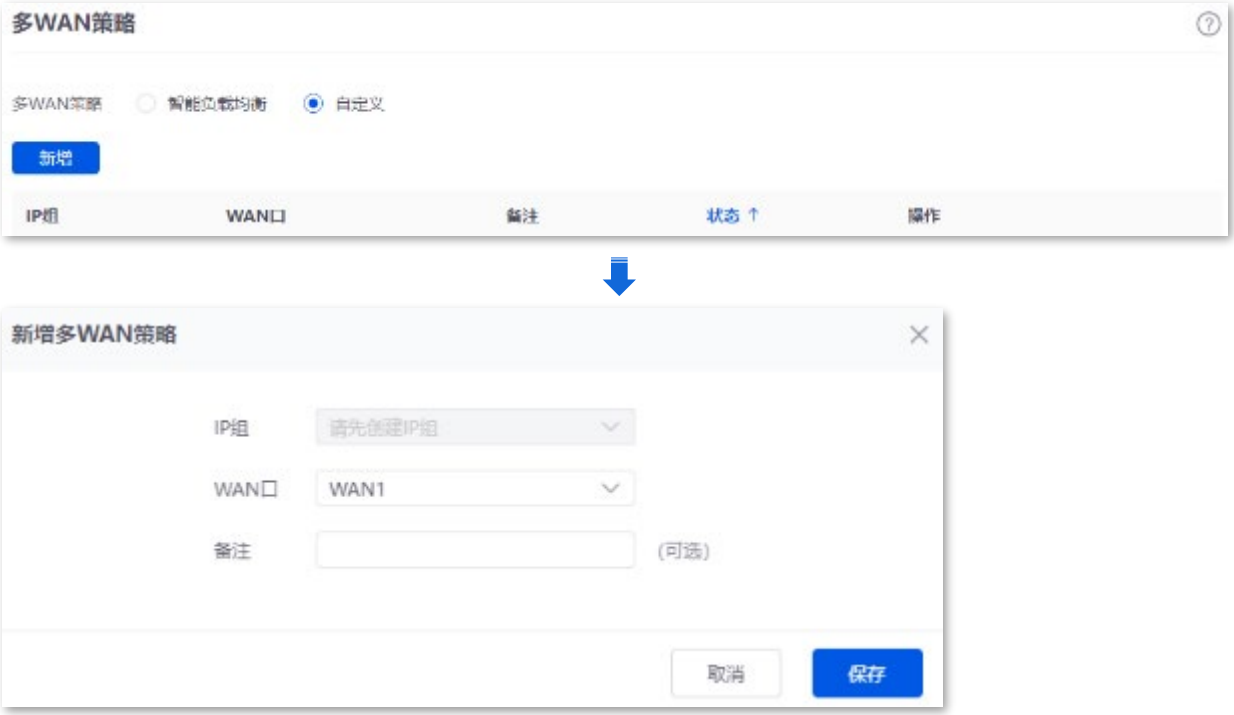
合理的设置多 WAN 策略可以大幅提升路由器的带宽利用率。

- 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。
- 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。

■ **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。

路由器的多 WAN 策略默认为“智能负载均衡”。选择“自定义”时，页面如下所示。点击 新增 可以自定义多 WAN 策略。



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。
备注	自定义多 WAN 策略的备注信息。
状态	自定义多 WAN 策略的状态。包括已启用、已停用。

自定义多 WAN 策略配置举例

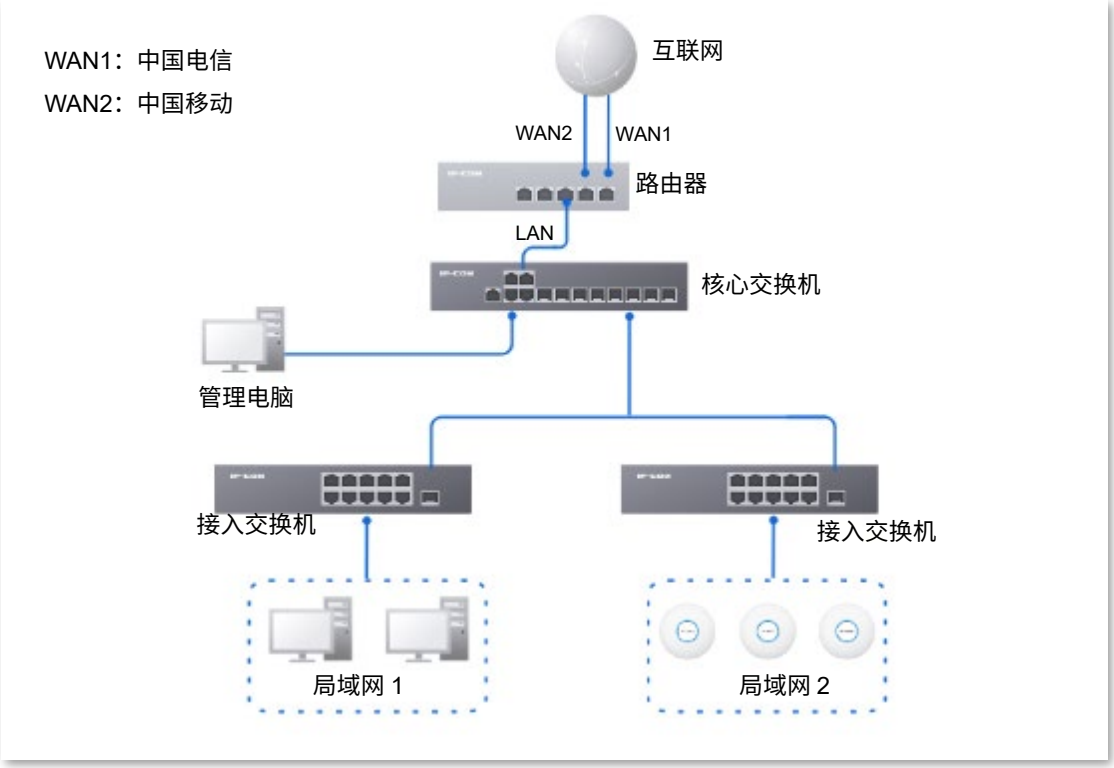
组网需求

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。

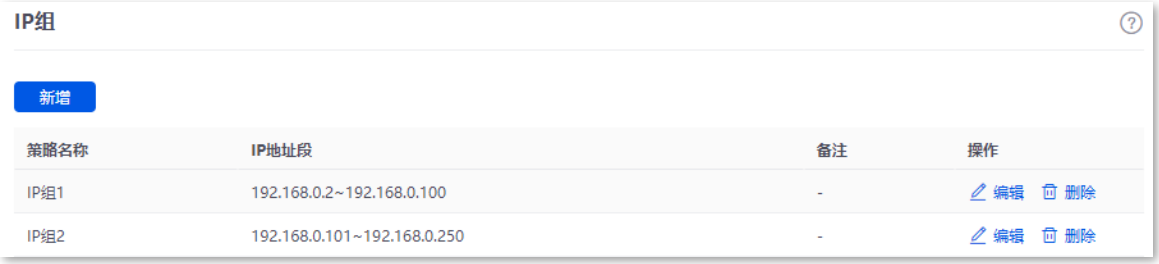


配置步骤

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

1. 登录到路由器 Web 管理页面。
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。



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 。

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。

10.1.3 静态路由

概述

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

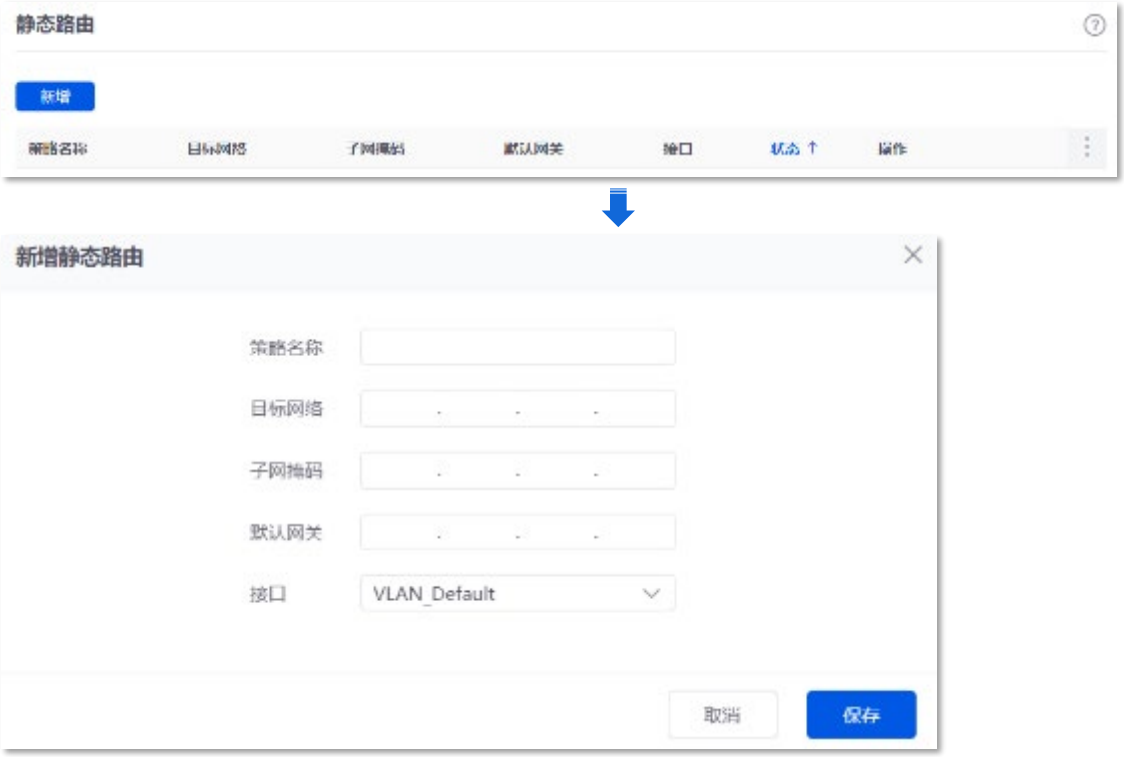
通过设置目标网络、子网掩码、默认网关和接口来确定一条静态路由，其中，目标网络和子网掩码用来确定一个目标网络或主机。静态路由设置完成后，所有目的地址为静态路由目标网络的数据均直接通过该静态路由接口转发至网关地址。

注意

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

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

在这里，您可以根据实际网络情况配置相应的静态路由。点击 新增 可以新建静态路由。



参数说明

标题项	说明
策略名称	静态路由策略的名称。

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。
状态	静态路由策略的状态。

静态路由配置举例

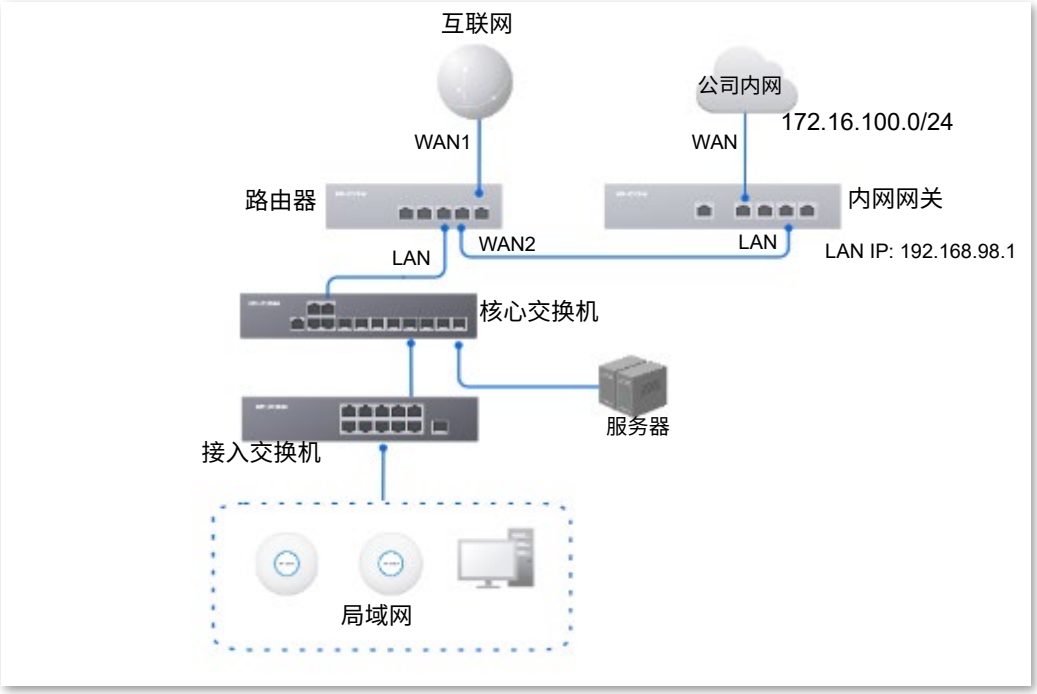
组网需求

某企业使用路由器进行网络搭建。路由器的 WAN1 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 WAN2 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

1. 登录到路由器 Web 管理页面。
2. 启用 2 个 WAN 口，并设置 WAN2 联网。
   1) 点击「网络」>「联网设置」。
   2) 设置“WAN 口个数”为“2”。

