
# 网关路由器

## 操作手册

## 关于本产品

本手册描述的产品仅供中国大陆地区销售和使用。本产品只能在购买地所在国家或地区享受售后服务及维保方案。

## 关于本手册

本手册仅作为相关产品的指导说明，可能与实际产品存在差异，请以实物为准。因产品版本升级或其他需要，海康威视可能对本手册进行更新，如您需要最新版手册，请您登录海康威视官网查阅（www.hikvision.com）。

海康威视建议您在专业人员的指导下使用本手册。

## 商标声明

- HIKVISION 海康威视 为海康威视的注册商标。
- 本手册涉及的其他商标由其所有人各自拥有。

## 责任声明

- 在法律允许的最大范围内，本手册以及所描述的产品（包含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵或错误。海康威视不提供任何形式的明示或默示保证，包括但不限于适销性、质量满意度、适合特定目的等保证；亦不对使用本手册或使用海康威视产品导致的任何特殊、附带、偶然或间接的损害进行赔偿，包括但不限于商业利润损失、系统故障、数据或文档丢失产生的损失。
- 您知悉互联网的开放性特点，您将产品接入互联网可能存在网络攻击、黑客攻击、病毒感染等风险，海康威视不对因此造成的产品工作异常、信息泄露等问题承担责任，但海康威视将及时为您提供产品相关技术支持。
- 使用本产品时，请您严格遵循适用的法律法规，避免侵犯第三方权利，包括但不限于公开权、知识产权、数据权利或其他隐私权。您亦不得将本产品用于大规模杀伤性武器、生化武器、核爆炸或任何不安全的核能利用或侵犯人权的用途。
- 如本手册内容与适用的法律相冲突，则以法律规定为准。

# 前　言

本节内容的目的是确保用户通过本手册能够正确使用产品，以避免操作中的危险或财产损失。在使用此产品之前，请认真阅读产品手册并妥善保存以备日后参考。

## 概述

本说明书适用于以下型号的 HIKVISION 网关路由器：DS-3WS05P-E，文中若无特殊说明，产品图片以 DS-3WS05P-E 为例。

## 符号约定

对于文档中出现的符号，说明如下所示。

| 符号 | 说明 |
| --- | --- |
|  说明 | 说明类文字，表示对正文的补充和解释。 |
|  注意 | 注意类文字，表示提醒用户一些重要的操作或者防范潜在的伤害和财产损失危险。 |
|  警告 | 警告类文字，表示有潜在风险，如果不加避免，有可能造成伤害事故、设备损坏或业务中断。 |

## 安全使用注意事项

 警告

- 设备安装使用过程中，必须严格遵守国家和使用地区的各项电气安全规定。
- 在接线、拆装等操作时请一定要将设备电源断开，切勿带电操作。

 注意

- 设备接入互联网可能面临网络安全问题，请您加强个人信息及数据安全的保护。当您发现设备可能存在网络安全隐患时，请及时与我们联系。
- 请您理解，您有责任合理配置所有的密码及其他相关产品安全设置，并妥善保管好您的用户名和密码。

## 文档版本 02 (2022-03-20)

第二次正式发布。

# 目 录

# 第1章 登录 Web 管理界面

## 1.1 登录

如果您是首次使用路由器或已将路由器恢复出厂设置，请参考相关路由器的快速操作指南。否则，请参考下文。

步骤1 用网线将管理电脑接到路由器的任一内网接口（LAN 口）。

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

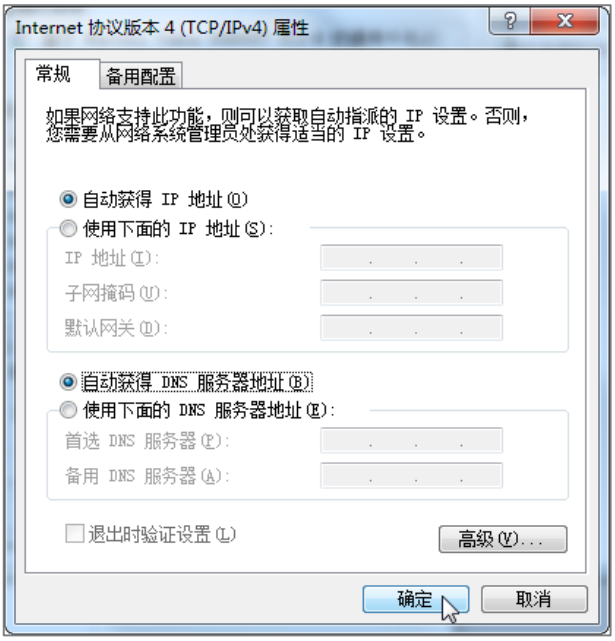


图1-1 本地连接

步骤3 打开电脑上的浏览器，访问路由器的管理地址（默认为“192.168.0.252”），进入路由器的登录页面。


图1-2 浏览器

步骤4 设置登录密码，点击 登录 。


图1-3 登录页面

**说明**

如果忘记登录密码，请将多业务无线控制器恢复出厂设置后，重新尝试。

注意，恢复出厂设置后需要重新多业务无线控制器联网。

恢复出厂设置方法：多业务无线控制器 SYS 灯闪烁状态下，用尖状物按住机身上的复位按钮（Reset）约 8 秒，待指示灯全亮时松开。当 SYS 灯重新闪烁时，多业务无线控制器恢复出厂设置成功。

成功登录路由器管理页面。


图1-4 路由器的管理页面

## 1.2 退出登录

您登录到路由器的管理页面后，如果在 5 分钟内没有任何操作，系统将自动退出登录。此外，在管理页面上，单击右上角的 退出登录 ，也可以安全地退出管理页面。

# 第2章 Web 界面简介

## 2.1 页面布局

路由器的管理页面共分为：一级导航栏、二级导航栏和配置区三部分。如下图所示。


图2-1 路由器的管理页面

表2-1 布局说明

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

## 2.2 管理页面常用按钮

以下是管理页面中常用按钮的功能介绍。

表2-2 常用按钮

| 常用元素 | 说明 |
| --- | --- |
| 确定 | 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。 |
| ? | 位于配置区的右上角。点击可查看对应页面功能的帮助信息。 |
| 退出登录 | 点击此链接可返回到路由器的登录页面。 |

# 第3章 系统状态

在路由器的「系统状态」模块，您可以：

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

## 3.1 查看连线状态及系统状态

进入页面：点击「系统状态」。

在这里，您可以查看路由器的物理连线是否正常，也可以查看路由器系统状态。

### 3.1.1 查看连线状态

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

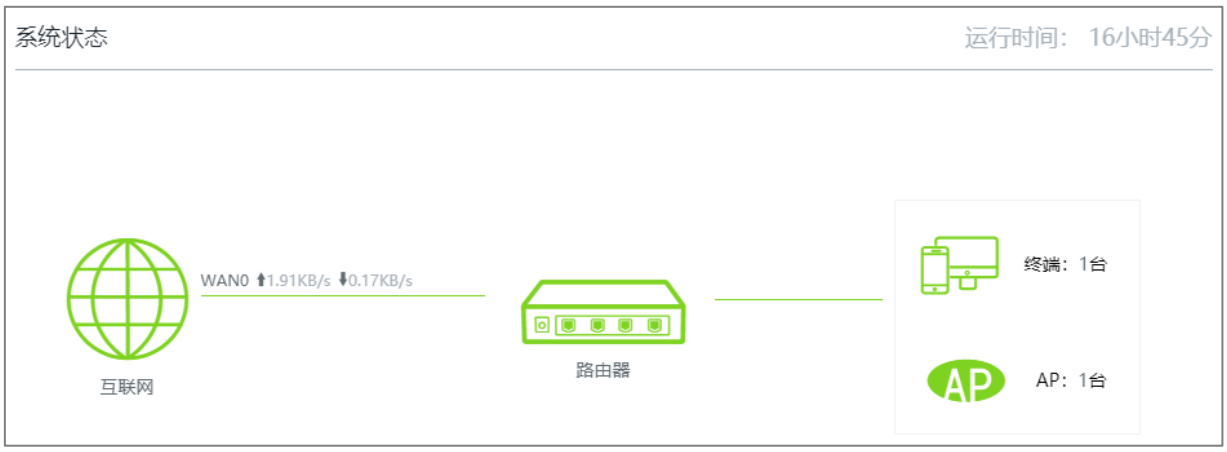


图3-1 已联网时系统状态

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

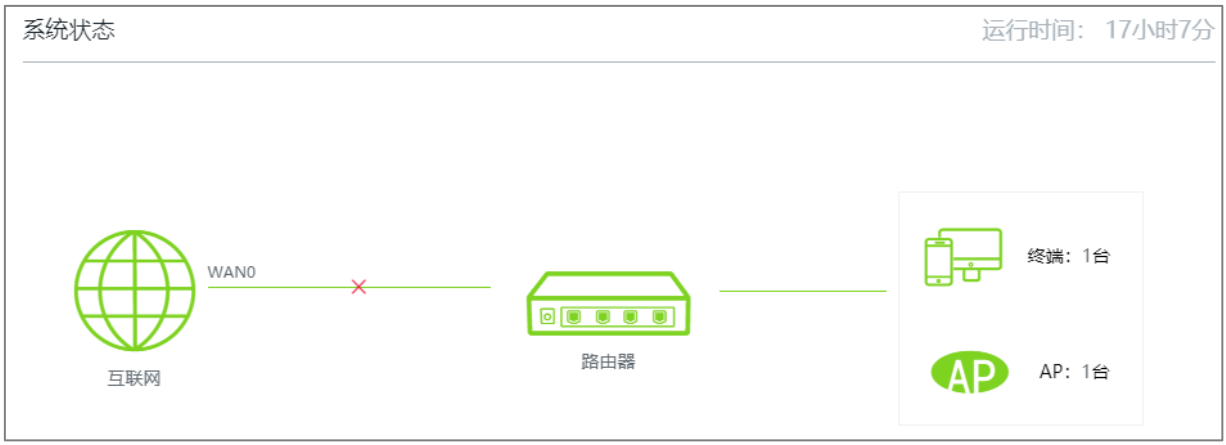


图3-2 未联网时系统状态

### 3.1.2 查看系统状态

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

在“运行状态”模块，您可以查看路由器的系统时间、运行时间、软件版本等信息。

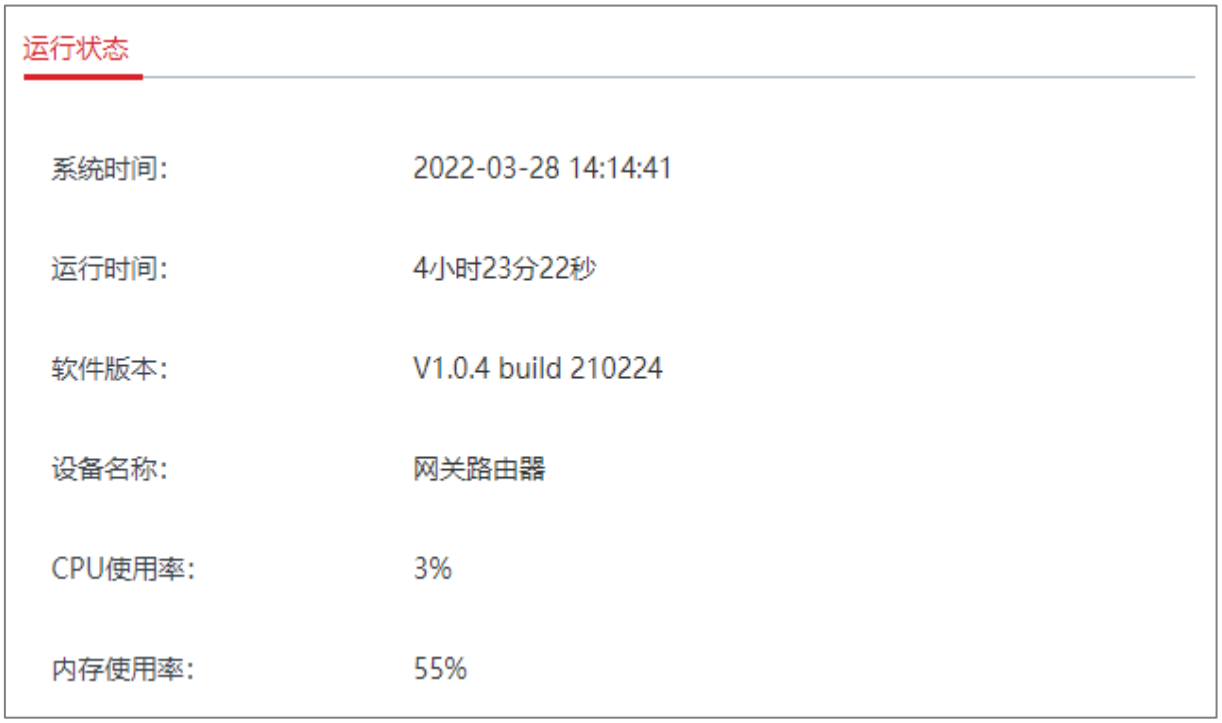


图3-3 运行状态

表3-1 参数说明

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

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

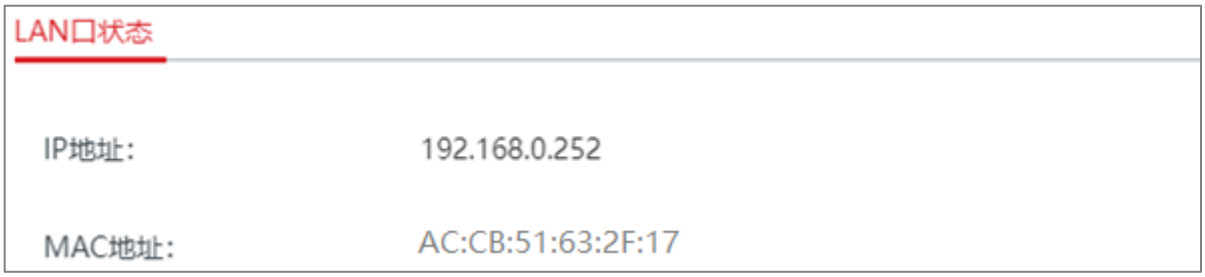


图3-4 LAN 口状态

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


图3-5 WAN 口联网信息

表3-2 参数说明

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

## 3.2 查看流量统计

进入页面：点击「系统状态」，然后点击“更多统计”。

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


图3-6 流量统计

表3-3 参数说明

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

## 3.3 管理在线用户

进入页面：点击「系统状态」。

在这里，您可以查看或管理局域网内网速最高的 5 台终端，也可以点击“终端”进入网速控制与黑名单页面查看或管理所有的在线终端。

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


图3-7 系统状态

## 3.4 添加/移出黑名单

进入页面：点击「系统状态」。

在这里，您可以添加/移出黑名单。

### 3.4.1 添加黑名单

加入黑名单的设备，不能通过路由器上网。

**将网速排在前五的设备加入黑名单：**

步骤1 在“系统状态”页面找到要加入黑名单的设备。

步骤2 点击 禁止上网 。

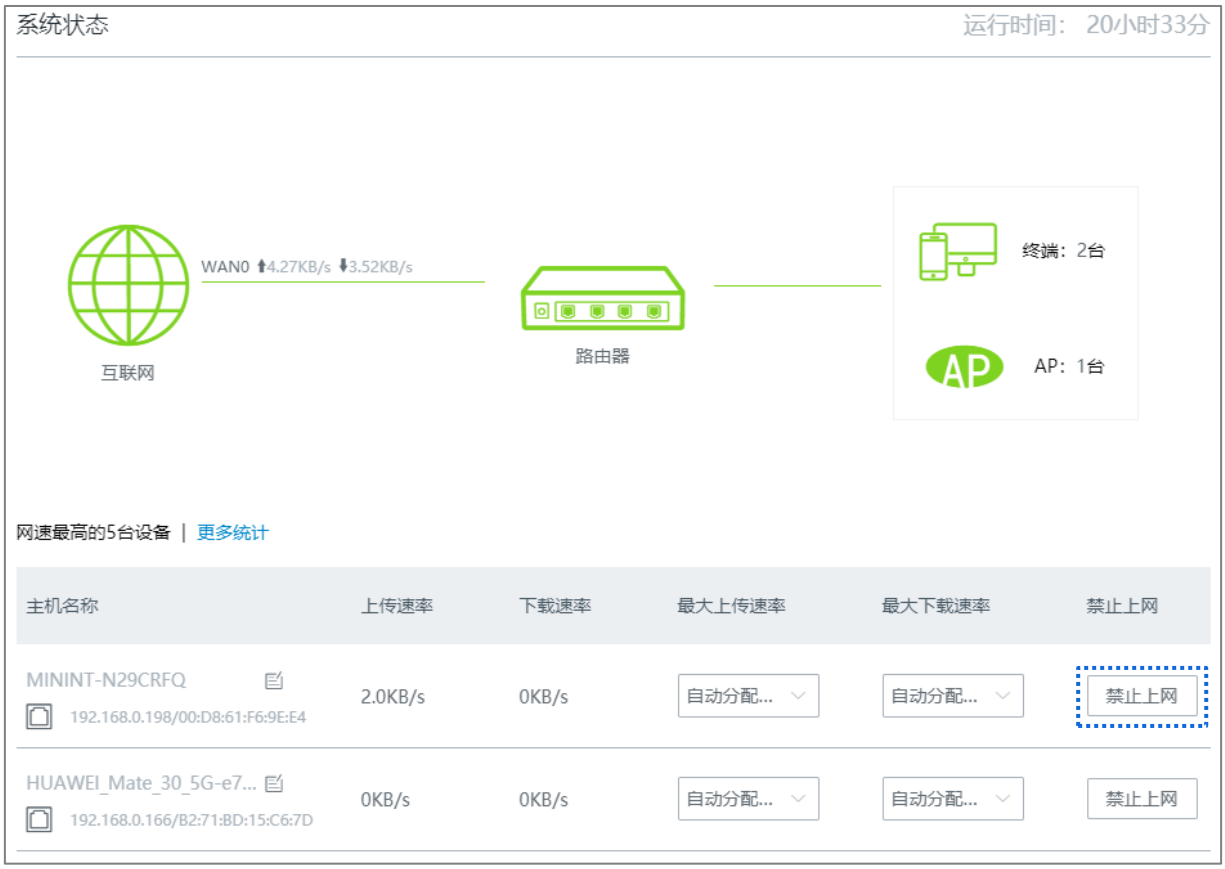


图3-8 禁止网速排前五的设备上网

**将其它在线设备加入黑名单：**

步骤1 在“系统状态”页面点击  ，进入“网速控制与黑名单”页面。

步骤2 在“在线设备”列表中找到要加入黑名单的设备，点击 禁止上网 。


图3-9 在线设备列表

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


图3-10 黑名单列表

## 3.4.2 移出黑名单

如果需要将设备从黑名单中移出，可在“黑名单”页面设置。

步骤1 在“系统状态”页面点击进入“网速控制与黑名单”页面。

步骤2 点击**黑名单**，进入“黑名单”列表。

步骤3 找到要移出黑名单的设备，点击 移出 。


网速控制与黑名单
在线设备
黑名单
刷新
主机名称/MAC
主机名称 (1)
MAC地址
移出黑名单
MININT-N29CRFQ
00:D8:61:F6:9E:E4
移出

图3-11 移除黑名单

## 3.5 管理在线 AP

进入页面：点击「系统状态」。

在这里，您可以查看或管理网络中的在线 AP。

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

**查看或管理网络中的在线 AP：**

步骤1 在“系统状态”页面点击 AP。

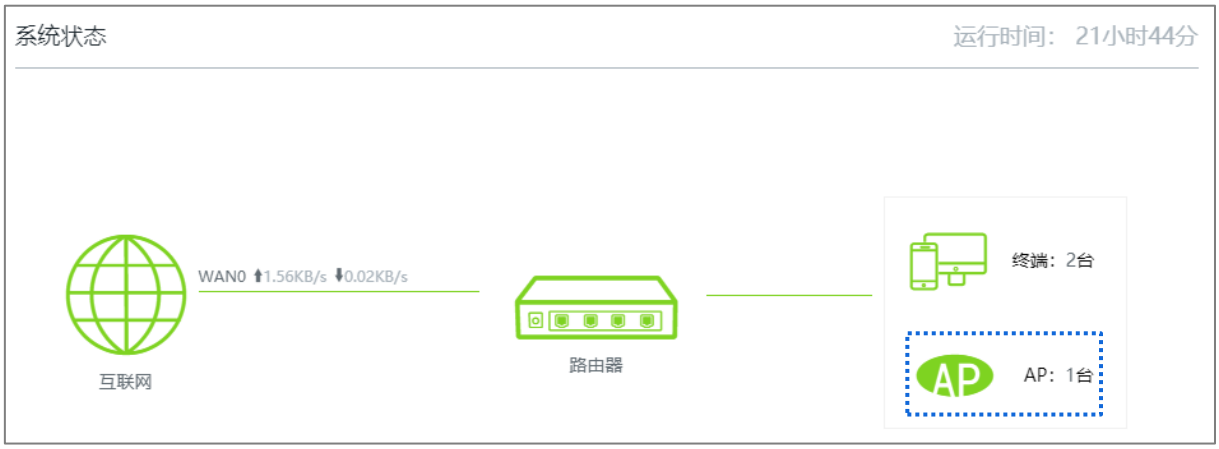


图3-12 系统状态页面

步骤2 根据需要查看或管理在线 AP。


图3-13 管理查看在线 AP

表3-4 界面元素说明

| 标题项 | 说明 |
| --- | --- |
| 跳转到 AP 管理 | 点击可转到路由器的“AP 管理”页面，对 AP 进行管理，详情请参考 AP 管理。 |
|  | 点击可跳转到 AP 的管理页面。例如：AP 的型号为 DS-3WA12T-E，点击  ，即可跳转到 DS-3WA12T-E 的管理页面。 |

# 第4章 联网设置

## 4.1 概述

进入页面：点击「联网设置」。

通过联网设置，可以实现局域网内的多台设备共享您办理的宽带服务上网。

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

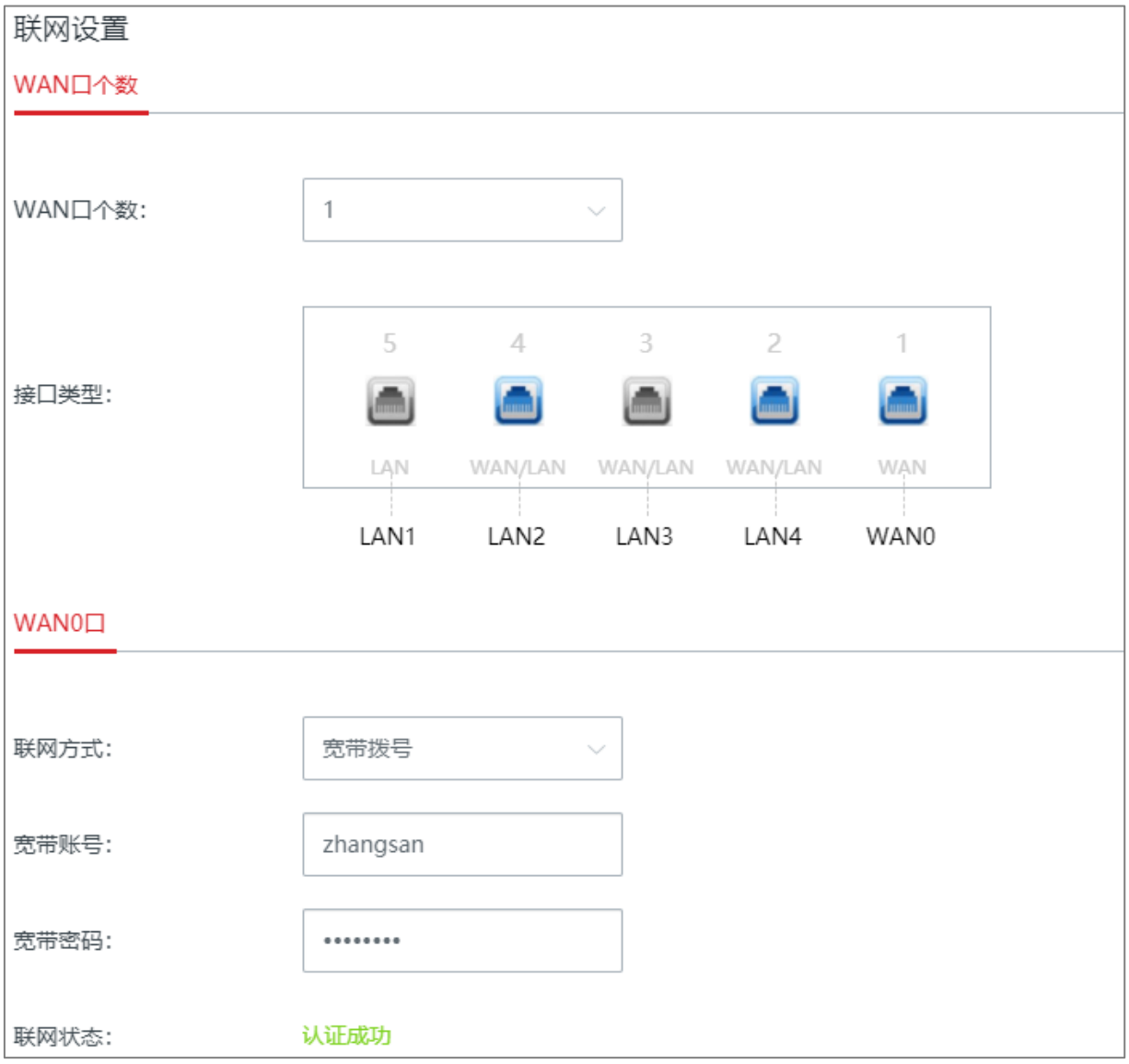


图4-1 联网设置

表4-1 参数说明

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

# 4.2 设置联网

**说明**

- 路由器默认只提供 1 个 WAN 口，即 WAN0。下文以 WAN0 设置为例，其他 WAN 口的设置方法与 WAN0 类似。
- 各上网参数均由 ISP 提供，如不清楚，请咨询您的 ISP。

## 4.2.1 宽带拨号

步骤1 点击「联网设置」。

步骤2 选择“联网方式”为“宽带拨号”。

步骤3 输入 ISP 提供的“宽带账号”和“宽带密码”。

步骤4 点击页面底端的 保存 。

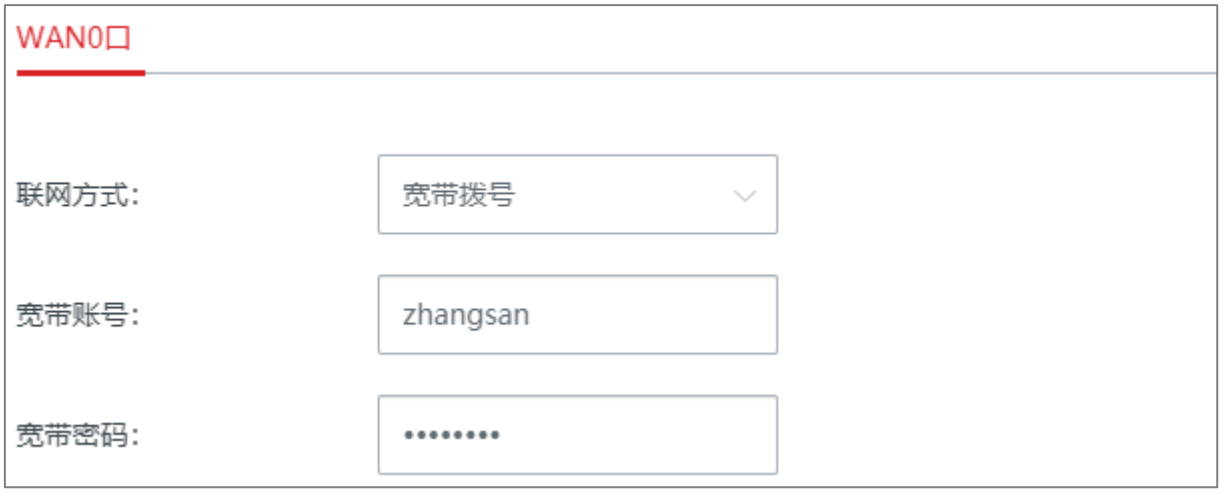


图4-2 设置宽带拨号联网

稍等片刻，当联网状态显示“认证成功”时，您可以尝试上网了。

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


图4-3 宽带拨号联网成功

### 4.2.2 动态 IP

步骤1 点击「联网设置」。

步骤2 选择“联网方式”为“动态 IP”。

步骤3 点击页面底端的 保存 。


图4-4 设置动态 IP 联网

稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。

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

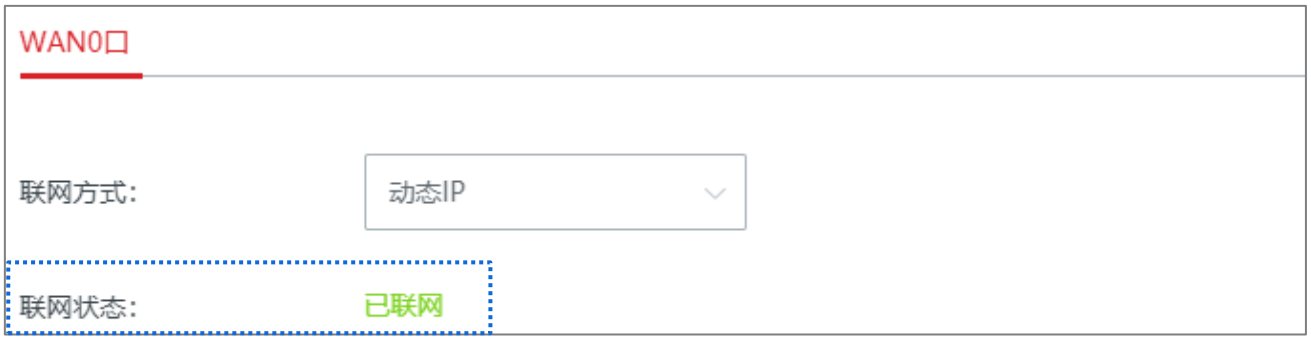


图4-5 动态 IP 联网成功

### 4.2.3 静态 IP

步骤1 点击「联网设置」。

步骤2 选择“联网方式”为“静态 IP”。

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

步骤4 点击页面底端的 保存 。


图4-6 静态 IP 联网设置

稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。

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

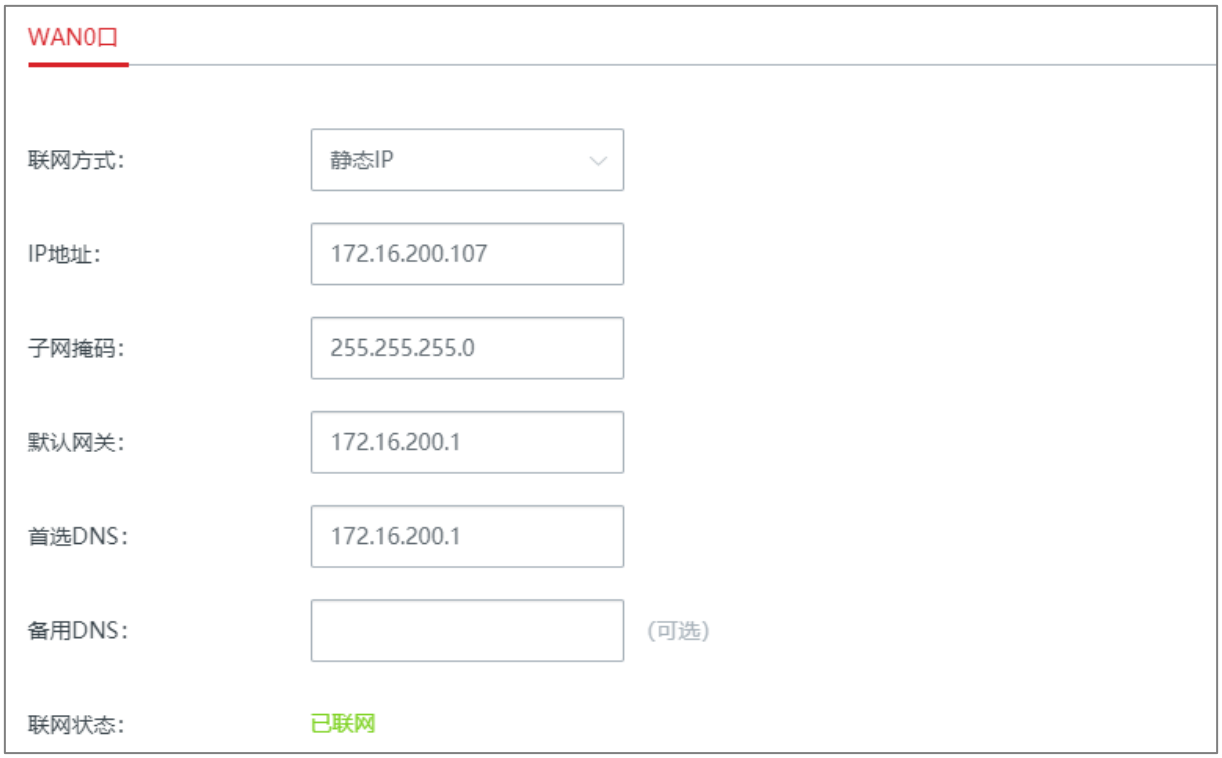


图4-7 静态 IP 联网成功

# 第5章 静态 IP 分配

## 5.1 概述

进入页面：点击「静态 IP 分配」。

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

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

- 基于在线用户快速绑定：可以查看从路由器 DHCP 服务器自动获取 IP 地址的终端设备信息，并一键绑定终端设备，使 DHCP 服务器始终给同一终端设备分配固定的 IP 地址。
- 手动分配 IP 地址：可以手动绑定终端设备，使 DHCP 服务器始终给同一终端设备分配固定的 IP 地址。

