www.ip-com.com.cn

Web 配置指南

IP-COM 企业免布线无线覆盖系统

IP-COM

无线网络解决方案专家

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。

本手册介绍 IP-COM 企业免布线产品 Web 页面的各种功能，文中如无特别说明，Web 页面截图均以 EW12 为例。

提示

不同型号产品的 Web 页面功能存在差异，请在实际使用中以设备实际显示的 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 。
窗口	【】	在【新增】窗口。

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	表示有助于节省时间或资源的方法。

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	描述
产品彩页	帮助您了解设备的基本参数。包括产品概述、产品卖点、产品规格等。

文档名称	描述
快速安装指南	帮助您快速设置设备联网。包括设备的上网设置指导、指示灯/接口/按钮说明、常见问题解答、保修条款等。
Web 配置指南	帮助您了解设备的更多功能配置。包括设备 Web 界面上的所有功能介绍。

技术支持

如需了解更多信息，请通过以下方式与我们联系。

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

目录

1 登录 Web 管理界面

1.1 登录

如果您是首次使用本设备或已将本设备恢复出厂设置，请参考相应型号免布线设备的快速安装指南（前往 www.ip-com.com.cn 可下载快速安装指南）。否则，请参考下文。

1.1.1 登录免布线路由模式设备

提示

- 免布线路由模式下，设备的 PoE WAN/LAN1 接口为 WAN 口。
- 设备默认工作在免布线路由模式。

使用电脑登录

1. 用网线将管理电脑接到免布线设备的内网接口（LAN）。
2. 打开电脑上的浏览器（如 IE），访问免布线设备的管理地址“www.ipcwifi.com”。

3. 在登录页面输入登录密码，点击 登录 。

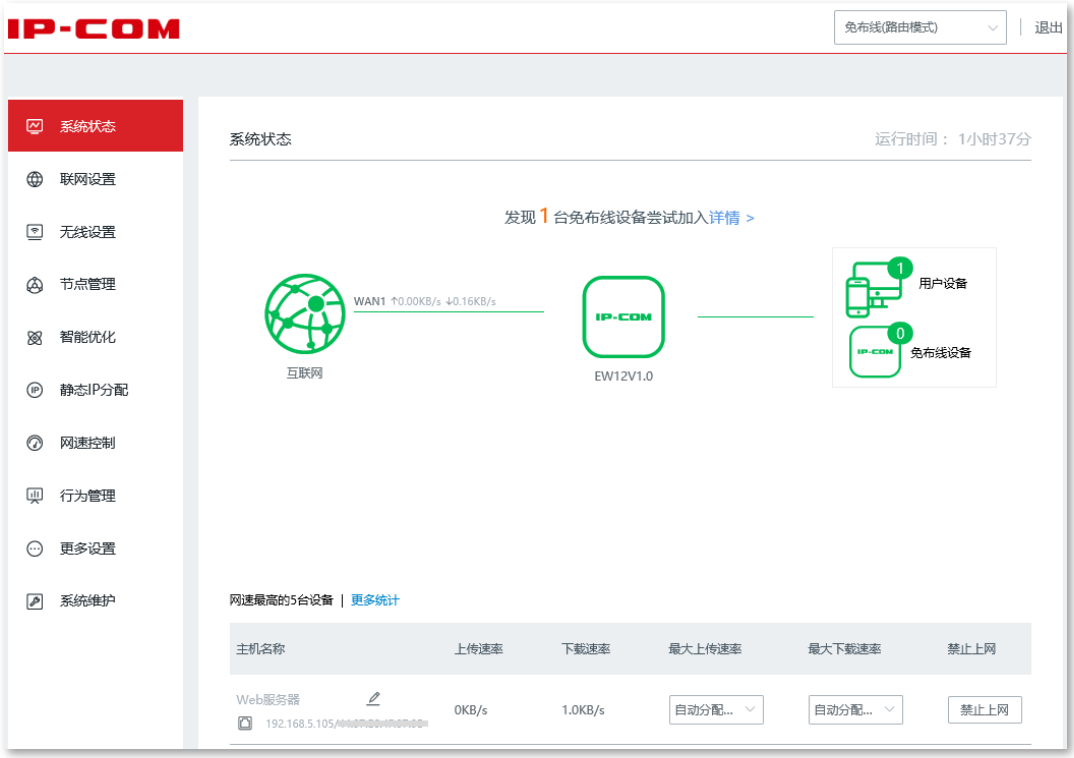
提示

若未出现上述页面，请尝试使用以下方法解决：

- 确保免布线设备通电正常。
- 确保电脑已连接到免布线设备的 LAN 口，且电脑的以太网（或本地连接）IP 地址已设为自动获得 IP 地址，自动获得 DNS 服务器地址。
- 将免布线设备恢复到出厂设置，然后重新登录。恢复出厂设置方法：免布线设备系统已启动的状态下（SYS 灯闪烁），用尖状物按住复位按钮（RESET）约 8 秒，当 SYS 灯长亮时松开，设备将会恢复出厂设置。当 SYS 灯重新闪烁时，恢复出厂设置完成。

----完成

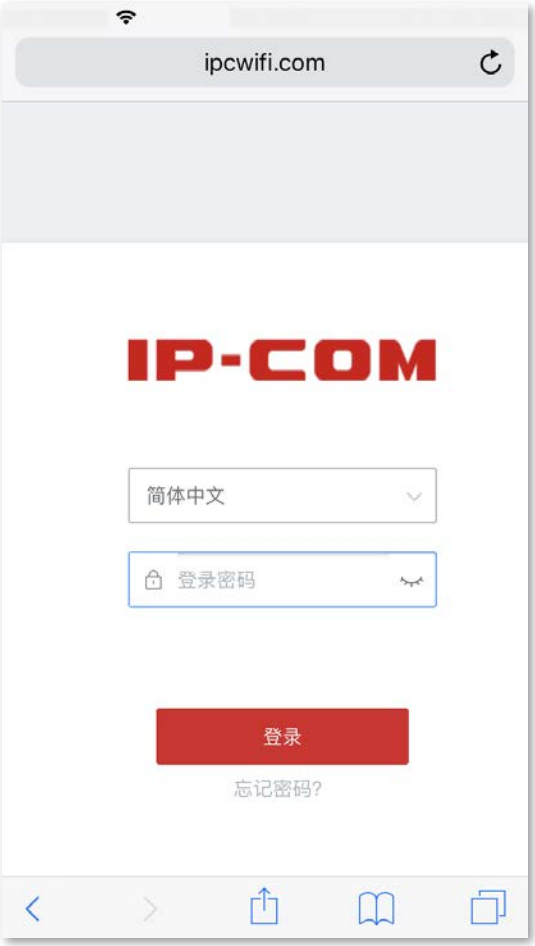
成功登录免布线设备的管理页面。



使用手机/平板登录

此处以手机为例，平板类似。

1. 手机连接到免布线网络的 WiFi。
2. 打开手机上的浏览器，在地址栏（非搜索栏）输入免布线设备的管理地址“www.ipcwifi.com”并访问。
3. 在登录页面输入登录密码，点击 登录 。



提示

若未出现上述页面，请尝试使用以下方法解决：

- 确保手机已成功连接免布线网络的 WiFi。
- 确保已关闭手机数据流量。
- 将免布线设备恢复到出厂设置，然后重新登录。恢复出厂设置方法：免布线设备系统已启动的状态下（SYS 灯闪烁），用尖状物按住复位按钮（RESET）约 8 秒，当 SYS 灯长亮时松开，设备将会恢复出厂设置。当 SYS 灯重新闪烁时，恢复出厂设置完成。

----完成

成功登录免布线设备的管理页面。

1.1.2 登录免布线 AP 模式设备

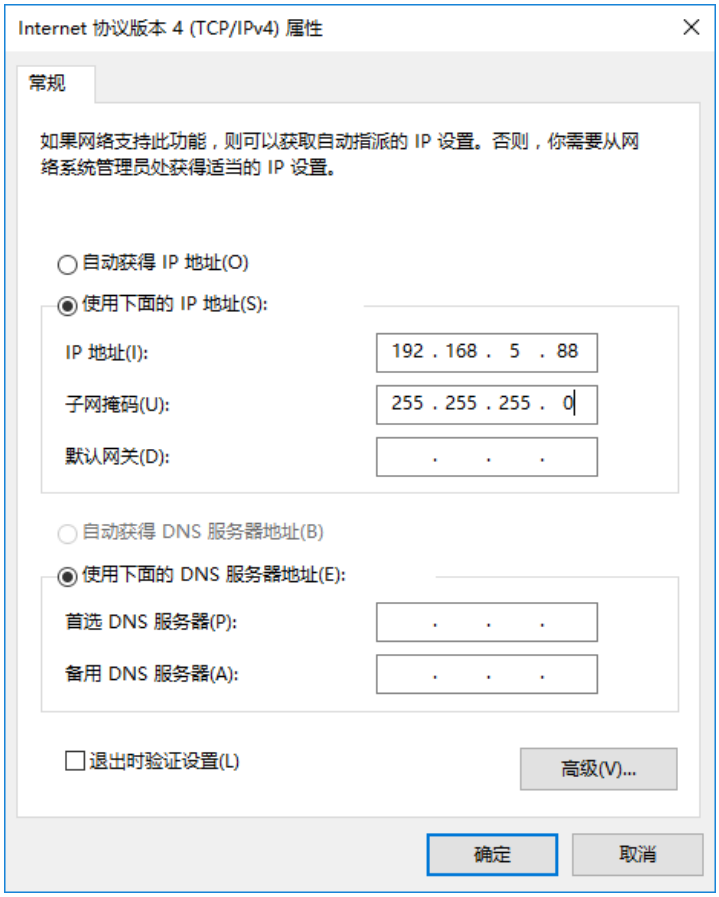
提示

免布线 AP 模式下，设备的 PoE WAN/LAN1 接口为 LAN 口。

使用电脑登录

1. 用网线将管理电脑接到免布线设备的内网接口（LAN）。
2. 设置电脑的以太网（或本地连接）IP 地址，使其和免布线设备的 IP 地址在同一网段。

   例如：免布线设备的 IP 地址为 192.168.5.1，则电脑的 IP 地址可以设为“192.168.5.X”（X 为 2~254，且未被其它设备占用），子网掩码为“255.255.255.0”。



3. 打开电脑上的浏览器（如 IE），访问免布线设备的管理 IP 地址，本例为“192.168.5.1”。

4. 在登录页面输入登录密码，点击 登录 。

提示

若未出现上述页面，请尝试使用以下方法解决：

- 确保免布线设备通电正常。
- 确保电脑已连接到免布线设备的 LAN 口，且电脑的以太网（或本地连接）IP 地址已设为与免布线设备的 IP 地址在同一网段。

----完成

成功登录免布线设备的管理页面。

使用手机/平板登录

此处以手机为例，平板类似。

1. 手机连接到免布线设备的 WiFi。
2. 手动配置手机的 IP 地址，使其和免布线设备的 IP 地址在同一网段。

   例如：免布线设备的 IP 地址为 192.168.5.1，则手机的 IP 地址可以设为“192.168.5.X”（X 为 2~254，且未被其它设备占用），子网掩码为“255.255.255.0”。
3. 打开手机上的浏览器，在地址栏（非搜索栏）输入免布线设备的管理 IP 地址（本例为“192.168.5.1”）并访问。
4. 在登录页面输入登录密码，点击 登录 。