   3) 在 WAN2 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，WAN2 口联网成功。

3. 配置静态路由。

1） 获取 WAN2 口的 IP 地址信息。

进入「网络」>「联网设置」页面，查看 WAN2 获取的 IP 地址信息，本例中相关信息如下。

WAN2 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。

10.1.4 路由表

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「路由表」。

在这里，您可以查看路由器的详细路由信息。

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。

10.1.5 策略路由

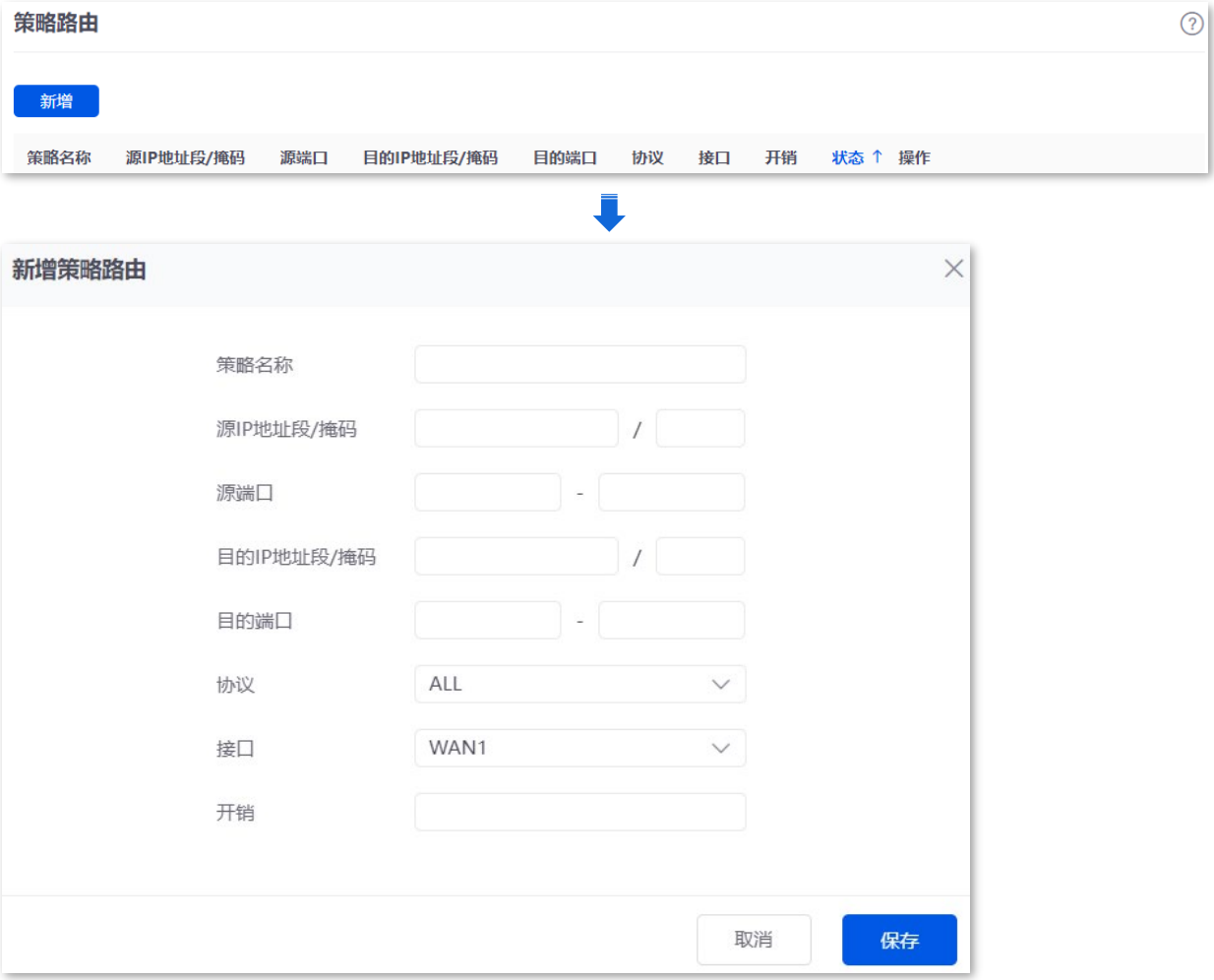
概述

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。

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「高级路由」>「策略路由」。

在这里，您可以配置策略路由。点击 新增 可以新建策略路由。



参数说明

标题项	说明
策略名称	策略路由的策略名称。
源 IP 地址段/掩码	要进行精确路由转发的源 IP 地址段。

标题项	说明
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	该策略的优先级，值越小，策略路由优先级越高。
状态	策略的状态。

策略路由配置举例

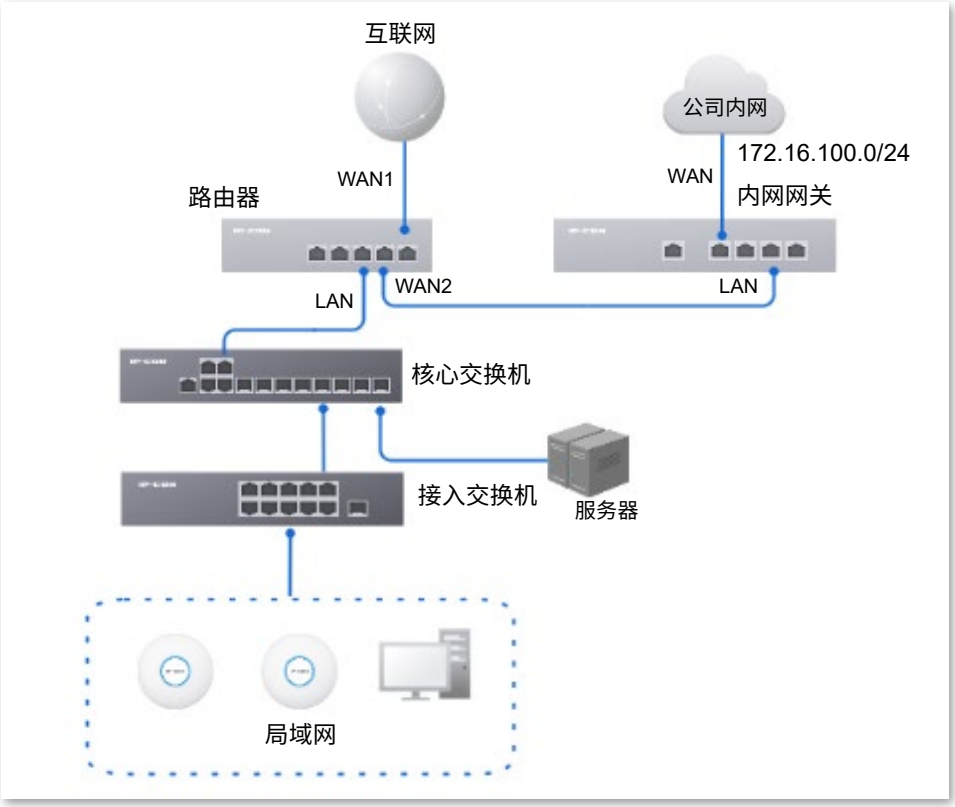
组网需求

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 WAN2 口联网 → 配置策略路由

1. 登录到路由器 Web 管理页面。
2. 配置 WAN2 口联网。
   1) 点击「网络」>「联网设置」。
   2) 设置“WAN 口个数”为“2”。

   3) 在 WAN2 处选择“联网方式”为“动态 IP”，然后点击 连接 。

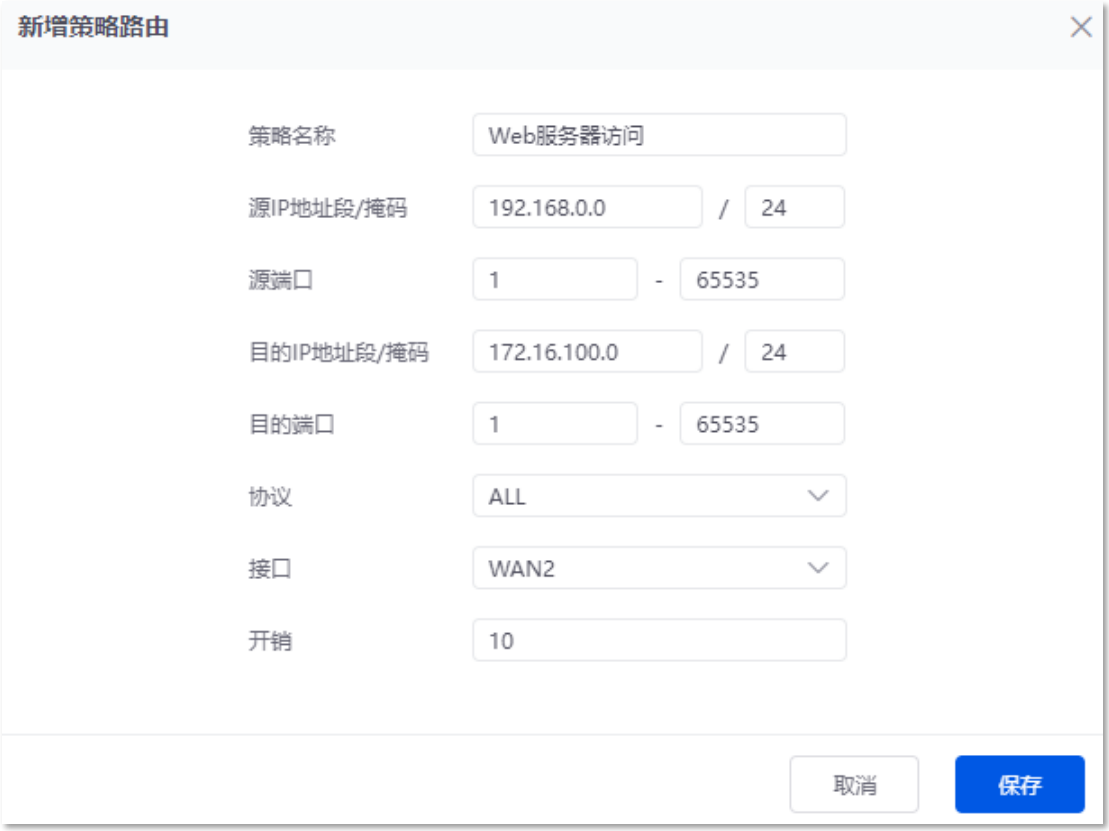
稍等片刻，当联网状态显示“已联网”时，WAN2 口联网成功。

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	WAN2	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。

10.2 虚拟服务

10.2.1 DMZ

概述

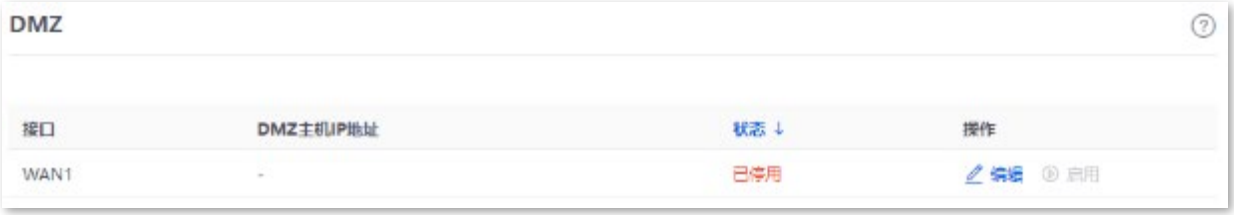
将局域网中某台设备设置为 DMZ 主机后，该设备与互联网通信时将不受限制。如某台电脑正在进行视频会议或在线游戏，可将该电脑设置为 DMZ 主机，使视频会议和在线游戏更加顺畅。另外，在互联网用户需要访问局域网资源时，也可将该服务器设置为 DMZ 主机。

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。

进入页面：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。



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。
状态	DMZ 策略的状态，包括已启用和已停用。

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

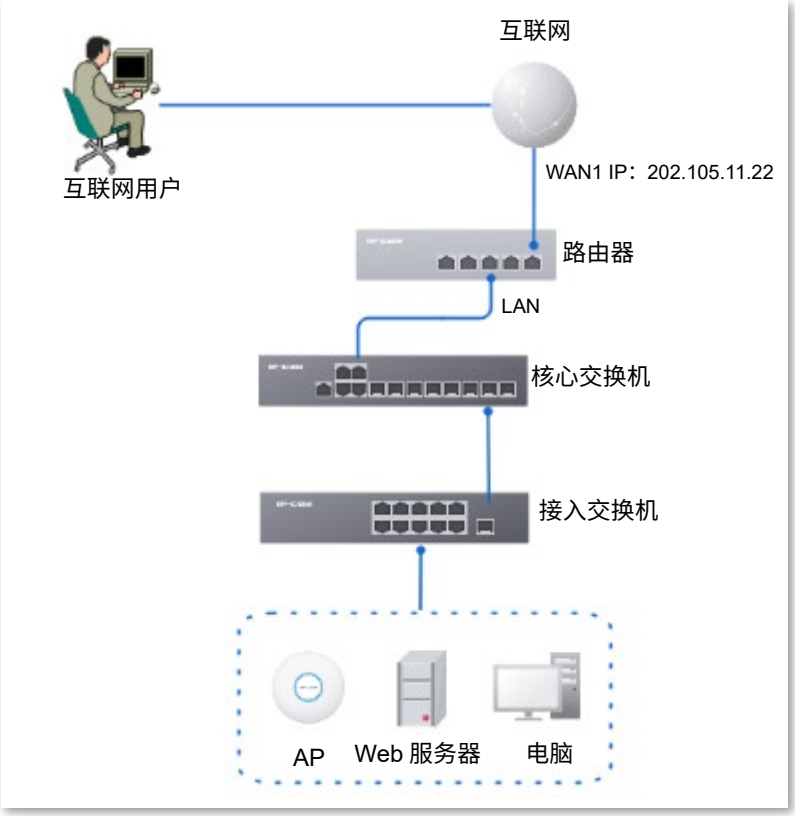
- 采用路由器的 DMZ 功能实现互联网用户访问企业内部 Web 服务器的需求。
- 采用路由器的静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