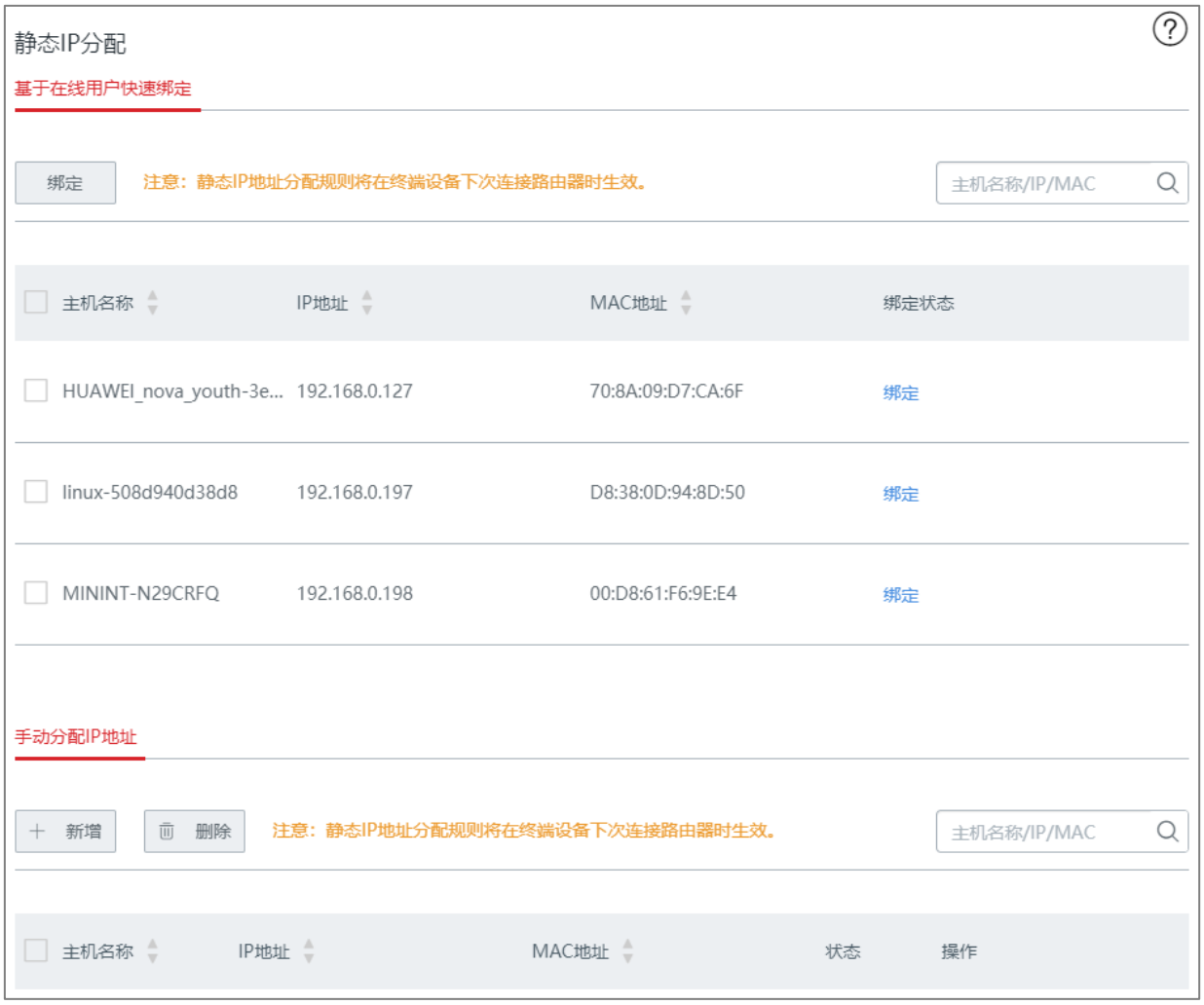


图5-1 静态 IP 分配页面

表5-1 参数说明

| 标题项 | | 说明 |
| --- | --- | --- |
| 基于在线用户快速绑定 | 绑定 | 将选中的终端设备都进行 IP 地址、MAC 地址绑定。 |
| | 主机名称 | 终端设备的名称。 |
| | IP 地址 | 终端设备的 IP 地址。 |
| | MAC 地址 | 终端设备的 MAC 地址。 |
| | 绑定状态 | 点击绑定即可一键绑定终端设备 IP 地址、MAC 地址，使终端设备始终获取同一 IP 地址。绑定成功后将显示“已绑定”。 |
| 手动分配 IP 地址 | 主机名称 | 终端设备的名称或静态 IP 分配规则的备注信息。 |
| | IP 地址 | 为对应 MAC 地址的终端设备预留的 IP 地址。 |
| | MAC 地址 | 终端设备的 MAC 地址。 |
| | 状态 | 开启或禁用该规则。 |
| | 操作 | 可对规则进行如下操作：<br>● 点击可以修改规则。<br>● 点击可以删除规则。 |
| | 导出静态 IP 地址分配表 | 可将静态 IP 地址分配表备份到本地电脑。 |
| | 导入静态 IP 地址分配表 | 可将之前备份的静态 IP 地址分配表文件导入到路由器。 |

## 5.2 为终端设备分配固定 IP 地址

如果要给已连接到路由器的终端设备分配 IP 地址，推荐在“基于在线用户快速绑定”模块进行设置。终端设备未连接到路由器时，请在“手动分配 IP 地址”模块进行设置。

### 5.2.1 基于在线用户快速绑定

- 绑定单个在线终端设备的 IP 地址

步骤1 点击「静态 IP 分配」，找到“基于在线用户快速绑定”模块。

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


图5-2 静态 IP 分配

- 同时绑定多个在线终端设备的 IP 地址

步骤1 点击「静态 IP 分配」，找到“基于在线用户快速绑定”模块。

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

步骤3 点击 绑定 。

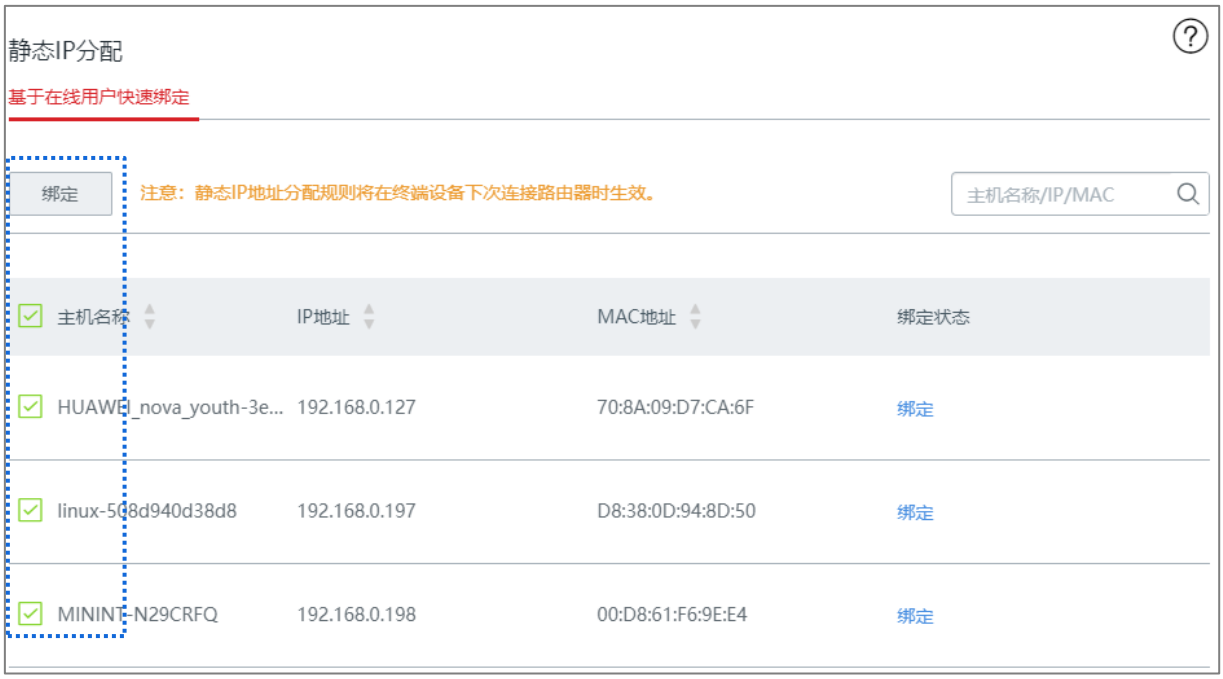


图5-3 同时分配多个终端设备静态 IP

绑定成功后，您可以在「静态 IP 分配」的“手动分配 IP 地址”页面查看到已添加的规则。如下图示例。规则将在终端设备下一次连接路由器时生效。


图5-4 成功分配静态 IP

## 5.2.2 手动分配 IP 地址

**设置步骤：**

步骤1 点击「静态 IP 分配」，找到“手动分配 IP 地址”模块。

步骤2 点击 +新增 。


图5-5 手动添加静态 IP 分配规则

步骤3 在【新增】窗口配置各项参数，然后点击 保存 。

**说明**

点击 + 可以新增一条规则；点击 − 可以删除未保存的规则。


图5-6 新增静态 IP 分配规则

规则添加成功后，您可以在「静态 IP 分配」的“手动分配 IP 地址”页面查看到已添加的规则。如下图示例。规则将在终端设备下一次连接路由器时生效。


手动分配IP地址
新增
删除
注意：静态IP地址分配规则将在终端设备下次连接路由器时生效。
主机名称/IP/MAC
主机名称
IP地址
MAC地址
状态
操作
未知
192.168.0.100
6C:4D:73:D5:75:A6

图5-7 添加规则成功

# 第6章 网速控制

## 6.1 概述

进入页面：点击「网速控制」。

在“网速控制”页面，您可以设置各 WAN 口的最大上传/下载速度，添加网速控制规则，实现对数据传输的带宽控制，从而使有限的带宽资源得到合理分配，达到有效利用现有带宽的目的。


图6-1 网速控制页面

表6-1 参数说明

| 标题项 | | 说明 |
| --- | --- | --- |
| WAN 口带宽 | 上传速率 | 需填入所办理的宽带的带宽值。不清楚时，可以咨询您的ISP。 |
| | 下载速率 | |
| 限速方式 | 不限速 | 不对局域网用户的上传/下载速率进行限制。 |
| | 自定义限速 | 为连接到路由器的单台或多台局域网终端设备设置最大上传/下载速率。<br>相较于分组限速来说，设置更加灵活。 |
| | 自动分配网速 | 系统根据「网速控制」页面设置的 WAN 口上传/下载速率，平均地给局域网终端设备分配带宽。 |
| | 分组限速 | 通过分组设置网速控制规则。<br>控制指定 IP 组内的用户在指定时间组内共享或独享所设置的上传/下载速率，并设置单台设备并发连接数等。 |

## 6.2 自定义限速

假设要为连接到路由器的终端设备单独设置最大上传/下载速率。

步骤1 点击「网速控制」。

步骤2 选择“限速方式”为“自定义限速”。

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

步骤4 设置对应设备的最大上传/下载速率。

步骤5 点击页面底端的 保存 。


图6-2 自定义限速

表6-2 参数说明

| 标题项 | 说明 |
| --- | --- |
| 主机名称 | 终端设备名称，可根据需要修改。 |
| 下载总流量 | 该用户下载数据的总量。 |
| 离线时间 | 该用户的离线时间。 |
| 上传速率 | 该用户当前的上传/下载速率。 |
| 下载速率 | |
| 最大上传速率 | 限定该用户使用的最大上传/下载速率。 |
| 最大下载速率 | |

## 假设要为局域网所有在线用户或离线用户统一设置最大上传/下载速率

步骤1 点击「网速控制」。

步骤2 选择“限速方式”为“自定义限速”。

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

步骤4 点击 全部限速 。


图6-3 统一设置局域网网速控制

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


图6-4 统一网速限制标准

## 6.3 自动分配网速

为连接到路由器的在线用户平均分配网速。

**设置步骤：**

步骤1 点击「网速控制」。

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

步骤3 选择“限速方式”为“自动分配网速”。

步骤4 点击页面底端的 保存 。


图6-5 自动分配网速

## 6.4 分组限速

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

**说明**

配置分组限速规则前，请先配置好相应的 IP 组和时间组。

步骤1 点击「网速控制」。

步骤2 选择“限速方式”为“分组限速”。

步骤3 点击 +新增 。


图6-6 新增分组限速规则

步骤4 在【新增】窗口配置各项参数，然后点击 保存 。

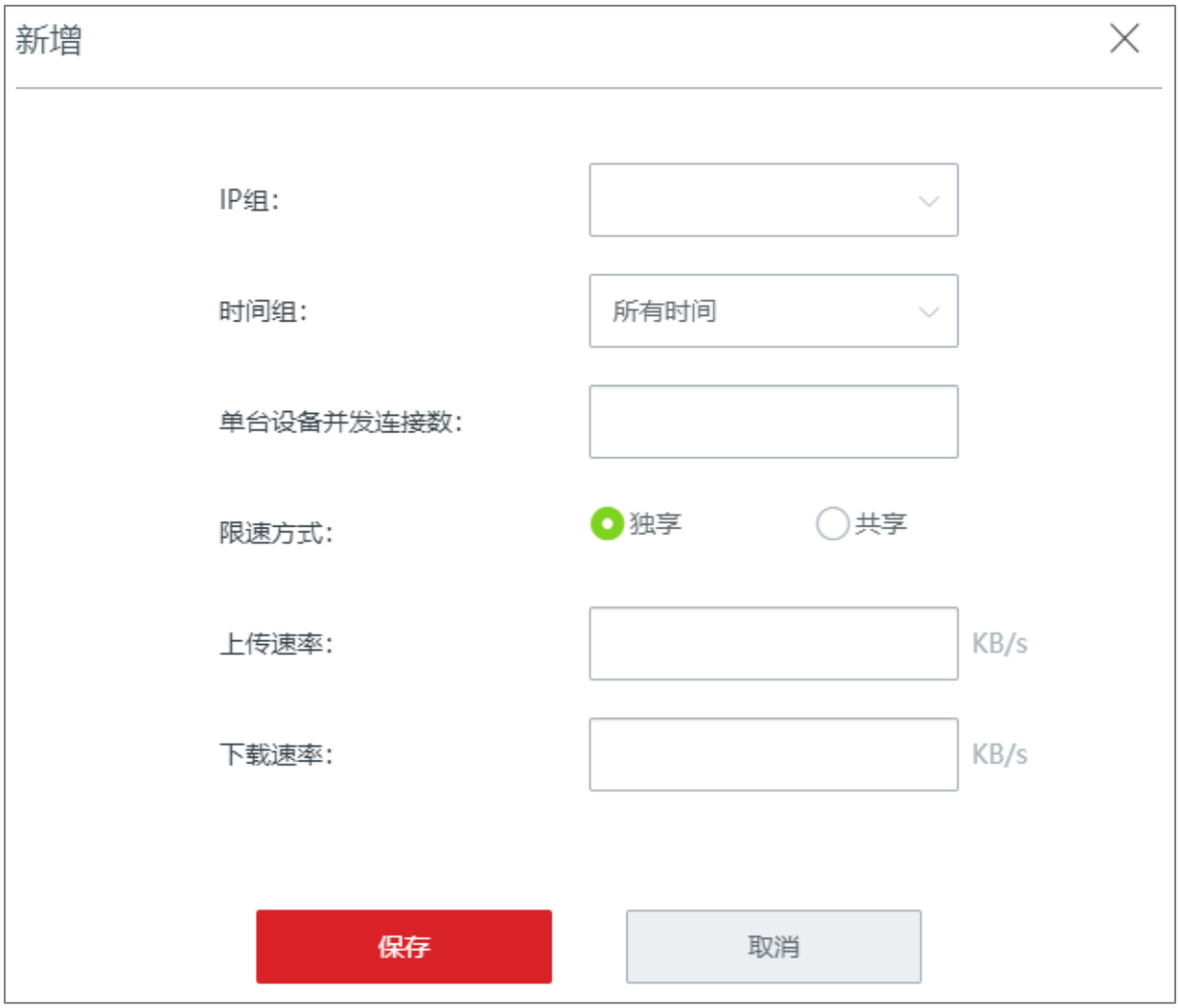


图6-7 设置分组限速规则

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


图6-8 规则添加成功

表6-3 参数说明

| 标题项 | 说明 |
| --- | --- |
| IP 组 | 规则引用的 IP 组，以指定规则对应的用户。IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 时间组 | 规则引用的时间组，以指定规则的生效时间。时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 并发连接数（单台设备并发连接数） | 受控 IP 地址范围中，每台终端设备所能使用的最大连接数。若无特殊需求，建议设置为 600。 |
| 限速模式（限速方式） | 设置网速控制的模式。<br>● 独享：受控 IP 地址范围内每一台端设备都应用当前规则设置的上传/下载速率。此模式下，每台终端设备所获得的带宽都是一样的。<br>● 共享：受控 IP 地址范围内所有终端设备带宽总和为当前规则设置的上传/下载速率。此模式下，每台终端设备所获得的带宽可能不一样。 |
| 上传速率 | 限制的上传/下载速率。 |
| 下载速率 | |
| 状态 | 启用/禁用规则。 |
| 操作 | 可对规则进行如下操作：<br>● 点击可以修改规则。<br>● 点击可以删除规则。 |

# 6.5 分组限速举例

## 组网需求

某企业使用企业级路由器进行网络搭建。

要求：局域网中采购部（IP 地址为 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。

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

## 配置步骤

步骤1 配置时间组。

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。


图6-9 添加时间组

步骤2 配置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。


图6-10 新增 IP 组

步骤3 开启分组限速功能。

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


图6-11 选择分组限速

步骤4 添加分组限速规则。

1. 进入“网速控制”页面，点击 +新增 。


图6-12 新增分组限速规则

2. 在【新增】窗口进行如下配置，然后点击 保存 。

- 点击下拉框，选择规则应用的 IP 组，本例为“采购部”。
- 点击下拉框，选择规则应用的时间组，本例为“上班时间”。
- 设置单台设备并发连接数，本例为“600”。
- 选择限速方式，本例为“独享”。
- 设置终端设备的最大上传速率和下载速率，本例均为“128KB/s”。


图6-13 设置分组限速规则

## 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。

# 第7章 AP 管理

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

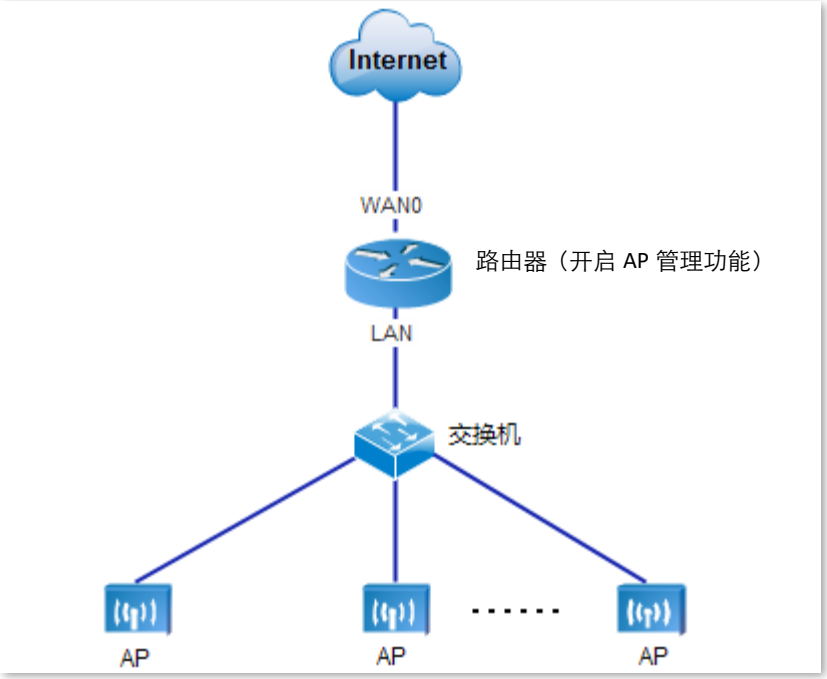


图7-1 AP 管理网络应用拓扑图

## 7.2 基本配置

### 7.2.1 概述

进入页面：点击「AP 管理」>「基本配置」。

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

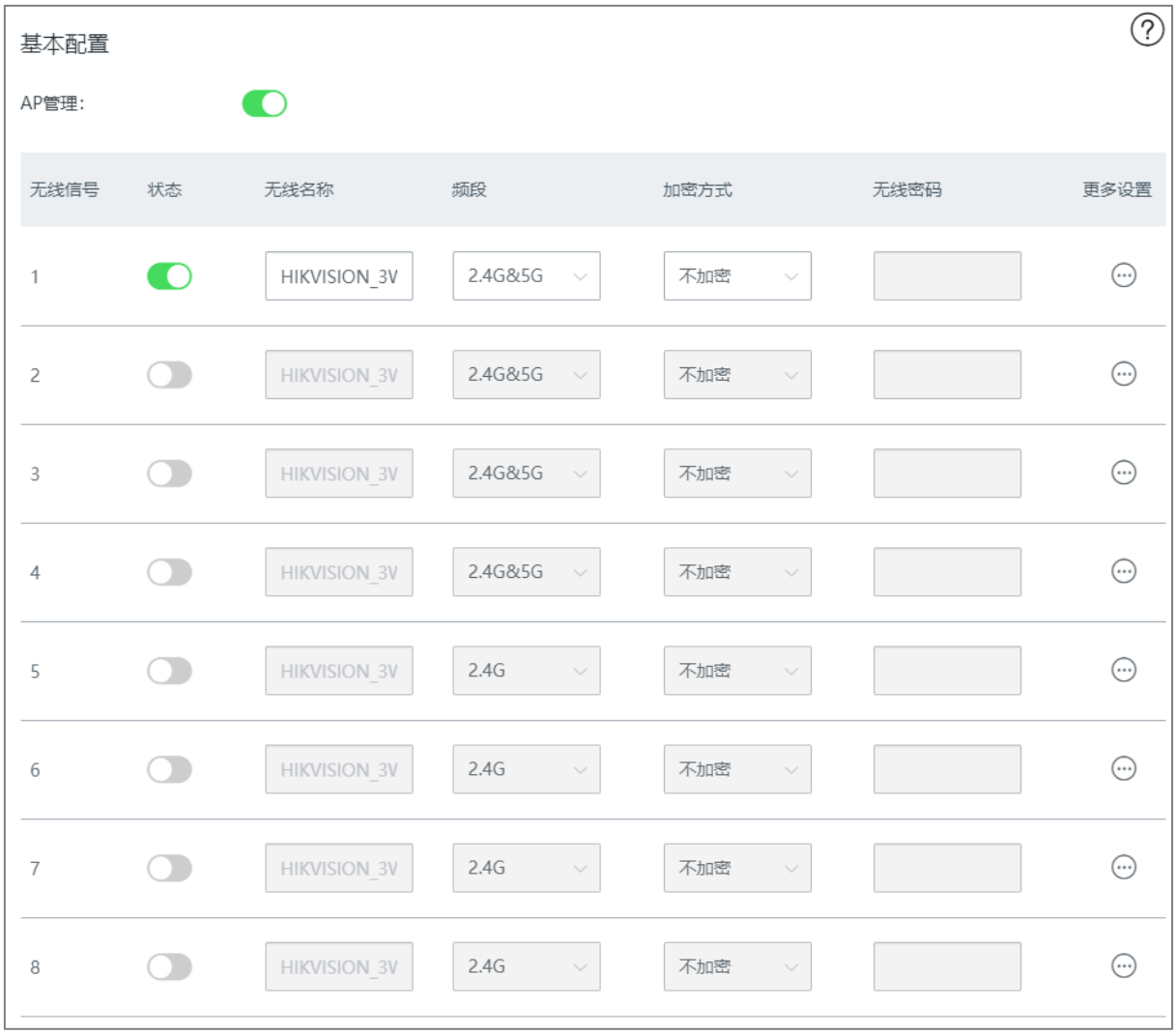


图7-2 AP 管理基本配置

表7-1 参数说明

| 标题项 | 说明 |
| --- | --- |
| 无线信号 | 无线策略的序号。<br>● 1~4：用于修改 AP 2.4GHz 或 5GHz 频段的第 1~4 个 SSID（无线信号）的相关参数。<br>● 5~8：用于修改 AP 2.4GHz 频段的第 5~8 个 SSID 的相关参数。 |
| 状态 | 无线策略的状态，也是 AP 对应 SSID 的启用/禁用状态。默认启用第一条无线策略，禁用其他无线策略。 |
| 无线名称 | 无线网络名称，可根据需要自定义。 |
| 频段 | 无线策略的应用频段，即，该无线策略要下发到 AP 的哪个频段。<br>● 2.4G：无线策略下发到 AP 的 2.4GHz 频段。<br>● 5G：无线策略下发到 AP 的 5GHz 频段。<br>● 2.4G&5G：无线策略同时下发到 AP 的 2.4GHz 频段和 5GHz 频段。<br>**说明**<br>**若第 1 条无线策略的频段为单频，如 2.4G（或 5G），则点击 保存 后，AP 将关闭对应 SSID 另一频段如 5G（或 2.4G）的无线功能。** |
| 加密方式 | 无线网络的加密方式。<br>● 不加密：不加密无线网络，用户连接无线网络时，无需输入密码即可接入。为保障网络安全，不建议选择此项。<br>● WPA-PSK：无线网络采用 WPA-PSK 认证方式（AES 加密规则）,此加密方式的兼容性比 WPA2-PSK 好。<br>● WPA2-PSK：无线网络采用 WPA2-PSK 认证方式（AES 加密规则），此加密方式的安全等级比 WPA-PSK 高。 |
| 无线密码 | WPA-PSK 或 WPA2-PSK 的预共享密码，也是用户连接无线网络时需要输入的无线密码。 |
| 更多设置 | 点击…可进行高级参数设置，包括：终端设备隔离、隐藏无线网络、最大用户数、VLAN ID。<br>● 终端设备隔离：启用后，连接到该无线网络下的设备之间不能互相通信，可增强无线网络的安全性。<br>● 隐藏无线网络：启用后，其他无线设备不能扫描到该 SSID。 |

| 标题项 | 说明 |
| --- | --- |
| | ● 最大用户数：无线网络最多允许接入的无线设备数量。默认为 48。<br>● VLAN ID：SSID 对应的 VLAN ID。默认均为“1000”。 |

## 7.2.1 下发无线策略到 AP

**注意**

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

步骤1 点击「AP 管理」>「基本配置」。

步骤2 修改无线网络参数。

步骤3 点击页面底端的 保存 。


图7-3 修改分配给 AP 的无线策略

稍等片刻，局域网中 AP 的相关无线设置会变为与无线策略一致。

# 7.3 AP 配置

## 7.3.1 概述

进入页面：点击「AP 管理」>「AP 配置」。

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

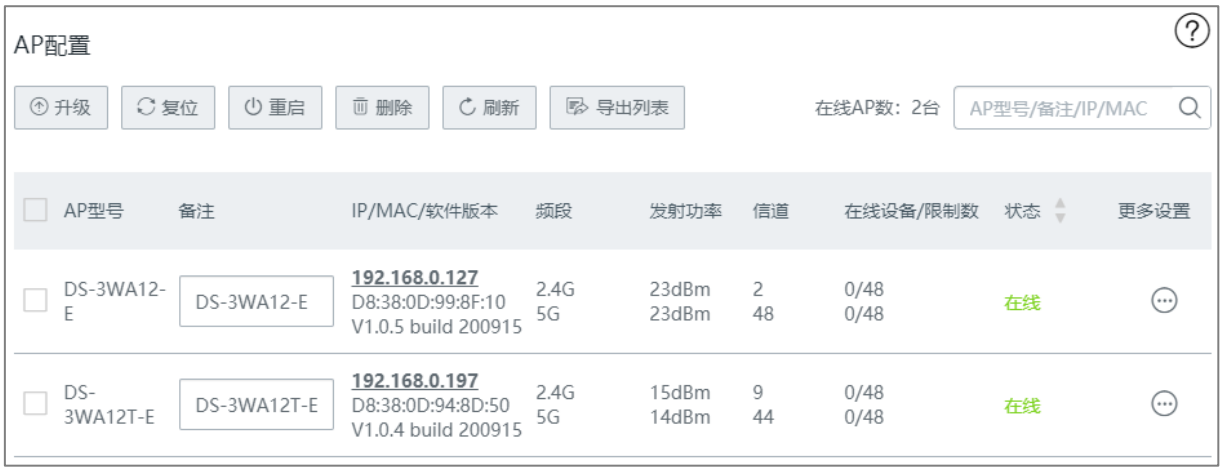


图7-4 AP 配置

表7-2 参数说明

| 标题项 | 说明 |
| --- | --- |
| AP 型号 | AP 的型号。 |
| 备注 | AP 的备注信息，可根据需要自定义。 |
| IP/MAC/ 软 件版本 | AP 的 IP 地址、MAC 地址和对应的软件版本。<br>说明<br>点击 IP 地址可以跳转至 AP 管理页面。 |
| 频段 | 无线策略的应用频段，即，该无线策略要下发到 AP 的哪个频段。<br>● 2.4G：无线策略下发到 AP 的 2.4GHz 频段。<br>● 5G：无线策略下发到 AP 的 5GHz 频段。<br>● 2.4G&5G：无线策略同时下发到 AP 的 2.4GHz 频段和 5GHz 频段。<br>说明<br>若第 1 条无线策略的频段为单频，如 2.4G（或 5G），则点击 保存 后，AP 将关闭对应 SSID 另一频段如 5G（或 2.4G）的无线功能。 |
| 发射功率 | AP 的发射功率。<br>若 AP 不支持设置的功率，则配置下发后，以 AP 支持的最大范围为准生效。即，当功率超过 AP 的上限功率时，只使用 AP 的最大功率；当功率小于 AP 的下限功率时，只使用 AP 的最小功率 |
| 信道 | AP 的无线工作信道。 |
| 在线设备/限制数 | 已连接到 AP 的在线设备数和限制连接到 AP 的最多终端设备数。 |
| 状态 | AP 的状态。 |
| 更多设置 | 点击⋯可进行高级参数设置，详情请参考高级设置。 |