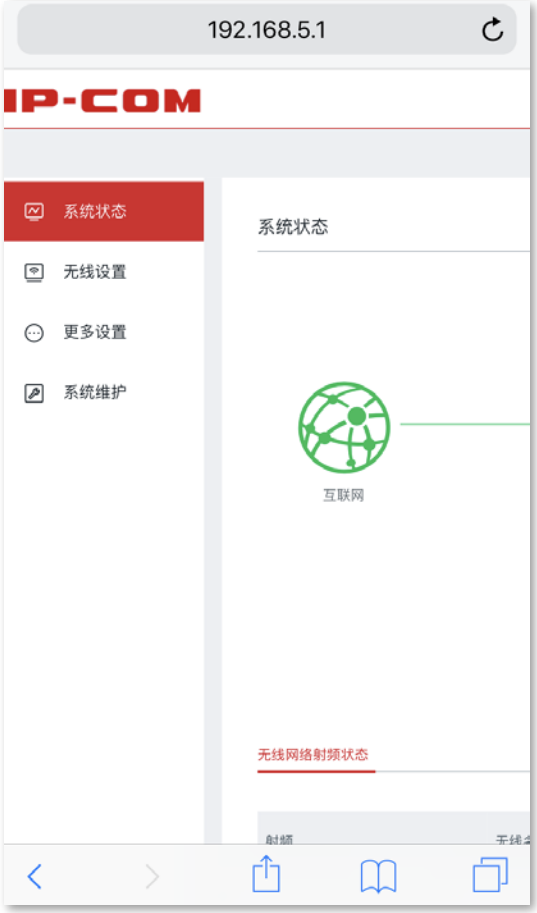
提示

若未出现上述页面，请尝试使用以下方法解决：

- 确保手机已成功连接免布线设备的 WiFi。
- 确保已关闭手机数据流量。

----完成

成功登录免布线设备的管理页面。



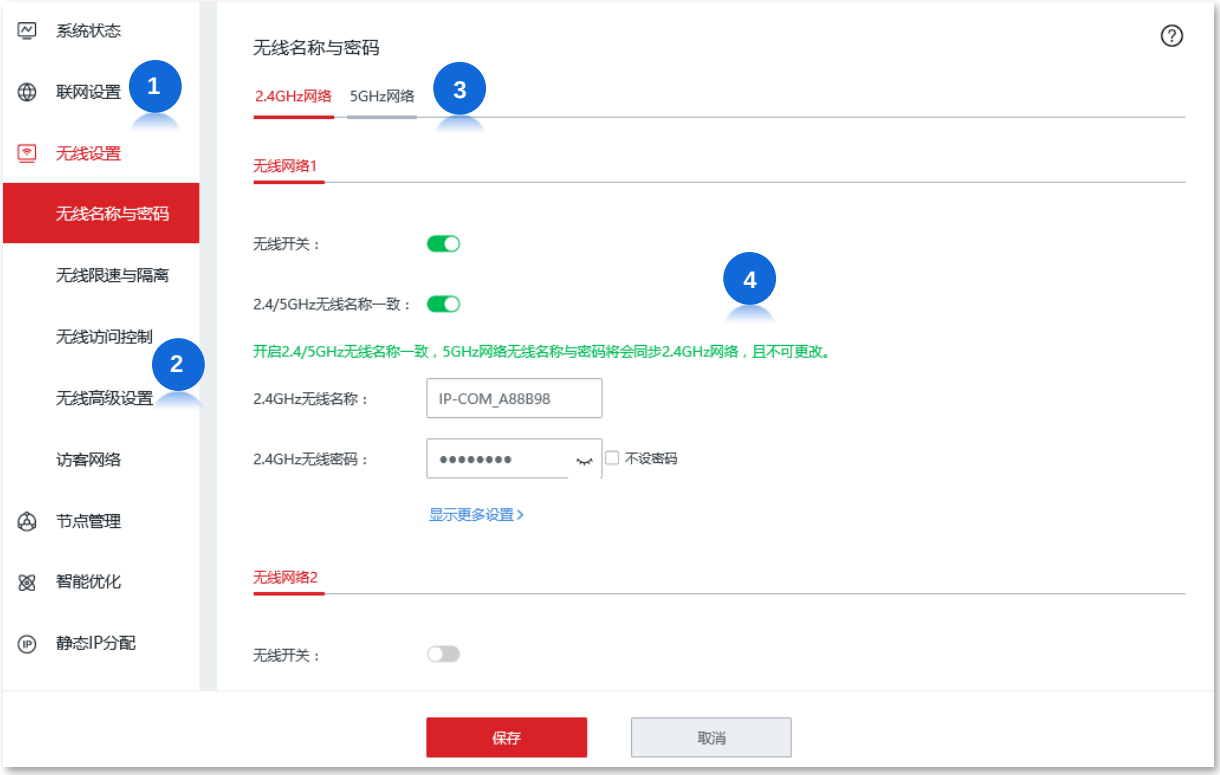
1.2 退出登录

您登录到免布线设备的管理页面后，如果在 20 分钟内没有任何操作，将自动退出登录。此外，在管理页面上，点击右上角的 退出 ，也可以安全地退出管理页面。

2 Web 界面简介

2.1 页面布局

免布线设备的管理页面共分为：一级导航栏、二级导航栏、页签和配置区四部分。如下图所示。



提示

管理页面上显示为灰色的功能或参数，表示免布线设备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免布线设备的功能菜单。用户在导航栏中可以方便地选择功

序号	名称	说明
❷	二级导航栏	能菜单，选择结果显示在配置区。
❸	页签	
❹	配置区	用户进行配置或查看配置的区域。

2.2 常用元素

免布线设备管理页面中常用元素的功能介绍如下表。

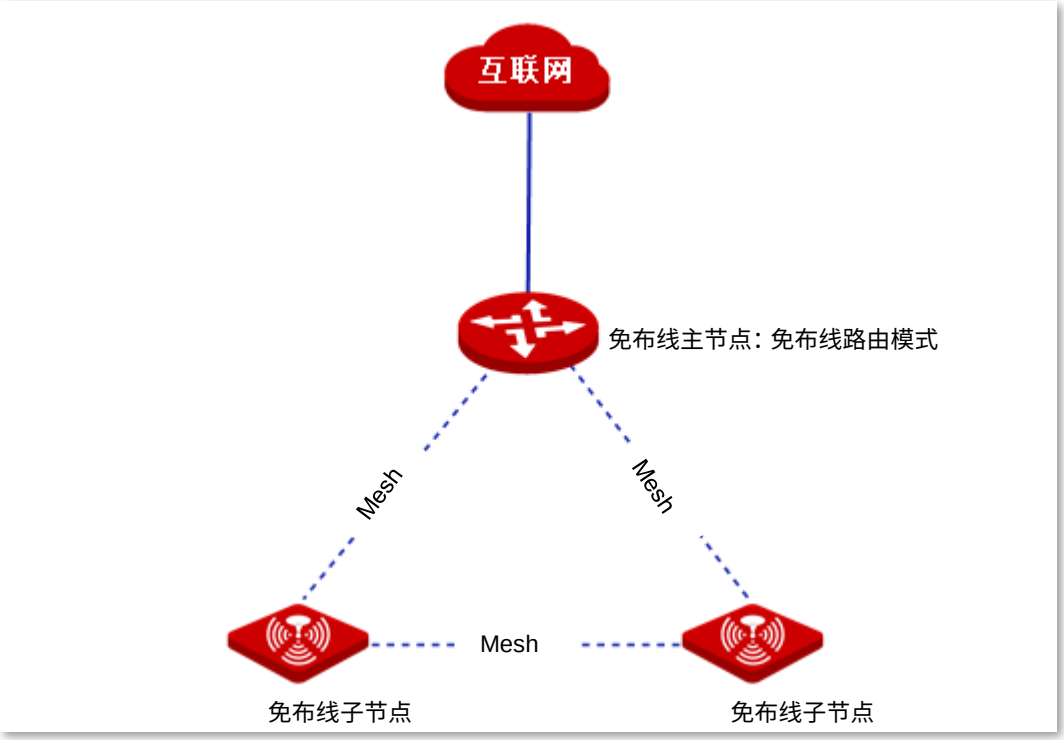
常用元素	说明
保存	用于保存当前页面配置，并使配置生效。
取消	用于取消当前页面未保存的配置，并恢复到修改前的配置。
刷新	用于刷新当前的页面信息。
?	用于查看当前页面的设置帮助信息。
免布线(路由模式)	点击下拉框，选择并切换免布线设备的工作模式。 支持在免布线路由模式和免布线 AP 模式之间切换。
+ 新增	用于新建一条规则或策略。
删除	用于删除选中的规则、策略或信息。
	用于修改对应的规则、策略或信息。
	用于删除对应的规则、策略或信息。
，	开关。表示开启，表示关闭。
主机名称/IP/MAC	用于搜索页面相关内容。搜索栏支持的关键字见搜索栏预置内容。

3 免布线路由模式

免布线设备默认工作在免布线路由模式。

此模式下，免布线设备作为路由器，提供互联网接入，可与其它免布线设备组成一个独立的免布线网络。

应用拓扑图如下。



提示

免布线路由模式节点的“PoE WAN/LAN1”口为 WAN 口，通常连接到 Modem（如光猫）或宽带网口，并通过宽带拨号、动态 IP 或静态 IP 联网方式连接到互联网。

3.1 系统状态

在「系统状态」模块，您可以：

- 查看连线状态及设备信息
- 添加免布线子节点
- 查看流量统计
- 管理在线用户
- 添加/移出黑名单

3.1.1 查看连线状态及设备信息

进入页面：点击「系统状态」。

在这里，您可以查看免布线路由模式节点的物理连线是否正常，也可以查看和设置免布线网络各节点的基本信息。

查看连线状态

当互联网与免布线路由模式节点之间线路正常，如下图示，表示 WAN 口网线连接正常。

当互联网与主节点之间线路打叉，如下图示，表示 WAN 口网线连接异常，请检查并接好 WAN 口网线。

查看免布线主节点信息

点击“系统状态”页面中与互联网直连的免布线设备，进入设备信息窗口。在这里，您可以查看免布线主节点的设备基本信息、运行状态、LAN 口状态、WAN 口状态。

基本信息

参数说明

标题项	说明
设备位置	节点的位置信息。建议设置为节点的安装位置描述，方便在管理时，快速定位节点。 您可以选择内置的位置描述，也可以自定义。
LED 开关	开启/关闭节点的指示灯。 开启后，您可根据指示灯判断节点的工作状态。默认为“开启”。

标题项	说明
SN	节点的序列号。
软件版本	节点系统软件的版本号。

运行状态

参数说明

标题项	说明
设备名称	节点的名称描述。
工作模式	节点当前的工作模式。 – 免布线主节点：节点作为免布线网络的主节点，上联到有线网络，是免布线网络中唯一访问外部网络的出口，实现 Mesh 网络和有线网络的数据转换。 – 免布线节点：节点作为免布线网络的子节点，通过 Mesh 自组网，扩展现有免布线网络的覆盖范围。 提示 免布线子节点的 PoE WAN/LAN1 口为 LAN 口。
已连接终端	当前连接到免布线网络的终端数量。
系统时间	节点当前的系统时间。

标题项	说明
运行时间	节点最近一次启动后连续运行的时长。
CPU 使用率	节点当前的 CPU 使用率。
内存使用率	节点当前的内存使用率。

LAN 口状态

参数说明

标题项	说明
IP 地址	节点的 LAN 口 IP 地址，也是节点的管理 IP 地址，局域网用户可访问该 IP 地址登录到节点的管理页面。 免布线主节点的 LAN 口 IP 地址默认为“192.168.5.1”。子节点的 IP 地址从主节点的 DHCP 服务器自动获取。
MAC 地址	节点 LAN 口的物理地址。

WAN 口状态

参数说明

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

查看免布线子节点信息

点击“系统状态”页面中用户设备旁的免布线设备，在出现的窗口中，您可以查看免布线子节点的设备信息。

如需了解更多信息，请点击对应节点后的 详情 展开页面。

在这里，您可以查看或设置节点的基本信息，查看运行状态、LAN 口状态、免布线链路信息，重启或删除节点。

免布线链路信息

参数说明

标题项	说明
上级节点的 MAC 地址	Mesh 自组网链路上级节点用于组建 Mesh 链路的接口的物理地址。
免布线链路质量	免布线链路的连接质量。
与上级链接方式/强度	本节点与上级节点的组网方式/本节点接收到的上级节点的信号强度。

重启节点

点击 重启 ，可以立即重启该节点。

删除节点

点击 删除节点 ，可以将该节点从免布线网络中移除。从免布线网络中移除的节点，配置会恢复到出厂状态。

3.1.2 添加免布线子节点

免布线主节点可以自动发现已通电并处于出厂设置状态的其他免布线设备，您可根据需要添加这些设备为免布线网络子节点。

进入页面：点击「系统状态」。

添加免布线子节点：

如果系统已自动发现新的免布线设备，直接在页面点击“详情”添加即可。如果系统没有发现新的免布线设备，请按以下步骤操作。

1. 点击“添加”。

2. 输入要添加的免布线设备的 SN（见设备底面贴纸）。
3. 点击 添加 。

----完成

免布线子节点添加成功后，可以点击“系统状态”模块右侧的“免布线设备”查看该节点详情。

3.1.3 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，您可以查看免布线主节点 WAN 口的上传和下载流量动态图，也可以了解局域网某个用户的基本信息，如上传/下载速率，在线时长等。

参数说明

标题项	说明
主机名称	用户设备的基本信息，包括设备上报的设备名称、连接到免布线网络的方式、IP 地址和 MAC 地址。
并发连接数	用户设备的并发连接数。
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。