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

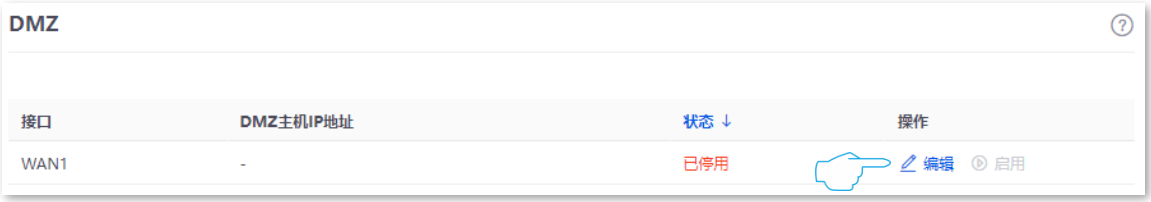
- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持访问未经报备使用默认端口号 80 的 Web 服务。因此，在使用 DMZ 功能时，建议将内网服务端口设为非熟知端口（1024~65535），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



配置步骤

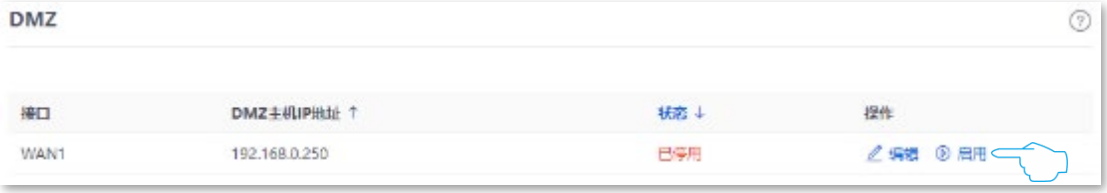
配置 DMZ 主机 → 给 DMZ 主机分配固定 IP 地址

1. 登录到路由器 Web 管理页面。
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。



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。

10.2.2 DDNS

概述

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

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

进入页面：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“未启用”。您根据实际情况修改相应的 DDNS 策略。

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。设置为除 oray 外的其他 DDNS 提供商时，需要手动输入在对应网站上申请的域名。
状态	DDNS 策略的状态。

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

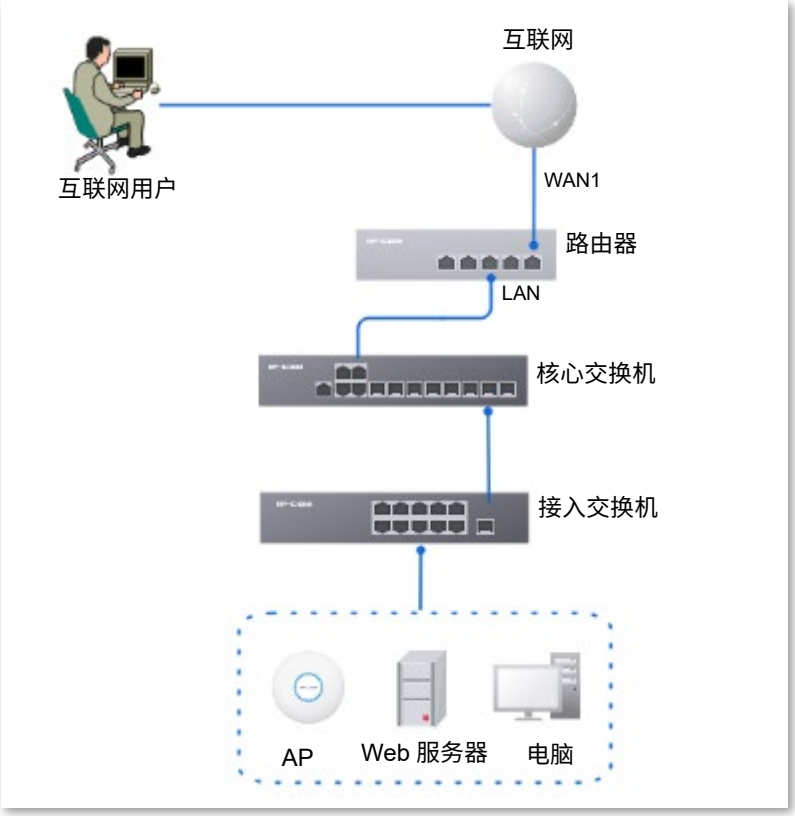
- 采用路由器的端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。
- 采用路由器的 DDNS 功能让互联网用户可以通过固定域名访问企业内部 Web 服务器，防止因 WAN 口 IP 地址变化导致访问失败。
- 采用路由器的静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

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

1. 登录到路由器 Web 管理页面。
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。

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 。

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。

5. 配置 DDNS。

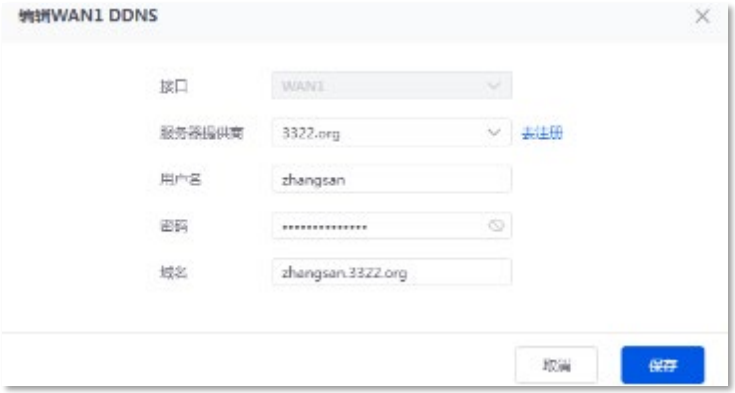
1） 点击「更多」>「虚拟服务」>「DDNS」，点击对应 WAN 口规则后的编辑，本例为“WAN1”。

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。

10.2.3 DNS 劫持

概述

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。

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

在这里，您可以根据实际需要配置 DNS 劫持策略。

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。
状态	DNS 劫持策略的状态，包括已启用和已停用。

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

1. 登录到路由器 Web 管理页面。
2. 点击「更多」>「虚拟服务」>「DNS 劫持」，然后点击 新增 。

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”。

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。

10.2.4 IP 劫持

概述

启用 IP 劫持后，局域网内的用户访问指定 IP 地址的端口服务时，直接劫持到映射 IP 地址。

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「IP 劫持」。

在这里，您可以根据实际需要配置 IP 劫持策略。

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。
状态	IP 劫持策略的状态，包括已启用和已停用。

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

1. 登录到路由器 Web 管理页面。
2. 点击「更多」>「虚拟服务」>「IP 劫持」，然后点击 新增 。

3. 输入目的 IP 地址，本例为“1.1.1.1”。
4. 输入映射的路由器 IP 地址，本例为“192.168.0.252”。
5. 输入端口号，本例为“443”。
6. 点击 保存 。

----完成

验证配置

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

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。

进入页面：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，在这里，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。如下图示例。

10.2.6 端口镜像

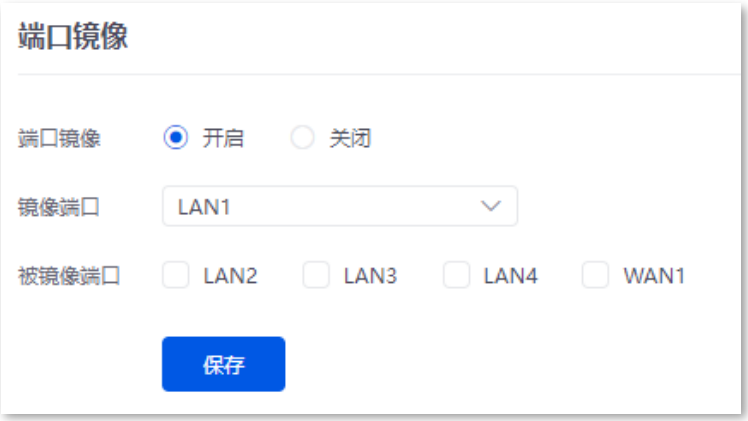
概述

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

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「虚拟服务」>「端口镜像」。

在这里，您可以根据实际需要配置端口镜像。

端口镜像默认关闭，开启后，页面显示如下：



参数说明

标题项	说明
端口镜像	开启/关闭端口镜像功能。
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。

端口镜像配置举例

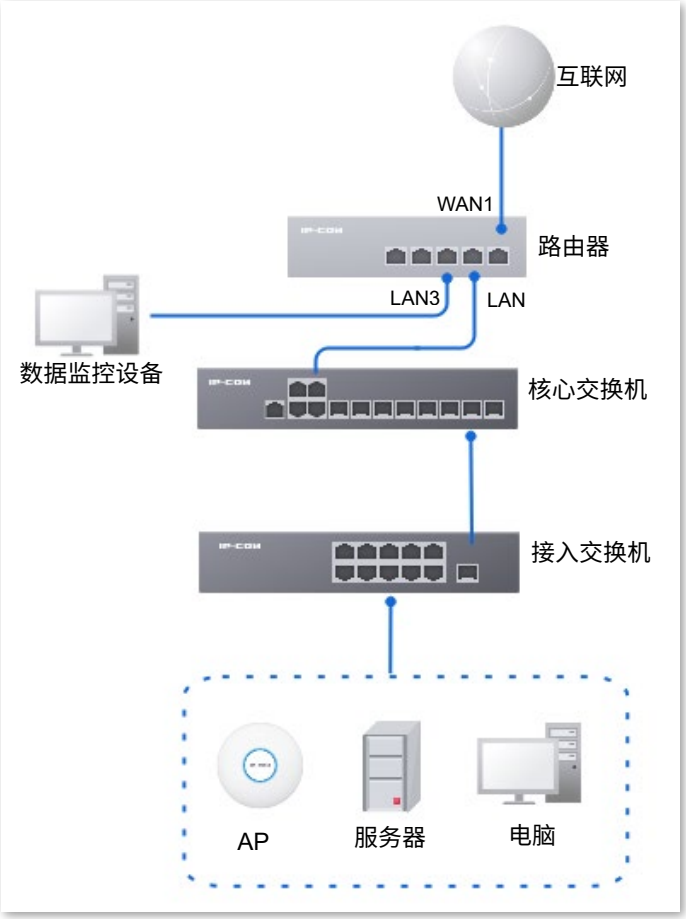
组网需求

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

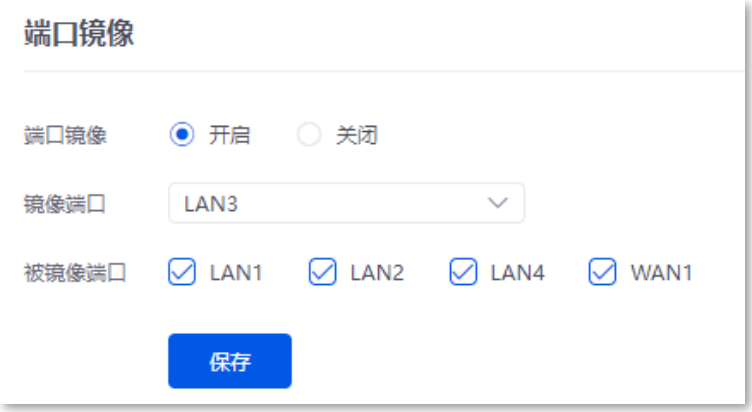
可以采用路由器的端口镜像功能实现上述需求。

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

1. 登录到路由器 Web 管理页面。
2. 点击「更多」>「虚拟服务」>「端口镜像」。
3. 开启“镜像端口”功能。
4. 选择“镜像端口”，本例为“LAN3”。
5. 选择“被镜像端口”，本例为“LAN1、LAN2、LAN4、WAN1”。
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。

10.2.7 端口映射

概述

默认情况下，广域网中的用户不能访问局域网内的设备。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。

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

在这里，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，开启后显示如下。

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。
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。
状态	规则的状态，包括已启用、已禁用。

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

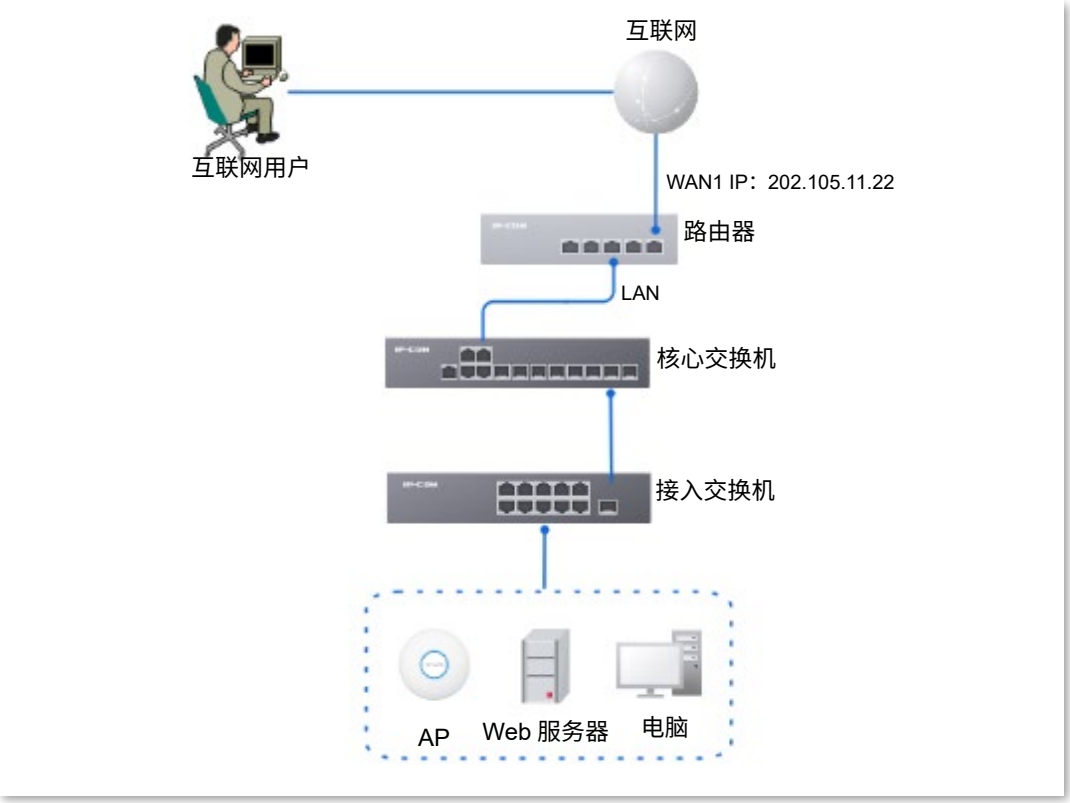
- 采用路由器的端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。假设路由器开放的外网端口为 9999。
- 采用路由器的 DHCP 静态分配功能，防止因 Web 服务器 IP 地址改变导致互联网用户访问企业内部 Web 服务器失败。