## 7.3.2 升级

使用升级功能，可以升级 AP 的软件版本。

**注意**

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

**设置步骤：**

步骤1 下载对应型号的 AP 软件到本地电脑并解压。

步骤2 登录路由器管理页面，点击「AP 管理」>「AP 配置」。

步骤3 选择需要进行软件升级的 AP。

步骤4 点击 升级 ，之后按页面提示操作。

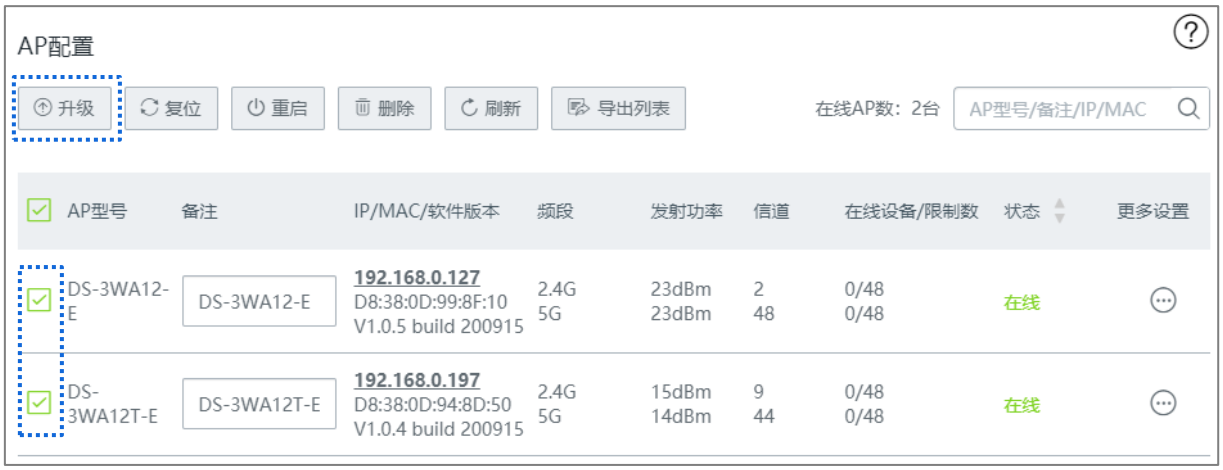


图7-5 AP 升级

## 7.3.3 复位

使用复位功能，可以将 AP 恢复出厂设置。

**设置步骤：**

步骤1 点击「AP 管理」>「AP 配置」。

步骤2 选择需要恢复出厂设置的 AP。

步骤3 点击 复位 ，之后按页面提示操作。

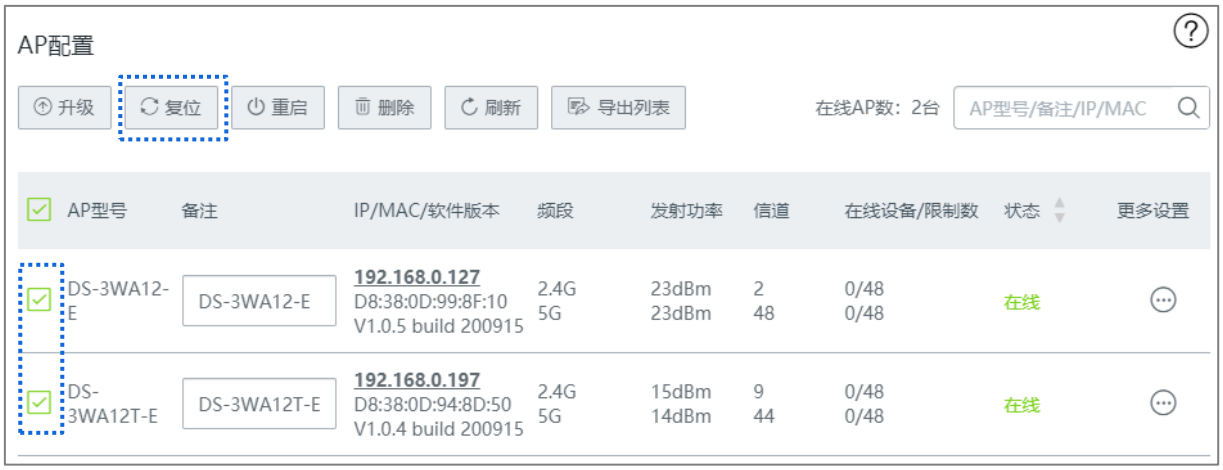


图7-6 复位 AP

## 7.3.4 重启

重启可以预防 AP 长时间运行导致 WLAN 出现性能降低、不稳定等现象，当您设置的某项参数不能正常生效或 AP 不能正常使用时，可以尝试重启 AP。

**设置步骤：**

步骤1 点击「AP 管理」>「AP 配置」。

步骤2 选择需要重新启动的 AP。

步骤3 点击 重启 ，之后按页面提示操作。

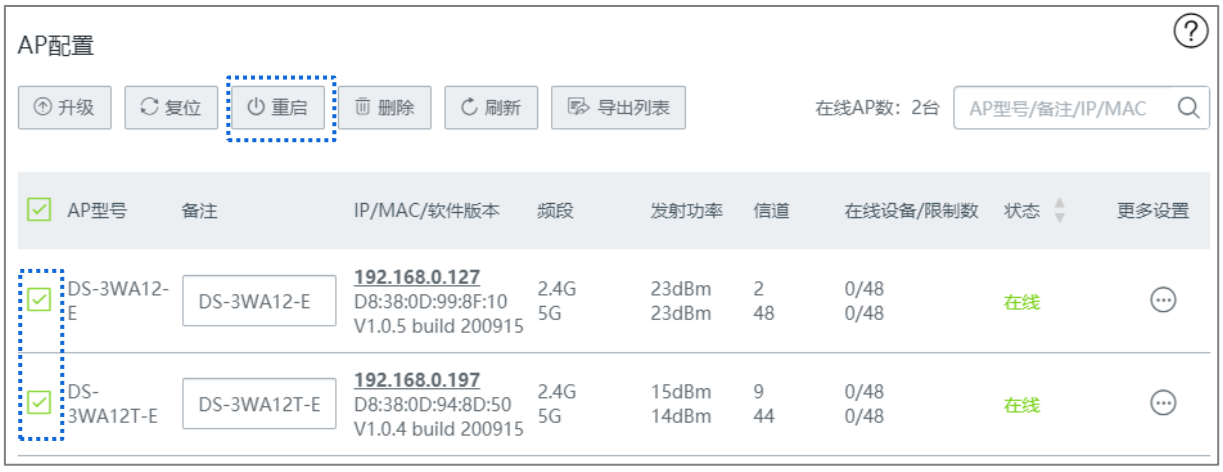


图7-7 重启 AP

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

## 7.3.5 删除

使用删除功能，可以删除处于离线状态的 AP。

**设置步骤：**

步骤1 点击「AP 管理」>「AP 配置」。

步骤2 选择需要删除的离线 AP。

步骤3 点击 删除 ，之后按页面提示操作。


图7-8 删除 AP

## 7.3.6 刷新

如果要更新页面显示的 AP 信息，请点击 刷新 。

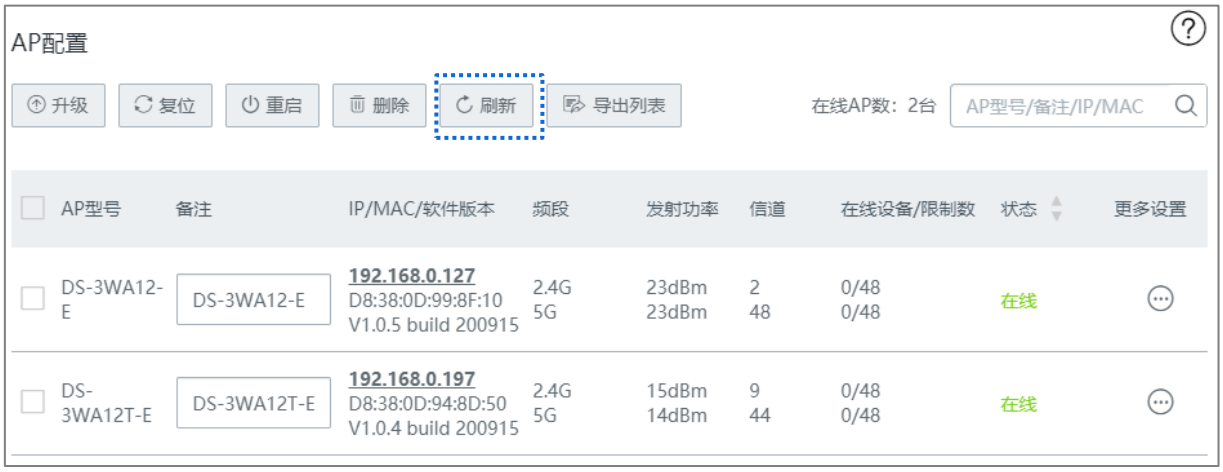


图7-9 刷新 AP 信息

## 7.3.7 导出

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

**设置步骤：**

步骤1 点击「AP 管理」>「AP 配置」。

步骤2 点击 导出列表 ，之后按页面提示操作。

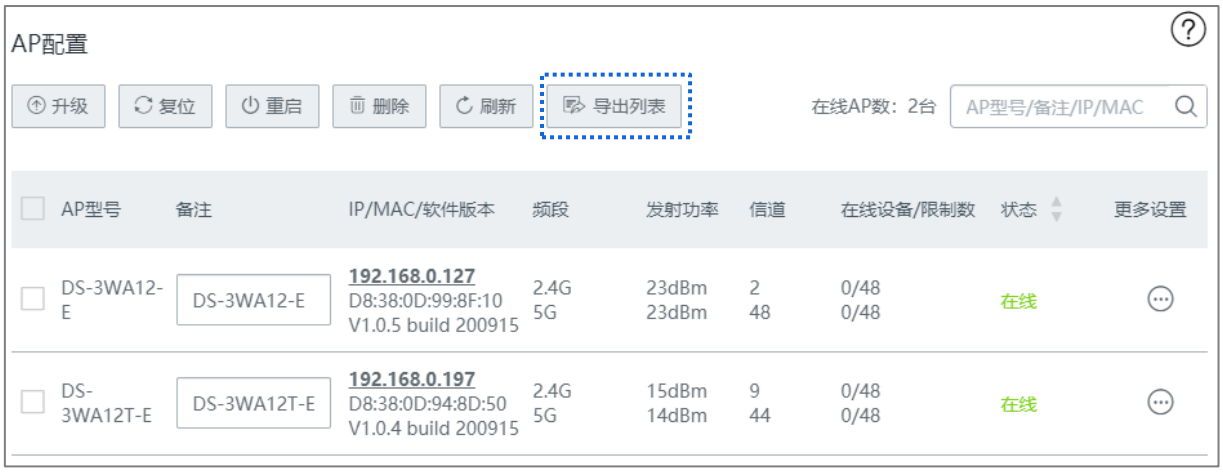


图7-10 导出 AP 信息

## 7.3.8 更多设置

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

**设置步骤：**

步骤1 点击「AP 管理」>「AP 配置」。

步骤2 找到需要修改配置的 AP，然后点击对应操作栏的 。

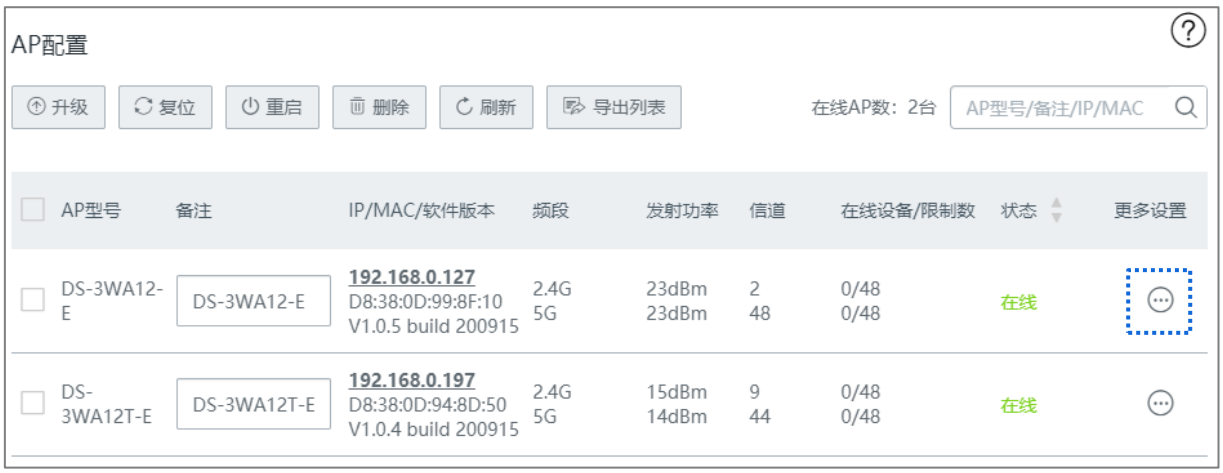


图7-11 AP 更多设置

步骤3 根据需要修改 AP 的配置，然后点击页面底端的 保存 。

# 7.4 高级设置

## 7.4.1 概述

进入页面：点击「AP 管理」>「高级设置」。

在这里，可以集中配置局域网中 AP 的高级参数。

### 2.4GHz/5GHz 高级设置

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


图7-12 2.4GHz 高级设置

表7-3 2.4GHz/5GHz 高级设置参数说明

| 标题项 | 说明 |
| --- | --- |
| 国家或地区 | AP 当前所在的国家或地区。 |
| 网络模式 | AP 的无线网络模式。2.4GHz 无线网络模式包括 11b、11g、11b/g、11b/g/n。<br>● 11b：AP 工作在 802.11b 无线网络模式下。<br>● 11g：AP 工作在 802.11g 无线网络模式下。<br>● 11b/g：AP 工作在 802.11b、802.11g 无线网络模式下。<br>● 11b/g/n：AP 工作在 802.11b、802.11g、802.11n 无线网络模式下。<br>5GHz 无线网络模式包括 11a、11ac、11a/n。<br>● 11a：AP 工作在 802.11a 无线网络模式下。<br>● 11ac：AP 工作在 802.11ac 无线网络模式下。<br>● 11a/n：AP 工作在 802.11a、802.11n 无线网络模式下。 |
| 信道带宽 | AP 的无线信道带宽。<br>● 20MHz：AP 使用 20MHz 的信道带宽。<br>● 40MHz：AP 使用 40MHz 的信道带宽。<br>● 80MHz：仅适用 5GHz，AP 根据周围环境，自动调整信道带宽为 20MHz、40MHz 或 80MHz。<br>● 自动：仅适用于 2.4GHz，AP 根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。 |
| 信道 | AP 的无线工作信道。<br>信道的可选择范围由当前选择的“国家或地区”和“频段”（2.4GHz 或 5GHz）决定。 |
| 发射功率 | AP 的发射功率。<br>若 AP 不支持设置的功率，则配置下发后，以 AP 支持的最大范围为准生效。即，当功率超过 AP 的上限功率时，只使用 AP 的最大功率；当功率小于 AP 的下限功率时，只使用 AP 的最小功率。 |
| 接入信号强度限制 | AP 相关射频可接受的无线终端设备信号强度。如果无线终端设备信号强度比此阈值小，AP 将主动断开无线终端设备。 |
| 客户端老化时 | 终端设备连接到 AP 的 WiFi 后，如果在该时间段内与 AP 没有数据通信，AP 将主动断开该终端设备；如果在该时间段内与 AP 有数据通信， |

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

## 全局设置

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


图7-13 全局设置模块

表7-4 参数说明

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

点击显示更多设置>，可以配置 AP 的 VLAN 相关参数。


图7-14 AP 的 VLAN 相关参数

表7-5 参数说明

| 标题项 | 说明 |
| --- | --- |
| VLAN | 开启/关闭 AP 的 802.1Q VLAN 功能。 |
| 管理 VLAN ID | AP 的管理 VLAN ID。<br>更改管理 VLAN 后，管理电脑或路由器需要重新连接到新的管理 VLAN，才能管理 AP。 |
| PVID | AP Trunk 口默认所属的 VLAN 的 ID。 |
| Trunk 口 | 设置 AP 的 Trunk 口。Trunk 口允许所有 VLAN 通过。 |

## 7.4.2 下发 2.4GHz/5GHz 网络配置到 AP

步骤1 点击「AP 管理」>「高级设置」。

步骤2 在“高级设置”模块修改相关参数。

步骤3 点击页面底端的 保存 。


图7-15 下发给 AP 的 2.4GHz/5GHz 网络配置

稍等片刻，局域网中 AP 的相关网络配置会变为与此处下发的策略一致。

### 7.4.3 下发端口驱动模式等其他配置到 AP

步骤1 点击「AP 管理」>「高级设置」。

步骤2 在“全局设置”模块修改相关参数。

步骤3 点击页面底端的 保存 。


图7-16 下发给 AP 的 2.4GHz/5GHz 其他配置

稍等片刻，局域网中 AP 的相关配置会变为与此处下发的策略一致。

# 第8章 行为管理

## 8.1 IP 组与时间组

### 8.1.1 概述

进入页面：点击「行为管理」>「IP 组与时间组」。

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

路由器默认已添加 1 条时间组，如下图示。默认时间组不支持删除和编辑操作。

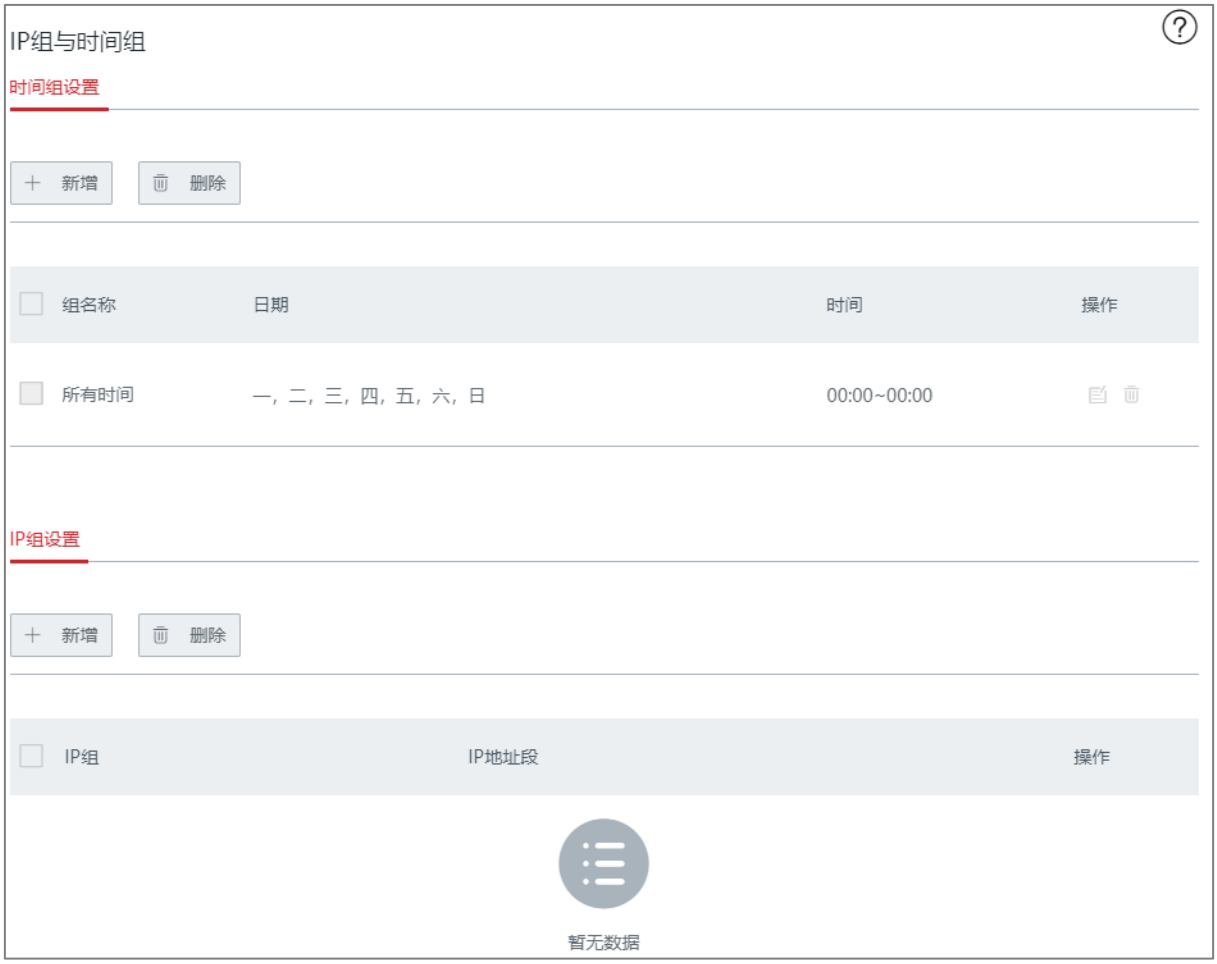


图8-1 IP 组与时间组

表8-1 参数说明

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

## 8.1.2 新增时间组

步骤1 点击「行为管理」>「IP 组与时间组」。

步骤2 在“时间组设置”模块，点击 +新增 。


图8-2 新增时间组规则

步骤3 在【新增】窗口配置各项参数，然后点击 保存 。


图8-3 编辑新增时间组规则

### 8.1.3 新增 IP 组

步骤1 点击「行为管理」>「IP 组与时间组」。

步骤2 在“IP 组设置”模块，点击 +新增 。


图8-4 新增 IP 组规则

步骤3 在【新增】窗口配置各项参数，然后点击 保存 。


图8-5 编辑新增 IP 组规则

# 8.2 MAC 地址过滤

## 8.2.1 概述

进入页面：点击「行为管理」>「MAC 地址过滤」。

通过 MAC 地址过滤功能，可以允许或禁止指定用户通过路由器上网。

MAC 地址过滤功能默认关闭，开启后，页面显示如下：


图8-6 MAC 地址过滤

表8-2 参数说明

| 标题项 | 说明 |
| --- | --- |
| MAC 地址过滤 | 开启/关闭 MAC 地址过滤功能。 |
| 过滤模式 | MAC 地址过滤模式。<br>● 白名单：即，允许访问互联网。使用此模式时，指定 MAC 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。<br>● 黑名单：即，禁止访问互联网。使用此模式时，指定 MAC 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。 |
| MAC 地址 | 规则对应的终端设备的 MAC 地址。 |
| 时间组 | 规则引用的时间组，以指定规则的生效时间。<br>时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 备注 | 规则的备注信息。 |
| 状态 | 启用/禁用规则。 |
| 操作 | 可对规则进行如下操作：<br>● 点击可以修改规则。<br>● 点击可以删除规则。 |
| 允许未启用规则中的主机和列表外的主机访问互联网 | ● 勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都可以访问互联网。<br>● 未勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都不能访问互联网。 |

## 8.2.2 新增 MAC 地址过滤规则

**说明**

配置 MAC 地址过滤规则前，请先配置好相应的时间组。

步骤1 开启 MAC 地址过滤功能。

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


图8-7 开启 MAC 地址过滤

步骤2 添加 MAC 地址过滤规则。

1. 点击 +新增 。


图8-8 新增 MAC 过滤规则

2. 在【新增】窗口配置各项参数，然后点击 保存 。


图8-9 编辑 MAC 过滤规则

## 8.2.3 MAC 地址过滤配置举例

### 组网需求

某企业使用企业级路由器进行网络搭建。

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

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

### 配置步骤

步骤1 配置时间组。

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组，点击 保存 。


图8-10

步骤2 开启 MAC 地址过滤功能。

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


图8-11 开启 MAC 地址过滤

步骤3 添加 MAC 地址过滤规则。

1. 点击 +新增 。


图8-12 新增 MAC 地址过滤规则

2. 在【新增】窗口进行如下配置，然后点击 保存 。

- 选择“过滤模式”，本例为“白名单（允许访问互联网）”。
- 选择规则生效的时间组，本例为“上班时间”。
- 输入采购人员电脑的物理地址，本例为“CC:3A:61:71:1B:6E”。
- （可选）设置本规则的备注，如“允许上网”。


图8-13 编辑 MAC 地址规则

3. 禁止未启用规则中的主机和列表外的主机访问互联网。

- 取消勾选“允许未启用规则中的主机和列表外的主机访问互联网”。

- 点击页面底端的 保存 。


图8-14 MAC 地址过滤规则添加成功

## 验证配置

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

# 8.3 IP 地址过滤

## 8.3.1 概述

进入页面：点击「行为管理」>「IP 地址过滤」。

通过 IP 地址过滤功能，可以允许或禁止指定用户通过路由器上网。

IP 地址过滤功能默认关闭，开启后，页面显示如下：


图8-15 开启 IP 地址过滤

表8-3 参数说明

| 标题项 | 说明 |
| --- | --- |
| IP 地址过滤 | 开启/关闭 IP 地址过滤功能。 |
| 过滤模式 | IP 地址过滤模式。<br>● 白名单：即，允许访问互联网。使用此模式时，指定 IP 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。<br>● 黑名单：即，禁止访问互联网。使用此模式时，指定 IP 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。 |
| IP 组 | 规则引用的 IP 组，以指定规则对应的用户。<br>IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 时间组 | 规则引用的时间组，以指定规则的生效时间。<br>时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 备注 | 规则的备注信息。 |
| 状态 | 启用/禁用规则。 |
| 操作 | 可对规则进行如下操作：<br>● 点击可以修改规则。<br>● 点击可以删除规则。 |
| 允许未启用规则中的主机和列表外的主机访问互联网 | ● 勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都可以访问互联网。<br>● 未勾选时：列表中“未启用”规则对应的设备，以及不在列表中的设备，都不能访问互联网。 |

## 8.3.2 新增 IP 地址过滤规则

**说明**

配置 IP 地址过滤规则前，请先配置好相应的 IP 组和时间组。

步骤1 开启 IP 地址过滤功能。

1. 点击「行为管理」>「IP 地址过滤」。

2. 点击滑块至 。

3. 点击页面底端的 保存 。


图8-16 开启 IP 地址过滤

步骤2 添加 IP 地址过滤规则。

1. 点击 +新增 。


图8-17 新增 IP 地址过滤规则

2. 在【新增】窗口配置各项参数，然后点击 保存 。


图8-18 编辑 IP 地址过滤规则

## 8.3.3 IP 地址过滤配置举例

### 组网需求

某企业使用企业级路由器进行网络搭建。

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

可以使用路由器的 IP 地址过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.50。

### 配置步骤

步骤1 配置时间组。

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。


图8-19 编辑时间组规则

步骤2 配置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。


图8-20 编辑 IP 组规则

步骤3 开启 IP 地址过滤功能。

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


图8-21 开启 IP 地址过滤

步骤4 添加 IP 地址过滤规则。

1. 点击 +新增 。


图8-22 新增 IP 地址过滤规则

2. 在【新增】窗口进行如下配置，然后点击 保存 。

- 选择“过滤模式”，本例为“白名单（允许访问互联网）”。
- 选择规则生效的时间组，本例为“上班时间”。
- 选择规则生效的 IP 组，本例为“采购部”。
- （可选）设置本规则的备注，如“允许上网”。


图8-23 编辑 IP 地址过滤规则

3. 禁止未启用规则中的主机和列表外的主机访问互联网。

- 取消勾选“允许未启用规则中的主机和列表外的主机访问互联网”。
- 点击页面底端的 保存 。


图8-24 成功添加 IP 地址过滤规则

### 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）才能访问互联网，使用其他员工的电脑不能访问互联网。

## 8.4 端口过滤

### 8.4.1 概述

进入页面：点击「行为管理」>「端口过滤」。

互联网上众多服务所涉及的应用协议都有特定的端口号，从 0 到 1023 是常用服务的端口号，这些端口号一般固定分配给特定的服务。为了方便管理局域网的终端设备，可以通过设置端口过滤功能来控制局域网中终端设备对互联网上某些端口的访问。

端口过滤功能默认关闭，开启后，页面显示如下：


图8-25 开启端口过滤

表8-4 参数说明

| 标题项 | 说明 |
| --- | --- |
| 端口过滤 | 开启/关闭端口过滤功能。 |
| IP 组 | 规则引用的 IP 组，以指定规则对应的用户。<br>IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 时间组 | 规则引用的时间组，以指定规则的生效时间。<br>时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 端口 | 禁止访问的服务使用的 TCP 或 UDP 端口号。 |
| 协议 | 禁止访问的服务使用的协议。“全部”表示 TCP 和 UDP。 |
| 状态 | 启用/禁用规则。 |
| 操作 | 可对规则进行如下操作：<br>● 点击可以修改规则。<br>● 点击可以删除规则。 |

## 8.4.2 新增端口过滤规则

**说明**

配置端口过滤规则前，请先配置好相应的 IP 组和时间组。

步骤1 开启端口过滤功能。

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


图8-26 开启端口过滤

步骤2 添加端口过滤规则。

1. 点击 +新增 。


图8-27 新增端口过滤规则

2. 在【新增】窗口配置各项参数，然后点击 保存 。


图8-28 编辑端口过滤规则

## 8.4.3 端口过滤配置举例

### 组网需求

某企业使用企业级路由器进行网络搭建。

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

可以使用路由器的端口过滤功能实现上述需求。假设财务部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.50。