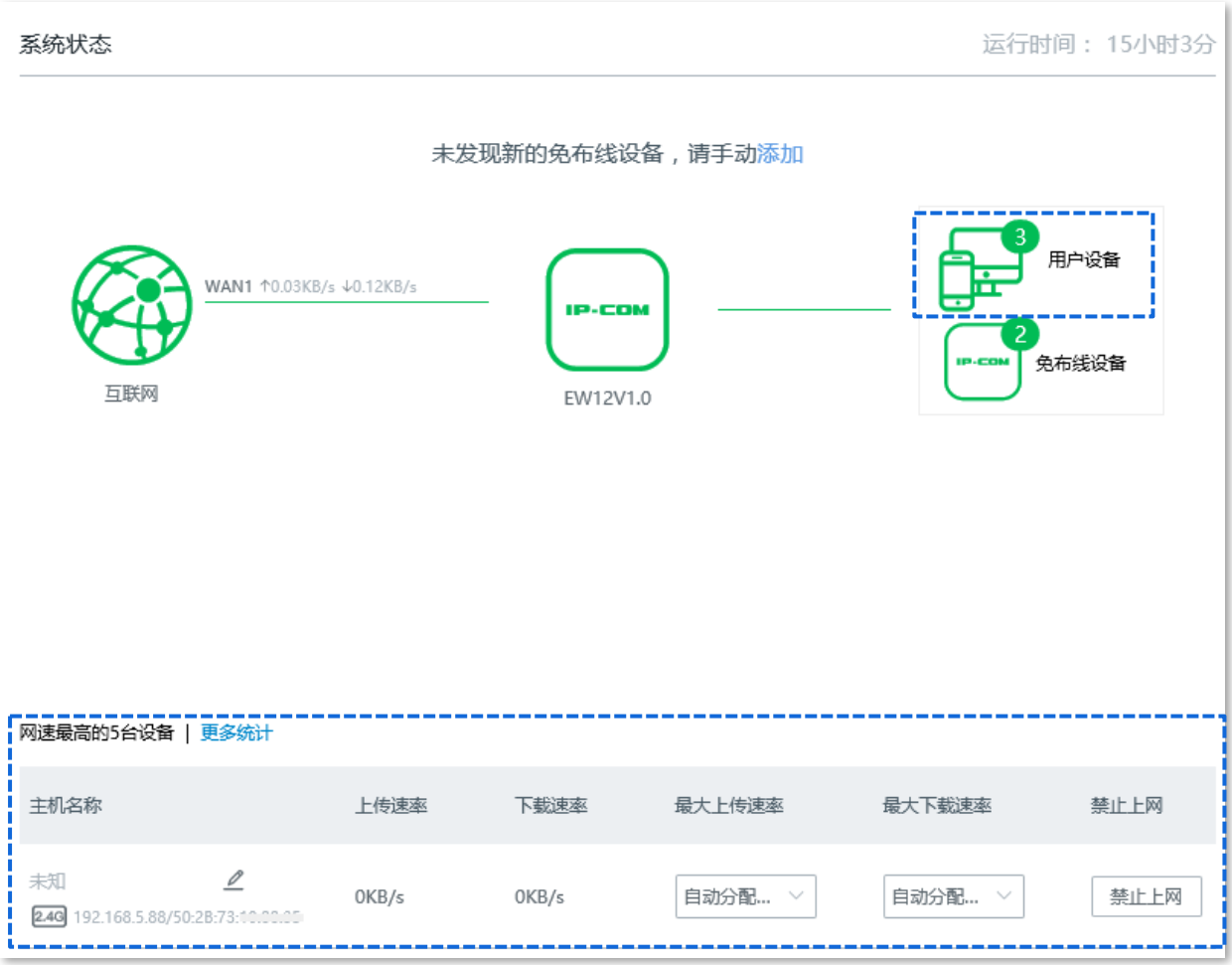
标题项	说明
在线时长	用户的在线时长。

3.1.4 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中网速最高的 5 台终端，也可以点击“用户设备”查看或管理所有的在线终端。

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



3.1.5 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。

添加黑名单

加入黑名单的设备，不能通过免布线网络上网。

将网速排在前五的设备加入黑名单

1. 在“系统状态”页面找到要加入黑名单的设备。
2. 点击 禁止上网 。

----完成

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

将其它在线设备加入黑名单

1. 在“系统状态”页面点击 ，进入“网速控制与黑名单”窗口。
2. 在“在线设备”列表中找到要加入黑名单的设备，点击 禁止上网 。

----完成

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

移出黑名单

如果需要将设备移出黑名单，可在“黑名单”页面设置。

设置步骤：

1. 在“系统状态”页面点击 ，进入“网速控制与黑名单”窗口。
2. 点击**黑名单**，进入“黑名单”列表。
3. 找到要移出黑名单的设备，点击 移出 。

----完成

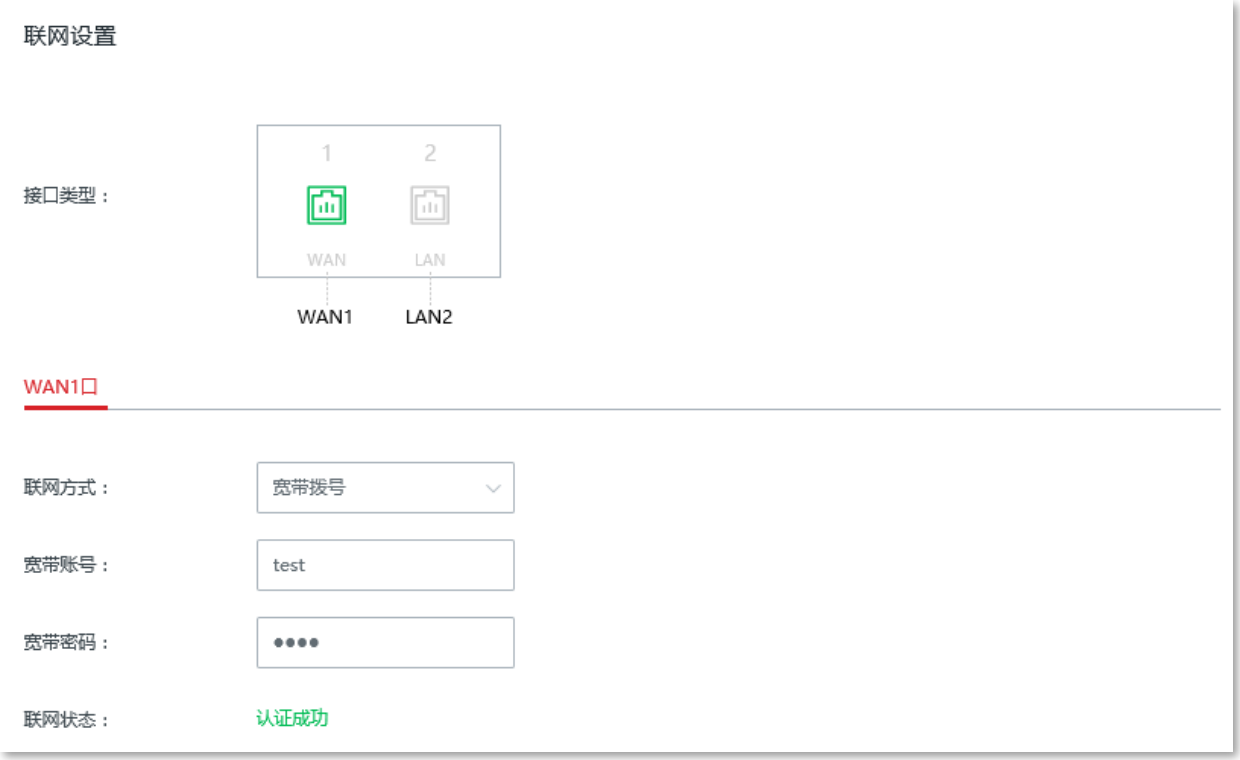
3.2 联网设置

3.2.1 概述

通过联网设置，可以实现局域网内的多台设备共享您办理的宽带服务上网。

若您是首次使用免布线设备或已将免布线设备恢复出厂设置，请根据设置向导完成联网设置。之后，如果要修改或设置更多联网参数，可在本模块设置。

进入页面：点击「联网设置」。



参数说明

标题项	说明
接口类型	显示免布线路由模式节点接口的类型，及连线状态。 ：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	免布线路由模式节点的联网方式，支持宽带拨号、静态 IP、动态 IP。 - 宽带拨号：节点使用 ISP（互联网服务提供商）提供的宽带账号和密码拨号上网。 - 静态 IP：节点使用 ISP 提供的固定 IP 地址、子网掩码、默认网关、DNS 服务器信

标题项	说明
	息上网。 – 动态 IP：节点使用 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。 提示 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	显示节点 WAN 口的连接状态。 – 已联网：节点 WAN 口已插网线，且已成功连接至上级网络设备。 – 已连接：节点 WAN 口已插网线，但未成功连接至上级网络设备。 – 认证成功：节点拨号成功，并已经获得 IP 地址信息。 – 连接中…：节点正在连接到上级网络设备。 – 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。 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。