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

1. 登录到路由器 Web 管理页面。
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：WAN1	

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。

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。

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。

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

在这里，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

概述

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。

进入页面：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」。

在这里，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，开启后，页面显示如下。

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。

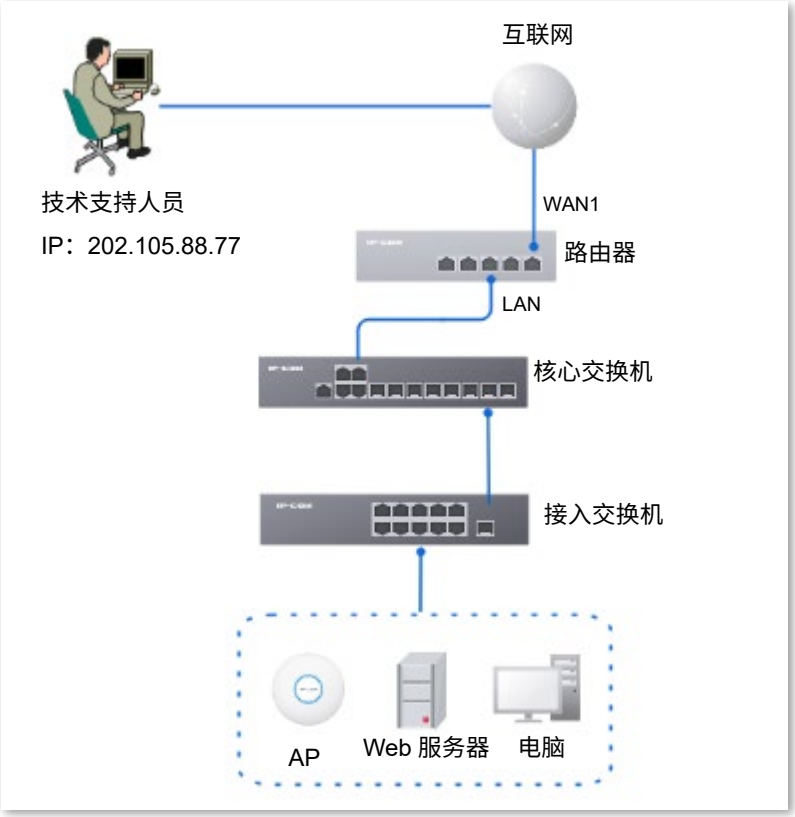
远程 WEB 管理配置举例

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 IP-COM 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

1. 登录到路由器 Web 管理页面。
2. 点击「更多」>「维护服务」>「远程 WEB 管理」。
3. 开启“远程 WEB 管理”功能。
4. 选择远程访问路由器时所使用的 WAN 口，本例为“WAN1”。
5. 选择“指定地址”，然后输入 IP-COM 技术支持的电脑的 IP 地址，本例为“202.105.88.77”。
6. 点击 保存 。

----完成

验证配置

IP-COM 技术支持在其电脑（IP 地址为 202.105.88.77）上访问“https://48cf23bf106f4a60.web.ip-com.com.cn:8082”，即可登录路由器管理页面并对其进行管理。

10.3.2 AP 管理模式

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「维护服务」>「AP 管理模式」。

在这里，您可以设置 AP 的管理方式以及为 VLAN 接口添加 AP DHCP 策略。本路由器只支持管理 IP-COM 公司的胖 AP。

AP 管理模式功能默认为“胖 AP 管理”，并为 VLAN_Default 接口添加了 AP_DHCP_Default 策略。

点击 新增 为 VLAN 接口添加 AP DHCP 策略，为 AP 分配 IP 地址。

参数说明

标题项	说明
AP 管理模式	开启/关闭 AP 管理功能。
管理端口	VLAN 接口。 路由器只能管理接在该管理口下的 AP。
DHCP 策略	对应管理接口下 AP 的 DHCP 策略。 提示 如果是新增 VLAN，需先在「网络」>「DHCP 设置」>「DHCP 服务器」页面添加 AP DHCP 策略。
DHCP 开始地址	对应管理接口下 AP 的 IP 地址范围。
DHCP 结束地址	
子网掩码	对应管理接口下 AP 的子网掩码。
网关地址	对应管理接口下 AP 的网关地址。
状态	AP DHCP 策略的状态。支持已停用、已启用、已失效三种状态。
备注	AP DHCP 策略的备注信息。

10.3.3 安全设置

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

在这里，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。

10.3.4 云维护

概述

工程宝云管理系统是 IP-COM 公司提供的一个云平台，可以统一管理支持云管理的 IP-COM 设备。

将本路由器加入云平台后，您既可以在云平台查看和配置本路由器的相关参数，也可以本地登录路由器 Web 管理页面进行查看和配置。

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

在这里，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
云维护	开启/关闭云维护功能。
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，同时通过 IP-COM 云管理系统（工程宝云管理系统 Web 或工程宝 App）配置维护的场景。路由器可被 IP-COM 云管理系统管理，且相关功能的配置信息由云管理系统下发，本地登录路由器的 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 IP-COM 云管理系统管理，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。获取方式如下。 – 在 IP-COM 工程宝云管理系统 Web 界面，点击右上角账户，即可在下拉菜单中获取。 – 在 IP-COM 工程宝 App 中，可以在个人中心中获取。