### 配置步骤

步骤1 设置时间组。

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。


图8-29 配置时间组

步骤2 设置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。


图8-30 设置 IP 组

步骤3 开启端口过滤功能。

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

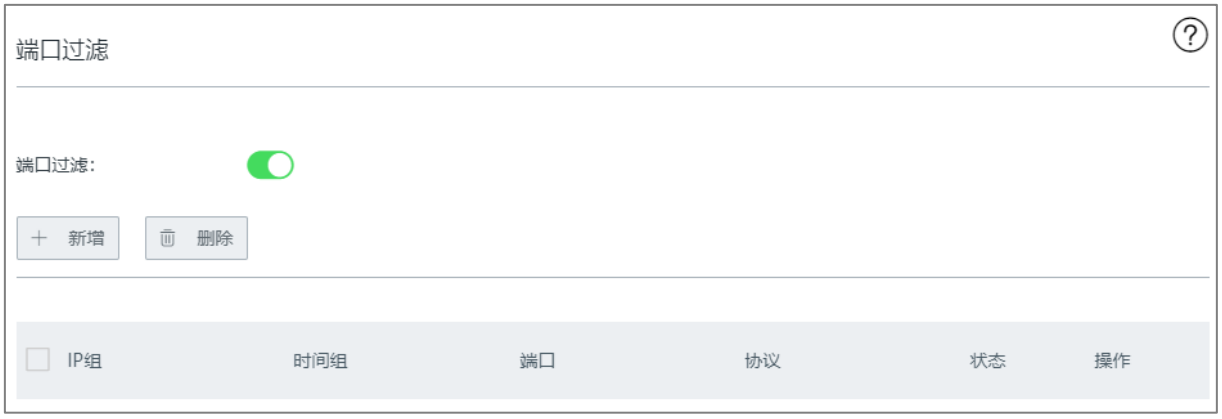


图8-31 开启端口过滤功能

步骤4 添加端口过滤规则。

1. 点击 +新增 。


图8-32 新增端口过滤规则

2. 在【新增】窗口进行如下配置，然后点击 保存 。

- 选择规则生效的 IP 组，本例为“财务部”。
- 选择规则生效的时间组，本例为“上班时间”。
- 输入浏览网页服务使用的端口号“80”。
- 选择服务使用的协议，建议保持默认“全部”。


图8-33 设置端口过滤规则

添加成功，如下图示:


图8-34 成功添加端口过滤规则

## 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 范围内的终端设备不能进行网页浏览服务。

# 8.5 网站过滤

## 8.5.1 概述

进入页面：点击「行为管理」>「网站过滤」。

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

网站过滤功能默认关闭，开启后，页面显示如下：


图8-35 网站过滤

表8-5 参数说明

| 标题项 | 说明 |
| --- | --- |
| 网站过滤 | 开启/关闭网站过滤功能。 |
| 过滤模式 | 网站过滤模式。<br>● 白名单（仅允许访问）：即，允许访问互联网。允许 IP 组内的用户在对应时间段内访问指定的网站，不能访问其他网站；在其他时间段内可以访问所有网站。<br>● 黑名单（仅禁止访问）：即，禁止访问互联网。禁止 IP 组内的用户在对应时间段内访问指定的网站，可以访问其他网站；在其他时间段内可以访问所有网站。 |
| IP 组 | 规则引用的 IP 组，以指定规则对应的用户。<br>IP 组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 时间组 | 规则引用的时间组，以指定规则的生效时间。<br>时间组应事先在「行为管理」>「IP 组与时间组」页面配置好。 |
| 网址 | 规则对应的网址分类。 |
| 状态 | 启用/禁用规则。 |
| 操作 | 可对规则进行如下操作：<br>● 点击可以修改规则。<br>● 点击可以删除规则。 |
| 网址管理 | 路由器管理网址分类，可以点击 网址管理 查看、增加网址。 |

## 8.5.2 新增网址分类

步骤1 开启网站过滤功能

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


图8-36 开启网站过滤功能

步骤2 添加网址分类。

1. 点击 网址管理 。


图8-37 网址管理

2. 点击 新增分类 。


图8-38 新增分类

3. 在【新增】窗口配置各项参数，然后点击 保存 。


图8-39 添加网址组

## 8.5.3 新增端口过滤规则

说明

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

步骤1 开启网站过滤功能

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


图8-40 开启网站过滤功能

步骤2 新增网站过滤规则

1. 在「行为管理」>「网站过滤」页面，点击 +新增 。

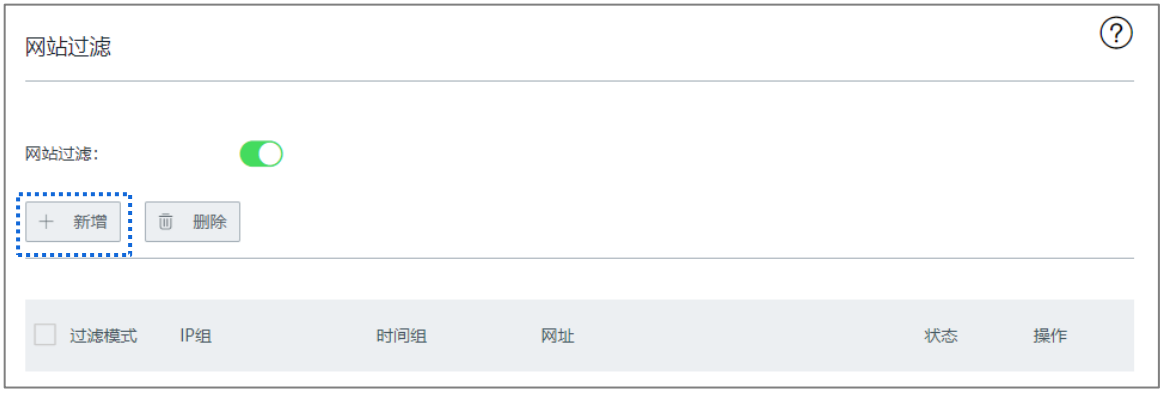


图8-41 添加网站过滤规则

2. 在【新增】窗口配置各项参数，然后点击 保存 。


图8-42 编辑网站过滤规则

## 8.5.4 网站过滤配置举例

### 组网需求

某企业使用企业级路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），禁止财务部门员工浏览购物网站（如 taobao.com、jd.com、vip.com）的网址。

可以使用路由器的端口过滤功能实现上述需求。假设财务部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.50。

### 配置步骤

步骤1 设置时间组。

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。


图8-43 配置时间组

步骤2 设置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。


图8-44 设置 IP 组

步骤3 新增网址分类。

1. 点击 网址管理 。


图8-45 网址管理

2. 点击 新增分类 。


图8-46 新增分类

3. 在【新增】窗口配置各项参数，然后点击 保存 。


图8-47 添加网址组

步骤4 开启网站过滤功能。

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


图8-48 开启网站过滤功能

步骤5 添加网站过滤规则。

1. 点击 +新增 。


图8-49 新增端口过滤规则

2. 在【新增】窗口进行如下配置，然后点击 保存 。

- 选择相应的过滤模式，本例为“仅禁止访问”。
- 选择规则生效的 IP 组，本例为“财务部”。
- 选择规则生效的时间组，本例为“上班时间”。
- （可选）设置备注，本例为“禁止访问”。
- 选择禁止终端设备访问的网址类别，本例为“自定义”。

- 选择禁止终端设备访问的网站，本例为“购物网站”。

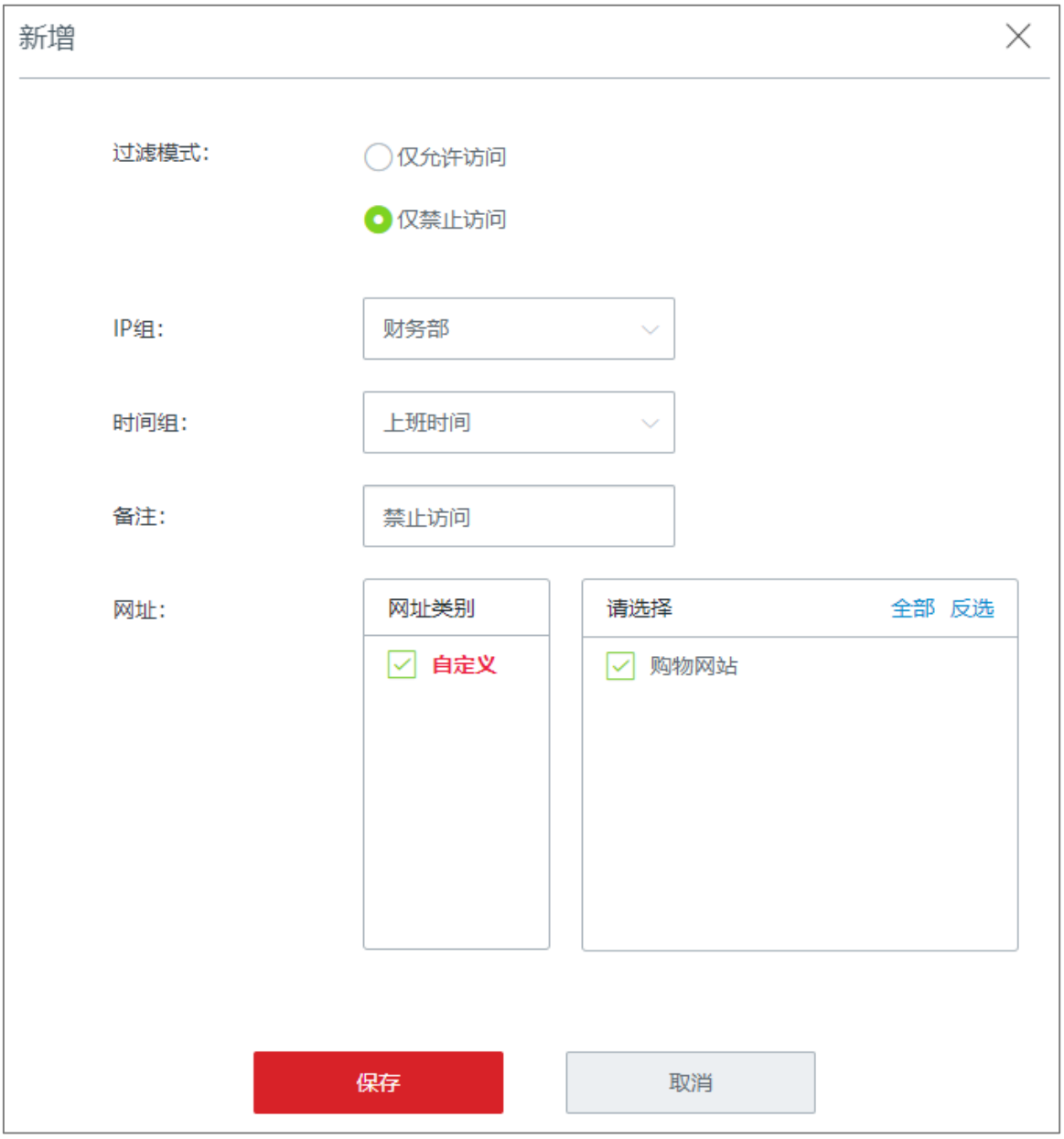


图8-50 设置网站过滤规则

添加成功，如下图示：


图8-51 成功添加端口过滤规则

## 验证配置

局域网中 192.168.0.2~192.168.0.50 的终端设备在星期一到星期五 8:00-18:00 不能浏览购物网站。

# 第9章 更多设置

## 9.1 局域网设置

进入页面：点击「更多设置」>「局域网设置」。

在这里，您可以设置路由器的 LAN 口 IP 地址和 DHCP 服务器。

### 9.1.1 LAN 口 IP 设置

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

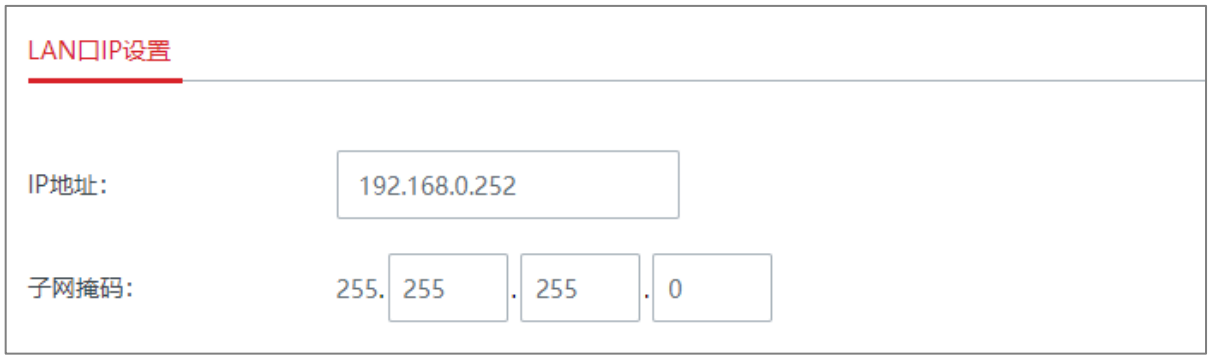


图9-1 LAN 口 IP 设置

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

修改 LAN 口 IP 地址后，系统出现如下提示。

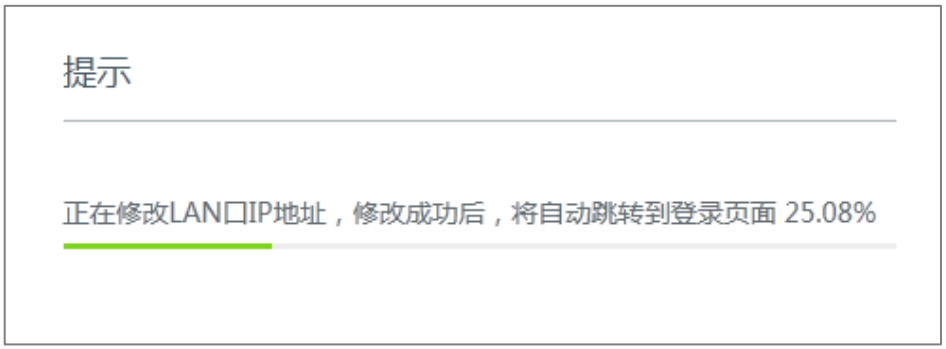


图9-2 修改 LAN 口 IP 提示

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

**说明**

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

## 9.1.2 DHCP 服务器

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

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


图9-3 DHCP 服务器

表9-1 参数说明

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

## 9.2 WAN 口参数

进入页面：点击「更多设置」>「WAN 口参数」。

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

### 9.2.1 WAN 口速率

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

否则，建议 WAN 口速率保持默认设置“自动协商”。


图9-4 WAN 口速率

### 9.2.2 MTU

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

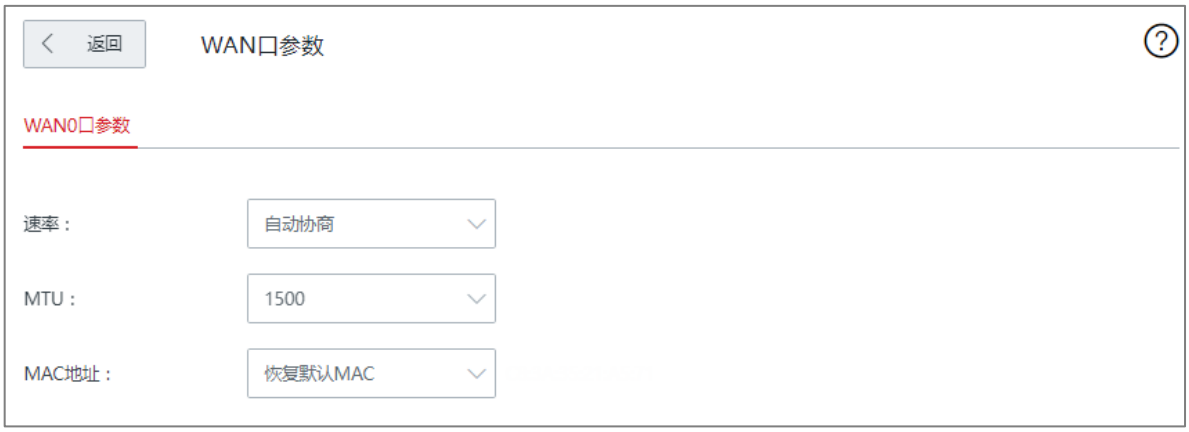


图9-5 MTU

一般情况下，建议保持 MTU 值为默认设置，除非您遇到以下情况：

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

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

表9-2 参数说明

| MTU 值 | 应用 |
| --- | --- |
| 1500 | 非宽带拨号、非 VPN 拨号环境下最常用的设置。 |
| 1492 | 用于宽带拨号环境。 |
| 1480 | 使用 ping 的最大值（大于此值的包会被分解）。 |
| 1450 | 用于一些 DHCP（动态 IP）环境。 |
| 1400 | 用于 VPN 或 PPTP 环境。 |

## 9.2.3 MAC 地址

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

**说明**

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

## 方法 1：克隆当前管理主机 MAC

步骤1 使用之前能正常上网的电脑连接路由器。

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

步骤3 点击页面底端的 保存 。


图9-6 克隆当前管理主机 MAC

## 方法 2：

步骤1 记录正确的 MAC 地址。

步骤2 登录路由器管理页面，点击「更多设置」>「WAN 口参数」。

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

步骤4 点击页面底端的 保存 。


图9-7 自定义 MAC

**说明**

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

## 9.2.4 快速转发

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


图9-8 快速转发

# 9.3 静态路由

## 9.3.1 概述

进入页面：点击「更多设置」>「静态路由」。

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

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

**说明**

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。


图9-9 静态路由

表9-3 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。<br>说明<br>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。<br>默认网关为“0.0.0.0”表示直连路由，即该目标网络是路由器该接口直连的网络。 |
| 接口 | 数据从路由器出去的接口。请根据需要选择相应接口。 |
| 操作 | 可对规则进行如下操作：<br>● 点击 可以修改规则。<br>● 点击 可以删除规则。 |

## 9.3.2 新增静态路由

说明

当静态路由规则和自定义的多 WAN 策略冲突时，静态路由优先生效。

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


图9-10 添加静态路由

## 9.3.3 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。互联网、公司内网在不同的网络，其中，WAN0 口通过宽带拨号接入互联网，WAN1 口通过动态 IP 接入公司内网。

要求：局域网的用户能同时访问互联网和公司内网。

### 方案设计

使用路由器的静态路由功能实现上述需求。

假设宽带账号和宽带密码均为 zhangsan。

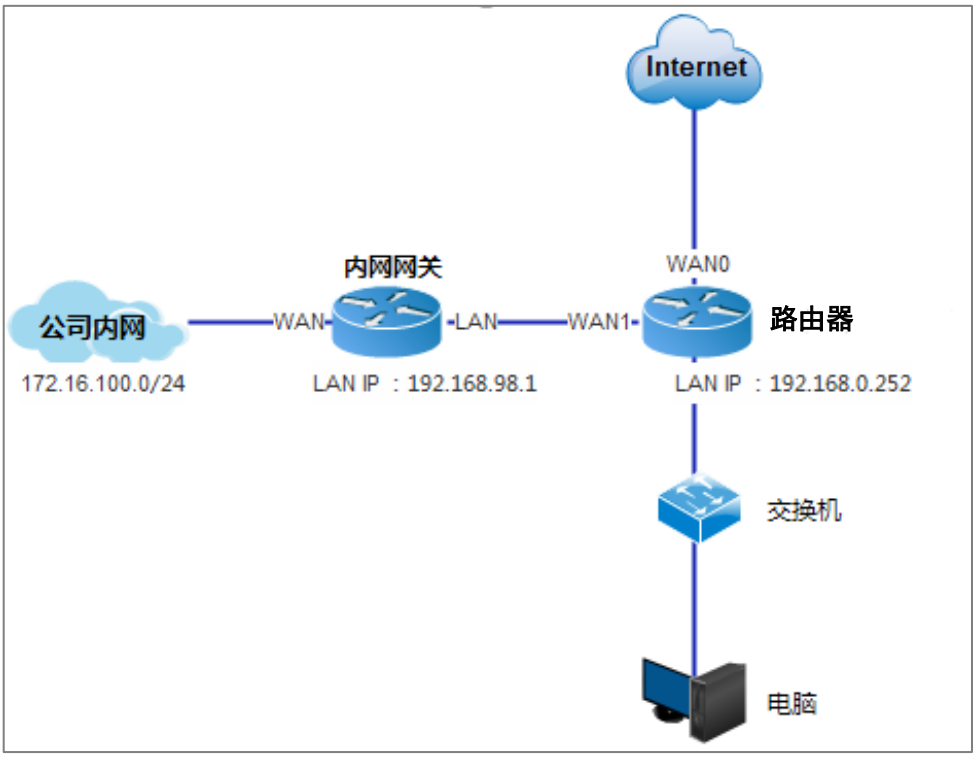


图9-11 静态路由网络拓扑图

## 配置步骤

步骤1 启用 2 个 WAN 口，并进行上网设置。

1. 点击「联网设置」，设置 WAN 口个数为“2”。
2. 在 WAN0 处选择“联网方式”为“宽带拨号”，输入 ISP 提供的“宽带账号”和“宽带密码”，本例均为“zhangsan”。

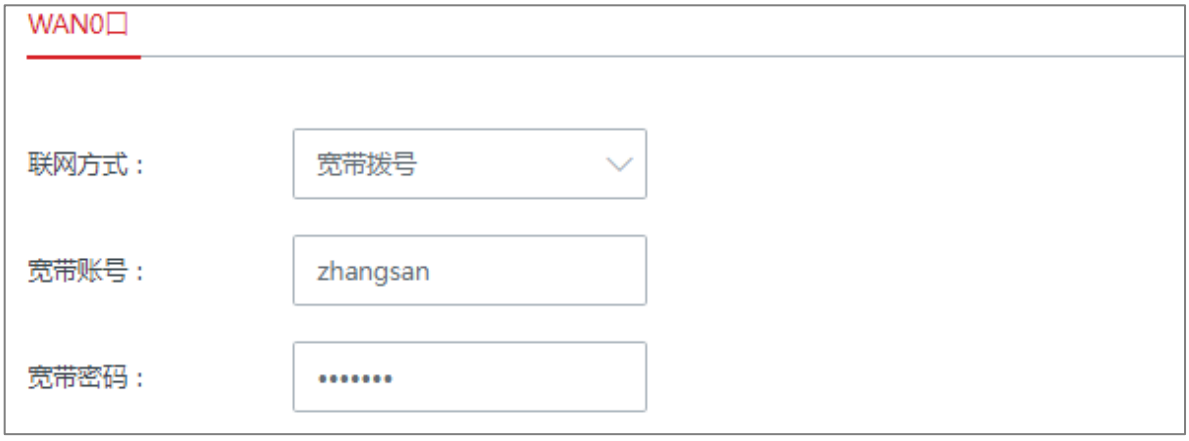


图9-12 设置 WAN0 口联网

3. 设置 WAN1 口的“联网方式”为“动态 IP”。

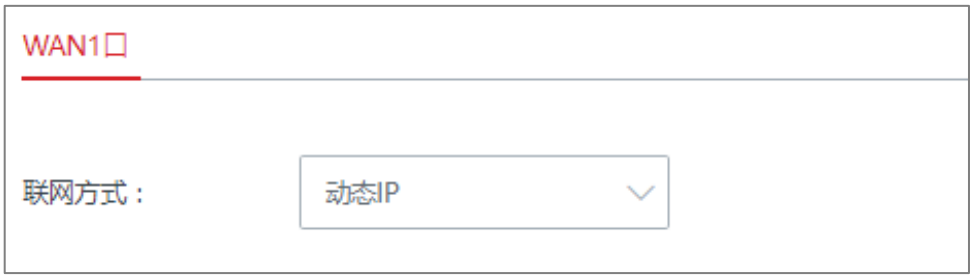


图9-13 设置 WAN1 口联网

4. 点击页面底端的 保存 ，之后按页面提示进行操作。

稍等路由器自动重启成功后重新进入「联网设置」，当 WAN0 口的联网状态显示“认证成功”时，WAN0 口联网成功；当 WAN1 口的联网状态显示“已联网”时，WAN1 口联网成功。

步骤2 设置静态路由。

点击「系统状态」，查看 WAN1 获取的 IP 地址信息，假设如下：

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

1. 点击「更多设置」>「静态路由」，然后点击 +新增 。


图9-14 添加静态路由

2. 在【新增】窗口配置下述参数，然后点击 保存 。
   - 输入目的网络的 IP 地址，本例为“172.16.100.0”。
   - 输入目的网络的子网掩码，本例为“255.255.255.0”。
   - 输入下一跳路由的入口 IP 地址，本例为“192.168.98.1”。
   - 选择路由器与目标网络通信的接口，本例为“WAN1”。

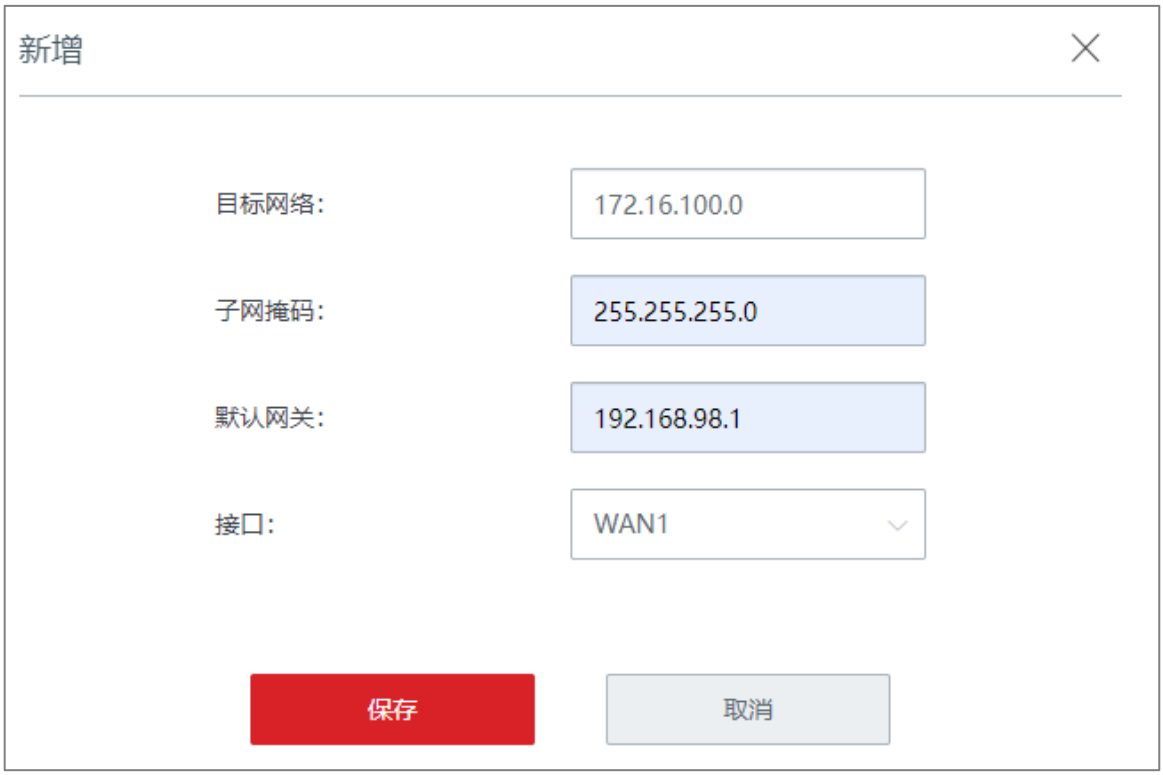


图9-15 设置静态路由参数

添加成功。


图9-16 静态路由添加成功

## 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。

# 9.4 端口镜像

## 9.4.1 概述

进入页面：点击「更多设置」>「端口镜像」。

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

端口镜像默认关闭，开启后，页面显示如下。


图9-17 端口镜像开启

表9-4 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 | 监控端口，该端口下的设备要安装监控软件。 |
| 被镜像端口 | 被监控端口。开启端口镜像功能后，被镜像端口的数据会被复制到镜像端口。 |

## 9.4.2 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

使用路由器的端口镜像功能实现上述需求。

假设监控设备接在 LAN3 上，需要监控其余接口的数据。

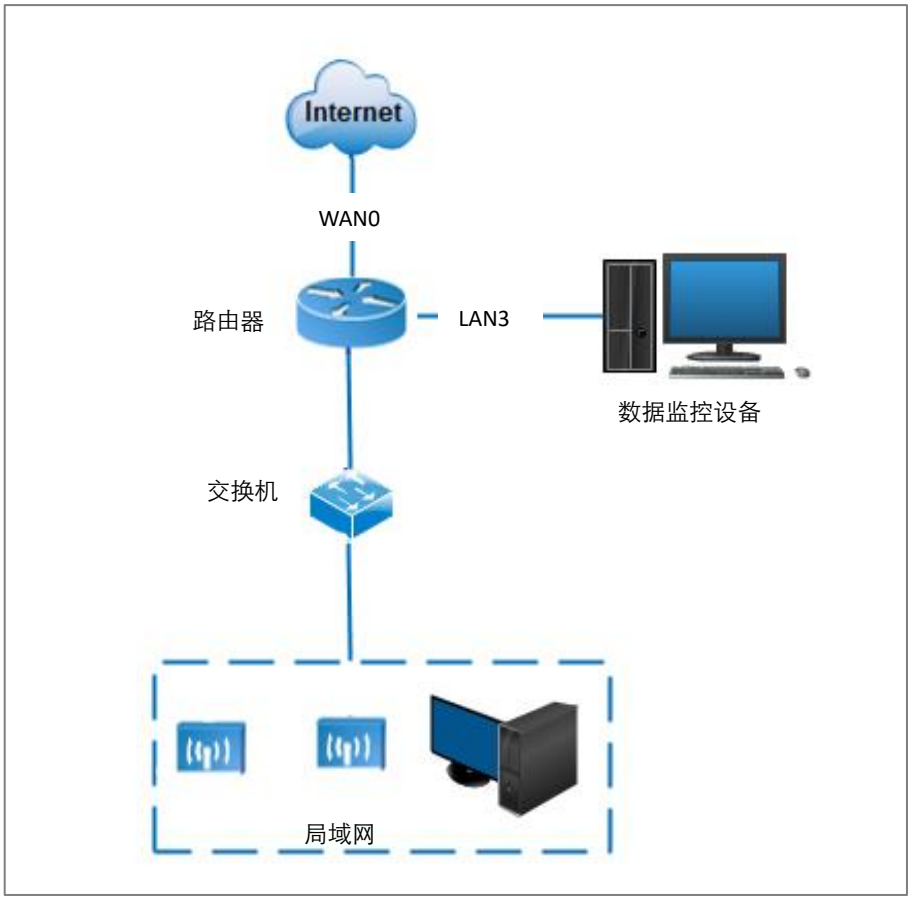


图9-18 端口镜像配置拓扑图

## 配置步骤

步骤1 点击「更多设置」>「端口镜像」。点击滑块至 。

步骤2 选择“镜像端口”，本例为“LAN3”。

步骤3 选择“被镜像端口”，本例为其余所有端口。

步骤4 点击页面底端的 保存 。


图9-19 配置端口镜像

## 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。

# 9.5 DDNS

## 9.5.1 概述

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

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

进入页面：点击「更多设置」>「DDNS」。

DDNS 默认关闭，开启后，页面显示如下。

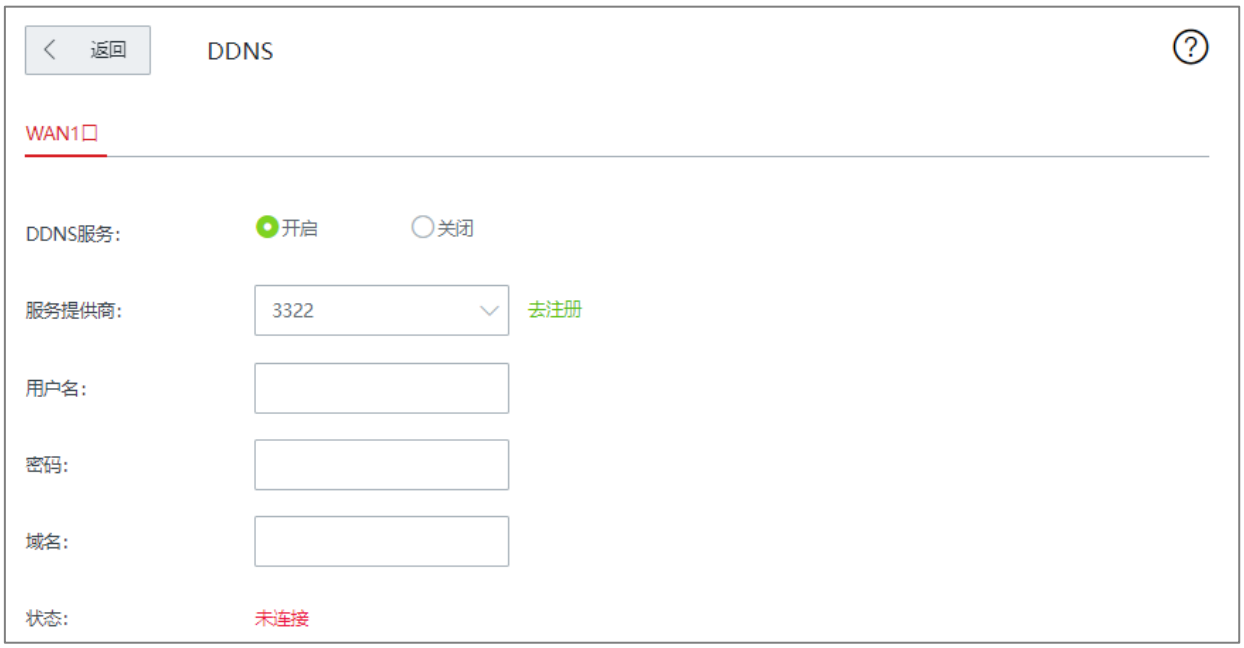


图9-20 开启 DDNS

表9-5 参数说明

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

## 9.5.2 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

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

假设 Web 服务器信息如下：

- 服务器地址：192.168.0.250
- 服务器主机 MAC 地址：58:50:ED:60:54:69
- 服务端口：9999

**说明**

- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地

址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。

- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在设置端口映射时，建议将外网端口设为非熟知端口（1024~65535），如 999，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。