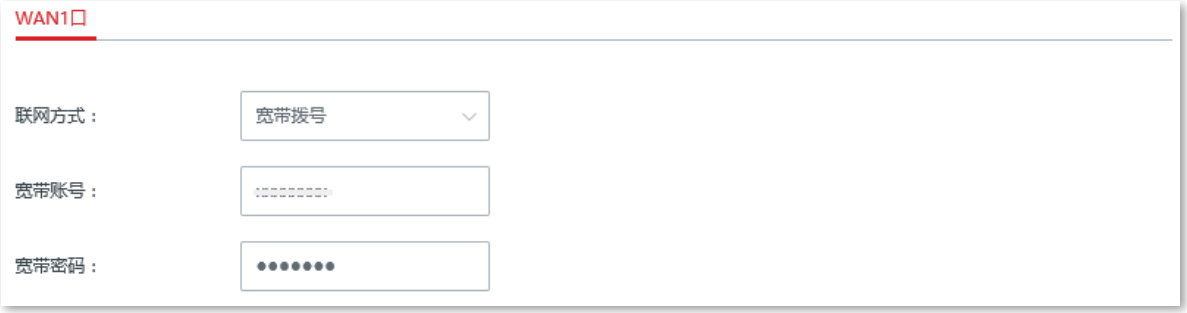
3.2.2 设置联网

提示

各上网参数均由 ISP 提供，如不清楚，请咨询您的 ISP。

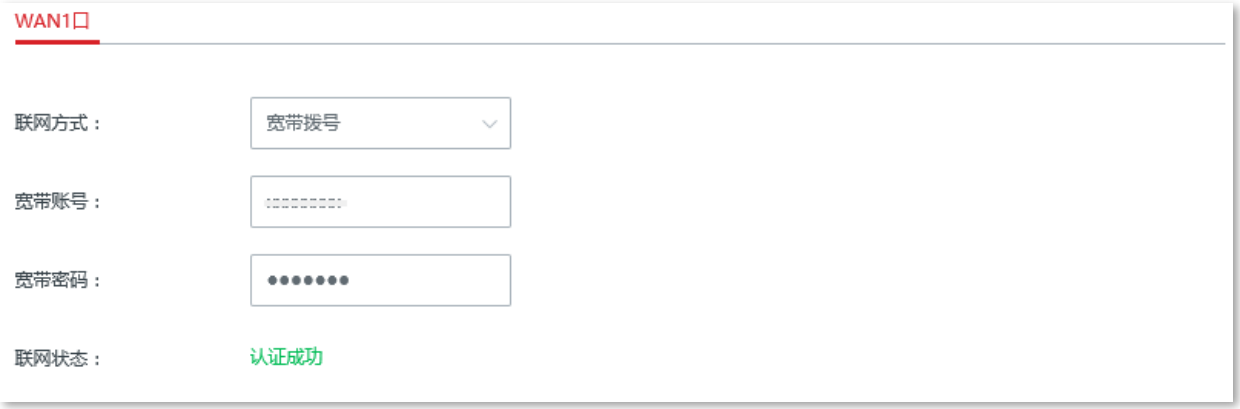
宽带拨号

1. 点击「联网设置」。
2. 选择“联网方式”为“宽带拨号”。
3. 输入 ISP 提供的“宽带账号”和“宽带密码”。
4. 点击页面底端的 保存 。



----完成

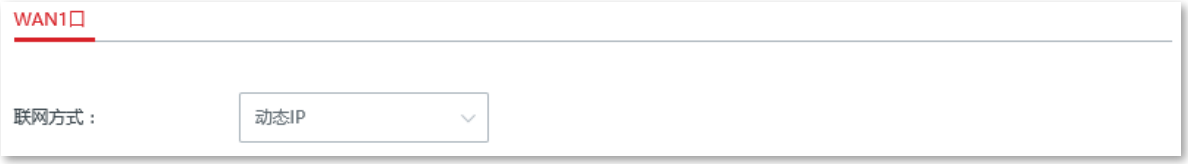
稍等片刻，当联网状态显示“认证成功”时，您可以尝试上网了。



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

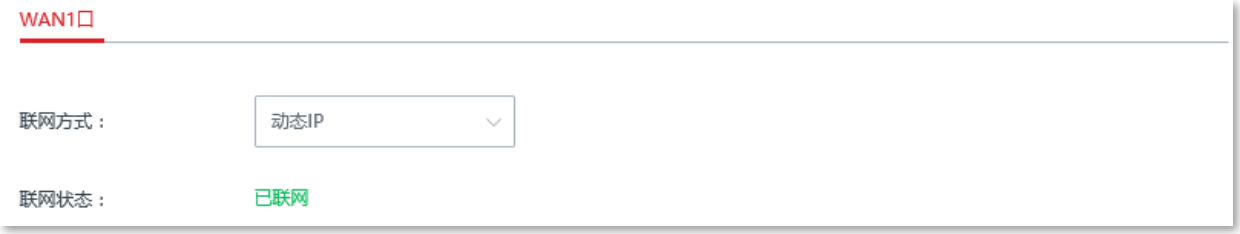
动态 IP

1. 点击「联网设置」。
2. 选择“联网方式”为“动态 IP”。
3. 点击页面底端的 保存 。



----完成

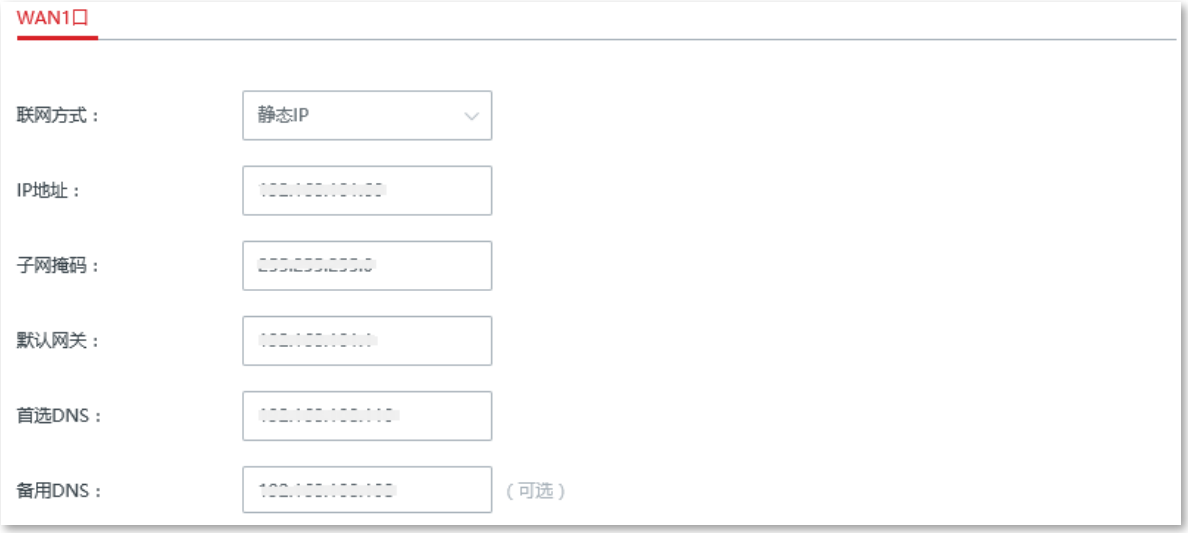
稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。



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

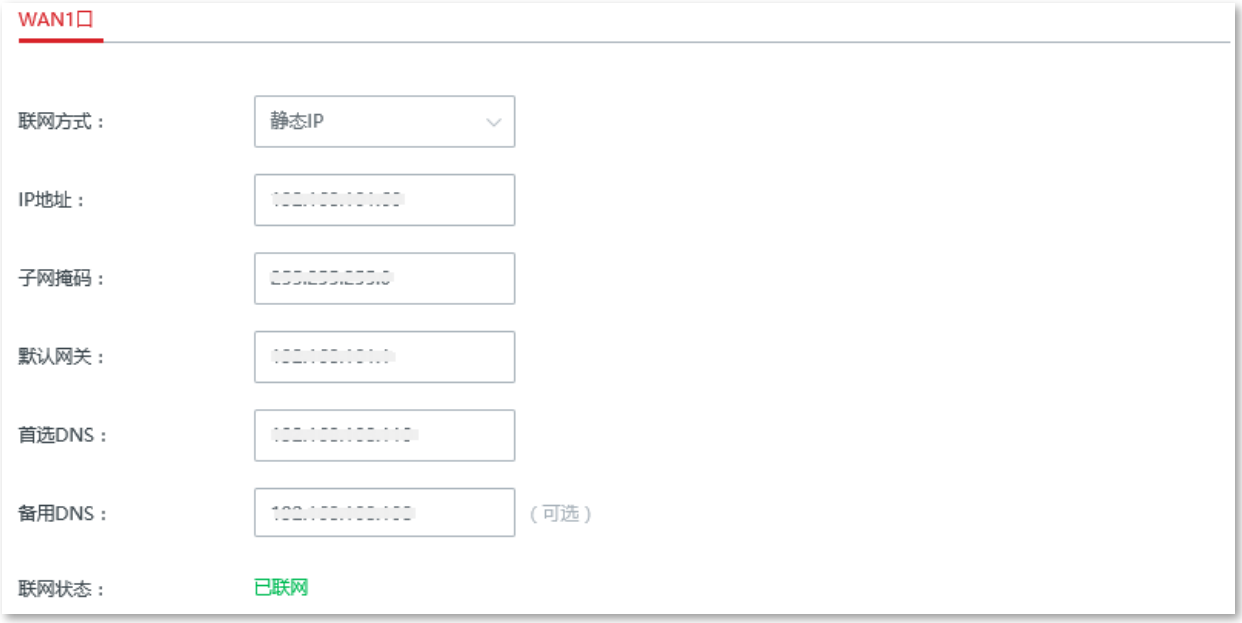
静态 IP

1. 点击「联网设置」。
2. 选择“联网方式”为“静态 IP”。
3. 输入 ISP 提供的“IP 地址”、“子网掩码”、“默认网关”和“首选/备用 DNS”。
4. 点击页面底端的 保存 。



----完成

稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。



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

3.3 无线设置

在这里，您可以修改免布线主节点的无线接入相关设置。

本设备最多支持三频无线网络。默认情况下，设备采用无线方式组建免布线网络，其中一个 5GHz 无线频段专用于建立免布线链路，2.4GHz 无线频段和另外一个 5GHz 无线频段用于终端设备接入。当设备采用有线方式组建免布线网络时，设备的三个无线频段都用于终端设备接入。

提示

对于免布线网络中的其他节点（子节点），如果未归属于任何节点分组，则本模块的配置会同步应用到该节点。

3.3.1 无线名称与密码

进入页面：点击「无线设置」>「无线名称与密码」。

在这里，您可以设置无线基本参数，包括开启/关闭无线网络、修改无线名称、设置无线密码等。

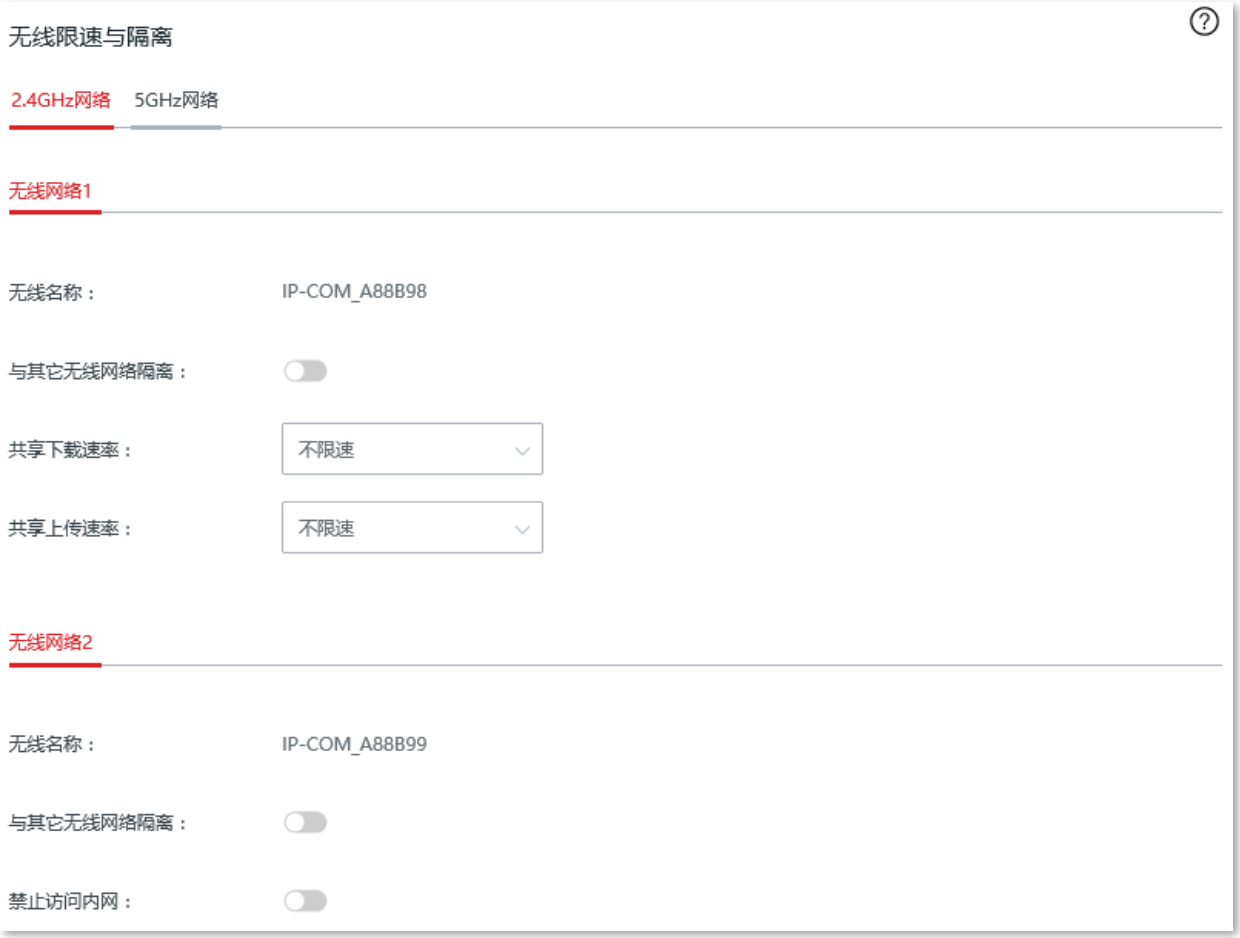
参数说明

标题项	说明
无线网络 1/2/3/4	节点每个频段均支持 4 个无线网络，默认只开启无线网络 1。
无线开关	开启/关闭对应无线网络的无线功能。
2.4/5GHz 无线名称一致	开启后，节点 2.4GHz 和 5GHz 网络的无线名称相同，且 5GHz 频段的“无线名称与密码”、“无线限速与隔离”相关参数自动同步 2.4GHz 相关设置，不可单独修改。用户连接 WiFi 时，将会自动连接到网络质量最好的 WiFi。 提示 如果您的网络中有仅支持 2.4GHz 网络的无线设备，为避免这些设备连接无线网络失败，建议不要开启此功能。
无线名称	节点的无线网络名称。
无线密码	无线网络密码。为了无线网络安全，强烈建议设置无线密码。
不设密码	不设置无线密码，此时对应的无线网络为不加密状态。
无线名称隐藏	开启后，无线网络名称会隐藏，该无线网络不会出现在终端设备（如手机）的可用无线网络列表中，一定程度上增强了无线网络的安全性。 如果要连接隐藏的无线网络，用户需要在终端设备上手动输入该无线网络名称。
最多可接入设备数	无线网络最多允许接入的无线设备数量。 若接入无线网络的无线设备达到此值，除非某些设备断开连接，否则新的无线设备不能接入该无线网络。