标题项	说明
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。

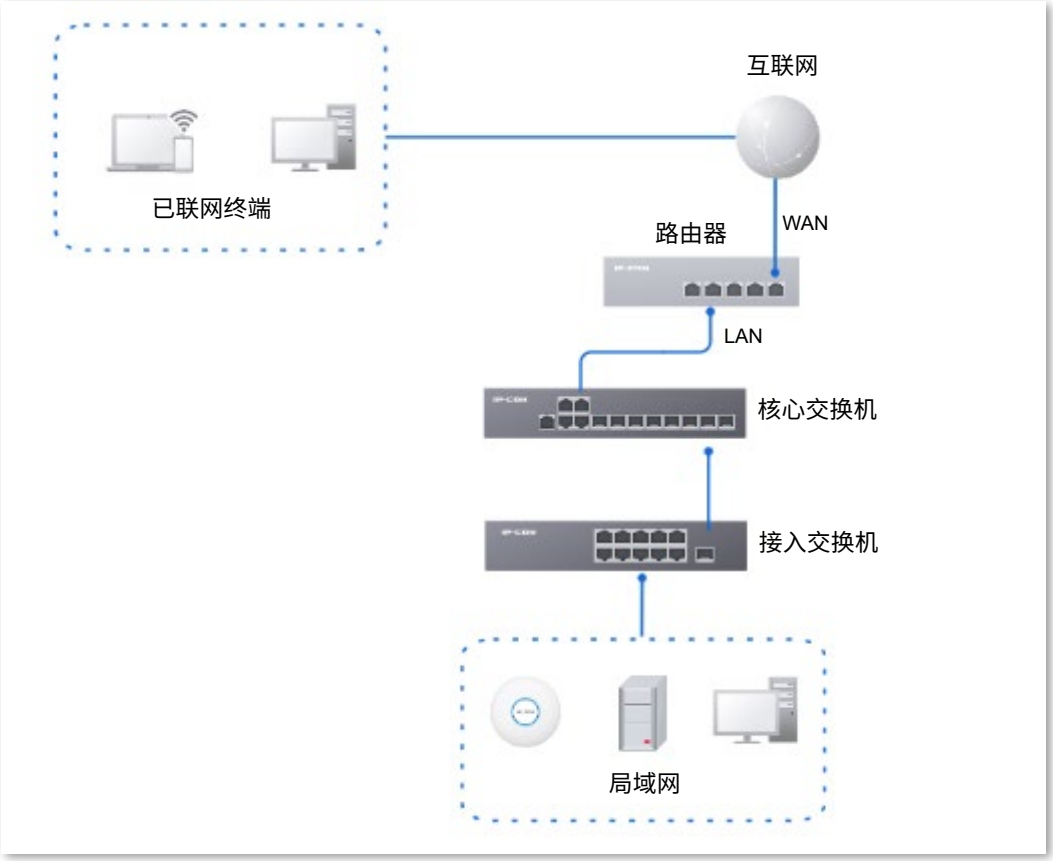
工程宝云管理系统配置举例

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+工程宝云管理系统实现上述需求。



配置步骤

提示

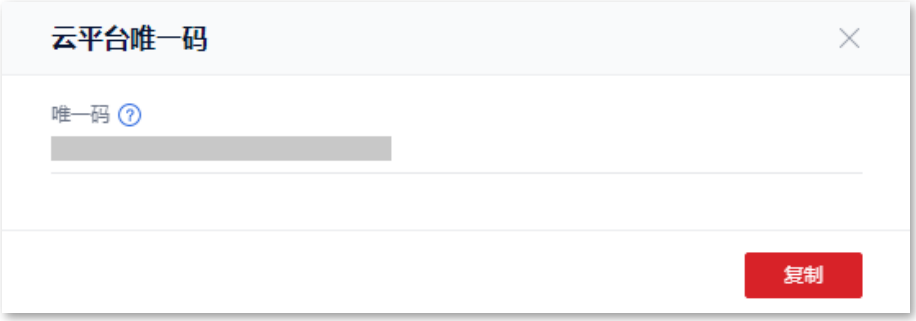
配置路由器的云维护功能之前，请确保路由器已成功联网。

1. 登录工程宝云管理系统，获取云平台唯一码。

1) 在已联网的电脑上，打开浏览器，访问“https://ims.ip-com.com.cn”，登录工程宝云管理系统 Web 管理页面。

2) 点击管理页面右上方的管理账号，选择“云平台唯一码”。

3) 点击 复制 ，复制该工程宝账号的云平台唯一码。



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 。

3. 在工程宝云管理系统上新建项目，并将路由器添加到项目中。

1） 登录工程宝云管理系统 Web 管理页面，点击「项目列表」，点击 新建项目 。

2） 配置项目的相关信息，然后点击 确认 。下图仅供参考。

添加成功。

3） 点击管理页面右上方的管理账号，选择“设备加入提醒”。

4) 选择要加入项目的路由器，点击 添加设备到项目 。

5) 选择要将路由器加入的项目，点击 确认 。下图仅供参考。

----完成

加入成功，进入该项目的管理页面即可查看。

验证配置

路由器可以通过工程宝云管理系统进行管理，相关配置信息可由云平台下发。

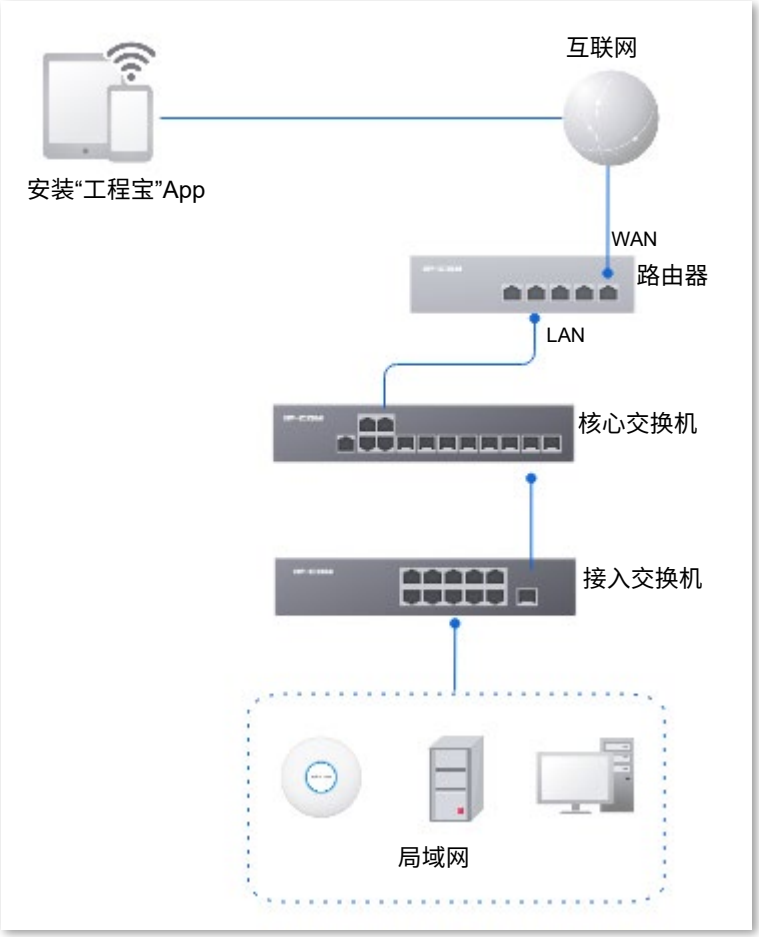
工程宝 App 配置举例

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+工程宝 App 实现上述需求。



配置步骤（方法 1）

提示

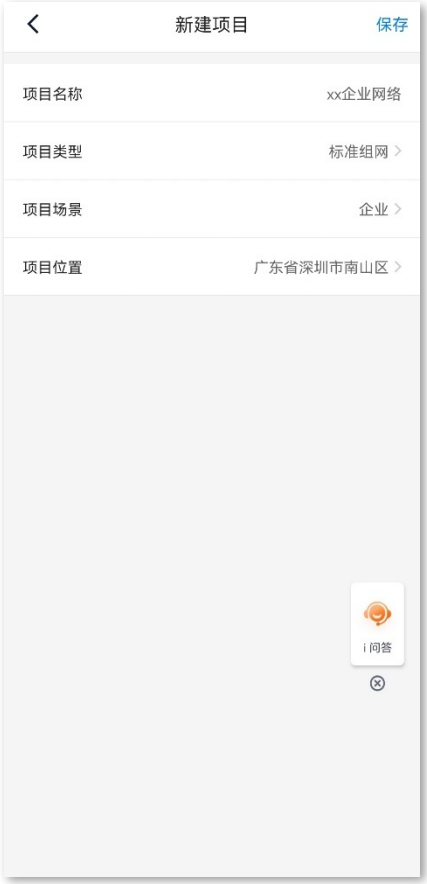
配置路由器的云维护功能之前，请确保路由器已成功联网。

下文以版本为 v1.4.5 的“工程宝”App 为例，具体以相应 App 版本实际操作与界面显示为准。

1. 在工程宝 App 上新建项目。

   1) 登录“工程宝”App，进入「项目」页面，点击⊕。根据实际情况选择添加项目的方式，下图仅供参考。

2） 配置项目的相关信息，然后点击保存。下图仅供参考。

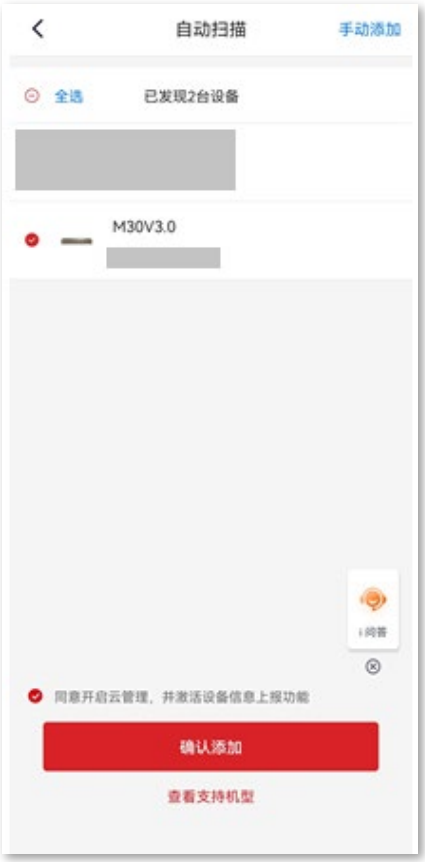


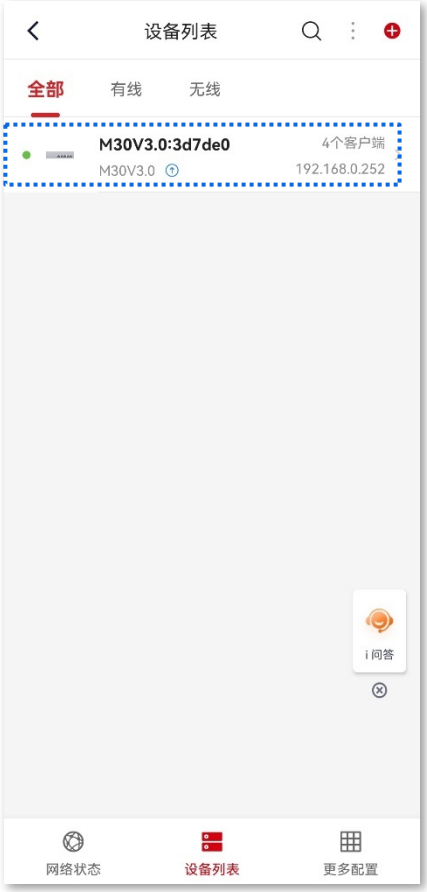
2. 将路由器添加到项目中。

1） 手机连接到路由器所在网络的 WiFi。进入工程宝 APP 中项目的管理页面。下图仅供参考。

2） 点击⊕，点击 我连接好了 。

3) 待自动扫描到路由器后，选择路由器，并勾选“同意开启云管理，并激活设备信息上报功能”，点击 确认添加 。稍等片刻，添加成功。





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。
- 下文以版本为 v1.4.5 的“工程宝”App 为例，具体以相应 App 版本实际操作与界面显示为准。

1. 登录 IP-COM“工程宝”App，获取云平台唯一码。

1) 扫描以下二维码，或者在手机的安卓应用市场或 App Store 中搜索“工程宝”App 并下载安装到您的手机上。

扫码下载“工程宝”App　　工程宝

2) 登录“工程宝”App，在「我的」页面点击“云平台唯一码”。

3) 点击 复制 ，复制该工程宝账号的云平台唯一码。

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」。

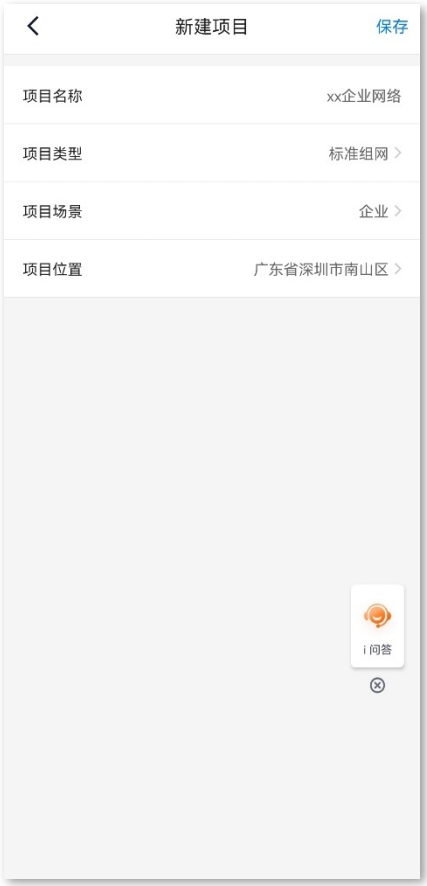
   2) 开启云维护功能。

   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 。

3. 在工程宝 App 上新建项目。

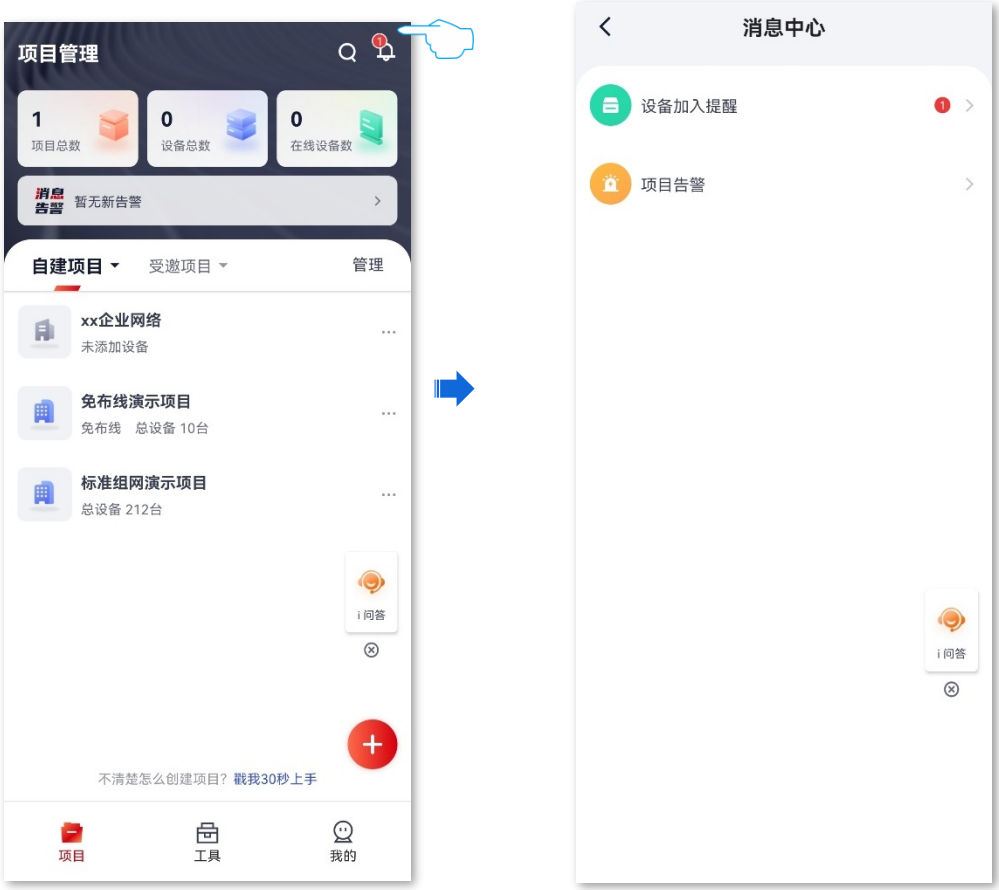
   1) 登录“工程宝”App，进入「项目」页面，点击⊕。根据实际情况选择添加项目的方式，下图仅供参考。

2） 配置项目的相关信息，然后点击保存。下图仅供参考。

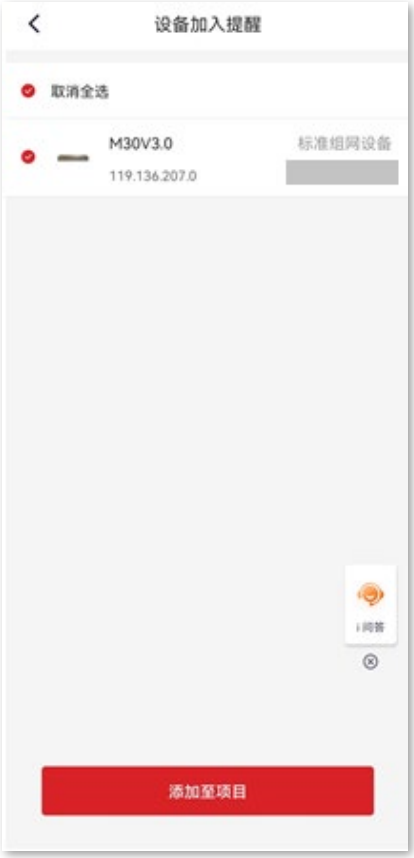


4. 将路由器添加到项目中。

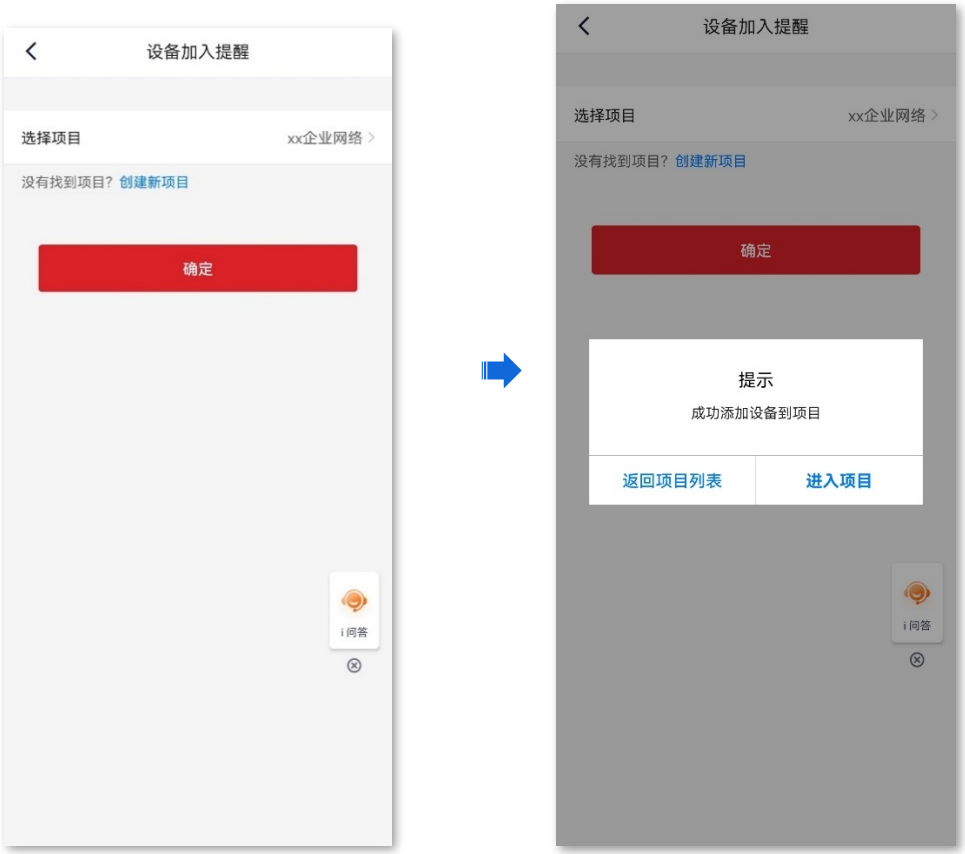
1） 进入“工程宝”App 的「项目」页面，点击右上方的消息图标 > 设备接入提醒。