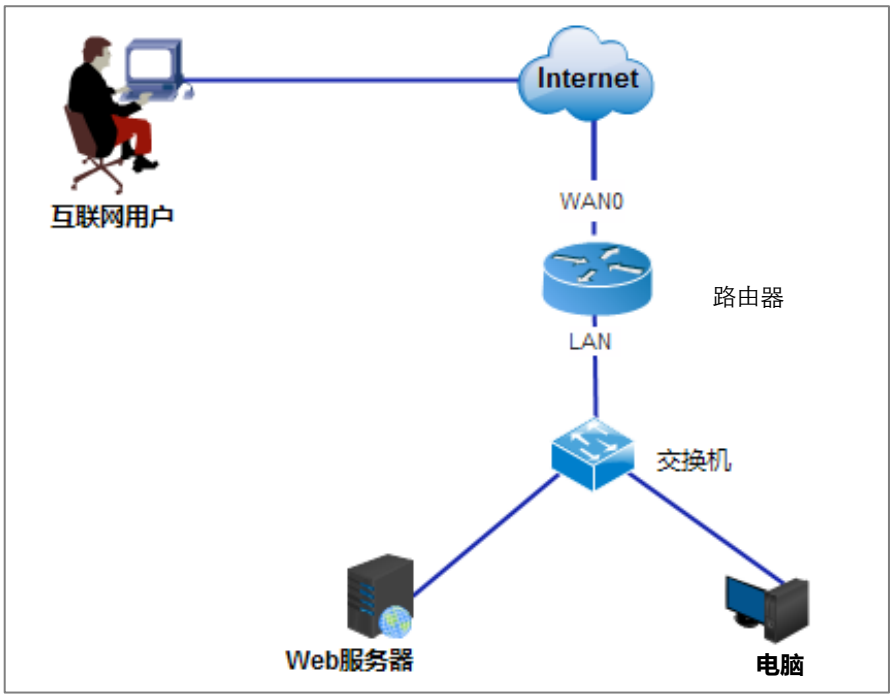


图9-21 DDNS 配置拓扑图

## 配置步骤

步骤1 配置端口映射。

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


图9-22 配置端口映射

步骤2 给服务器主机分配固定 IP 地址。

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

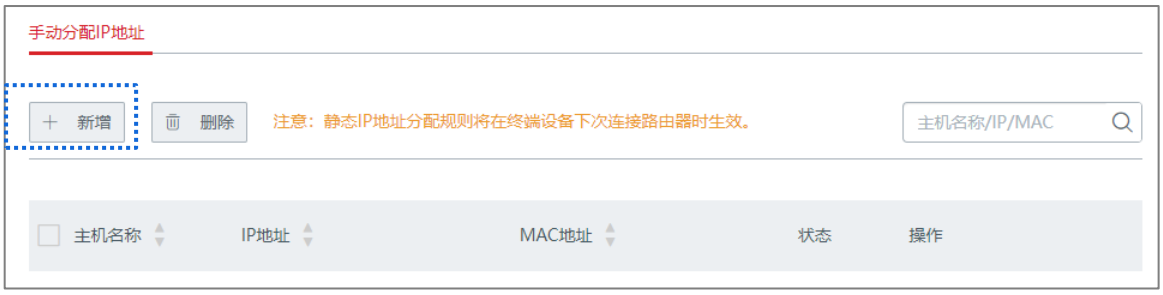


图9-23 手动分配 IP 地址

2. 在【新增】窗口进行如下配置，然后点击 保存 。

- 设置固定分配给服务器主机的 IP 地址，本例为“192.168.0.250”。
- 输入服务器主机的 MAC 地址，本例为“58:50:ED:60:54:69”。
- 设置服务器主机的备注，本例为“Web 服务器”。


图9-24 添加 IP 地址和 MAC 地址

固定 IP 地址分配完成，如下图示。


图9-25 固定 IP 地址分配完成

步骤3 配置 DDNS。

1. 注册 DDNS 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 UmXmL9UK，申请到的域名为 zhangsan.3322.org。
2. 登录到路由器的管理页面，设置 DDNS。
   - 点击「更多设置」>「DDNS」，找到对应 WAN 口模块，本例为“WAN0 口”。
   - 选择“DDNS 服务”为“开启”。
   - 选择您申请域名的 DDNS 提供商，本例为“3322”。
   - 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“UmXmL9UK”。
   - 输入您从 DDNS 服务提供商网站申请的域名，本例为“zhangsan.3322.org”。
   - 点击页面底端的 保存 。


图9-26 设置 DDNS 参数

DDNS 服务配置完成，刷新一下页面，稍等片刻。当 WAN0 口“状态”显示为“已联网”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。添加端口映射规则时，如果设置的外网端口号不是内网服务的默认端口号，访问格式为“内网服务应用层协议名称://对应 WAN 口域名:外网端口”。

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

**说明**

- 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。

# 9.6 端口映射

## 9.6.1 概述

进入页面：点击「更多设置」>「端口映射」。

默认情况下，广域网中的用户不能主动访问局域网内的计算机。端口映射开放了一个服务端口，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计算机，局域网也能避免受到侵袭。


图9-27 端口映射

表9-6 端口映射参数说明

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

## 9.6.2 新增端口映射规则

在「更多设置」>「端口映射」页面，点击 +新增 ，在【新增】窗口进行参数设置，然后点击 保存 。


图9-28 新增端口映射规则

## 9.6.3 端口映射配置举例

### 组网需求

**错误!未找到引用源。**，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

可以使用路由器的端口映射功能实现上述需求。假设路由器开放给广域网用户访问的端口为 9999。

## 方案设计

首先要在公司的电脑上建一个 FTP 服务器，并在服务器上存放要访问的资源，然后在路由器上设置端口映射功能。假设 FTP 服务器的基本信息如下：

- IP 地址：192.168.0.250
- 端口：9999
- MAC 地址：58:50:ED:60:54:69

参考拓扑图如下：

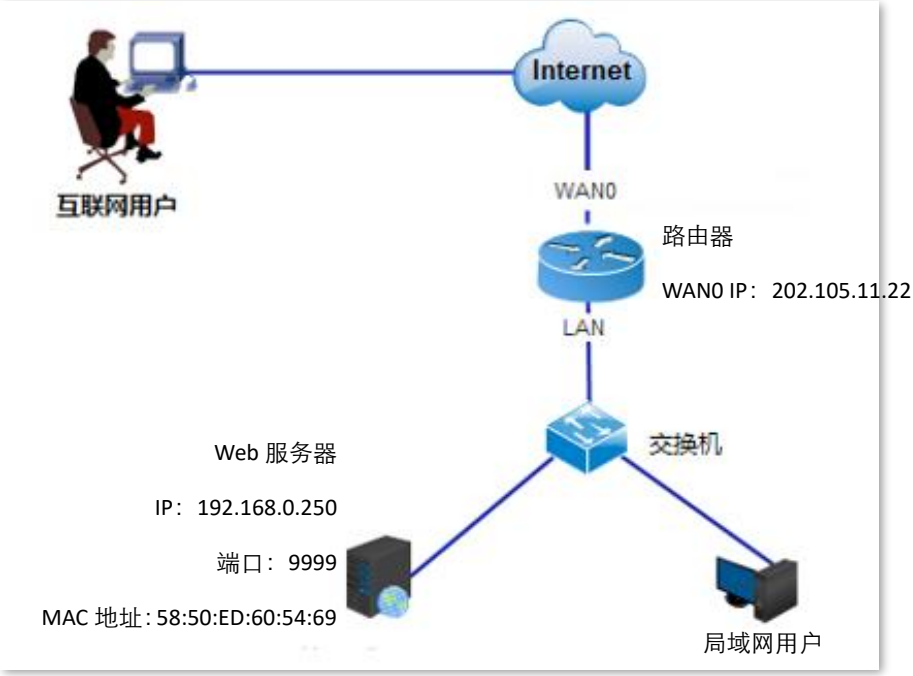


图9-29 端口映射拓扑图

## 配置步骤

步骤1 配置端口映射。

1. 点击「更多设置」>「端口映射」，点击 +新增 。


图9-30 新增端口映射

2. 在【新增】窗口进行如下配置，然后点击 保存 。

– 输入 Web 服务器的 IP 地址，本例为“192.168.0.250”。
– 输入内网端口，即 Web 服务器使用的端口，本例为“9999”。
– 输入外网端口，即路由器开放给广域网用户访问的端口，本例为“9999”。
– 选择 Web 服务器使用的协议“TCP”，若不清楚，可以选择“全部”。
– 选择互联网用户访问局域网服务器时使用的 WAN 口，本例为“WAN0”。


图9-31 添加端口映射参数

端口映射规则配置完成，如下图示。


图9-32 端口映射配置完成

步骤2 给服务器主机分配固定 IP 地址。

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

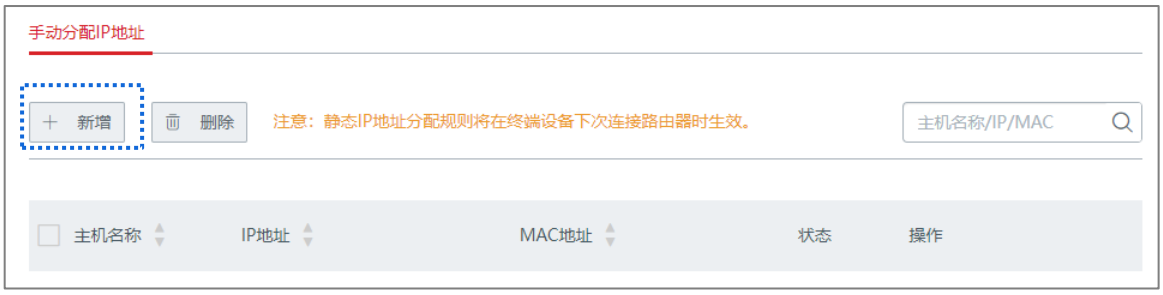


图9-33 手动分配 IP 地址

2. 在【新增】窗口进行如下配置，然后点击 保存 。

- 设置固定分配给服务器主机的 IP 地址，本例为“192.168.0.250”。
- 输入服务器主机的 MAC 地址，本例为“58:50:ED:60:54:69”。
- 设置服务器主机的备注，本例为“Web 服务器”。


图9-34 添加 IP 地址和 MAC 地址

固定 IP 地址分配完成，如下图示。


图9-35 固定 IP 地址分配完成

## 验证配置

互联网用户使用“内网服务应用层协议名称://对应 WAN 口 IP:外网端口”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://202.105.11.22:9999”。

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。

**说明**

**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。**

- 确保路由器 WAN 口获取的是公网 IP 地址，您填写的内网端口段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。

# 9.7 DMZ 主机

## 9.7.1 概述

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

**注意**

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

进入页面：点击「更多设置」>「DMZ 主机」。DMZ 主机默认关闭，开启后，页面显示如下。


图9-36 开启 DMZ 主机

表9-7 参数说明

| 标题项 | 说明 |
| --- | --- |
| DMZ 主机 | 开启/关闭 DMZ 主机功能。 |
| DMZ 主机 IP 地址 | 要设置为 DMZ 主机的局域网设备的 IP 地址。 |
| VPN 端口过滤 | 开启/关闭 VPN 端口过滤功能。<br>开启后，启用 DMZ 功能时，由路由器的 VPN 服务响应外网的 VPN 请求。<br>**说明**<br>路由器已开启 VPN 功能的情况下，开启 DMZ 主机功能时，请同时开启“VPN 端口过滤”功能。 |

## 9.7.2 DMZ 主机配置举例

### 组网需求

**错误!未找到引用源。**，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

可以使用路由器的 DMZ 功能实现上述需求。

## 网络拓扑

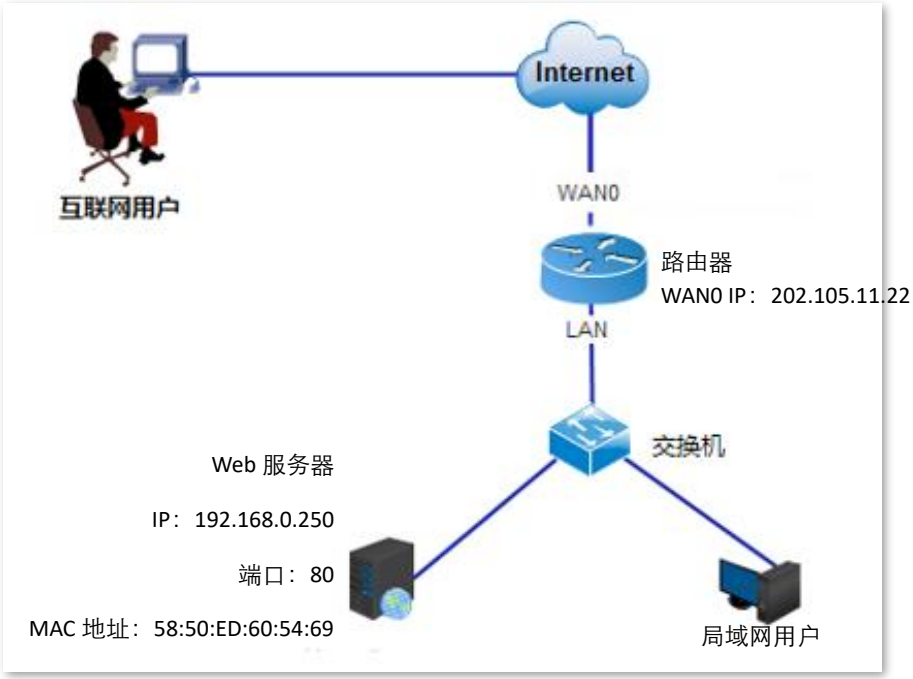


图9-37 DMZ 主机网络拓扑图

## 配置步骤

步骤1 配置 DMZ 主机。

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


图9-38 配置 DMZ 主机

步骤2 给服务器主机分配固定 IP 地址。

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

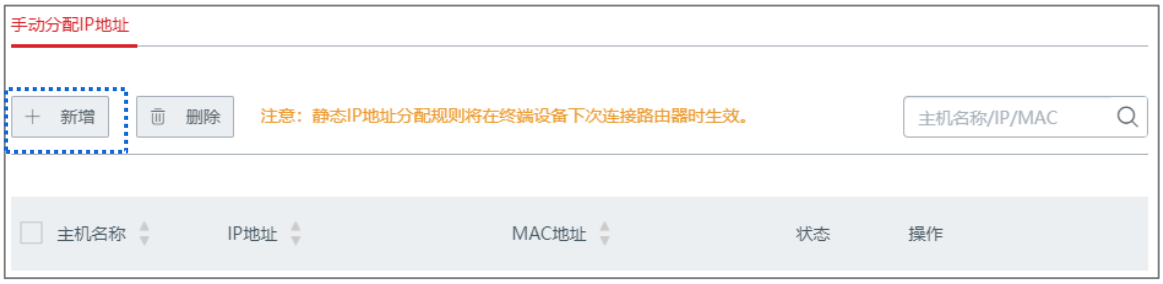


图9-39 手动分配 IP 地址

3. 在【新增】窗口进行如下配置，然后点击 保存 。
   - 设置固定分配给服务器主机的 IP 地址，本例为“192.168.0.250”。
   - 输入服务器主机的 MAC 地址，本例为“58:50:ED:60:54:69”。
   - 设置服务器主机的备注，本例为“Web 服务器”。


图9-40 添加 IP 地址和 MAC 地址

固定 IP 地址分配完成，如下图示。


图9-41 固定 IP 地址分配完成

## 验证配置

互联网用户使用“内网服务应用层协议名称://对应 WAN 口 IP”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://202.105.11.22”。

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”访问。

**说明**

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。

- 确保路由器 WAN 口获取的是公网 IP 地址。
- 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。

## 9.8 UPnP

### 9.8.1 概述

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

### 9.8.2 开启 UPnP

在「更多设置」>「UPnP」页面，点击滑块至 。


图9-42 开启 UPnP

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


图9-43 查看端口转换信息

## 9.9 攻击防御

进入页面：点击「更多设置」>「攻击防御」。

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

- ARP 攻击防御：路由器可以抵御局域网的 ARP 欺骗、ARP 广播等攻击。
- DDoS 防御：DDoS 攻击，即分布式拒绝服务（Distributed Denial of Service）攻击。利用 DDoS 攻击，攻击者可以消耗目标系统资源，使该目标系统无法提供正常服务。路由器可以防止的 DDoS 攻击类型包括：ICMP flood、UDP flood、SYN flood 攻击。
- IP 攻击防御：路由器可以按照要求拦截具有一些特殊 IP 选项的数据包，这些 IP 选项包括：IP Timestamp Option、IP Security Option、IP Stream Option、IP Record Route Option、IP Loose Source Route Option 及非法 IP 选项等。
- 防 WAN 口 Ping：广域网计算机 Ping 路由器 WAN 口 IP 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。

启用对应的攻击防御后，如果发生攻击，路由器可以将攻击信息如攻击时间、类型、次数，攻击者 IP、MAC 等记录在「系统状态」>「防攻击日志」页面的防攻击日志中，助力网络管理员进行网络安全管理。

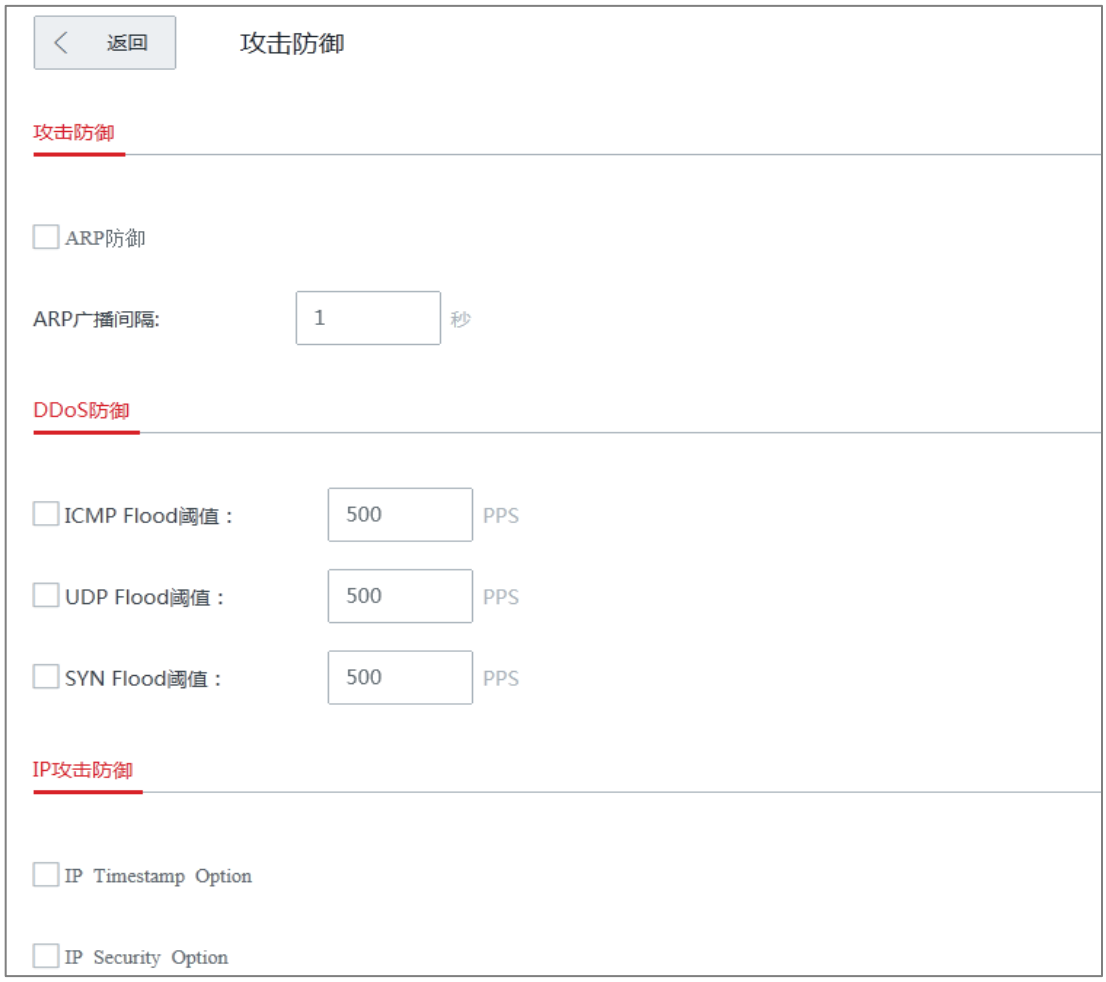


图9-44 攻击防御

表9-8 攻击防御参数说明

| 标题项 | | 说明 |
|---|---|---|
| ARP 攻击防御 | 启用 ARP 防御 | 开启/关闭 ARP 防御（包括防 ARP 攻击、防 ARP 欺骗、防 ARP 广播等）功能。 |
| | ARP 广播间隔 | 路由器发送 ARP 广播的时间间隔。 |
| DDoS 防御 | ICMP Flood 阈值 | 一秒钟内，如果路由器收到超过此阈值的 ICMP 请求包，则认为路由器正受到 ICMP Flood 攻击。 |
| | UDP Flood 阈值 | 一秒钟内，如果路由器某一端口收到超过此阈值的 UDP 包，则认为路由器该端口正受到 UDP Flood 攻击。 |

| 标题项 | | 说明 |
| --- | --- | --- |
| | SYN Flood 阈值 | 一秒钟内，如果路由器某一端口收到超过此阈值的 TCP SYN 包，则认为路由器该端口正受到 SYN Flood 攻击。 |
| IP 攻击防御 | IP Timestamp Option | 启用后，路由器将拦截带有 Internet Timestamp 选项的 IP 包。 |
| | IP Security Option | 启用后，路由器将拦截带有 Security 选项的 IP 包。 |
| | IP Stream Option | 启用后，路由器将拦截带有 Stream ID 选项的 IP 包。 |
| | IP Record Route Option | 启用后，路由器将拦截带有 Record Route 选项的 IP 包。 |
| | IP Loose Source Route Option | 启用后，路由器将拦截带有 Loose Source Route 选项的 IP 包。 |
| | 非法 IP 选项 | 启用后，路由器将检查 IP 包的完整性、正确性，如果不符合，则拦截。 |
| 防 WAN 口 Ping | | 开启/关闭路由器的防 WAN 口 Ping 功能。默认“关闭”。<br>开启防 WAN 口 Ping 功能后，广域网的设备不能 Ping 通路由器的 WAN 口 IP 地址。 |

# 9.10 VPN 服务

## 9.10.1 概述

VPN（Virtual Private Network，虚拟专用网），是一个建立在公用网（通常是互联网）上的专用网络，这个专用网络只在逻辑上存在，并没有实际物理线路。使用 VPN 技术，可以让企业的分公司员工在方便共享对方或公司总部局域网资源的同时，保证这些资源不会暴露给互联网上的其他用户。

VPN 典型网络拓扑图如下。

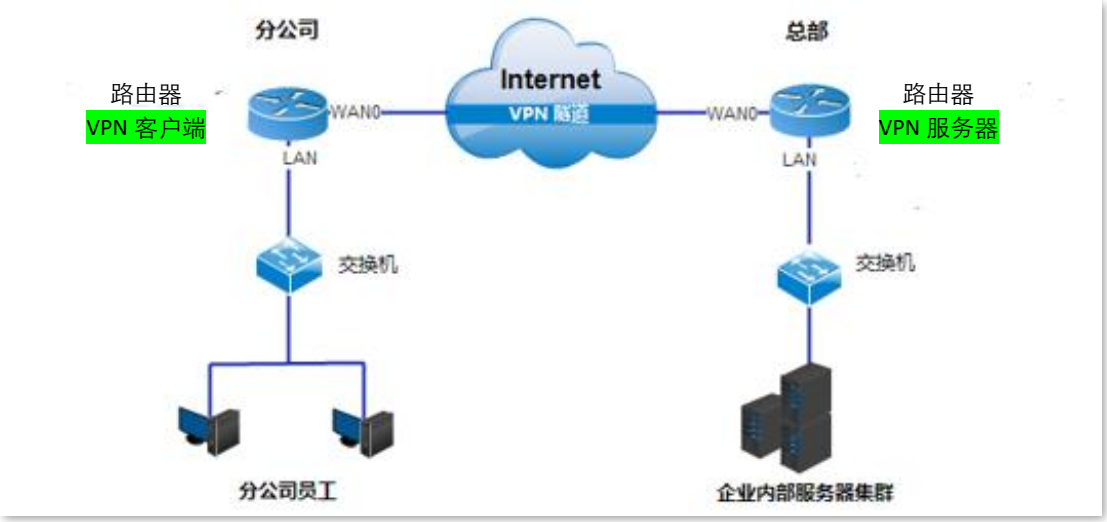


图9-45 VPN 网络拓扑图

路由器的「VPN 服务」模块包括：VPN 服务器、VPN 客户端。

## 9.10.2 VPN 服务器

进入页面：点击「更多设置」>「VPN 服务器」。

本路由器可以作为 PPTP/L2TP 服务器，接受 PPTP/L2TP 终端设备的连接。

VPN 服务器默认关闭，开启后，页面显示如下。

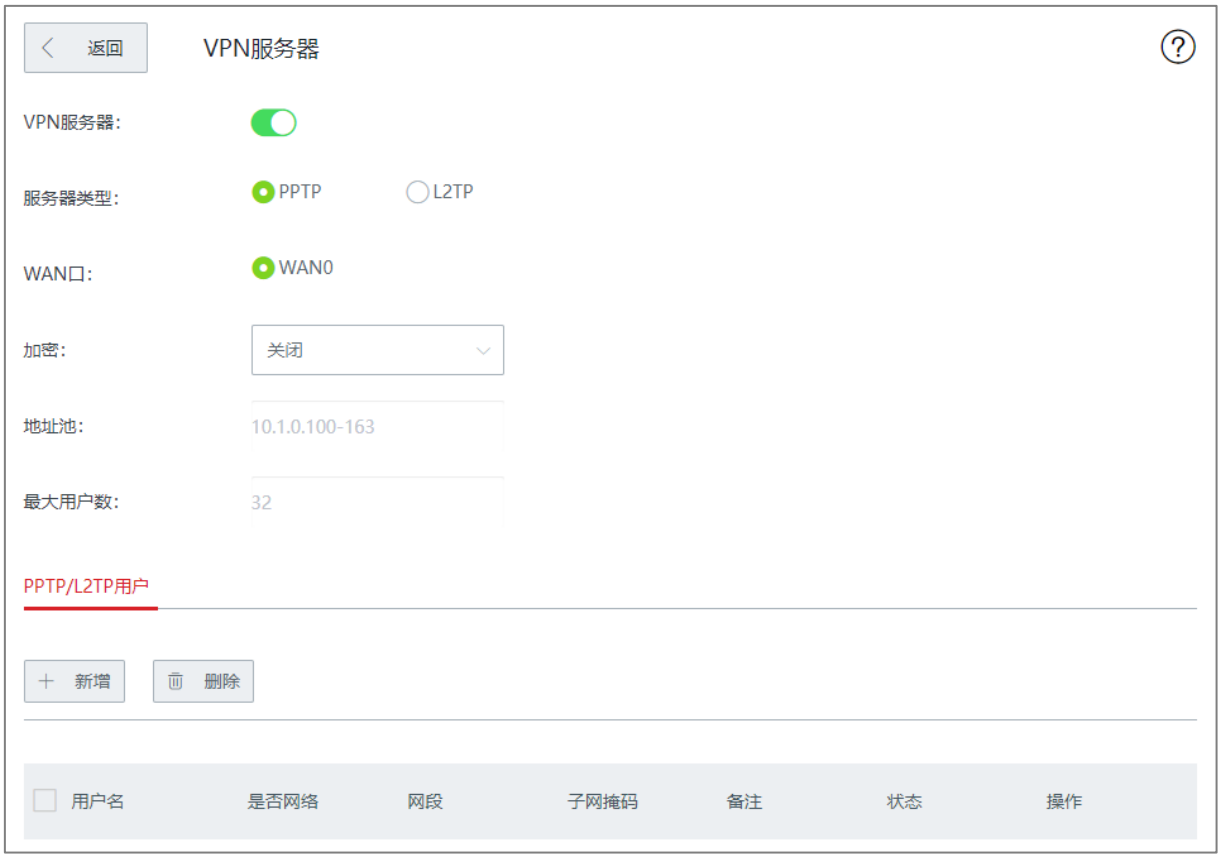


图9-46 开启 VPN 服务器

表9-9 PPTP/L2TP 服务器参数说明

| 标题项 | 说明 |
| --- | --- |
| VPN 服务器 | 开启/关闭 VPN 服务器功能。<br>开启后，路由器作为 VPN 服务器。 |
| 服务器类型 | 路由器使用的 VPN 协议类型，PPTP 或 L2TP。PPTP 和 L2TP 都是二层 VPN 隧道协议，使用 PPP（点到点协议）进行数据封装，并都为数据增添额外首部。<br>● PPTP：路由器作为 PPTP 服务器，接受 PPTP 终端设备的连接。<br>● L2TP：路由器作为 L2TP 服务器，接受 L2TP 终端设备的连接。 |
| WAN 口 | VPN 服务器与终端设备建立 VPN 隧道的 WAN 口。该 WAN 口的 IP 地址或域名是 VPN 终端设备的“服务器 IP 地址/域名”。 |
| 加密 | 只有 PPTP VPN 才支持此选项。<br>是否启用数据加密。终端设备、服务器双方的加密设置需保持一致，否则将不能正常通信。 |
| IPSec 加密 | 只有 L2TP VPN 才支持此选项。<br>是否启用 IPSec 加密。如果要进行 IPSec 加密，请选择在 IPSec 页面已建立的封装模式为“传输模式”的 IPSec 规则。 |
| 地址池 | VPN 服务器可分配给 VPN 终端设备的 IP 地址范围。 |
| 最大用户数 | VPN 服务器最多支持的 VPN 终端设备数量。系统固定为 32 个。 |
| 用户名<br>密码 | VPN 用户账号和密码，即 VPN 用户进行 PPTP/L2TP 拨号（VPN 连接）时需要输入的用户名/密码。 |
| 是否网络 | VPN 客户端类型。<br>● 是：VPN 客户端是一个网络时选择。此时，需要设置 VPN 客户端的“网段”、“子网掩码”参数。<br>● 否：VPN 客户端是一台主机。 |
| 网段 | VPN 客户端为一个网络时，在此输入客户端的内网网络号。 |
| 子网掩码 | VPN 客户端为一个网络时，在此输入客户端内网的子网掩码。 |
| 备注 | 该账号的描述信息。 |
| 状态 | 该账号的使用状态，可以根据需要启用或禁用。 |