3.3.2 无线限速与隔离

进入页面：点击「无线设置」>「无线限速与隔离」。

在这里，您可以设置无线网络限速与隔离。本功能默认关闭。



参数说明

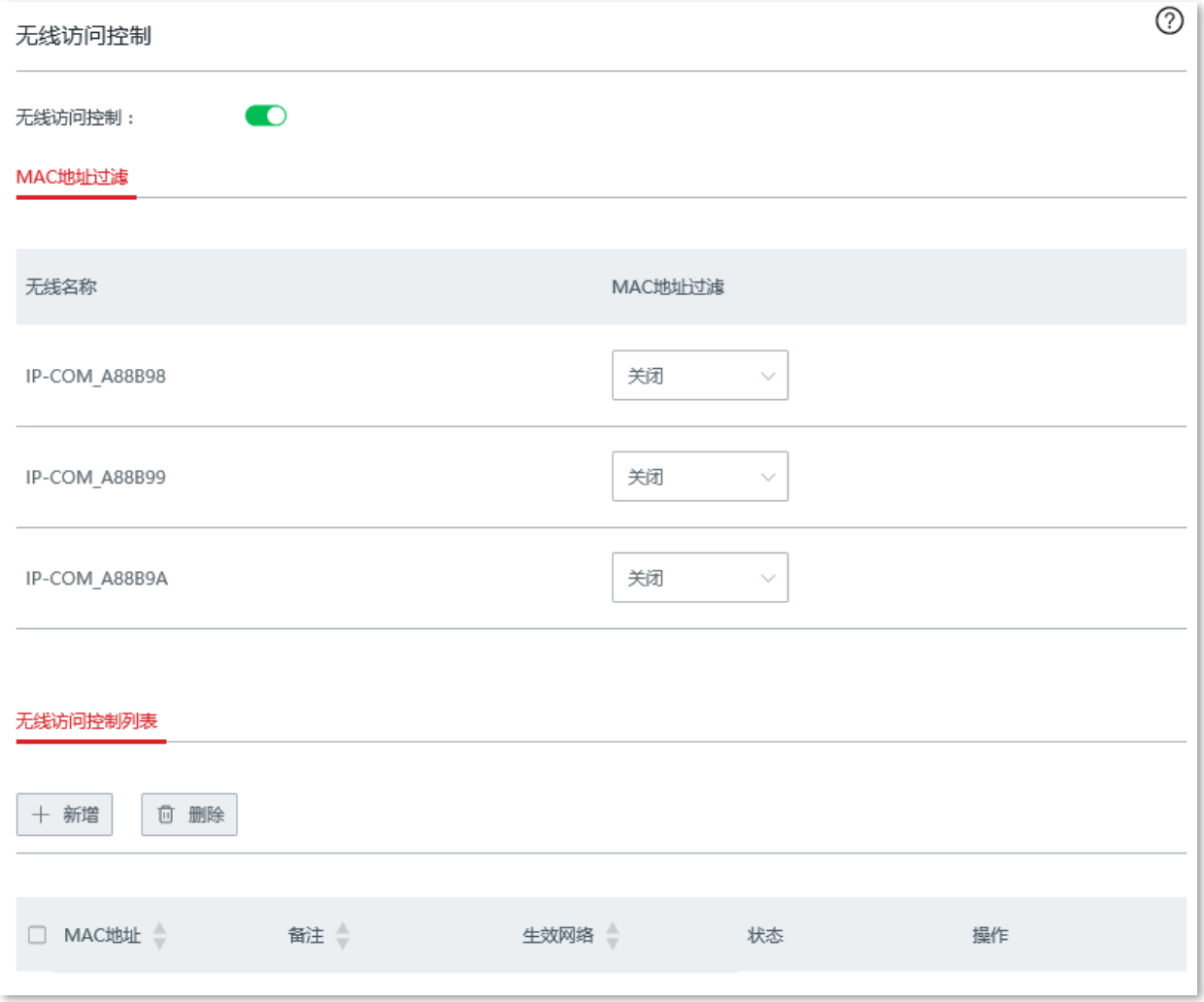
标题项	说明
无线名称	节点的无线网络名称。
与其它无线网络隔离	开启后，连接到该无线网络的用户与连接到免布线系统其他无线网络的用户之间不能互相通信，可增强无线网络的安全性。
共享下载/上传速率	连接到该无线网络的用户共享的最大下载/上传速率。 不限制：不限制该无线网络的最大下载/上传速率。
禁止访问内网	开启后，连接到该无线网络的用户只能访问互联网，不能访问局域网，也不能访问节点的管理页面。

3.3.3 无线访问控制

概述

进入页面：点击「无线设置」>「无线访问控制」。

在这里，您可以通过设置无线访问控制规则，允许或禁止指定设备连接到对应的无线网络。无线访问控制功能默认关闭，开启后，页面显示如下。



参数说明

标题项		说明
无线访问控制		无线访问控制功能开关。表示关闭，表示开启。
MAC 地址过滤	无线名称	节点当前启用的无线网络的名称。

标题项		说明
	MAC 地址过滤	MAC 地址过滤模式。 – 关闭：该无线网络不启用 MAC 地址过滤功能，允许所有无线客户端连接。 – 仅允许：仅允许无线访问控制列表中指定的无线客户端连接到该无线网络。 – 仅禁止：仅禁止无线访问控制列表中指定的无线客户端连接到该无线网络，其他无线客户端可以连接到该无线网络。
无线访问控制列表	MAC 地址	无线客户端的 MAC 地址。
	备注	MAC 地址的备注信息。
	生效网络	规则生效的无线网络。
	状态	规则的状态，可根据需要开启或关闭。
	操作	可对规则进行如下操作： – 点击 可以修改规则。 – 点击 可以删除规则。

配置无线访问控制

开启无线访问控制功能

在「无线设置」>「无线访问控制」页面，点击滑块至，然后点击页面底端的 保存 。

设置 MAC 地址过滤模式

在「无线设置」>「无线访问控制」页面，根据需要选择无线网络的“MAC 地址过滤”模式，然后点击页面底端的 保存 。

添加无线访问控制规则

1. 在「无线设置」>「无线访问控制」页面，点击 + 新增 进入配置窗口。
2. 设置无线访问控制规则。
   (1) 输入要限制连接无线网络的无线客户端的 MAC 地址。
   (2) （可选）设置该 MAC 地址的备注信息。
   (3) 选择规则生效的无线网络。

提示

点击 + ，可同时添加多条访问控制规则，点击 – 可删除未保存的访问控制规则。

3. 点击 保存 。

----完成

您可以在「无线设置」>「无线访问控制」页面看到新增的无线访问控制规则。

无线访问控制配置举例

组网需求

某企业使用免布线设备进行网络搭建。

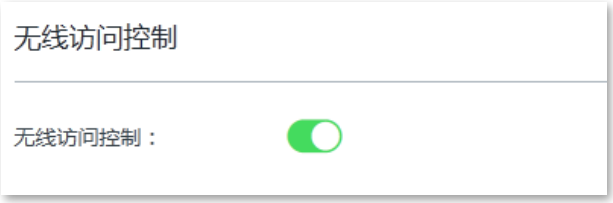
要求：仅允许某一采购人员连接免布线主节点 WiFi（caigou）访问互联网，其他员工禁止连接。

方案设计

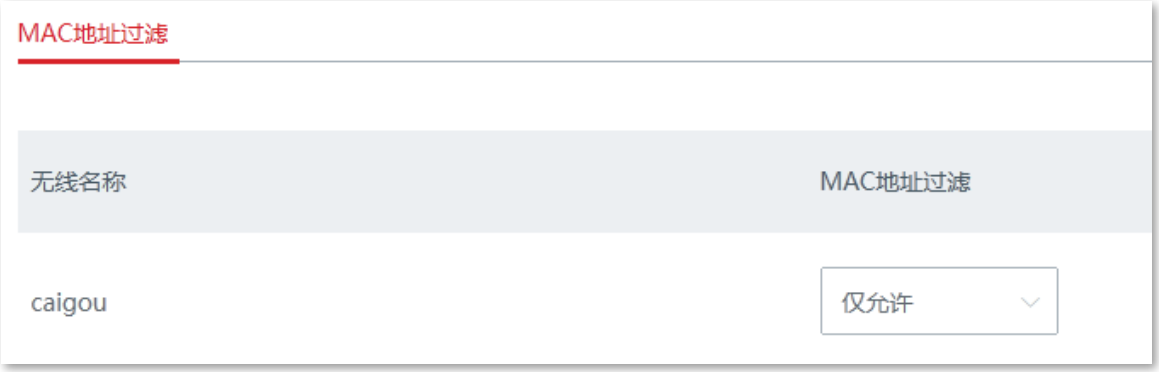
使用无线访问控制功能实现上述需求。假设该采购人员电脑的物理地址为 CC:3A:61:71:1B:6E。

配置步骤

1. 点击「无线设置」>「无线访问控制」进入配置页面。
2. 开启无线访问控制功能。
   (1) 点击滑块至。
   (2) 点击页面底端的 保存 。



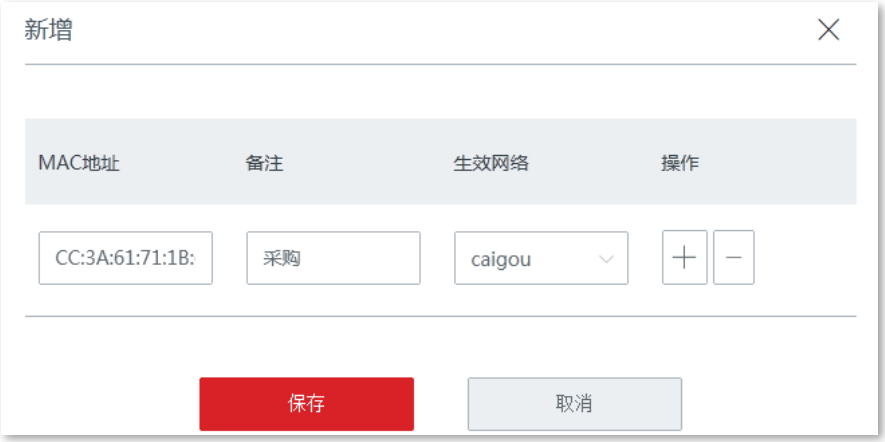
3. 设置 MAC 地址过滤模式。
   (1) 选择无线网络“caigou”的“MAC 地址过滤”模式，本例为“仅允许”。
   (2) 点击页面底端的 保存 。



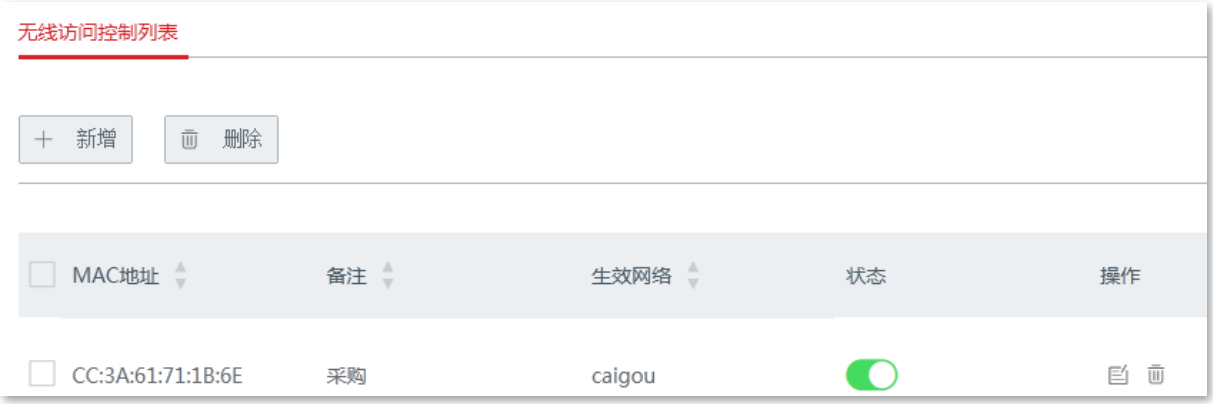
4. 添加无线访问控制规则。
   (1) 点击 + 新增 。

(2) 在【新增】窗口进行如下配置，然后点击 保存 。

- 输入采购人员电脑的 MAC 地址（物理地址），本例为“CC:3A:61:71:1B:6E”。
- （可选）设置本规则的备注，如“采购”。
- 选择规则生效的无线网络，本例为“caigou”。



添加成功，如下图示。



----完成

验证配置

只有上述 1 台无线设备可以接入无线网络“caigou”，其他设备无法连接到该网络。

3.3.4 无线高级设置

进入页面：点击「无线设置」>「无线高级设置」。

在这里，您可以设置无线高级参数，包括发射功率、网络模式、信道、信道带宽等。

参数说明

标题项	说明
2.4GHz/5GHz 网络	开启/关闭对应无线频段的无线功能。
发射功率	节点对应频段的无线发射功率。 发射功率越大，无线覆盖范围越广。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。
国家或地区	选择节点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。
网络模式	节点对应频段的无线网络模式。