2） 选择要加入项目的路由器，点击 添加至项目 。



3） 选择要将路由器加入的项目，点击 确定 。添加成功，您可以根据实际情况“返回项目列表”或“进入项目”。下图仅供参考。



----完成

验证配置

路由器可以通过“工程宝”App 进行管理，相关配置信息可由云平台下发。

10.3.5 远程调试

概述

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

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「维护服务」>「远程调试」。

在这里，您可以配置远程调试功能。远程调试功能默认关闭，下图仅供参考。

参数说明

标题项	说明
远程调试	开启/关闭远程调试功能。
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。
远程调试地址	远程 SSH 连接本设备的地址。
状态	本设备与服务器之间的连接状态。

通过 SSH 终端工具远程接入路由器

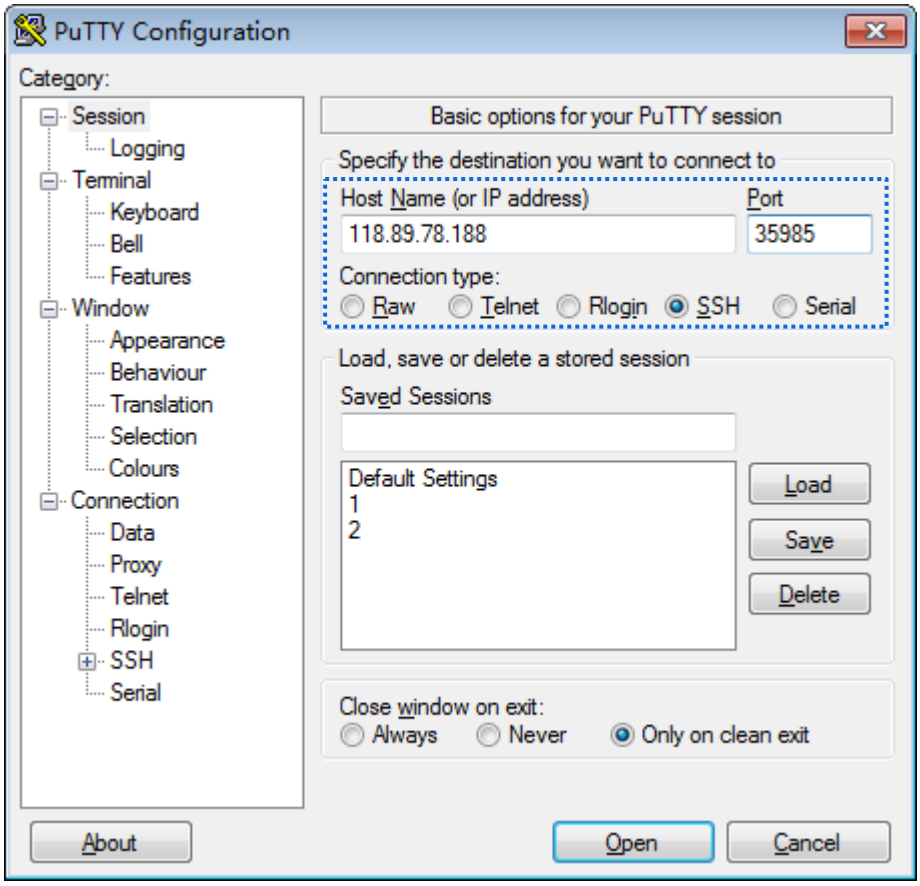
开启路由器远程调试功能

1. 登录到路由器 Web 管理页面。
2. 点击「更多」>「维护服务」>「远程调试」。
3. 开启远程调试功能，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“远程调试地址”远程接入路由器了。

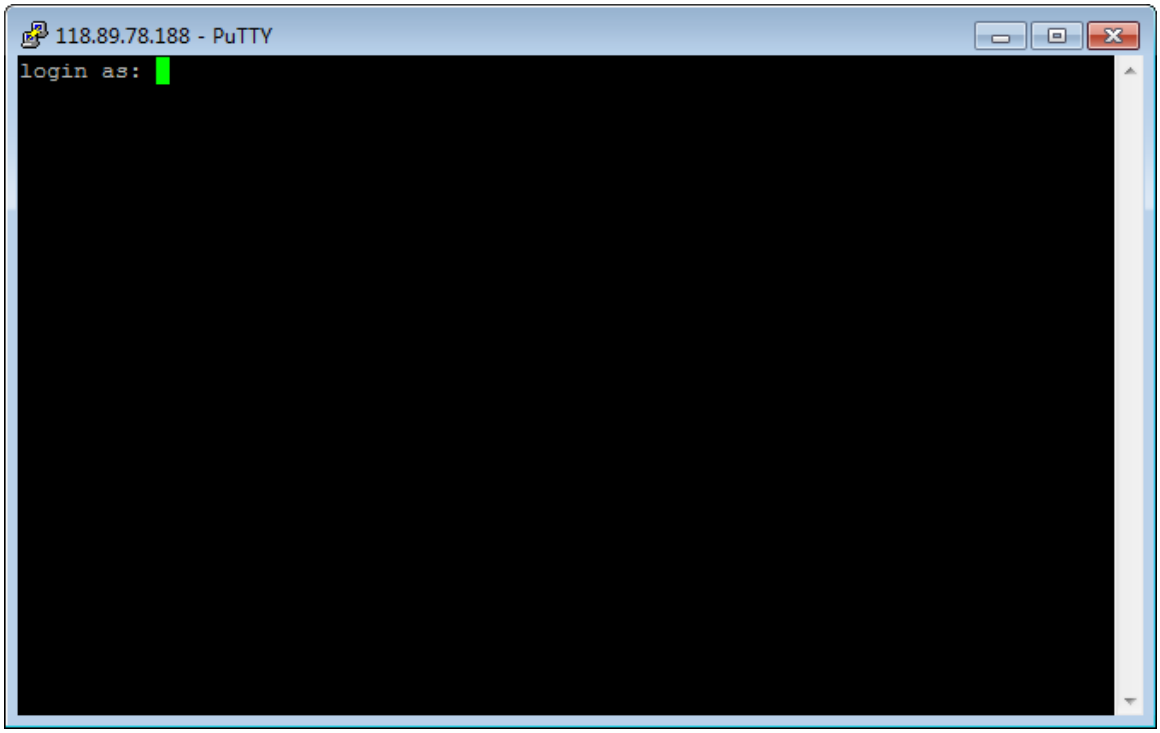
通过 SSH 终端工具远程接入路由器

1. 在远端已联网的电脑上运行 SSH 终端工具，下文以 Putty 为例。
2. 选择“Connection type”为“SSH”。
3. 输入要接入的路由器远程调试地址（Host Name or IP adress）及端口，下图仅供参考。
4. 点击 Open 。


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
118.89.78.188
35985
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
1
2
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

----完成

成功连接到路由器。


118.89.78.188 - PuTTY
login as:

10.4 IPv6

10.4.1 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。

10.4.2 外网

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「IPv6」>「外网」。

在这里，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+SLAA	自动配置
上级设备为网络运营商设备，且运营商提供支持 IPv6 业务的宽带账号和宽带密码	
上级设备为网络运营商设备，且运营商未提供具体上网参数	
上级设备不分配 IP 地址	手动设定
上级设备为网络运营商设备，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	

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，请先与您的网络运营商联系。
- 联网方式为其他特殊 ISP 接入的 WAN 口不支持 IPv6 功能。

自动配置

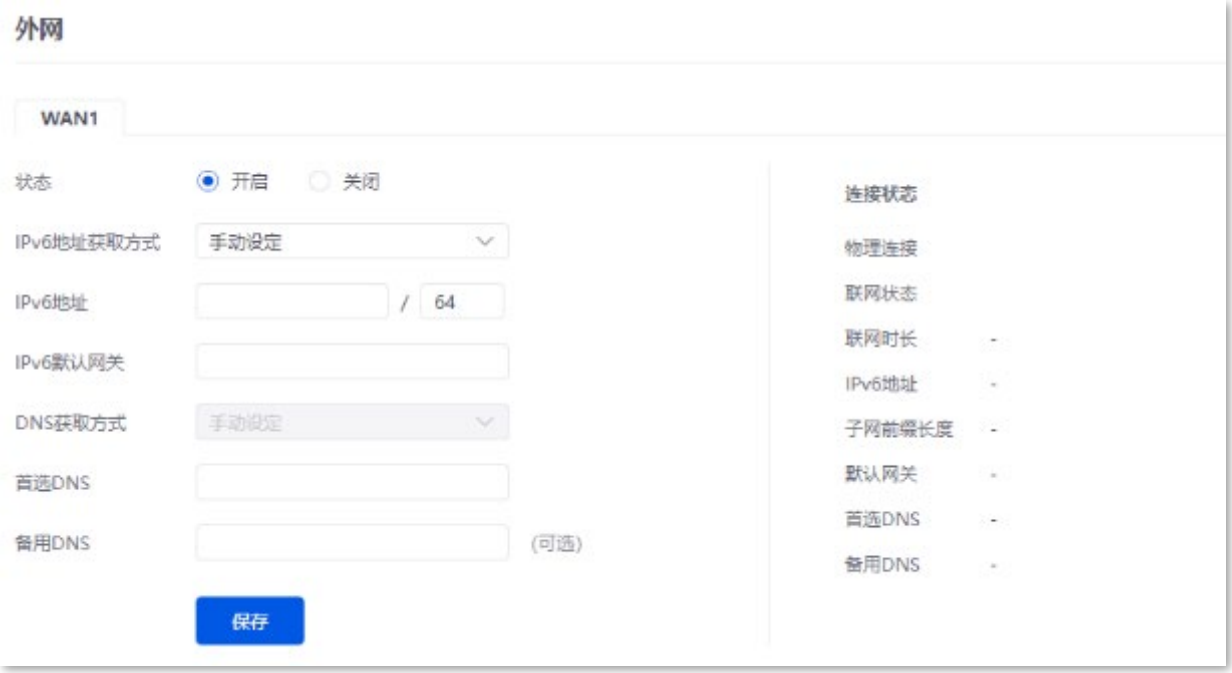
自动配置，即 WAN 口通过 DHCPv6 或 SLAAC 方式自动获取 IPv6 地址上网信息。WAN 口 IPv6 参数配置完成后，您可以在右侧“连接状态”模块查看 IPv6 联网状态。下图仅供参考。

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。 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	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网络运营商。
	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，即手动输入网络运营商提供的 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	请输入网络运营商提供的 IPv6 全球单播地址。
	IPv6 默认网关	请输入网络运营商提供的 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网络运营商。
	联网时长	对应 WAN 口最近一次成功接入 IPv6 网络的时长。

标题项		说明
	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	

10.4.3 局域网

进入页面：登录到路由器 Web 管理页面后，点击「更多」>「IPv6」>「局域网」。

在这里，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

标题项	说明
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	

11 系统工具

11.1 系统时间

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「系统时间」。

在这里，您可以设置路由器的系统时间。

为了保证路由器基于时间的功能正常生效，需要确保路由器的系统时间准确。路由器支持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。

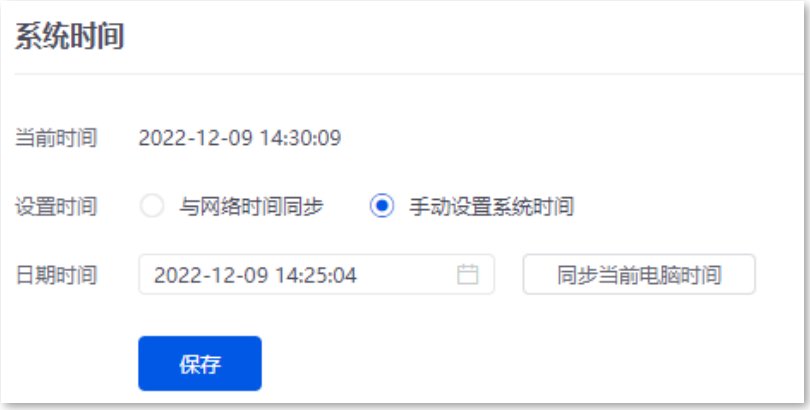
参数说明

标题项	说明
当前时间	路由器当前的系统时间。
设置时间	路由器系统时间的设置方式，选择与网络时间同步。
同步周期	路由器向互联网上的时间服务器校对系统时间的时间间隔。
选择时区	选择路由器当前所在地区的标准时区。

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。



参数说明

标题项	说明
当前时间	路由器当前的系统时间。
设置时间	路由器系统时间的设置方式，选择手动设置系统时间。
日期时间	点击 选择正确的时间，也可以点击 同步当前电脑时间 将正在管理路由器的电脑的时间同步到路由器。

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。

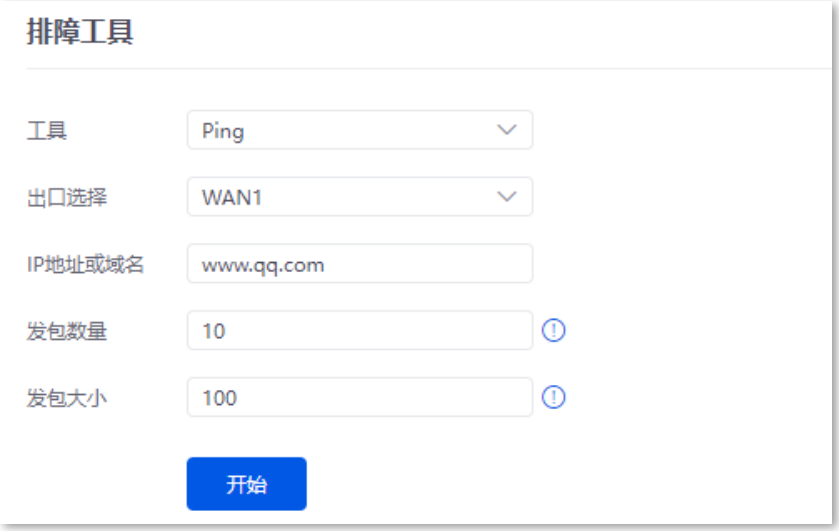
进入页面：登录到路由器 Web 管理页面后，点击「工具」>「排障工具」。

在这里，您可以通过 Ping 工具检测网络连通性和连通质量。

假设要检测路由器到 QQ 官网（www.qq.com）的链路是否畅通。

执行 Ping：

1. 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。
2. 选择“工具”为“Ping”。
3. 选择数据出去的接口，本例为“WAN1”。
4. 输入目的 IP 地址或域名，本例为“www.qq.com”。
5. 设置 ping 发送的数据包的个数，如“10”。
6. 设置 ping 发送的数据包的大小，如“100”。
7. 点击 开始 。