| 标题项 | 说明 |
| --- | --- |
| 操作 | 可对账号进行如下操作：<br>● 点击 可以修改规则。<br>● 点击 可以删除规则。 |

## 9.10.3 新增 PPTP/L2TP 用户账号

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


图9-47 新增 PPTP/L2TP 用户账号

## 9.10.4 VPN 客户端

进入页面：点击「更多设置」>「VPN 终端设备」。

本路由器可以作为 PPTP/L2TP 终端设备连接到 PPTP/L2TP 服务器。

VPN 终端设备默认关闭，开启后，页面显示如下。

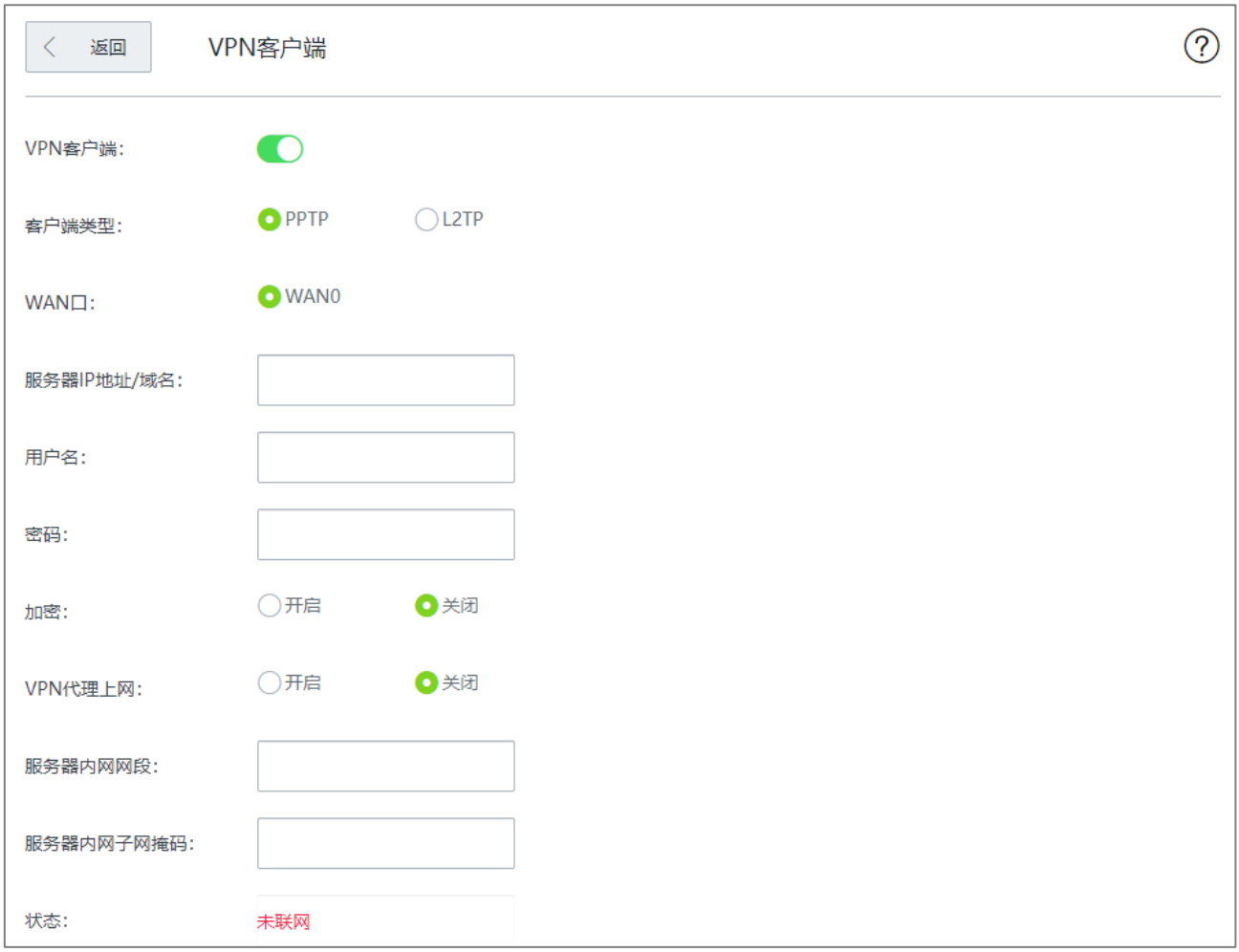


图9-48 开启 VPN 终端设备

表9-10 VPN 终端设备参数说明

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

## 9.10.5 PPTP/L2TP VPN 配置举例

### 组网需求

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

可以在路由器上设置 PPTP/L2TP VPN 服务，实现远端用户经互联网安全访问企业内部局域网的需求。本例以 PPTP VPN 为例说明，L2TP VPN 的设置方法类似。

## 网络拓扑

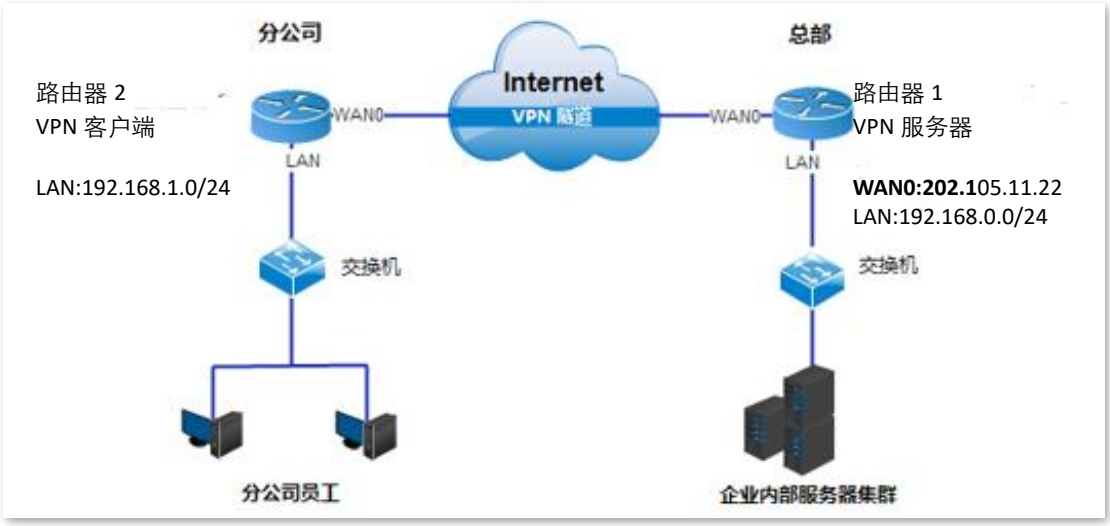


图9-49 PPTP/L2TP VPN 网络拓扑

## 配置步骤

配置路由器 1 为 PPTP 服务器

步骤1 开启 PPTP 服务器。

1. 登录路由器 1 的 Web 管理界面，然后点击「更多设置」>「VPN 服务器」进入设置页面。
2. 点击“VPN 服务器”滑块至 。
3. 点击页面底端的 保存 。


图9-50 开启 PPTP 服务器

步骤2 配置 PPTP/L2TP 用户。

1. 点击「更多设置」>「VPN 服务器」，找到“PPTP/L2TP 用户”模块。
2. 点击 +新增 。
3. 在【新增】窗口配置下述参数，然后点击 保存 。
   - 输入 VPN 终端设备进行 VPN 连接时所用的用户名，如“fengongsi1”。
   - 输入对应用户名的密码，如“fengongsi1”。
   - 选择“是否网络”为“是”。
   - 输入 VPN 终端设备局域网的网段，如“192.168.1.0”。
   - 输入子网掩码为“255.255.255.0”。
   - 输入该用户账号的描述信息，如“分公司 1”。

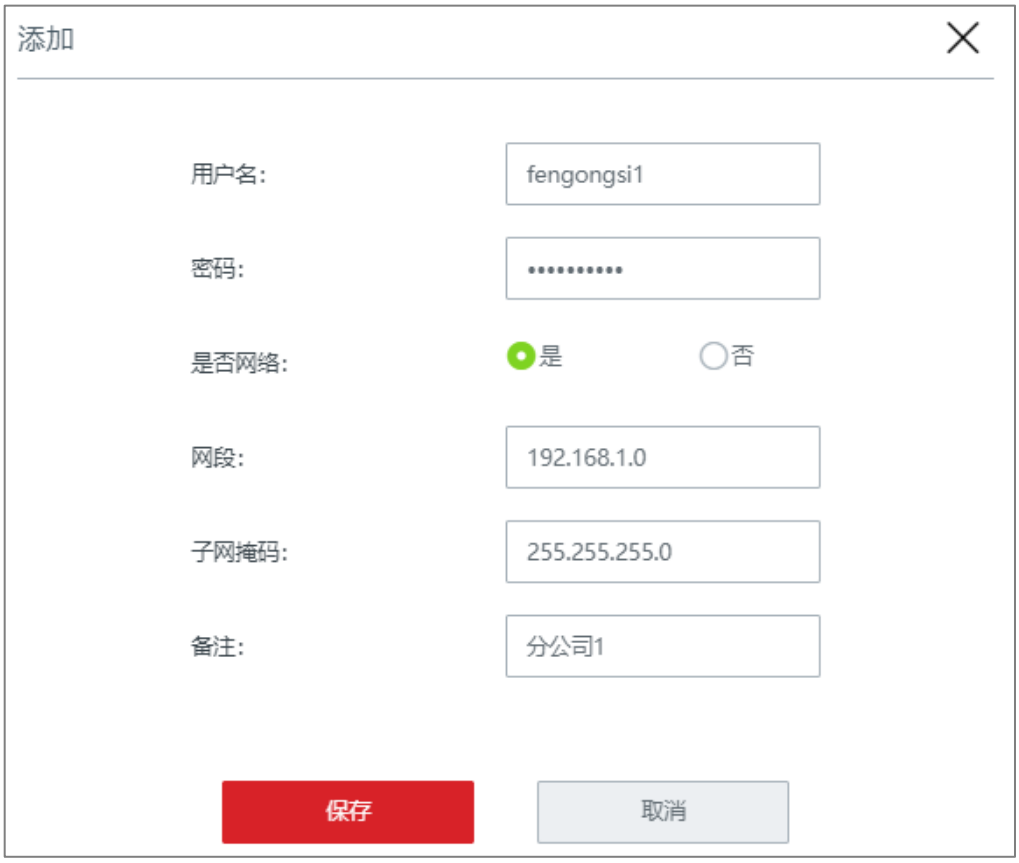


图9-51 配置 PPTP/L2TP 用户

添加完成，如下图示。


图9-52 成功添加 PPTP/L2TP 用户

配置路由器 2 为 PPTP 终端设备

步骤1 登录路由器 2 的 Web 管理界面，然后点击「更多设置」>「VPN 终端设备」进入设置页面。

步骤2 点击“VPN 终端设备”滑块至 。

步骤3 设置相关参数，然后点击页面底端的 保存 。

- 选择“终端设备类型”与 VPN 服务器侧一致，本例为“PPTP”。
- 指定 VPN 终端设备与服务器建立隧道的 WAN 口，本例为“WAN0”。
- 输入 VPN 服务器侧作为隧道出口的 WAN 口的 IP 地址/域名，本例为“202.105.11.22”。
- 输入 VPN 服务器分配的用户名，本例为“fengongsi1”。
- 输入 VPN 服务器分配的用户名对应的密码，本例为“fengongsi1”。
- 选择“加密”为“开启”，与 VPN 服务器侧配置保持一致。
- 输入 VPN 服务器内网的网段，本例为“192.168.0.0”。
- 输入 VPN 服务器内网的子网掩码，本例为“255.255.255.0”。


图9-53 开启 VPN 终端设备

当页面的状态显示为“已联网”时，VPN 连接成功。如下图示。


图9-54 VPN 连接成功

## 验证配置

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

- FTP 服务器 IP 地址：192.168.0.104

- 服务器端口：21
- 登录用户名/密码：zhangsan

当分公司员工访问总部项目资料时，步骤如下。

步骤1 在电脑上访问“ftp: //服务器 IP 地址:服务端口号”。本例中，因服务端口号是熟知端口，访问时可以免输服务端口号，即使用 ftp://192.168.0.104 进行访问。

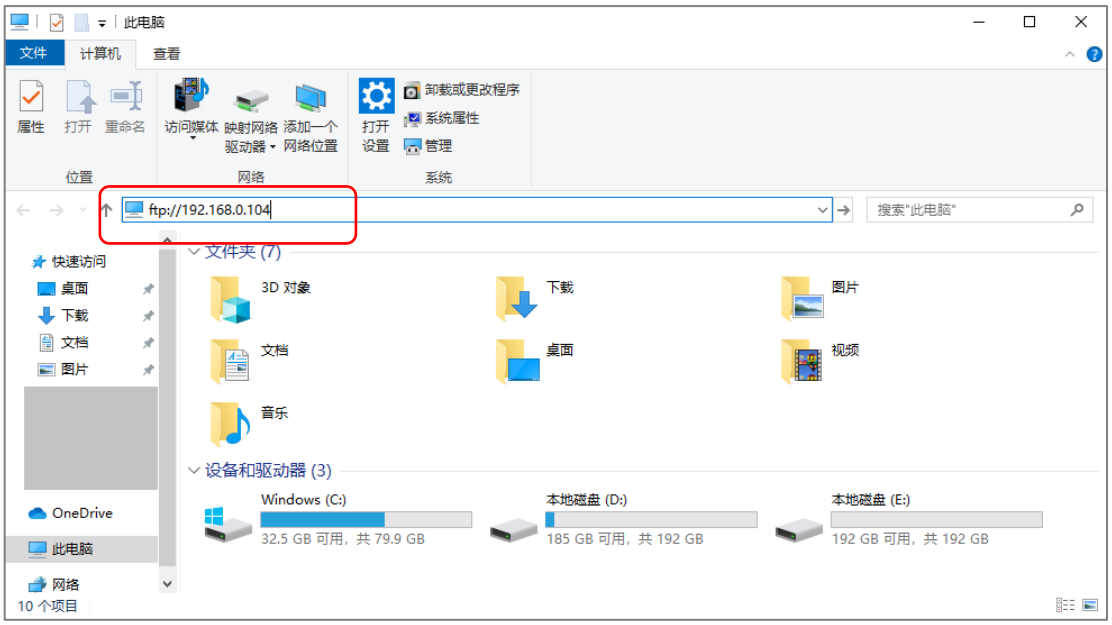


图9-55 访问 FTP 服务器

步骤2 在弹出的窗口输入登录用户名和密码，本例均为“zhangsan”。

步骤3 点击 登录 。

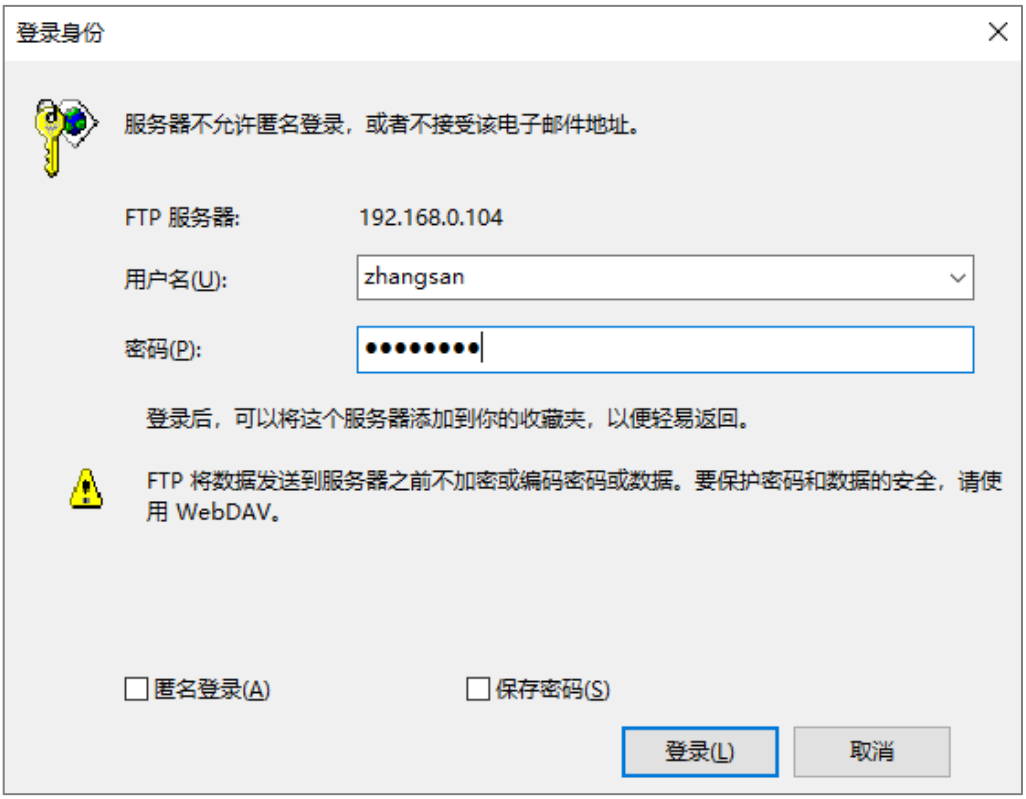


图9-56 验证身份

访问成功。

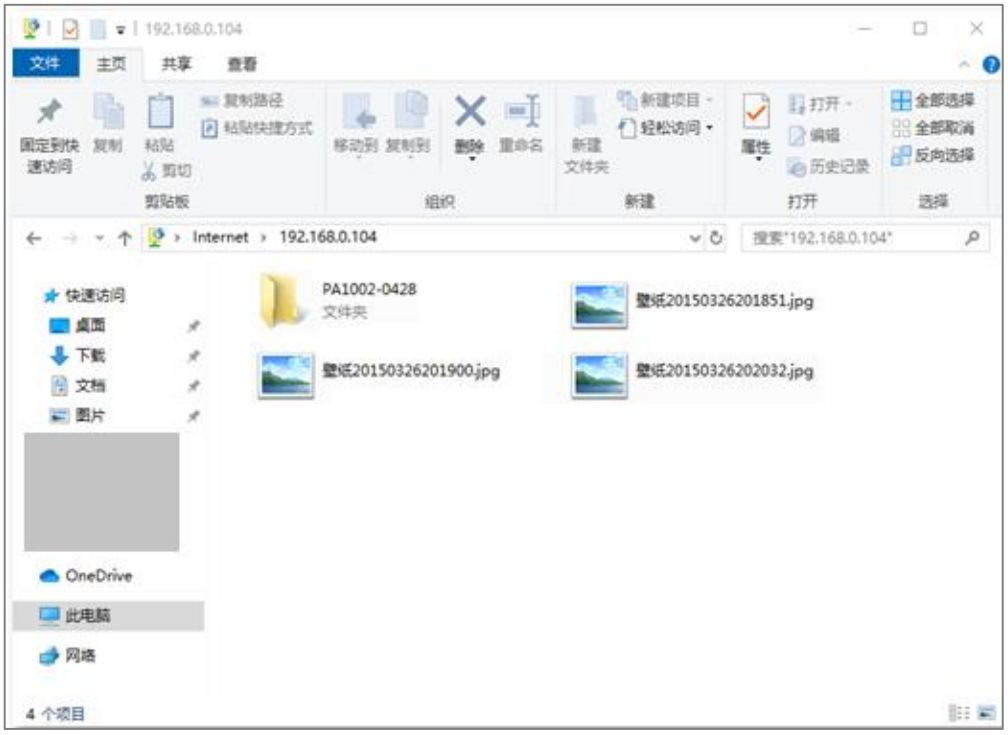


图9-57 成功访问 ftp 服务器

# 9.11 IPSec

## 9.11.1 概述

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

IPSec 相关概念如下。

- 封装模式

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

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

- 安全网关

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

- IPSec 对等体

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

- SA

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

  - 由{SPI，IP 目的地址，安全协议标识符}三元组唯一标识。
  - 它决定了对报文进行何种处理：协议、算法、密钥。
  - 每个 IPSec SA 都是单向的，并且是具有生命周期的。
  - SA 可以手工建立或由 IKE（Internet Key Exchange，互联网密钥交换）协商生成。

## 9.11.2 新增 IPSec 连接

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

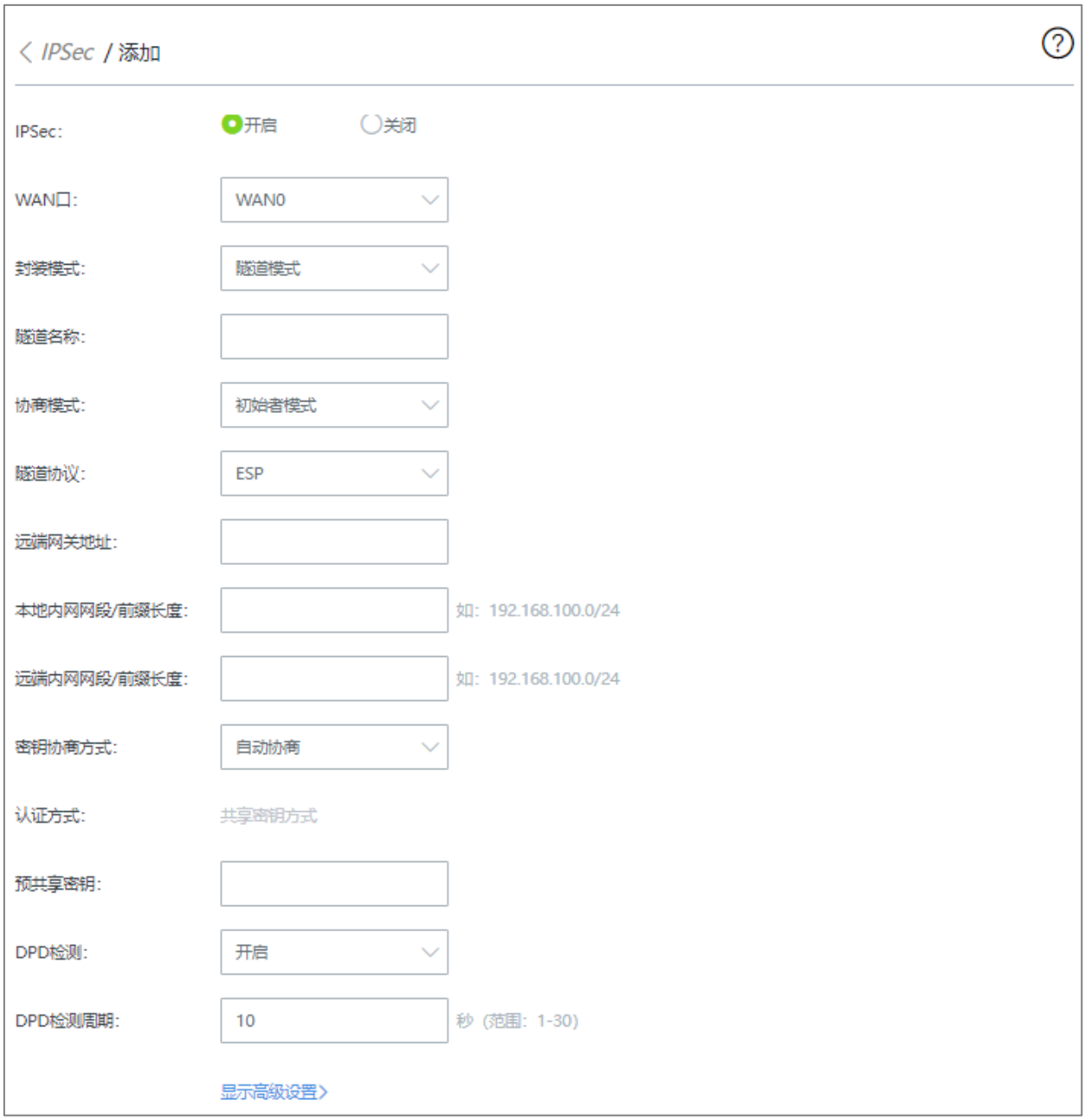


图9-58 新增 IPSec 连接

表9-11 IPSec 参数说明

| 标题项 | 说明 |
| --- | --- |
| 封装模式 | 选择 IPSec 数据的封装模式。<br>隧道模式通常用于两个安全网关之间的通讯；传输模式通常用于主机和主机、主机与网关之间的通信。 |
| WAN 口 | 选择设置 IPSec 连接的 WAN 口。 |
| 隧道名称 | 该 IPSec 连接的名称。 |
| 协商模式 | IPSec 隧道的协商模式。<br>● 初始者模式：主动向对端发起连接。<br>● 响应者模式：等待对端发起连接。<br>**说明**<br>**请勿将 IPSec 隧道两端都设置为“响应者模式”，否则会导致 IPSec 隧道建立失败。** |
| 隧道协议 | 为 IPSec 提供安全服务的协议。<br>● AH：Authentication Header，鉴别首部。该协议主要提供数据完整性校验功能，若数据报文在传输过程中被篡改，则接收方将在完整性验证时丢弃该报文。<br>● ESP：Encapsulating Security Payload，封装安全性载荷。该协议可以对数据的完整性进行检查，还对数据进行加密，这样，即使报文在传输过程中被截获，截取方也难以获取到真实信息。<br>● AH+ESP：同时使用上述两种协议。 |
| 远端网关地址 | IPSec 隧道对端网关的 IP 地址或域名。 |
| 本地内网网段/前缀长度 | 本路由器局域网的网段/前缀长度。例如：本路由器的 LAN 口 IP 地址为 192.168.0.252，子网掩码为 255.255.255.0，则本地内网网段/前缀长度可填为 192.168.0.0/24。 |
| 远端内网网段/前缀长度 | IPSec 隧道对端网关局域网的网段/前缀长度。若对端是一台特定主机，则此参数设置为“该设备的 IP 地址/32”。 |

| 标题项 | 说明 |
| --- | --- |
| 密钥协商方式 | 建立 IPSec 安全隧道的密钥协商方式。本路由器支持“自动协商”和“手动设置”。<br>● 自动协商：默认模式。通过 IKE 自动建立 SA，并进行动态维护、删除，降低了手工配置的复杂度，简化 IPSec 的使用、管理工作。自动建立的 SA 有生命周期，会定时更新，增强了安全性。<br>● 手动设置：用户手动设置加密/认证算法及密钥来建立 SA。手动建立的 SA 没有生命周期限制，除非手动删除，否则永不过期，因此有安全隐患。该方式常用于调试阶段。 |

**密钥协商方式--自动协商**

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

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

IKE 协商过程分为两个阶段：

- **阶段 1**：通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在阶段 2 中安全交换更多信息。
- **阶段 2**：使用阶段 1 中建立的 ISAKMP SA 为 IPSec 的安全性协议协商参数，创建 IPSec SA，用于对双方的通信数据进行保护。

密钥协商方式为“自动协商”时，如下图。


图9-59 自动协商

表9-12 自动协商参数说明

| 标题项 | 说明 |
| --- | --- |
| 认证方式 | 显示为“共享密钥”，表示 IPSec 双方事先通过某种方式协商好一个双方共享的密钥字符串。 |
| 预共享密钥 | 输入协商时所用的预共享密钥，需要保持与对端网关设备一致。最长为 128 字符。 |
| DPD 检测 | DPD，Dead Peer Detection，失效对等体检测。开启/关闭对等体检测功能。<br>通过 DPD 检测可以检测远端的隧道站点是否有效。 |
| DPD 检测周期 | 发送 DPD 报文的周期。<br>路由器会按照设置的周期定时发送 DPD 报文。如果 DPD 报文在有效时间内没有得到远端的确认，则重新初始化本地到远端的 IPSec SA。 |