标题项	说明
	2.4GHz 包括 11b、11g、11b/g、11b/g/n，默认工作在 n+256QAM。 – 11b：此模式下，仅允许 802.11b 无线设备接入节点的 2.4GHz 无线网络。 – 11g：此模式下，仅允许 802.11g 无线设备接入节点的 2.4GHz 无线网络。 – 11b/g：此模式下，802.11b、802.11g 的无线设备可以接入节点的 2.4GHz 无线网络。 – 11b/g/n：此模式下，802.11b、802.11g 以及工作在 2.4GHz 的 802.11n 无线设备可以接入节点的 2.4GHz 无线网络。 – n+256QAM：802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备可以接入节点的 2.4GHz 无线网络。 QAM，Quadrature Amplitude Modulation，正交幅度调制。QAM 是一种在两个正交载波上进行幅度调制的调制方式，它利用正弦波和余弦波的正交性，同时调制两路信号，提高了调制效率。n+256QAM 是在 2.4GHz 频段，让 IEEE 802.11n 标准改用 IEEE 802.11ac 的 256-QAM 调制模式，单流速率也从 IEEE 802.11n 标准的 150Mbps 提升至 IEEE 802.11ac 标准的 200Mbps。 需要注意的是，这种提升只有在 2.4GHz 频段且发射端和接收端均支持的情况下才有效，任何一方不支持 n+256QAM，那 2.4GHz 频段下单流速率最高仍然是 150Mbps。而且在调制模式改为 n+256QAM 后，网络的稳定度及抗干扰性都比其他模式下要逊色。 5GHz 包括 11a、11ac、11a/n，默认工作在 11ac。 – 11a：此模式下，仅允许 802.11a 无线设备接入节点的 5GHz 无线网络。 – 11ac：此模式下，仅允许 802.11ac 无线设备接入节点的 5GHz 无线网络。 – 11a/n：此模式下，802.11a 以及工作在 5GHz 的 802.11n 无线设备可以接入节点的 5GHz 无线网络。
信道	节点无线数据传输的通道。可选择范围由当前选择的国家或地区、无线工作频段来决定。 自动：节点自动检测各信道利用率，并据此选择合适的工作信道。 如果使用节点无线网络时，经常出现掉线、卡顿或网速慢现象，可以尝试修改节点的信道来解决问题。您可以通过工具软件（如 WiFi 分析仪）获得周边较少用到、干扰较小的信道。
信道带宽	节点无线信道的频带宽度。高信道带宽下，更容易获得较高的传输速率，但穿透性稍差，传输距离近。 – 20MHz：节点使用 20MHz 的信道带宽。 – 40MHz：节点使用 40MHz 的信道带宽。 – 20MHz/40MHz：仅适用于 2.4GHz。节点根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。 – 80MHz：仅适用于 5GHz。节点使用 80MHz 的信道带宽。
接入信号强度限制	节点对应频段可接受的最低无线信号强度，信号强度低于此值的设备将无法接入节点。 当环境中存在多个节点时，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

标题项	说明
	强的节点。
部署模式	根据节点的部署密度情况选择。 – 强覆盖：常用于节点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节点的覆盖范围。 – 高密度：常用于节点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节点相互之间的干扰。
空口调度	开启该功能后，节点公平地分配下行传输时间，使得高速终端和低速终端获得相同的下行传输时间，帮助高速终端传输更多的数据，从而使节点实现更高的系统吞吐率和用户接入数。
Short GI	短保护间隔，仅“2.4GHz 网络”支持。 无线信号在空间传输时会因多径等因素在接收侧形成时延，如果后面的数据块发送过快，会对前一个数据块形成干扰，短保护间隔可以用来规避这个干扰。开启 Short GI 时，可提高无线吞吐量。
APSD	仅“5GHz 网络”支持。 Automatic Power Save Delivery，即“自动省电模式”，是 WiFi 联盟的 WMM 省电认证协议。开启“APSD”能降低节点的电能消耗。默认关闭。
客户端老化时间	客户端连接到节点的无线网络后，如果在该时间段内没有数据通信，节点主动断开该客户端。
强制速率	通过调整“强制速率”和“支持速率”，可以限制低速率客户端接入，从而提升其他客户端的上网体验。 – 强制速率：节点强制的一组速率。对于强制速率集，客户端必须支持，否则将无法连接到无线网络。 – 支持速率：在“强制速率集”基础上，节点能够支持的其他速率集合，支持让客户端在满足强制速率的前提下选择更高的速率与节点进行连接。
支持速率	

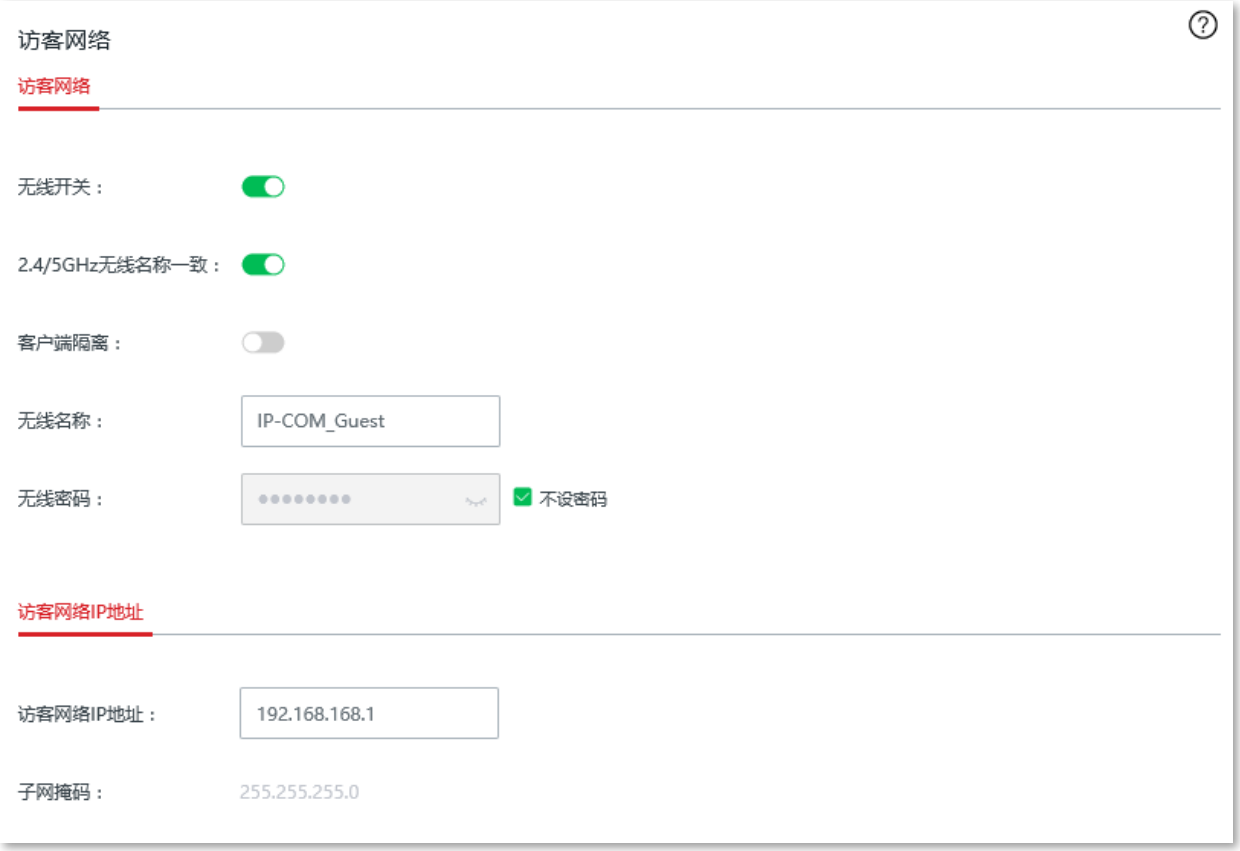
3.3.5 访客网络

进入页面：点击「无线设置」>「访客网络」。

在这里，您可以设置访客网络基本参数，包括开启/关闭访客网络、修改无线名称、设置无线密码等。

接入到访客网络的客户端只能访问互联网和访客网络下的其他无线客户端，不能访问节点管理页面和主网络局域网。设置访客网络可以满足客人上网需求，同时也确保主网络安全。

访客网络默认关闭，开启后，页面显示如下。



参数说明

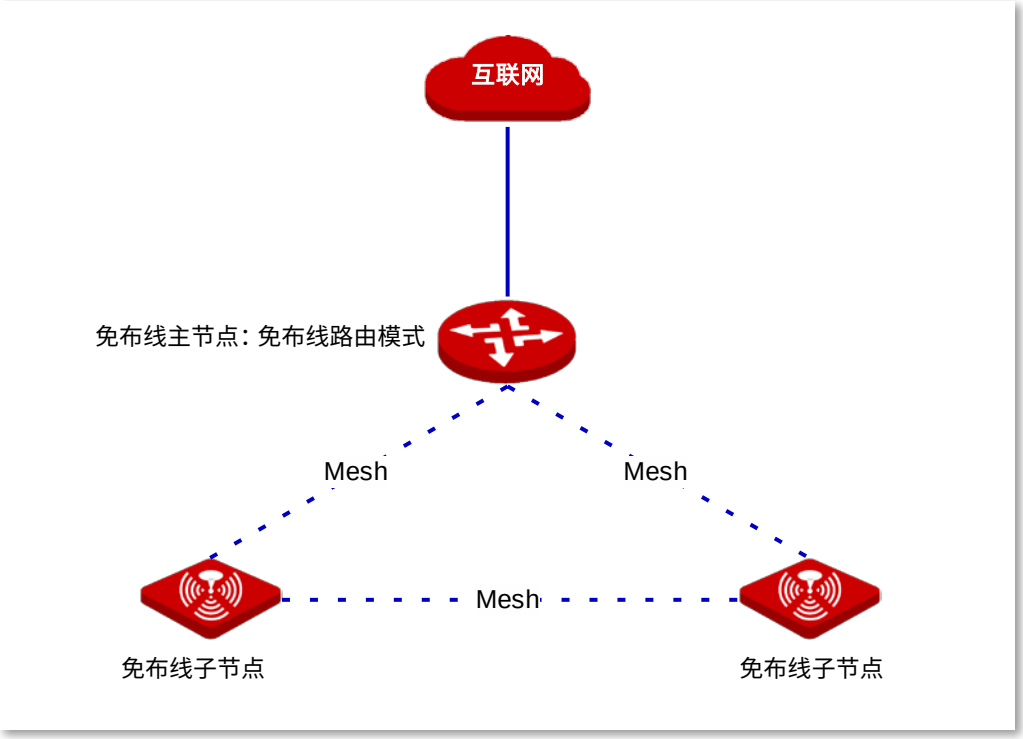
标题项		说明
访客网络	无线开关	开启/关闭访客网络。
	2.4/5GHz 无线名称一致	开启后，节点 2.4GHz 和 5GHz 访客网络的无线名称相同。用户连接 WiFi 时，将会自动连接到网络质量最好的 WiFi。 提示 如果您的网络中有仅支持 2.4GHz 网络的访客无线设备，为避免这些设备连接无线网络失败，建议不要开启此功能。

标题项		说明
	客户端隔离	连接到访客网络的无线用户的隔离状态。 开启后，连接到该访客网络的设备之间不能互相通信，可增强无线网络的安全性。
	无线名称	节点访客网络的无线名称。 提示 为了区别于主网络的无线名称，建议不要将访客网络的无线名称与节点主网络的无线名称设置成一样。
	无线密码	访客网络的无线密码。
	不设密码	不设置无线密码，对应的无线网络为不加密状态。
访客网络 IP 地址	访客网络 IP 地址	访客网络 IP 地址默认为 192.168.168.1，无线客户端连接访客网络后，会获取到 192.168.168.X 的 IP 地址。如无特殊需要请保持默认设置。
	子网掩码	访客网络的子网掩码，用于定义访客网络的地址空间。

3.4 节点管理

概述

免布线路由模式的节点集成了“节点管理”功能，可以集中管理同一网络中 IP-COM 品牌的其他免布线设备。网络应用拓扑图如下。



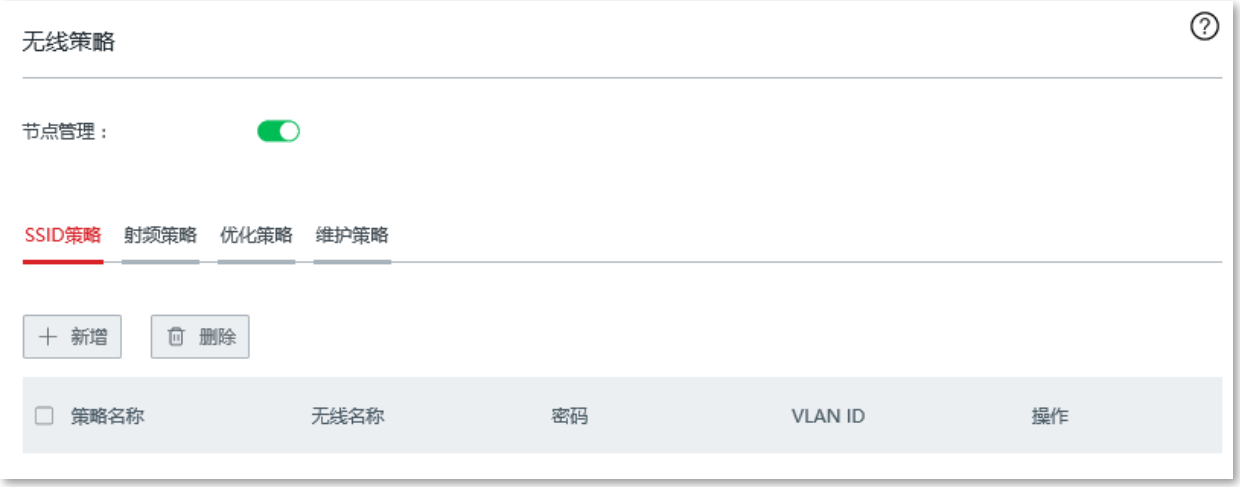
配置向导

免布线设备加入免布线网络后，就可以被统一管理了，配置步骤及任务说明如下表。

步骤	配置任务	说明
1	开启节点管理功能	可选。 默认情况下，节点管理功能为开启状态。
2	配置无线策略	必选。 以策略的形式，预置节点的配置信息。
3	配置节点分组	必选。 创建节点分组。
4	维护节点	必选。 将节点划分到指定的分组，并下发配置到节点。