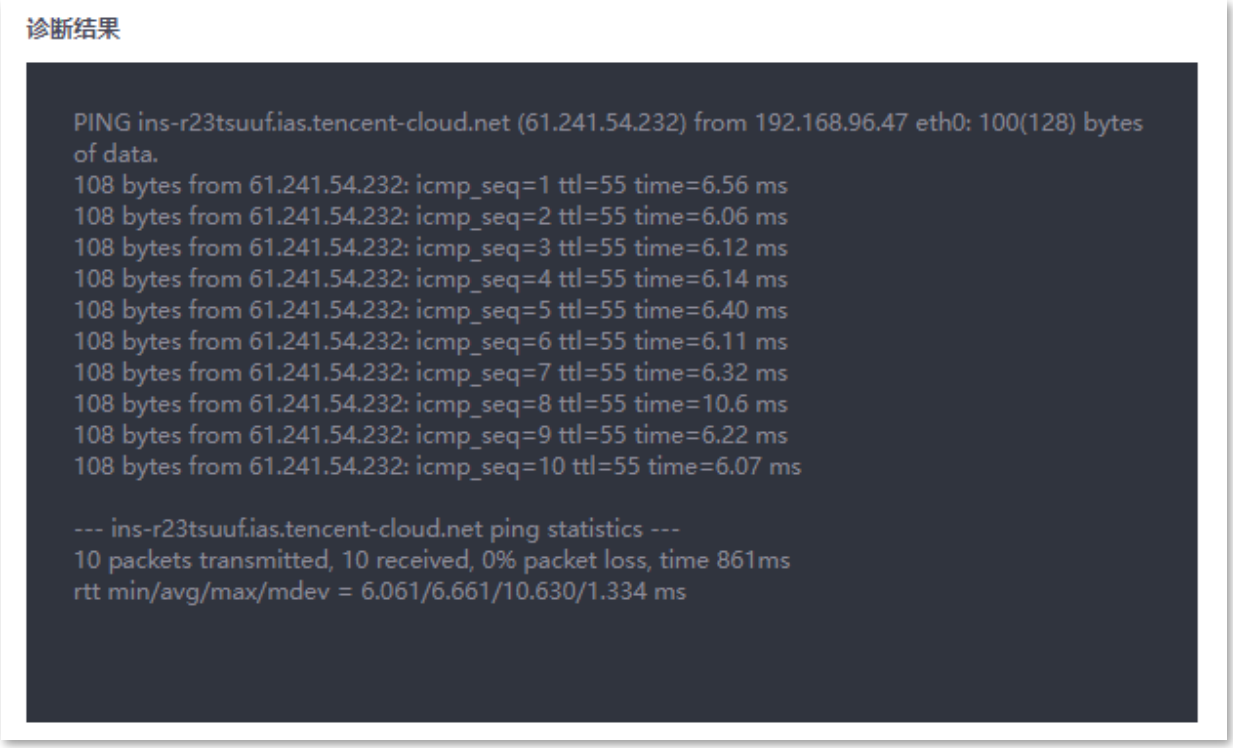
----完成

参数说明

标题项	说明
出口选择	选择数据出去的接口。
IP 地址或域名	要检测的目的 IP 地址或域名。

标题项	说明
发包数量	ping 发送的数据包的个数。
发包大小	ping 发送的数据包的大小。

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。

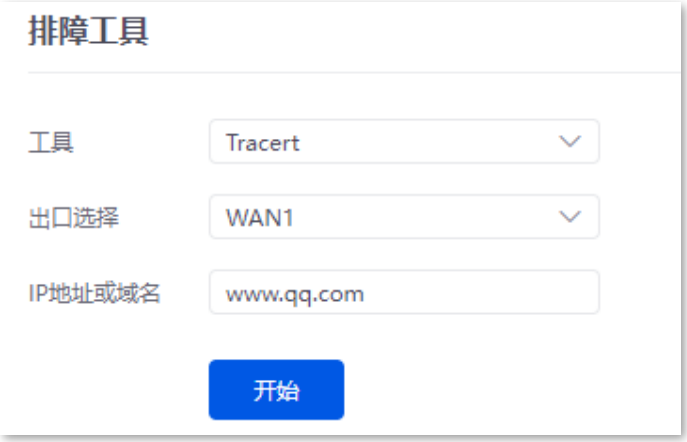
进入页面：登录到路由器 Web 管理页面后，点击「工具」>「排障工具」。

在这里，您可以通过 Tracert 工具检测数据包到达目标地址所经过的路由。

假设要检测路由器到 QQ 官网（www.qq.com）所经过的路由。

执行 Tracert：

1. 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。
2. 选择“工具”为“Tracert”。
3. 选择数据出去的接口，本例为“WAN1”。
4. 输入目的 IP 地址或域名，本例为“www.qq.com”。
5. 点击 开始 。

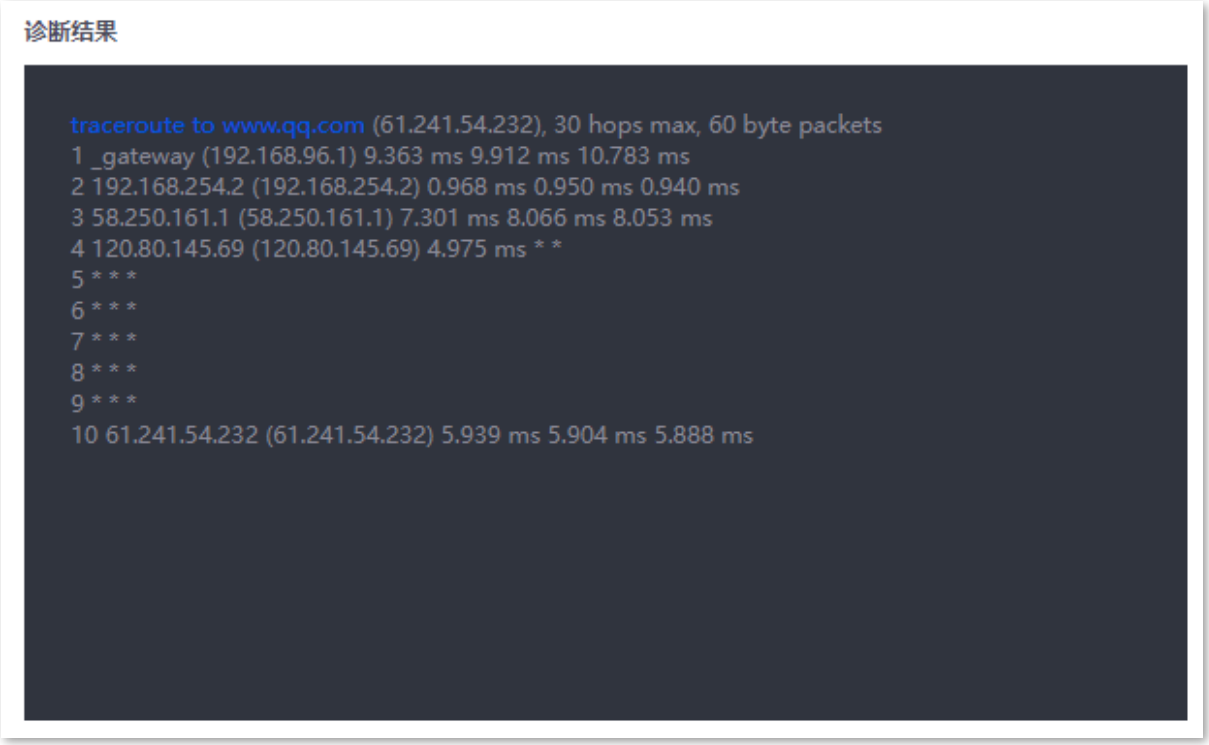


----完成

参数说明

标题项	说明
出口选择	选择数据出去的接口。
IP 地址或域名	要检测的目的 IP 地址或域名。

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提供分析。

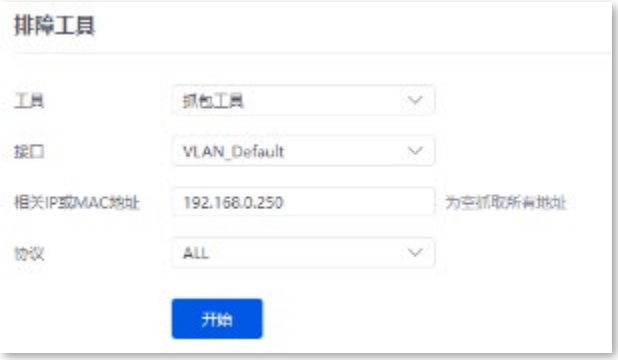
在进入页面：登录到路由器 Web 管理页面后，点击「工具」>「排障工具」。

在这里，您可以通过抓包工具对某一接口特定的数据包进行抓取。

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。

执行抓包：

1. 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。
2. 选择“工具”为“抓包工具”。
3. 选择要截获数据的 VLAN 接口，本例为“VLAN_Default”。
4. 输入 LAN4 口 IP 地址，本例为“192.168.0.250”。
5. 选择数据协议类型，本例为“ALL”。
6. 点击 开始 。



7. 抓包过程中，可根据需要点击 结束 。
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。
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

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「排障工具」。

在这里，您可以执行 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。

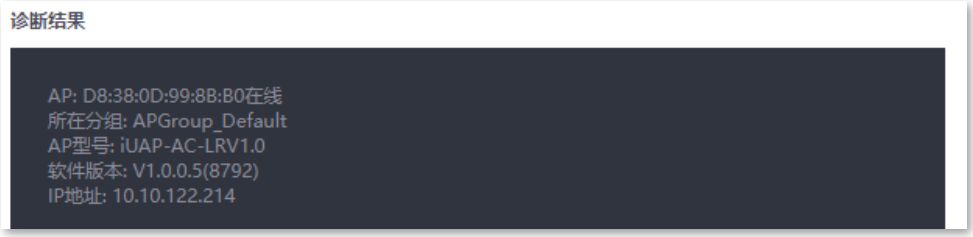
执行 AP 故障诊断：

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。

1. 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。
2. 选择“工具”为“AP 故障诊断”。
3. 输入要诊断的 AP 的 MAC 地址，本例为“D8:38:0D:99:8B:B0”。
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。



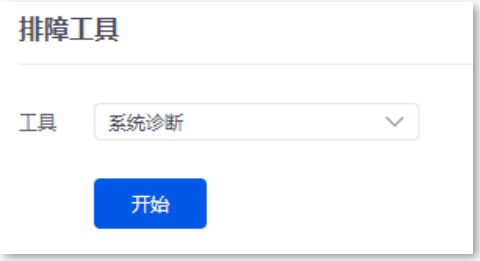
11.2.5 系统诊断

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「排障工具」。

在这里，您可以执行系统诊断，查看系统所有进程的状态信息。

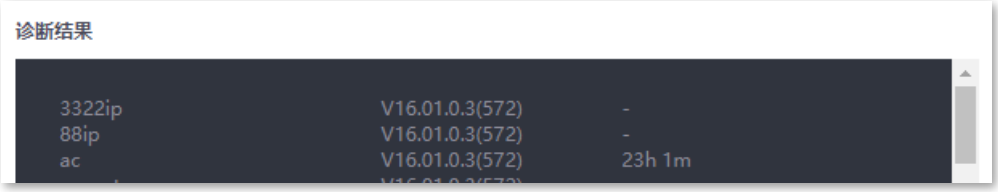
执行系统诊断：

1. 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。
2. 选择“工具”为“系统诊断”。
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

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「排障工具」。

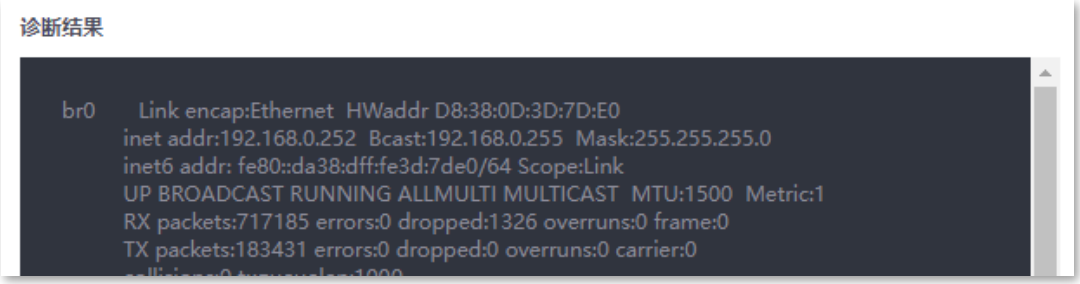
在这里，您可以查看设备接口信息，包括物理接口、桥接口、隧道接口、VLAN 虚拟接口。桥接口和 VLAN 虚拟接口在创建 VLAN 接口时生成，但 VLAN 为 1 时不生成 VLAN 虚拟接口；隧道接口在创建 SSID 策略时生成。

执行步骤：

1. 登录到路由器 Web 管理页面，点击「工具」>「排障工具」。
2. 选择“工具”为“接口信息”。
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