点击显示高级设置可显示自动协商的高级参数。点击后，页面如下图示。

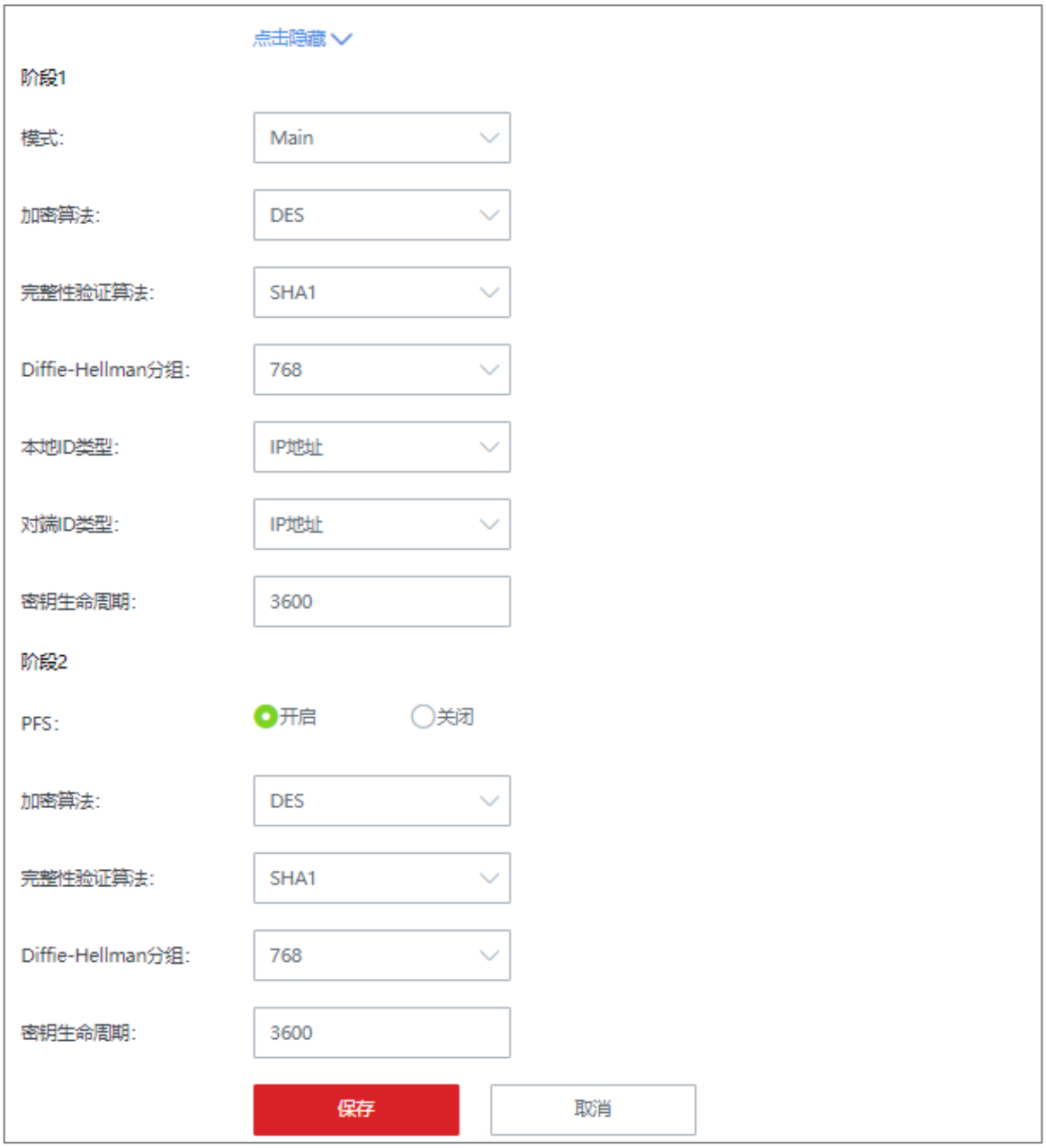
点击隐藏
阶段1
模式:
Main
加密算法:
DES
完整性验证算法:
SHA1
Diffie-Hellman分组:
768
本地ID类型:
IP地址
对端ID类型:
IP地址
密钥生命周期:
3600
阶段2
PFS:
开启
关闭
加密算法:
DES
完整性验证算法:
SHA1
Diffie-Hellman分组:
768
密钥生命周期:
3600
保存
取消

图9-60 高级设置

表9-13 高级设置参数说明

| 标题项 | 说明 |
| --- | --- |
| 模式 | 设置IKE阶段1的交换模式，该交换模式必须与对端设置相同。<br>● Main：主模式，该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。<br>● Aggressive：野蛮模式，又称主动模式，该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。 |
| 加密算法 | 选择应用于 IKE 会话的加密算法。本路由器支持以下加密算法：<br>● DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。<br>● AES（Advanced Encryption Standard，高级加密标准）：AES 128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。 |
| 完整性验证算法 | 选择应用于 IKE 会话的验证算法。本路由器支持以下验证算法：<br>● MD5：Message Digest Algorithm，消息摘要算法。对一段消息产生 128bit 的消息摘要，防止消息被篡改。<br>● SHA1：Secure Hash Algorithm，安全散列算法。对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。 |
| Diffie-Hellman 分组 | 选择 Diffie-Hellman 算法的组信息，用于产生加密 IKE 隧道的会话密钥。 |
| 本地 ID 类型 | 本地网关标识。<br>● IP 地址：本地路由器使用对应 WAN 口 IP 地址与对端网关协商。<br>● FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“本地 ID”输入框中输入任意字符串，用于与对端网关协商。“本地 ID”与远端网关的“对端 ID”必须相同。<br>**说明**<br>**“本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）** |

| 标题项 | 说明 |
| --- | --- |
| 对端 ID 类型 | 对端网关标识。<br>● IP 地址：本地网关默认对端网关使用其 WAN 口 IP 地址进行协商。<br>● FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“本地 ID”输入框中输入任意字符串，用于与对端网关协商。“本地 ID”与远端网关的“对端 ID”必须相同。<br>**说明**<br>**“本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）。** |
| 密钥生命周期 | 设置 IPSec SA 的生存时间。 |
| PFS | ● PFS（Perfect Forward Secrecy，完善的前向安全性）特性使得 IKE 阶段 2 协商生成一个新的密钥材料，该密钥材料与阶段 1 协商生成的密钥材料没有任何关联，这样即使 IKE1 阶段 1 的密钥被破解，阶段 2 的密钥仍然安全。<br>● 如果没有使用 PFS，阶段 2 的密钥将根据阶段 1 生成的密钥材料来产生，一旦阶段 1 的密钥被破解，用于保护通信数据的阶段 2 密钥也岌岌可危，这将严重威胁到双方的通信安全。 |

**密钥协商方式-手动设置**

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

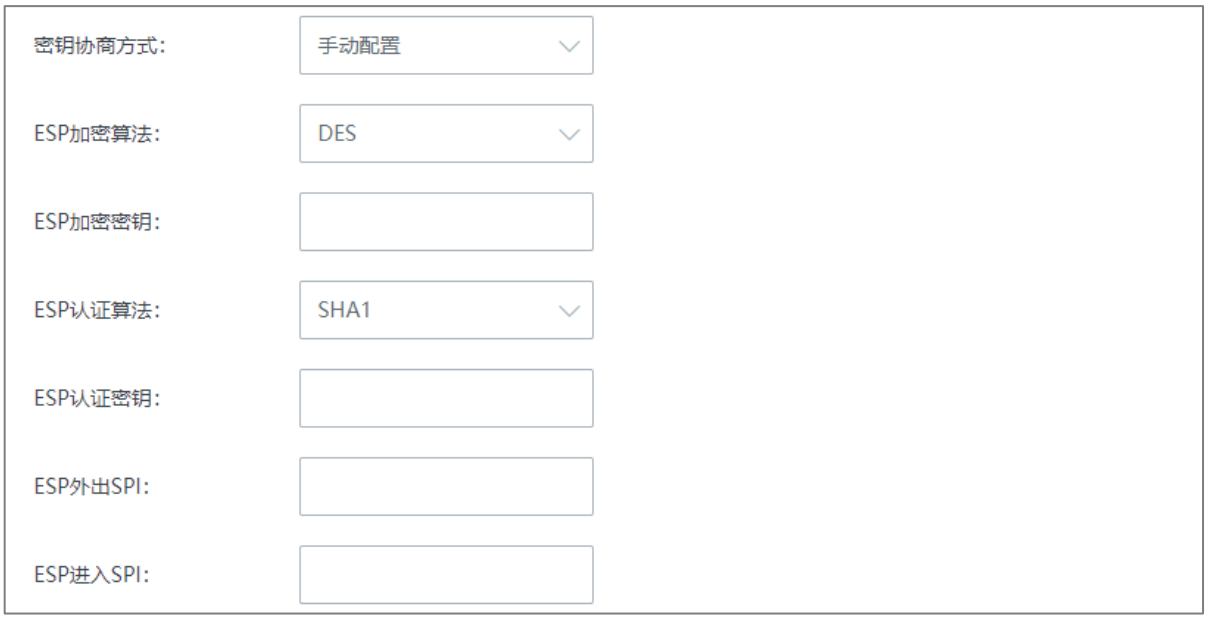


图9-61 密钥协商方式-手动配置

表9-14 密钥协商方式-手动设置参数说明

| 标题项 | 说明 |
| --- | --- |
| ESP 加密算法 | 当隧道协议选择“ESP”时需设置 ESP 加密算法。本路由器支持以下加密算法：<br>● DES：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。<br>● AES：AES128/192/256 表示使用长度为 128/192/256bit 的密钥进行加密。 |
| ESP 加密密钥 | 设置 ESP 加密密钥。IPSec 通信双方设置需保持一致。 |
| ESP/AH 认证算法 | 当隧道协议选择“ESP”时，需设置 ESP 认证算法；当隧道协议选择“AH”时，需设置 AH 认证算法。本路由器支持以下验证算法：<br>● MD5：对一段消息产生 128bit 的消息摘要，防止消息被篡改。<br>● SHA1：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。 |
| ESP/AH 认证密钥 | 当隧道协议选择“ESP”时，需设置 ESP 认证密钥；当隧道协议选择“AH”时，需设置 AH 认证密钥。<br>IPSec 通信双方设置需保持一致。 |
| ESP/AH 外出 SPI | 设置进入 SPI 参数。<br>SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“外出 SPI”值相同。 |
| ESP/AH 进入 SPI | 设置进入 SPI 参数。<br>SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“外出 SPI”值相同。 |

## 9.11.3 IPSec VPN 配置举例

### 组网需求

**错误!未找到引用源。**，并成功接入互联网。分公司员工需要经过互联网访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

可以在路由器上设置 IPSec VPN 服务，实现远端用户经互联网安全访问企业内部局域网的需求。

### 网络拓扑

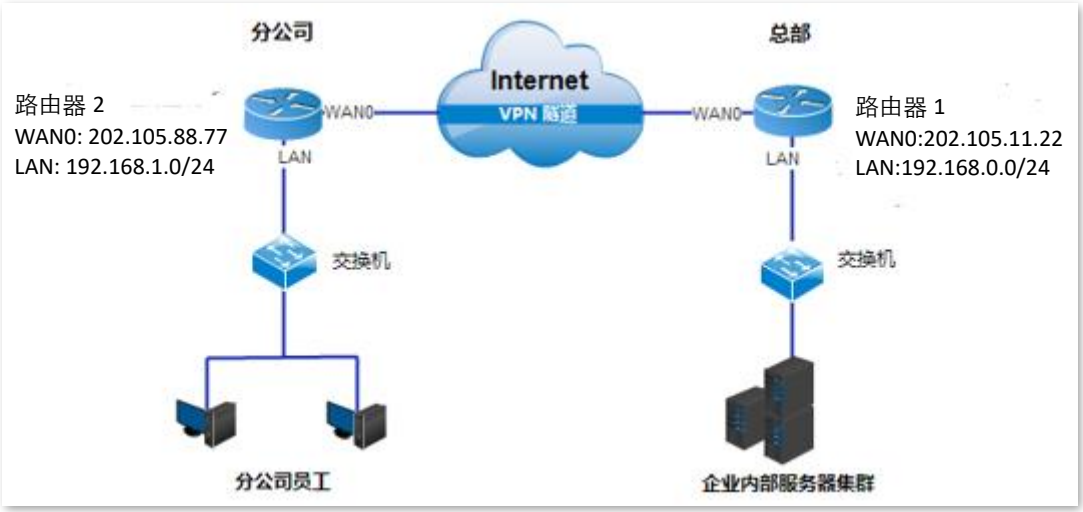


图9-62 IPsec VPN 组网拓扑

### 配置注意事项

- 配置过程中，如果需要设置 IPSec 连接的高级选项，请保持两台路由器的设置参数一致。
- 密钥协商方式为“手动设置”时，IPSec 两端的加密算法、加密密钥、认证算法需一致，多业务无线控制器 1 的外出 SPI 与多业务无线控制器 2 的进入 SPI 一致，路由器 1 的进入 SPI 与路由器 2 的外出 SPI 一致。

### 配置步骤

假设两台路由器的 IPSec 连接基本信息如下：

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

步骤1 设置路由器 1。

1. 登录到路由器 1 的 Web 管理页面，点击「更多设置」>「IPSec」进入设置页面。
2. 点击 +新增 。


图9-63 添加 IPSec

3. 在【新增】窗口配置各项参数，然后点击页面底端的 保存 。
   - 封装模式：选择“隧道模式”。
   - WAN 口：选择本条 IPSec 隧道绑定的 WAN 口，本例为“WAN0”。
   - 连接名称：为本条隧道设置一个名称，如“IPSec_1”。
   - 远端网关地址:输入对端多业务无线控制器上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.88.77”。
   - 本地内网网段/掩码：输入本多业务无线控制器内网的网段/子网掩码，本例为“192.168.0.0/24”。
   - 远端内网网段/掩码：输入对端多业务无线控制器内网的网段/子网掩码，本例为“192.168.1.0/24”。
   - 预共享密钥：本例为“12345678”。


图9-64 设置 IPSec 参数

添加完成，如下图示。


图9-65 成功添加 IPSec

步骤2 设置路由器 2。

1. 登录到路由器 2 的 Web 管理页面，点击「更多设置」>「IPSec」进入设置页面。
2. 点击 +新增 。


图9-66 添加多业务无线控制器 2 IPSec

3. 在【新增】窗口进行如下配置，然后点击页面底端的 保存 。
   - 选择本条 IPSec 隧道绑定的 WAN 口，本例为 “WAN0”。
   - 选择 “封装模式” 为 “隧道模式”。
   - 为本条隧道设置一个名称，如 “IPSec_1”。
   - 设置 “远端网关地址” 为对端多业务无线控制器上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为 “202.105.11.22”。
   - 输入本多业务无线控制器内网的网段/前缀长度，本例为 “192.168.1.0/24”。
   - 输入对端多业务无线控制器内网的网段/前缀长度，本例为 “192.168.0.0/24”。
   - 输入协商时所用的预共享密钥，本例为 “12345678”。

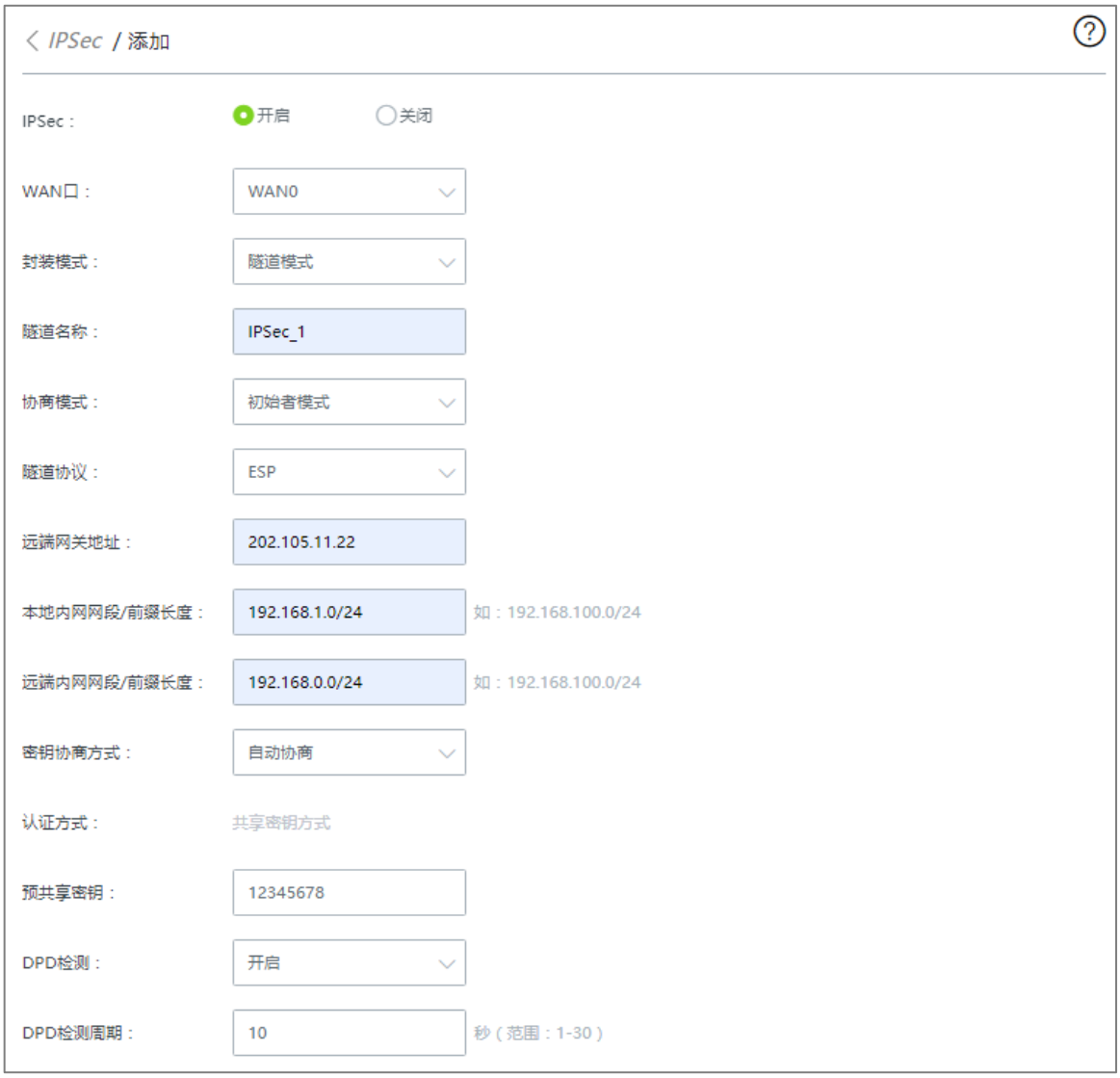


图9-67 设置 IPSec 参数

添加完成，如下图示。


图9-68 成功添加 IPSec

### 验证配置

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

## 9.11.4 L2TP over IPSec VPN 配置举例

### 组网需求

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

可以在路由器上设置 L2TP VPN 服务，实现远端用户经互联网安全访问企业内部局域网的需求。

### 网络拓扑

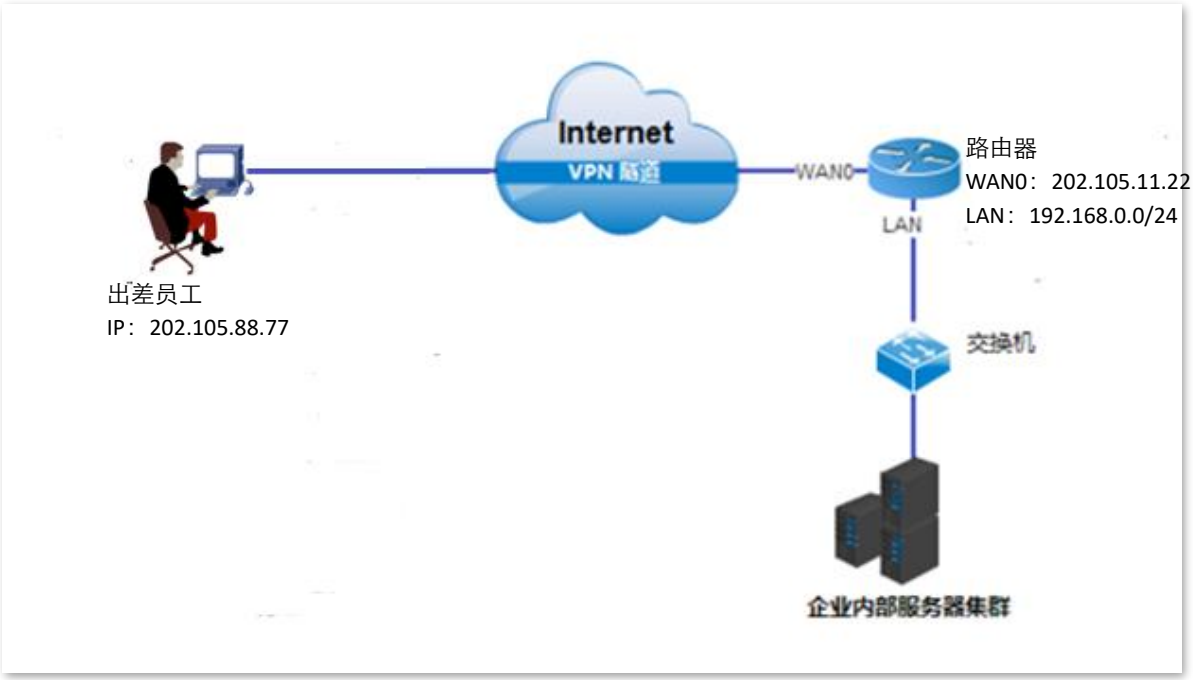


图9-69 L2TP over IPsec 网络拓扑

### 配置步骤

假设路由器的 IPSec 连接基本信息如下：

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

步骤1 建立 IPSec 连接。

1. 点击「更多设置」>「IPSec」。
2. 点击 +新增 。


图9-70 建立 IPsec 连接

3. 在【新增】窗口配置各项参数，然后点击 保存 。
   - 封装模式：选择“传输模式”。
   - WAN 口：选择本条 IPSec 连接绑定的 WAN 口，本例为“WAN0”。
   - 连接名称：为本条连接设置一个名称，如“公司总部”。
   - 预共享密钥：设置密码，用于出差员工建立 VPN 连接时输入，如“12345678”。


图9-71 建立 IPSec 连接

添加成功。


图9-72 成功建立 IPSec 连接

步骤2 开启 L2TP 服务器。

1. 点击「更多设置」>「VPN 服务器」，点击滑块至 。
2. 进行各项参数配置。
   - 服务器类型：选择 VPN 服务器的类型，本例为“L2TP”。
   - WAN 口：指定 VPN 服务器与终端设备建立隧道的出口，本例为“WAN0”。
   - IPSec 加密：选择已连接的 IPSec 隧道，本例为“公司总部”。
3. 点击页面底端的 保存 。


图9-73 开启 L2TP 服务器

步骤3 添加 L2TP 用户。

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


图9-74 添加 L2TP 用户

4. 在【新增】窗口配置下述参数，然后点击 保存 。

- 用户名：输入 VPN 终端设备进行 VPN 连接时所用的用户名，如“zhangsan”。
- 密码：输入对应用户名的密码，如“zhangsan”。
- 是否网段：选择“否”。
- 备注：输入该用户账号的描述信息，如“张三”。


图9-75 新增 L2TP 用户

添加完成，如下图示。


图9-76 成功添加 L2TP 用户

## 验证配置

### 出差员工进行 VPN 拨号

情景 1：在电脑上建立 VPN 与总部通信，请参考下文，以 Windows 10 为例说明。

步骤1 建立 VPN 连接。

1. 点击桌面右下角图标，选择“网络和 Internet 设置”。


图9-77 打开网络和 Internet 设置

2. 点击“VPN”，点击“添加 VPN 连接”。


图9-78 添加 VPN 连接

3. 设置“VPN 连接”的相关参数。
   - 选择“VPN 提供商”为“Windows（内置）”。
   - 设置 VPN 连接名称，如“VPN 访问”。
   - 输入 VPN 服务器的 IP 地址，本例为“202.105.11.22”。
   - 选择 VPN 类型，本例为“使用预共享密钥的 L2TP/IPsec”。
   - 输入 IPSec 隧道设置的预共享密钥，本例为“12345678”。
   - 向下拉动滚动条，选择登录信息的类型，本例为“用户名和密码”。
   - 输入 L2TP 服务器允许拨入的用户名及其密码，本例均为“zhangsan”。

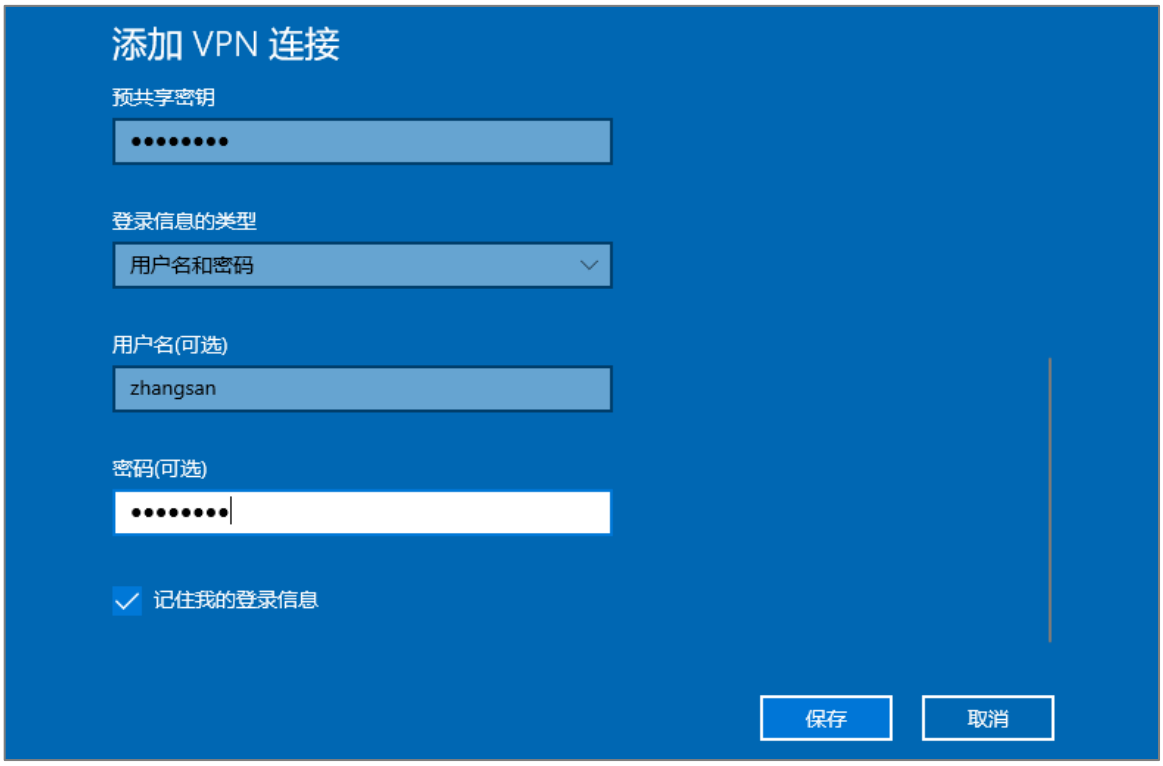


图9-79 设置 VPN 连接相关参数

步骤2 VPN 拨号。

点击“VPN 访问”，点击 连接 。


图9-80 VPN 访问

稍等片刻，连接成功。即可根据总部提供的账号信息进行访问。


图9-81 VPN 连接成功

情景 2：使用移动设备建立 VPN 连接访问公司总部时，请参考下文，以 iOS 系统为例说明。

步骤1 在手机界面上找到并点击“设置”图标。

步骤2 点击“VPN”。


图9-82 手机设置 VPN

步骤3 点击“添加 VPN 配置...”。


图9-83 添加 VPN 配置

步骤4 设置 VPN 相关参数。

- 类型：点击选择“L2TP”。
- 描述：设置此 VPN 连接的名称，如“总部”。
- 服务器：输入 L2TP 服务器的 IP 地址，本例为“202.105.11.22”。
- 帐户/密码：输入 L2TP 服务器允许拨入的用户及其密码，本例均为“zhangsan”。
- 密钥：输入 IPSec 隧道设置的预共享密钥，本例为“12345678”。
- 点击“完成”。