- **开启节点管理功能**

节点管理功能默认开启。若需修改功能状态，请进入「节点管理」>「无线策略」页面设置。



3.4.1 无线策略

无线策略模块用于预置节点的配置信息，以便后续进行节点分组时引用，包括 SSID 策略、射频策略、优化策略和维护策略。

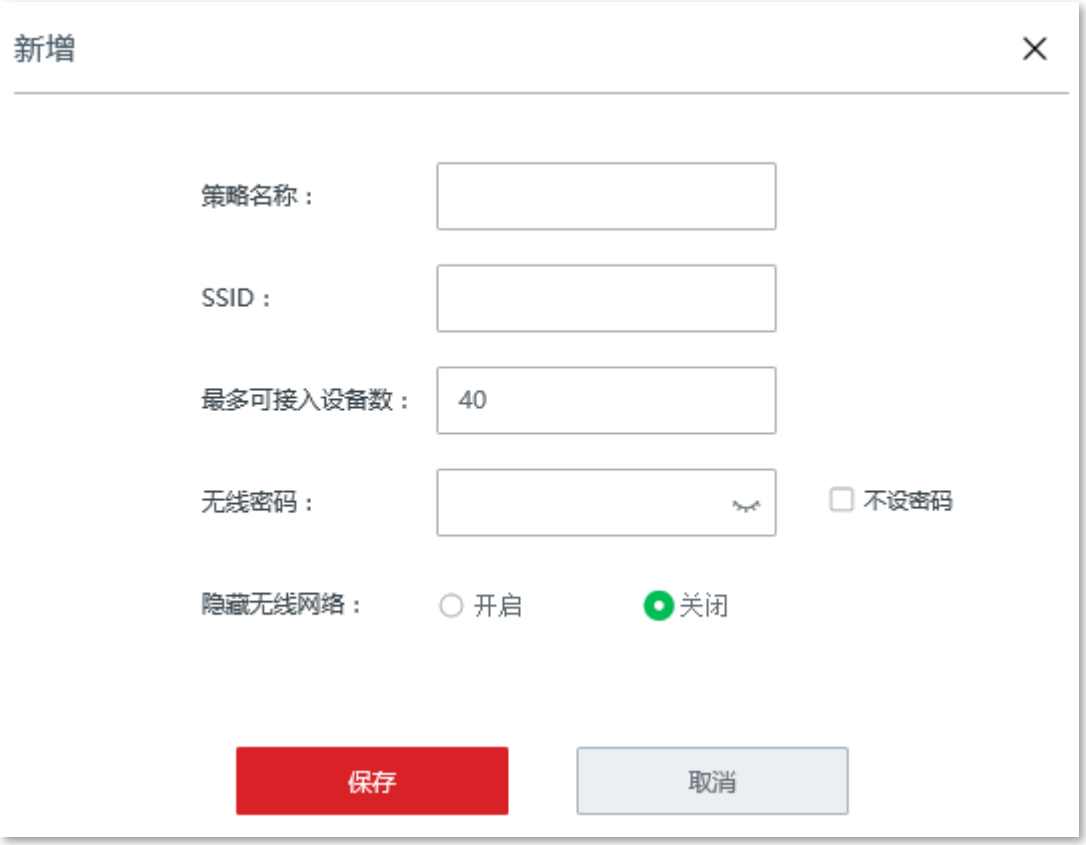
进入页面：点击「节点管理」>「无线策略」。

SSID 策略

SSID 策略用于配置节点的 SSID 相关参数。

新增策略

在「节点管理」>「无线策略」>「SSID 策略」页面，点击 + 新增 进入配置窗口。



参数说明

标题项	说明
策略名称	SSID 策略的名称。
SSID	无线网络名称。
最多可接入设备数	该无线网络最多允许接入的客户端数量。
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。 不设密码：不设置无线密码，该无线网络为不加密状态。
隐藏无线网络	开启后，无线网络名称会隐藏，该无线网络不会出现在终端设备（如手机）的可用无线网络列表中，一定程度上增强了无线网络的安全性。 如果要连接隐藏的无线网络，用户需要在终端设备上手动输入该无线网络名称。

修改策略

在「节点管理」>「无线策略」>「SSID 策略」页面，点击操作栏的✎，可以修改对应策略配置。

保存修改后，新的策略自动下发到对应分组的节点。

删除策略

您可以删除当前**未**使用（未被节点分组引用）的策略。

单个删除：在「节点管理」>「无线策略」>「SSID 策略」页面，点击对应策略操作栏的 。

批量删除：在「节点管理」>「无线策略」>「SSID 策略」页面，勾选要删除的策略，点击 删除 。

射频策略

射频策略用于配置节点的基本射频参数。

新增策略

在「节点管理」>「无线策略」>「射频策略」页面，点击 + 新增 进入配置窗口。

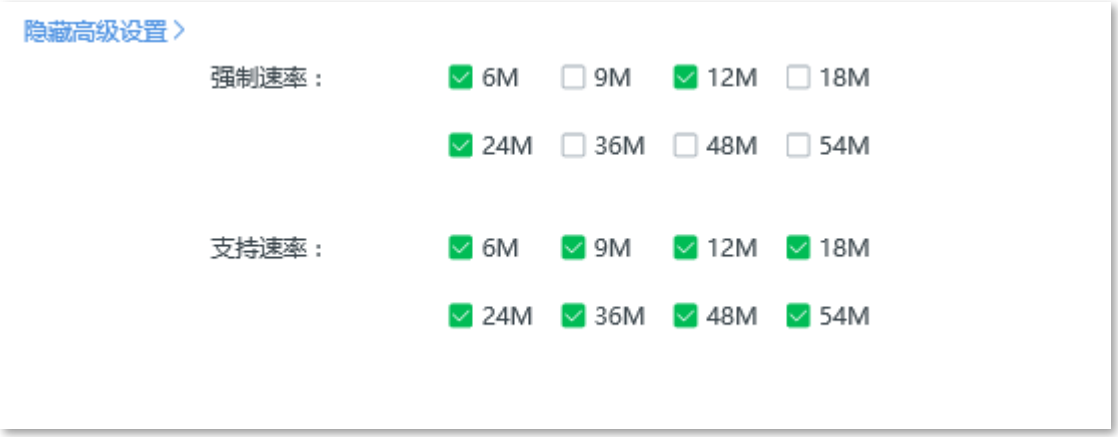
参数说明

标题项	说明
策略名称	射频策略的名称。

标题项	说明
2.4GHz 5GHz	选择要配置的频段。如果您只选择并配置了一个频段，则另一频段保持默认设置。
射频状态	无线功能的启用状态。 - 开启：开启该频段的无线功能。 - 关闭：关闭该频段的无线功能。
网络模式	该频段的无线网络模式。 2.4GHz 频段支持设置 11b、11g、11b/g、11b/g/n 和 n+256QAM。 - 11b：仅允许 802.11b 无线设备接入节点的 2.4GHz 无线网络。 - 11g：仅允许 802.11g 无线设备接入节点的 2.4GHz 无线网络。 - 11b/g：允许 802.11b、802.11g 无线设备接入节点的 2.4GHz 无线网络。 - 11b/g/n：允许 802.11b、802.11g 以及工作在 2.4 GHz 频段的 802.11n 无线设备接入节点的 2.4GHz 无线网络。 - n+256QAM：802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备可以接入节点的 2.4GHz 无线网络。 QAM，Quadrature Amplitude Modulation，正交幅度调制。QAM 是一种在两个正交载波上进行幅度调制的调制方式，它利用正弦波和余弦波的正交性，同时调制两路信号，提高了调制效率。n+256QAM 是在 2.4GHz 频段，让 IEEE 802.11n 标准改用 IEEE 802.11ac 的 256-QAM 调制模式，单流速率也从 IEEE 802.11n 标准的 150Mbps 提升至 IEEE 802.11ac 标准的 200Mbps。 需要注意的是，这种提升只有在 2.4GHz 频段且发射端和接收端均支持的情况下才有效，任何一方不支持 n+256QAM，那 2.4GHz 频段下单流速率最高仍然是 150Mbps。而且在调制模式改为 n+256QAM 后，网络的稳定度及抗干扰性都比其他模式下要逊色。 5GHz 频段支持设置 11a、11ac 和 11a/n。 - 11a：仅允许 802.11a 无线设备接入节点的 5GHz 无线网络。 - 11ac：仅允许 802.11ac 无线设备接入节点的 5GHz 无线网络。 - 11a/n：允许 802.11a 及工作在 5GHz 频段的 802.11n 无线设备接入节点的 5GHz 无线网络。
国家或地区	选择节点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。

标题项	说明
信道带宽	节点无线信道的频带宽度。高信道带宽下，更容易获得较高的传输速率，但穿透性稍差，传输距离近。 – 20MHz：节点使用 20MHz 的信道带宽。 – 40MHz：节点使用 40MHz 的信道带宽。 – 20/40MHz：节点根据周围环境干扰情况，自动调整其信道带宽为 20MHz 或 40MHz。仅 2.4GHz 无线网络支持。 – 80MHz：节点使用 80MHz 的信道带宽。仅 5GHz 无线网络支持。
信道	节点无线数据传输的通道，可选择范围由当前选择的国家或地区、无线工作频段来决定。 – 不配置：不改变节点当前配置。 – 自动：节点自动检测各信道利用率，并据此选择合适的工作信道。 如果使用节点无线网络时，经常出现掉线、卡顿或网速慢现象，可以尝试修改节点的信道来解决问题。您可以通过工具软件（如 WiFi 分析仪）获得周边较少用到、干扰较小的信道。
功率	节点对应频段的无线发射功率。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。 不配置：不改变节点当前的配置。
接入信号强度限制	节点对应频段可接受的最低无线信号强度，信号强度低于此值的设备将无法接入节点的无线网络。 当环境中存在多个节点时，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节点。
客户端老化时间	客户端连接到节点的无线网络后，如果在该时间段内没有数据通信，节点主动断开该客户端。
显示/隐藏高级设置	点击可展开/隐藏高级设置参数：强制速率、支持速率。
强制速率	通过调整“强制速率”和“支持速率”，可以限制低速率客户端接入，从而提升其他客户端的上网体验。 – 强制速率：节点强制的一组速率。对于强制速率集，客户端必须支持，否则将无法连接到无线网络。 – 支持速率：在“强制速率集”基础上，节点能够支持的其他速率集合，支持让客户端在满足强制速率的前提下选择更高的速率与节点进行连接。
支持速率	

展开后的高级配置内容，如下图所示。



修改策略

在「节点管理」>「无线策略」>「射频策略」页面，点击操作栏的，可以修改对应策略配置。

保存修改后，新的策略自动下发到对应分组的节点。

删除策略

您可以删除当前**未**使用（未被节点分组引用）的策略。

单个删除：在「节点管理」>「无线策略」>「射频策略」页面，点击对应策略操作栏的。

批量删除：在「节点管理」>「无线策略」>「射频策略」页面，勾选要删除的策略，点击 删除 。

优化策略

优化策略用于配置节点的高级射频参数。

新增策略

在「节点管理」>「无线策略」>「优化策略」页面，点击 + 新增 进入配置窗口。

参数说明

标题项	说明
策略名称	优化策略的名称。
空口调度	开启该功能后，节点公平地分配下行传输时间，使得高速终端和低速终端获得相同的下行传输时间，帮助高速终端传输更多的数据，从而使节点实现更高的系统吞吐率和用户接入数。

修改策略

在「节点管理」>「无线策略」>「优化策略」页面，点击操作栏的 ，可以修改对应策略配置。

保存修改后，新的策略自动下发到对应分组的节点。

删除策略

您可以删除当前未使用（未被节点分组引用）的策略。

单个删除：在「节点管理」>「无线策略」>「优化策略」页面，点击对应策略操作栏的 。

批量删除：在「节点管理」>「无线策略」>「优化策略」页面，勾选要删除的策略，点击 删除 。

维护策略

维护策略用于配置节点的“自定义重启”相关参数。合理地配置维护策略，可以预防长时间地运行节点导致免布线网络出现性能降低、不稳定等现象。

提示

- 维护策略针对节点分组生效，生效时间以被管理节点的系统时间为准，请确保被管理节点的系统时间准确。
- 重启过程中，会断开所有连接，因此，建议将“维护时间”设置在业务相对空闲的时间，以降低维护过程对业务的影响。