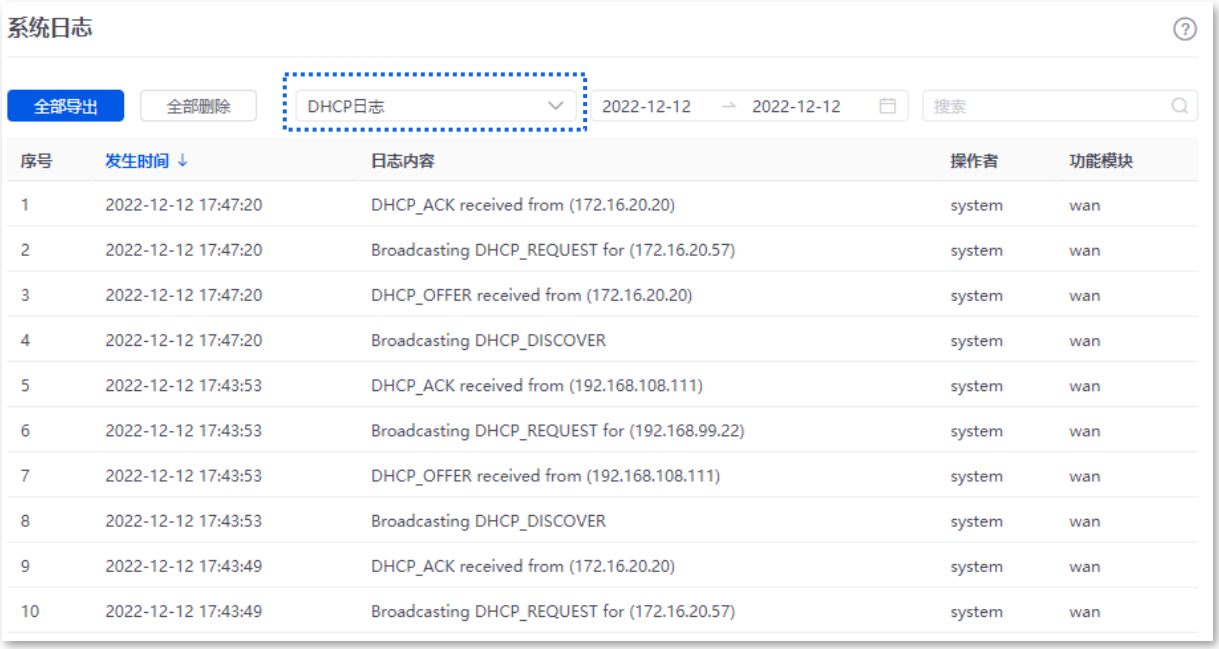
进入页面：登录到路由器 Web 管理页面后，点击「工具」>「日志中心」。

在这里，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。

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。

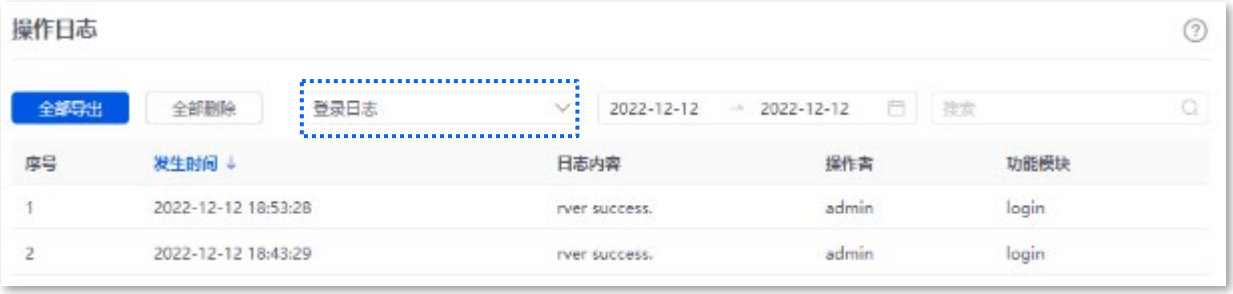


序号	发生时间	日志内容	操作者	功能模块
1	2022-12-12 17:47:20	DHCP_ACK received from (172.16.20.20)	system	wan
2	2022-12-12 17:47:20	Broadcasting DHCP_REQUEST for (172.16.20.57)	system	wan
3	2022-12-12 17:47:20	DHCP_OFFER received from (172.16.20.20)	system	wan
4	2022-12-12 17:47:20	Broadcasting DHCP_DISCOVER	system	wan
5	2022-12-12 17:43:53	DHCP_ACK received from (192.168.108.111)	system	wan
6	2022-12-12 17:43:53	Broadcasting DHCP_REQUEST for (192.168.99.22)	system	wan
7	2022-12-12 17:43:53	DHCP_OFFER received from (192.168.108.111)	system	wan
8	2022-12-12 17:43:53	Broadcasting DHCP_DISCOVER	system	wan
9	2022-12-12 17:43:49	DHCP_ACK received from (172.16.20.20)	system	wan
10	2022-12-12 17:43:49	Broadcasting DHCP_REQUEST for (172.16.20.57)	system	wan

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。

11.3.2 操作日志

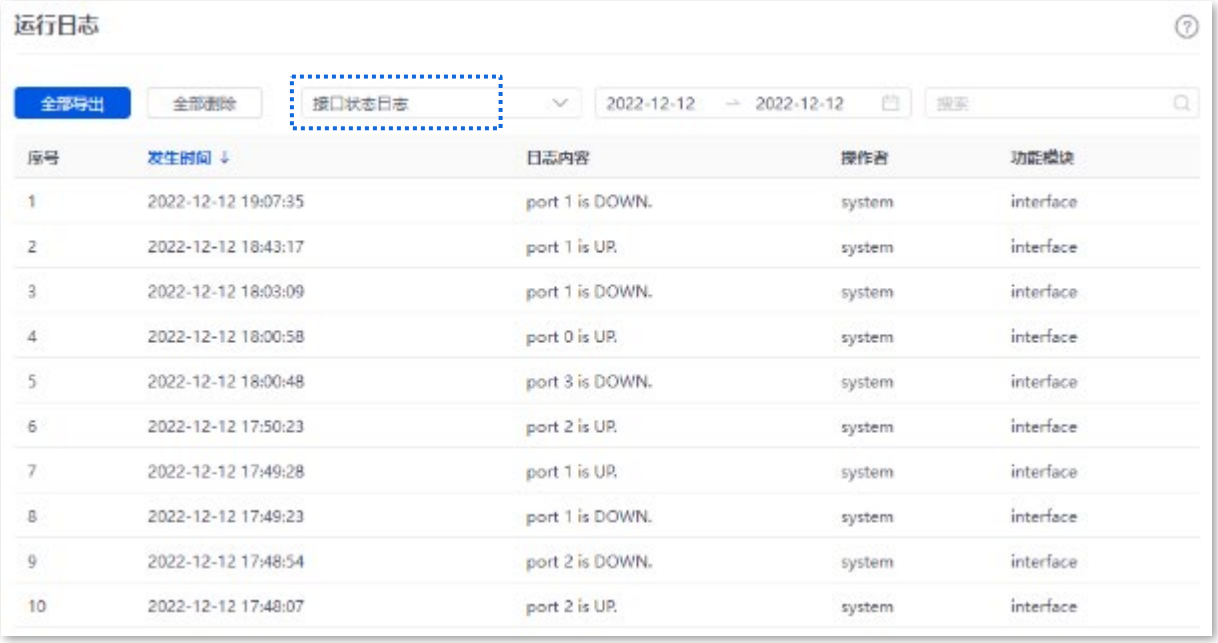
操作日志记录用户对路由器进行的操作，如登录日志、配置变更等。点击下拉框选择相应日志类型即可查看。



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。

11.3.3 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。



序号	发生时间	日志内容	操作者	功能模块
1	2022-12-12 19:07:35	port 1 is DOWN.	system	interface
2	2022-12-12 18:43:17	port 1 is UP.	system	interface
3	2022-12-12 18:03:09	port 1 is DOWN.	system	interface
4	2022-12-12 18:00:58	port 0 is UP.	system	interface
5	2022-12-12 18:00:48	port 3 is DOWN.	system	interface
6	2022-12-12 17:50:23	port 2 is UP.	system	interface
7	2022-12-12 17:49:28	port 1 is UP.	system	interface
8	2022-12-12 17:49:23	port 1 is DOWN.	system	interface
9	2022-12-12 17:48:54	port 2 is DOWN.	system	interface
10	2022-12-12 17:48:07	port 2 is UP.	system	interface

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。

11.4 系统维护

11.4.1 设备信息

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

在这里，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

概述

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。

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「系统维护」>「配置备份与恢复」。

在这里，您可以对路由器进行备份和恢复操作。

备份配置

1. 登录到路由器 Web 管理页面。
2. 点击「工具」>「系统维护」>「配置备份与恢复」。
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

1. 登录到路由器 Web 管理页面。
2. 点击「工具」>「系统维护」>「配置备份与恢复」。
3. 点击 浏览 ，选择并加载之前备份的配置文件。

4. 点击 导入 。

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

概述

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

1. 登录到路由器 Web 管理页面。
2. 点击「工具」>「系统维护」>「恢复出厂设置」。
3. 点击 恢复出厂 。

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 SYS 灯闪烁状态下，用针状物按住机身前面板上的复位按钮（RESET 或 Reset）约 8 秒，待指示灯全亮时松开。当 SYS 灯重新闪烁时，路由器恢复出厂设置成功。

11.5 升级服务

11.5.1 概述

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「升级服务」。

在这里，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”和“在线升级”两种升级方式。默认为“本地升级”。

参数说明

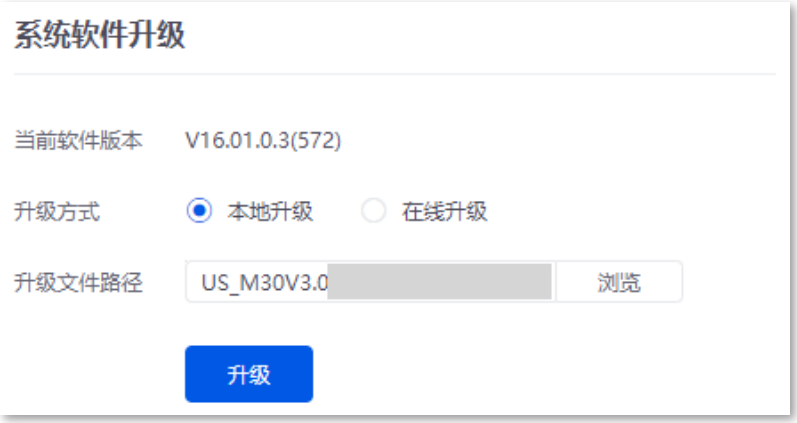
标题项	说明
本地升级	先访问 IP-COM 官方网站 www.ip-com.com.cn，搜索相应产品型号，下载升级文件到本地电脑，然后再进行升级。
在线升级	联网后，路由器系统自动检测是否有新的升级文件，并显示检测结果。如果检测到新的软件版本，您可以根据需要进行升级。升级时，点击 升级 ，系统将自动下载升级文件，并进行升级。

11.5.2 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。

1. 访问 IP-COM 官网 www.ip-com.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。
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」。
3. 选择“升级方式”为“本地升级”。
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 。



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。

提示

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

11.5.3 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。

1. 访问 IP-COM 官网 www.ip-com.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。
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」。
3. 选择“升级方式”为“本地升级”。
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

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「重启服务」>「重启」。

在这里，您可以重启路由器，使某些配置生效，也可以提升运行性能。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：

在「系统工具」>「重启服务」>「重启」页面，点击 重启设备 。

11.6.2 定时重启

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「重启服务」>「定时重启」。

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

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：

1. 登录到路由器 Web 管理页面。
2. 点击「工具」>「重启服务」>「定时重启」。
3. 开启定时重启功能。
4. 选择路由器自动重启的时间点，如“03:00”。
5. 设置重启日期，如“星期四”。
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 系统账号

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「系统账号」。

在这里，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，您可以能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。

11.8 诊断

进入页面：登录到路由器 Web 管理页面后，点击「工具」>「诊断」。

在这里，您可以点击 诊断 对路由器 WAN 口进行联网诊断。

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。
HTTP 访问诊断	检查 WAN 口是否能够正常收到 HTTP 响应。

附录

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）
ARP	地址解析协议（Address Resolution Protocol）
CHAP	询问握手认证协议（Challenge Handshake Authentication Protocol）
DDNS	动态域名服务（Dynamic Domain Name Server）
DDoS	分布式拒绝服务（Distributed Denial of Service）
DES	数据加密标准（Data Encryption Standard）
DHCP	动态主机配置协议（Dynamic Host Configuration Protocol）
DNS	域名系统（Domain Name System）
DPD	失效对等体检测（Dead Peer Detection）
ESP	封装安全载荷（Encapsulating Security Payload）
GRE	通用路由封装（Generic Routing Encapsulation）
HTTP	超文本传送协议（Hyper Text Transfer 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）
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）

缩略语	全称
MPPE	微软点对点加密（Microsoft Point-to-Point Encryption）
MSDU	MAC 服务数据单元（MAC Service Data 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）
PPTP	点对点隧道协议（Point to Point Tunneling Protocol）
SA	安全联盟（Security Association）
SDN	软件定义网络（Software Defined Network）
SMTP	简单邮件传输协议（Simple Mail Transfer Protocol）
SSID	服务集标识符（Service Set Identifier）
SPI	安全参数索引（Security Parameter Index）
TCP	传输控制协议（Transmission Control Protocol）
UDP	用户数据报协议（User Datagram Protocol）
URL	统一资源定位符（Uniform Resource Locator）
UPnP	通用即插即用（Universal Plug and Play）
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（WiFi Multimedia）