图9-84 添加 VPN 配置

步骤5 点击 。稍等片刻，当“状态”变为“已连接 ”时，拨号成功。


图9-85 开启 VPN 连接


图9-86 成功连接 VPN 连接

## 出差员工访问总部

下文以访问总部 FTP 服务器内容为例。公司总部的项目资料放在 FTP 服务器中，假设服务器信息如下：

- FTP 服务器 IP 地址：192.168.0.104

- 服务器端口：21
- FTP 服务器登录用户名和密码均为 zhangsan

访问步骤：

步骤1 在电脑上打开浏览器，访问“ftp://服务器 IP 地址:服务端口号”，本例为 ftp://192.168.0.104。

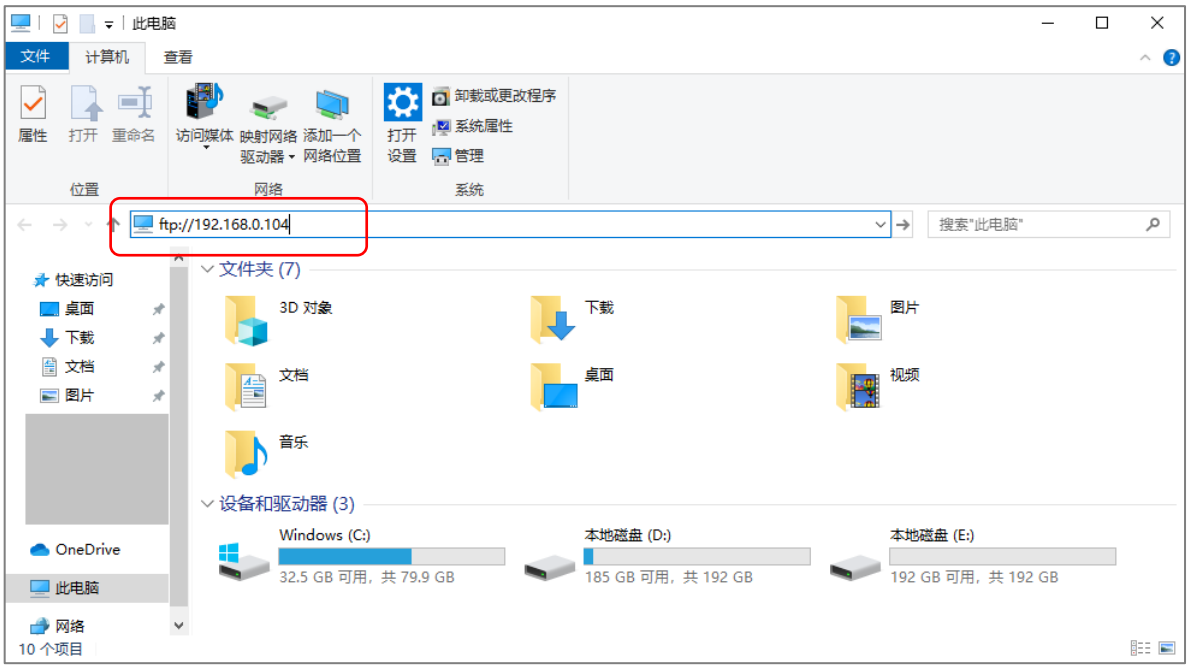


图9-87 访问服务器 IP 地址

**注意**

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

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

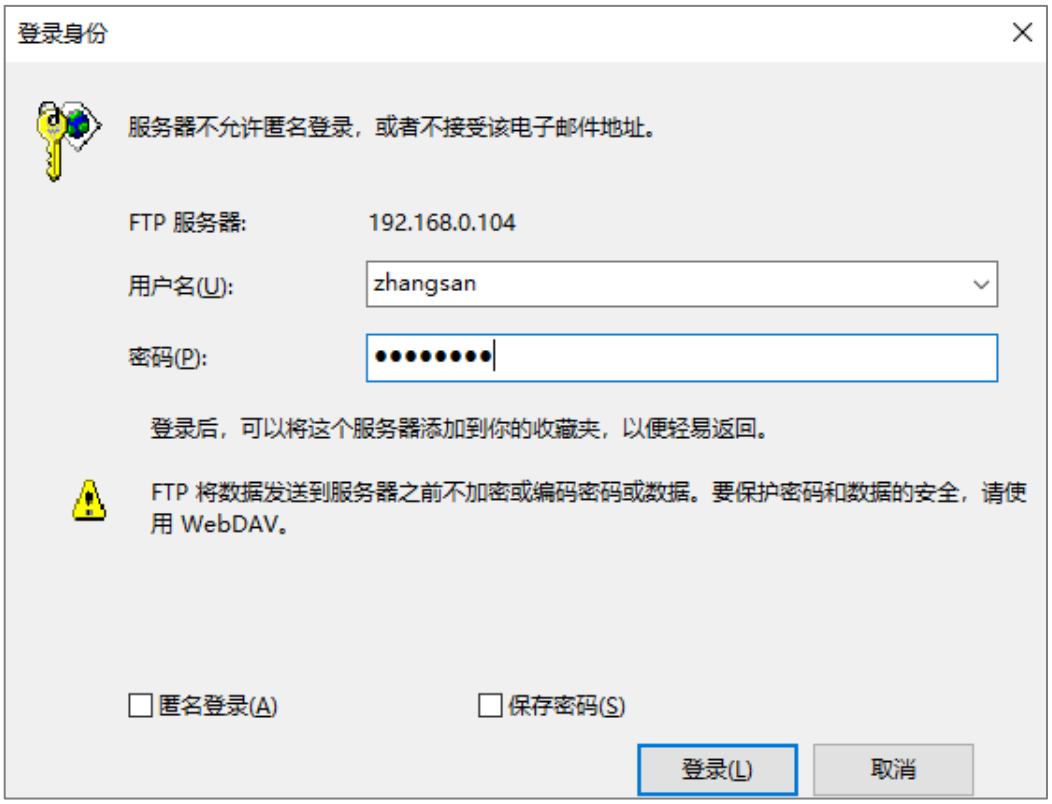


图9-88 输入登录用户名和密码

访问成功。

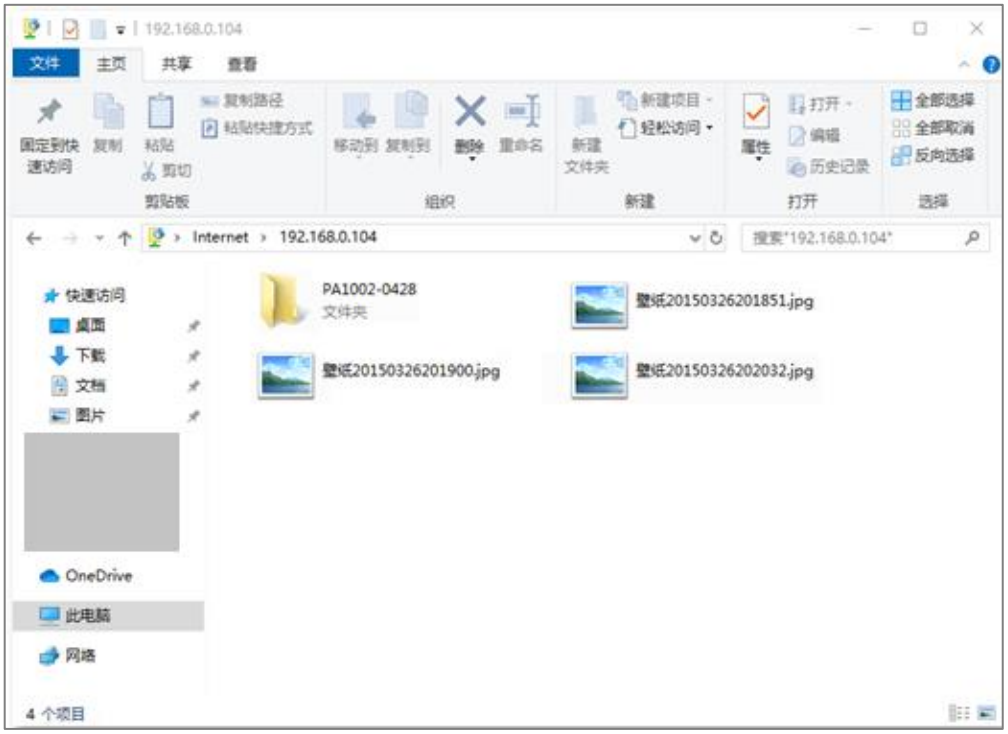


图9-89 访问成功

# 9.12 多 WAN 策略

## 9.12.1 概述

进入页面：点击「更多设置」>「多 WAN 策略」。

在“多 WAN 策略”模块，您可以设置多 WAN 策略和广域网线路检测。

- 多 WAN 策略

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

- 广域网线路检测

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

进入页面后，默认显示如下。


图9-90 多 WAN 策略

表9-15 多 WAN 策略参数说明

| 标题项 | 说明 |
| --- | --- |
| 多 WAN 策略 | 路由器多个 WAN 口同时工作时采用的数据转发策略。<br>● 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。<br>● 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。 |
| 广域网线路侦测 | 开启后，路由器会周期性地检测 WAN 口与“检测地址”的连通情况。 |
| 检测地址 | 需检测的目标主机的 IP 地址或域名。 |
| 检测间隔 | 路由器检测 WAN 口与“检测地址”连通情况的周期。 |

## 9.12.2 自定义多 WAN 策略

### 开启自定义多 WAN 策略功能

步骤1 点击「更多设置」>「多 WAN 策略」。

步骤2 选择“多 WAN 策略”为“自定义”。

步骤3 点击页面底端的 保存 。


图9-91 自定义多 WAN 策略

开启自定义多 WAN 策略功能后，您就可以自定义多 WAN 策略规则了。

### 自定义多 WAN 策略规则

步骤1 在「更多设置」>「多 WAN 策略」页面，点击 +新增 。

步骤2 在【新增】窗口进行参数配置。

步骤3 点击 保存 。


图9-92 新增多 WAN 策略

表9-16 多 WAN 策略参数说明

| 标题项 | 说明 |
| --- | --- |
| IP 组 | 选择引用的 IP 组，以指定规则对应的用户。IP 组应事先在「行为管理」>「IP 组与时间组」页面配置。 |
| 指定 WAN 口 | 对应 IP 组数据流量使用的 WAN 口。 |

## 9.12.3 自定义多 WAN 策略配置举例

### 组网需求

**错误!未找到引用源。**，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 的计算机通过电信宽带访问互联网。
- IP 地址为 192.168.0.101~192.168.0.200 的计算机通过移动宽带访问互联网。

可以使用路由器的多 WAN 策略功能实现上述需求。

## 网络拓扑

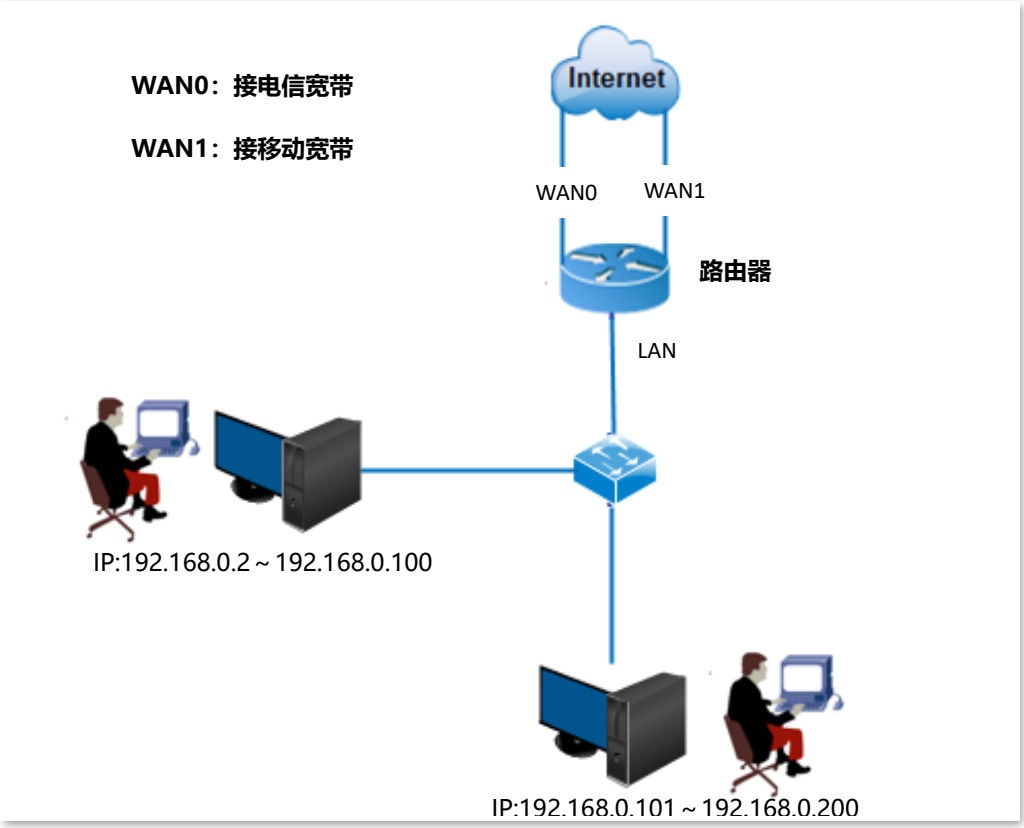


图9-93 自定义多 WAN 策略网络拓扑

## 配置步骤

步骤1 配置 IP 组。

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

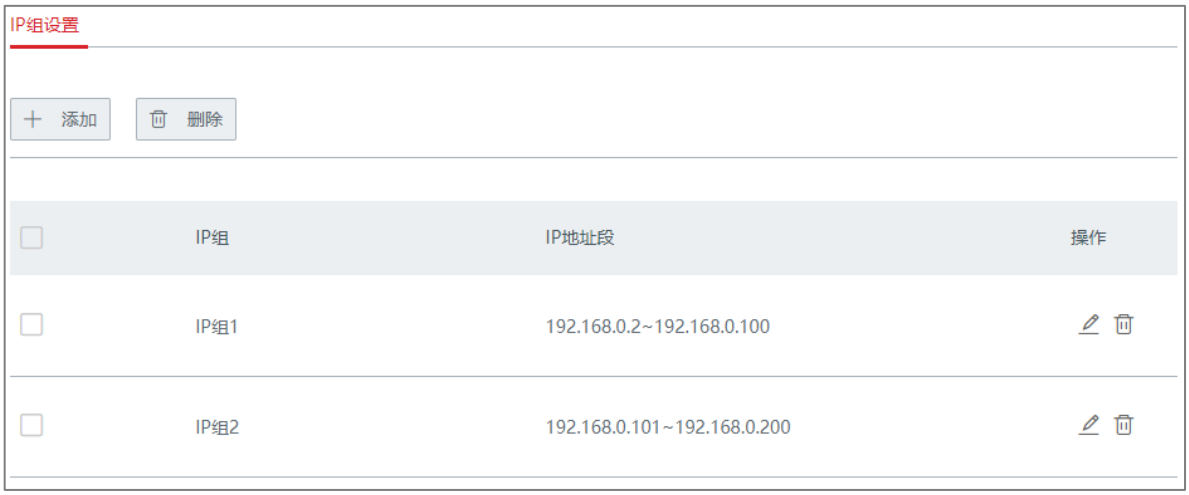


图9-94 IP 组设置

步骤2 自定义多 WAN 策略。

1. 开启自定义多 WAN 策略功能。


图9-95 开启自定义多 WAN 策略

2. 配置多 WAN 策略。

点击「更多设置」>「多 WAN 策略」，添加如下多 WAN 策略。


图9-96 成功添加多 WAN 策略

## 验证配置

局域网中 192.168.0.2~192.168.0.100 设备的数据将会走 WAN0 口；
192.168.0.101~192.168.0.250 设备的数据将会走 WAN1 口。

## 9.13 高级设置

在“高级设置”模块，您可以将路由器接入萤石云。

进入页面：点击「更多设置」>「高级设置」。进入页面后，默认显示如下。


图9-97 高级设置

表9-17 高级设置参数说明

| 标题项 | 说明 |
| --- | --- |
| 启用 | 勾选启用之后，设备会接入萤石云平台。启用之前，请确保设备已接入公网。 |
| 平台接入方式 | 目前只支持接入萤石云。 |
| 接入服务器 IP | 萤石云平台服务器的 IP 地址。用户也可自定义接入服务器的 IP 地址。 |
| 连接状态 | 设备连接到萤石云平台的状态。 |
| 操作码 | 用户通过海康互联 App 添加设备时，设备定义的验证用户对该设备具有所有权的凭证。 |

# 第10章 系统维护

## 10.1 重启

当您设置的某项参数不能正常生效时，可以尝试重启路由器解决。

进入页面：点击「系统维护」>「重启」。

确认信息后，点击 重启 。


图10-1 重启设备

## 10.2 升级

### 10.2.1 概述

使用升级功能，可以对路由器进行软件升级。

软件升级：您可以通过升级软件，体验更多功能，获得更好的用户体验。路由器支持“本地升级”。


图10-2 升级功能

表10-1 软件升级参数说明

| 标题项 | 说明 |
| --- | --- |
| 本地升级 | 先访问我们官方网站，下载对应型号的路由器的升级文件到本地电脑，然后再进行升级。 |

### 10.2.2 软件本地升级

**注意**

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

步骤1 访问我们官方网站，下载对应型号的路由器升级软件到本地电脑并解压。

步骤2 进入路由器的「系统维护」>「升级」页面，找到“软件升级”模块。

步骤3 选择“升级方式”为“本地升级”。

步骤4 点击 浏览 。

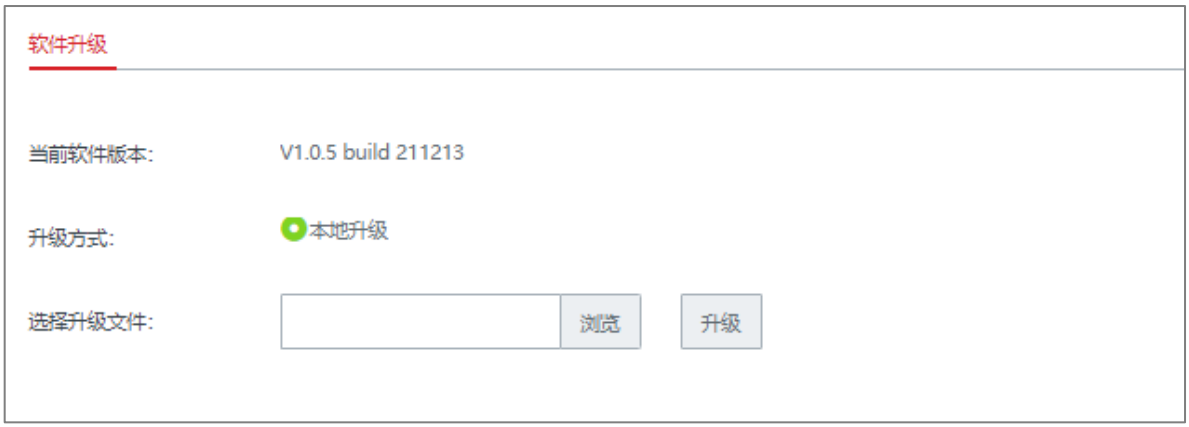


图10-3 软件本地升级

步骤5 找到并载入相应目录下已解压的升级软件（文件后缀为.bin）。

步骤6 点击 升级 。

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

## 10.3 复位

### 10.3.1 概述

进入页面：点击「系统维护」>「复位」。

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

复位后，路由器的默认 LAN 口 IP 地址为 192.168.0.252。

**注意**

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

## 10.3.2 软件复位

在「系统维护」>「复位」页面，确认信息后，点击 恢复出厂设置 。

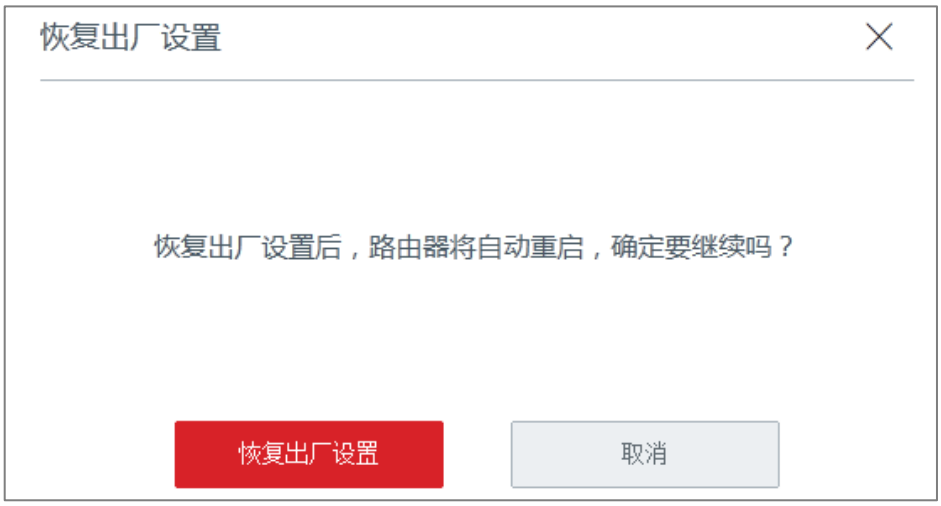


图10-4 恢复出厂设置

## 10.3.3 硬件复位

使用此方式时，您无需进入路由器管理页面就可以复位路由器。操作方法如下：

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

## 10.4 密码管理

### 10.4.1 概述

进入页面：点击「系统维护」>「密码管理」。

在这里，您可以修改路由器的管理员密码。

### 10.4.2 修改登录密码

步骤1 点击「系统维护」>「密码管理」。

步骤2 修改登录密码。


图10-5 修改登录密码

步骤3 点击页面底端的 保存 。

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

# 10.5 定时重启

## 10.5.1 概述

进入页面：点击「系统维护」>「定时重启」。

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

## 10.5.2 定时重启路由器

步骤1 点击「系统维护」>「定时重启」。

步骤2 点击滑块至  。

步骤3 选择路由器自动重启的时间点，如“3 时 0 分”。

步骤4 设置重启日期。

步骤5 点击页面底端的 保存 。


图10-6 定时重启

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。

# 10.6 备份与恢复

## 10.6.1 概述

进入页面：点击「系统维护」>「备份与恢复」。

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

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

## 10.6.2 备份配置

步骤1 点击「系统维护」>「备份与恢复」。

步骤2 点击 备份 。

**说明**

**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”。**


图10-7 备份与恢复

浏览器将下载文件名为 RouterCfm.cfg 的配置文件。

## 10.6.3 恢复配置

步骤1 点击「系统维护」>「备份与恢复」。

步骤2 点击 浏览 ，选择并加载之前备份的配置文件（文件后缀为.cfg）。


图10-8 加载备份文件

步骤3 点击 恢复 。


图10-9 点击恢复

将出现重启进度提示，请耐心等待。路由器重启后配置恢复完成。

# 10.7 系统日志

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

进入页面：点击「系统维护」>「系统日志」。

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


图10-10 系统日志

日志记录时间以路由器的系统时间为准，如果要让日志记录时间准确，请先确保路由器的系统时间准确。可以到系统时间页面校准路由器的系统时间。

**说明**

- 路由器重启后，之前的日志信息将丢失。
- 断电后重新通电、软件升级、备份/恢复设置、恢复出厂设置等操作都会导致路由器重启。

# 10.8 诊断工具

## 10.8.1 概述

进入页面：点击「系统维护」>「诊断工具」。

在这里，您可以进行 Ping/Traceroute 检测。

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

## 10.8.2 执行 Ping

假设要检测路由器到百度服务器的链路是否畅通。

步骤1 点击「系统维护」>「诊断工具」。

步骤2 选择“诊断工具”为“Ping”。

步骤3 输入目的 IP 地址或域名，本例为“www.baidu.com”。

步骤4 设置 ping 发送的数据包的个数，建议保持默认设置。

步骤5 设置 ping 发送的数据包的大小，建议保持默认设置。

步骤6 点击 开始 。

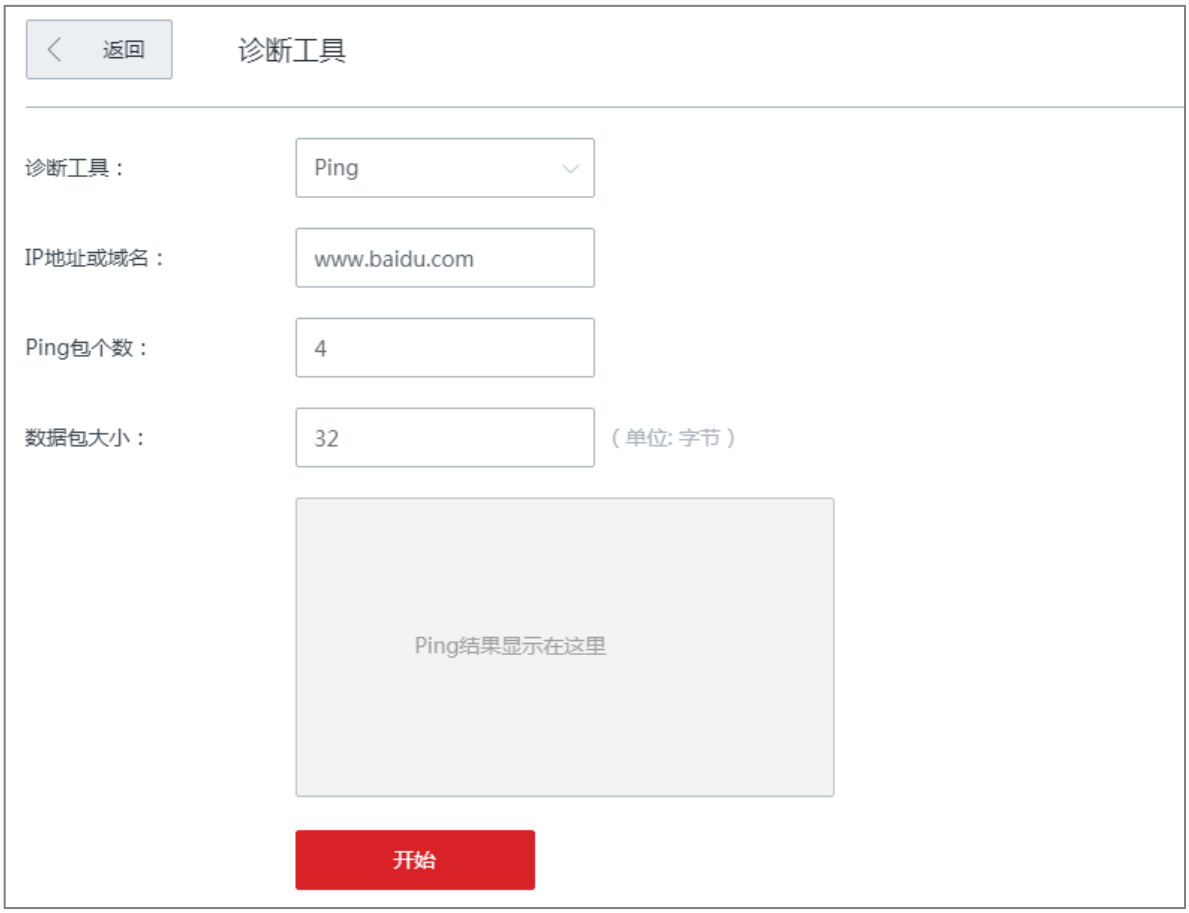


图10-11 执行 Ping

稍后，诊断结果将显示在页面下方。如下图示。

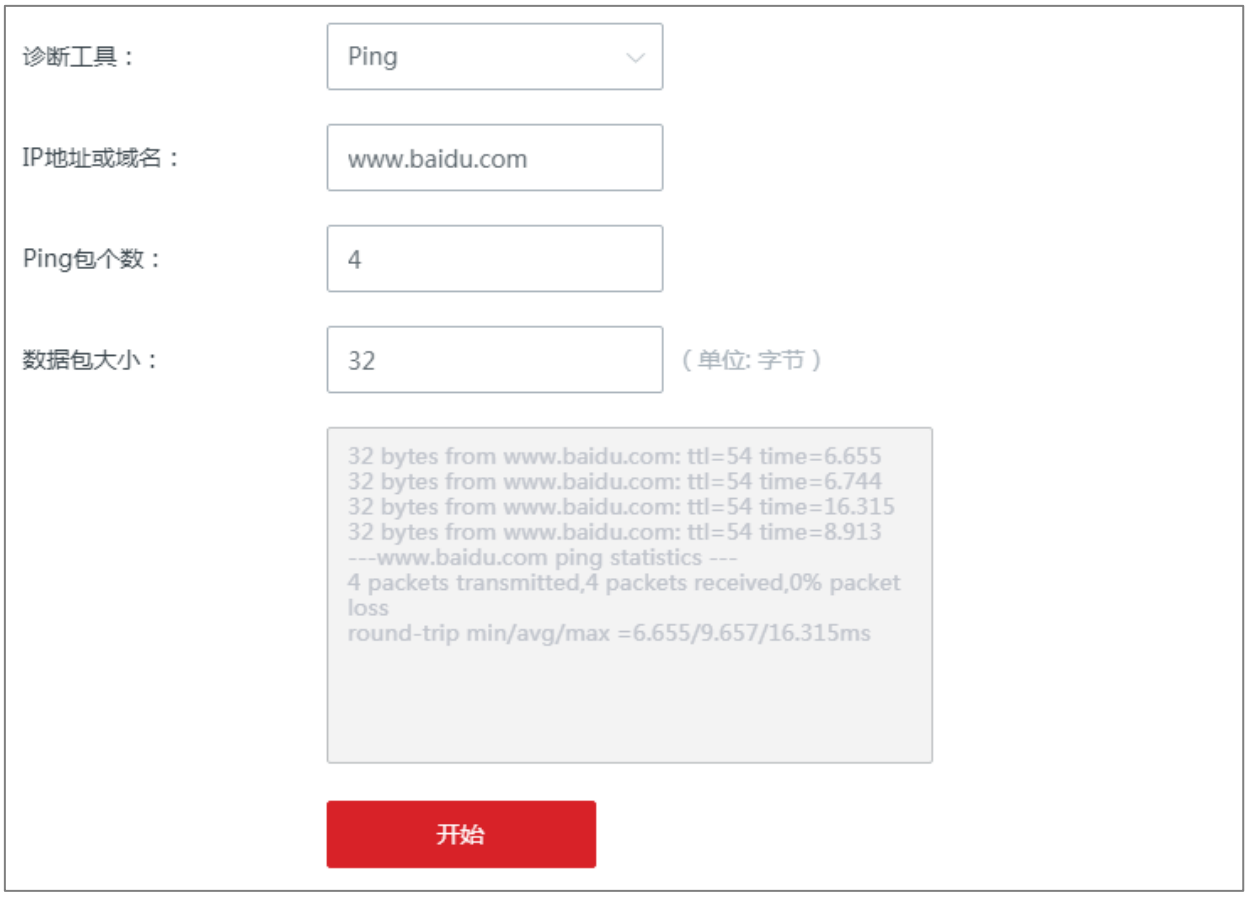


图10-12 诊断结果

### 10.8.3 执行 Traceroute

假设要检测路由器到百度服务器所经过的路由。

步骤1 点击「系统维护」>「诊断工具」。

步骤2 选择“诊断工具”为“Traceroute”。

步骤3 输入目的 IP 地址或域名，本例为“www.baidu.com”。

步骤4 点击 开始 。


图10-13 执行 Traceroute

稍后，诊断结果将显示在页面下方。如下图示。

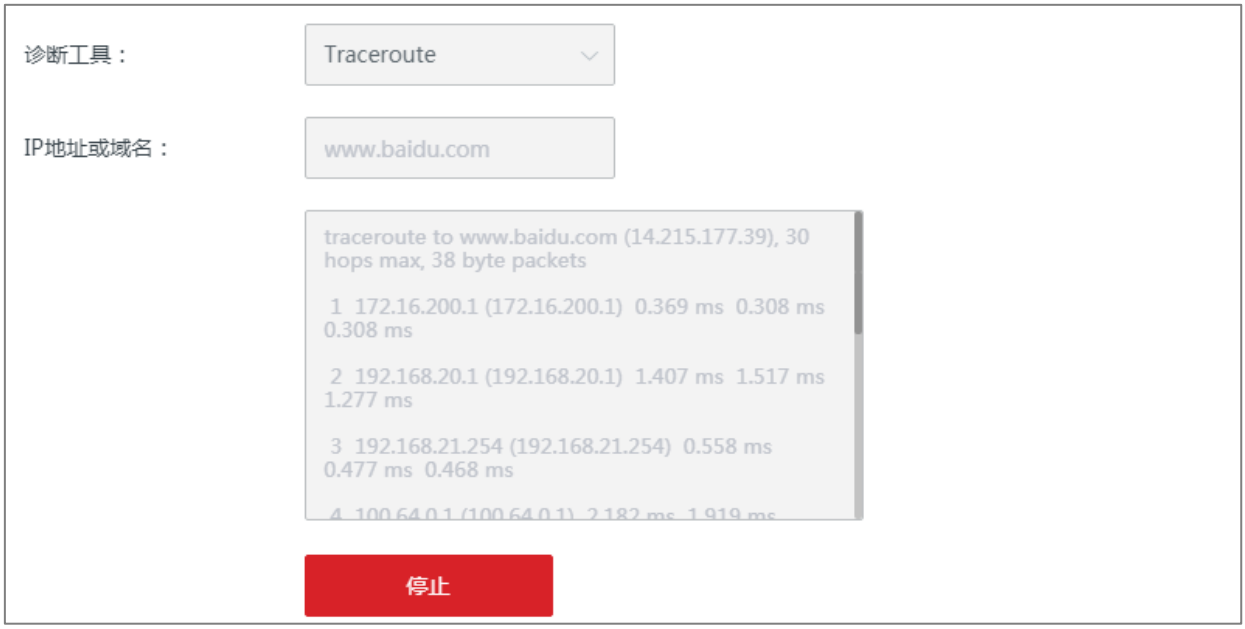


图10-14 诊断结果

# 10.9 系统时间

在“系统时间”页面，您可以设置路由器的系统时间。

为了保证路由器上行为管理等涉及时间的功能正常生效，需要确保路由器的系统时间准确。路由器支持“网络校时”和“手动配置”两种时间设置方式，默认为“网络校时”。

点击「系统维护」>「系统时间」进入页面。

## 10.9.1 网络校时

系统时间自动同步互联网上的时间服务器。使用此方式时，只要路由器成功连接至互联网就能自动校准其系统时间，即使路由器重启后，也能自行校准，无需网络管理员重新设置。


图10-15 网络校时

表10-2 网络校时参数说明

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

设置完成后，您可以进入「系统状态」页面，查看路由器的系统时间是否校对正确。

## 10.9.2 手动配置

网络管理员手动配置路由器的系统时间。如果使用此方式，则路由器每次重启后，您都需要重新设置路由器的系统时间。选择“手动配置”时，页面展开的相关参数如下图所示。


图10-16 系统时间

表10-3 系统时间参数说明

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

设置完成后，您可以进入「系统状态」页面，查看路由器的系统时间是否校对正确。

# 10.10 功能使用列表

进入页面：点击「系统维护」>「功能使用列表」。

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


图10-17 功能使用列表

# 附录A 缩略语

表A-1 缩略语

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

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


杭州海康威视数字技术股份有限公司
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.
www.hikvision.com
服务热线：400-800-5998