新增策略

在「节点管理」>「无线策略」>「维护策略」页面，点击 + 新增 进入配置窗口。

参数说明

标题项	说明
策略名称	维护策略的名称。

标题项	说明
维护方式	节点的维护方式，支持定制重启、循环重启。 - 定时重启：节点在指定日期的指定时间点自动重启一次。 - 循环重启：节点每隔一个指定的时间间隔自动重启一次。
时间 日期	维护方式为“定时重启”时，用于设置节点自动重启的时间点和日期。
重复	维护方式为“循环重启”时，用于选择自动重启的间隔时间。

修改策略

在「节点管理」>「无线策略」>「维护策略」页面，点击操作栏的 ，可以修改对应策略配置。

保存修改后，新的策略自动下发到对应分组的节点。

删除策略

您可以删除当前**未**使用（未被节点分组引用）的策略。

单个删除：在「节点管理」>「无线策略」>「维护策略」页面，点击对应策略操作栏的 。

批量删除：在「节点管理」>「无线策略」>「维护策略」页面，勾选要删除的策略，点击 删除 。

3.4.2 节点分组

实际无线组网应用中，节点数量可能很多，如果逐个配置节点，工作量太大；另外，由于节点的部署具有区域特性，即同一区域的节点配置大部分都一样，逐个配置会做很多重复工作。

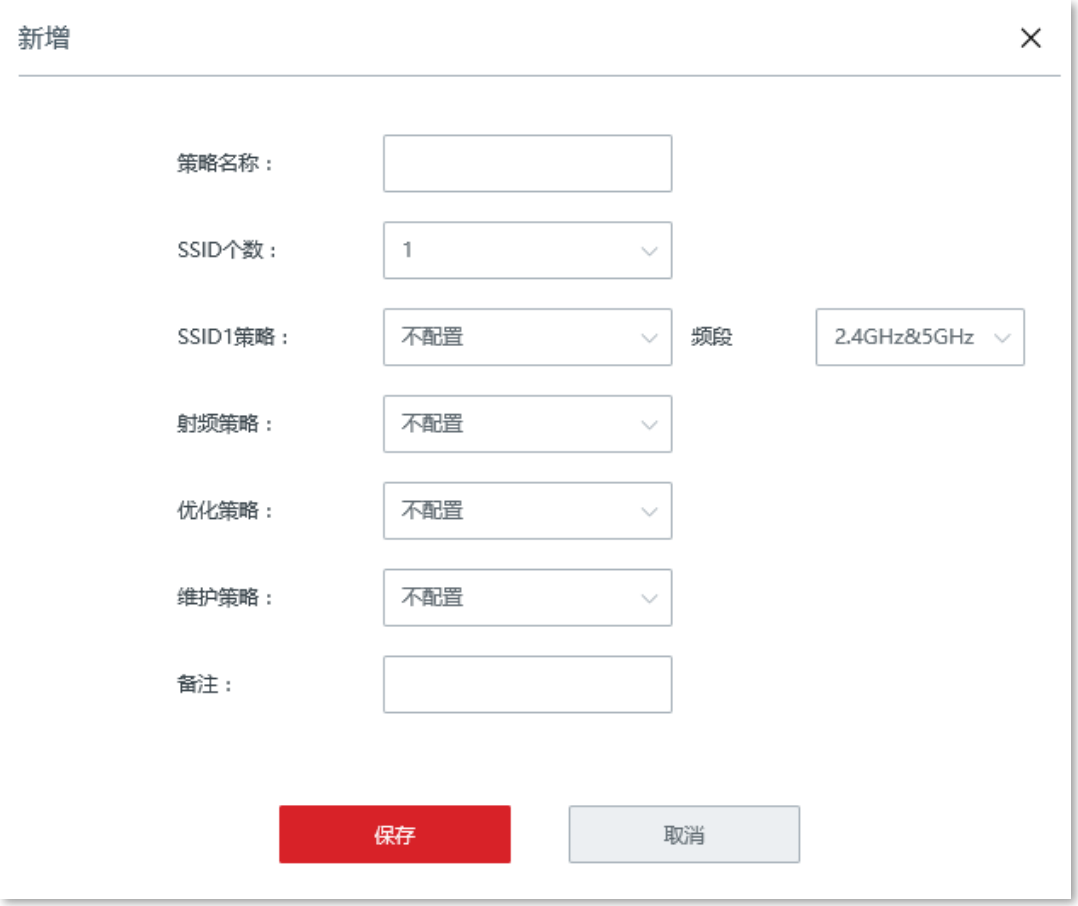
利用节点分组的形式，将具有相同配置的节点放到一个组，共同引用组里面的一份配置，可以有效地解决上述问题。

节点分组中的配置内容包括：SSID 策略、射频策略、优化策略、维护策略等。

进入页面：点击「节点管理」>「节点分组」。

新增分组

在「节点管理」>「节点分组」页面，点击 + 新增 进入配置窗口。



参数说明

标题项	说明
策略名称	节点分组的名称。

标题项	说明
SSID 个数	该分组节点开启的无线网络个数。
SSID 策略	选择引用的 SSID 策略。SSID 策略需事先已在 SSID 策略页面配置好。 若该分组节点开启的无线网络数量大于 1，则每个无线网络都要引用一个不同的 SSID 策略。 不配置：不改变节点当前配置。
频段	SSID 策略生效频段。 注意 如果节点只支持 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	选择引用的射频策略。射频策略需事先已在射频策略页面配置好。 不配置：不改变节点当前配置。
优化策略	选择引用的优化策略。优化策略需事先已在优化策略页面配置好。 不配置：不改变节点当前配置。
维护策略	选择引用的维护策略。维护策略需事先已在维护策略页面配置好。 不配置：不改变节点当前配置。
备注	节点分组的备注信息。

修改分组

在「节点管理」>「节点分组」页面，点击操作栏的 ，可以修改对应分组配置。

保存修改后，新的配置自动下发到对应分组的节点。

删除分组

您可以删除当前**未**使用（未被节点引用）的分组。

单个删除：在「节点管理」>「节点分组」页面，点击对应分组操作栏的 。

批量删除：在「节点管理」>「节点分组」页面，勾选要删除的分组，点击 删除 。

3.4.3 节点维护

进入页面：点击「节点管理」>「节点维护」。

在这里，您可以将节点划到指定的节点分组，批量重启/复位在线节点，批量删除离线节点信息，单独修改某一节点的配置信息、查看/导出已管理的节点的信息等。

分组

使用分组功能，您可以同时将多个节点划到一个节点分组，并引用相同的配置，有效提高管理效率。

节点分组：

1. 在「节点管理」>「节点维护」页面，选定需要划到同一节点分组的节点。
2. 点击 分组 进入配置窗口。
3. 在配置窗口中，点击下拉框，选择分组，然后点击 保存 。

----完成

保存成功后，分组中的节点自动同步所属分组的配置。

取消分组

使用取消分组功能，可以将节点从分组中移除。不在分组中的节点，将重新同步免布线路由模式节点的无线设置模块的配置。

节点移出分组：

1. 在「节点管理」>「节点维护」页面，选定需要从分组中移除的节点。
2. 点击 取消分组 。

   ----完成

重启

使用重启功能，可以同时将 1 个或多个节点重新启动。

重启节点：

1. 在「节点管理」>「节点维护」页面，选定需要重新启动的节点。
2. 点击 重启 ，之后按页面提示操作。

   ----完成

重启时，节点会离线一段时间。重启完成后，节点将自动上线。节点从离线到重新上线的过程可能需要 1~2 分钟，请耐心等待。您可以点击此页面的 刷新 查看节点最新状态。

复位

使用复位功能，可以同时将 1 个或多个节点恢复出厂设置。

复位节点：

1. 在「节点管理」>「节点维护」页面，选定需要复位的节点。
2. 点击 复位 ，之后按页面提示操作。

   ----完成

导出

使用导出功能，可以将节点列表信息以 Excel 的格式导出并保存到管理主机。

导出节点列表信息到管理主机：

在「节点管理」>「节点维护」页面，点击 导出 ，之后按页面提示操作。

删除

使用删除功能，可以同时删除 1 个或多个处于离线状态的节点的相关信息。

单个删除：在「节点管理」>「节点维护」页面，点击对应节点操作栏的 。

批量删除：在「节点管理」>「节点分组」页面，勾选要删除的节点，点击 删除 。

刷新

如果要更新页面显示的节点信息，请点击 刷新 。

修改

使用修改功能，可以单独修改某一节点的配置信息，如国家或地区、信道、发射功率等参数。

修改某一节点的配置：

1. 在「节点管理」>「节点维护」页面，找到需要修改配置的节点，然后点击对应操作栏的 进入配置窗口。
2. 根据需要修改各项参数。

3. 点击 保存 。

---完成

保存修改后，新的配置自动下发到对应节点。

参数说明

标题项	说明
国家或地区	选择节点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。
网络模式	该频段的无线网络模式。 2.4GHz 频段支持设置 11b、11g、11b/g、11b/g/n 和 n+256QAM。 – 11b：仅允许 802.11b 无线设备接入节点的 2.4GHz 无线网络。 – 11g：仅允许 802.11g 无线设备接入节点的 2.4GHz 无线网络。 – 11b/g：允许 802.11b、802.11g 无线设备接入节点的 2.4GHz 无线网络。 – 11b/g/n：允许 802.11b、802.11g 以及工作在 2.4GHz 频段的 802.11n 无线设备接入节点的 2.4GHz 无线网络。 – n+256QAM：802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备可以接入节点的 2.4GHz 无线网络。 QAM，Quadrature Amplitude Modulation，正交幅度调制。QAM 是一种在两个正交载波上进行幅度调制的调制方式，它利用正弦波和余弦波的正交性，同时调制两路信号，提高了调制效率。n+256QAM 是在 2.4GHz 频段，让 IEEE 802.11n 标准改用 IEEE 802.11ac 的 256-QAM 调制模式，单流速率也从 IEEE 802.11n 标准的 150Mbps 提升至 IEEE 802.11ac 标准的 200Mbps。 需要注意的是，这种提升只有在 2.4GHz 频段且发射端和接收端均支持的情况下才有效，任何一方不支持 n+256QAM，那 2.4GHz 频段下单流速率最高仍然是 150Mbps。而且在调制模式改为 n+256QAM 后，网络的稳定度及抗干扰性都比其他模式下要逊色。 5GHz 频段支持设置 11a、11ac 和 11a/n。 – 11a：仅允许 802.11a 无线设备接入节点的 5GHz 无线网络。 – 11ac：仅允许 802.11ac 无线设备接入节点的 5GHz 无线网络。 – 11a/n：允许 802.11a 及工作在 5GHz 频段的 802.11n 无线设备接入节点的 5GHz 无线网络。
信道带宽	节点无线信道的频带宽度。高信道带宽下，更容易获得较高的传输速率，但穿透性稍差，传输距离近。 – 20MHz：节点使用 20MHz 的信道带宽。 – 40MHz：节点使用 40MHz 的信道带宽。 – 20/40MHz：节点根据周围环境干扰情况，自动调整其信道带宽为 20MHz 或 40MHz。仅 2.4GHz 无线网络支持。 – 80MHz：节点使用 80MHz 的信道带宽。仅 5GHz 无线网络支持。

标题项	说明
信道	节点无线数据传输的通道，可选择范围由当前选择的国家或地区、无线工作频段来决定。 – 不配置：不改变节点当前配置。 – 自动：节点自动检测各信道利用率，并据此选择合适的工作信道。 如果在使用节点无线网络时，经常出现掉线、卡顿或网速慢现象，可以尝试修改节点的信道来解决问题。 您可以通过工具软件（如 WiFi 分析仪）获得周边较少用到、干扰较小的信道。
发射功率	节点对应频段的无线发射功率。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。 不配置：不改变节点当前的配置。
接入信号强度限制	节点对应频段可接受的最低无线信号强度，信号强度低于此值的设备将无法接入节点。 当环境中存在多个节点时，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节点。
客户端老化时间	客户端连接到节点的无线网络后，如果在该时间段内没有数据通信，节点主动断开该客户端。
APSD	Automatic Power Save Delivery，自动省电模式。是 Wi-Fi 联盟的 WMM 省电认证协议。启用 WMM 后，开启“APSD”能降低节点的电能消耗。

3.5 智能优化

通过智能优化功能，您可以对整个免布线网络系统进行优化，以获得更好的用户体验。

进入页面：点击「智能优化」。

3.5.1 有线组网

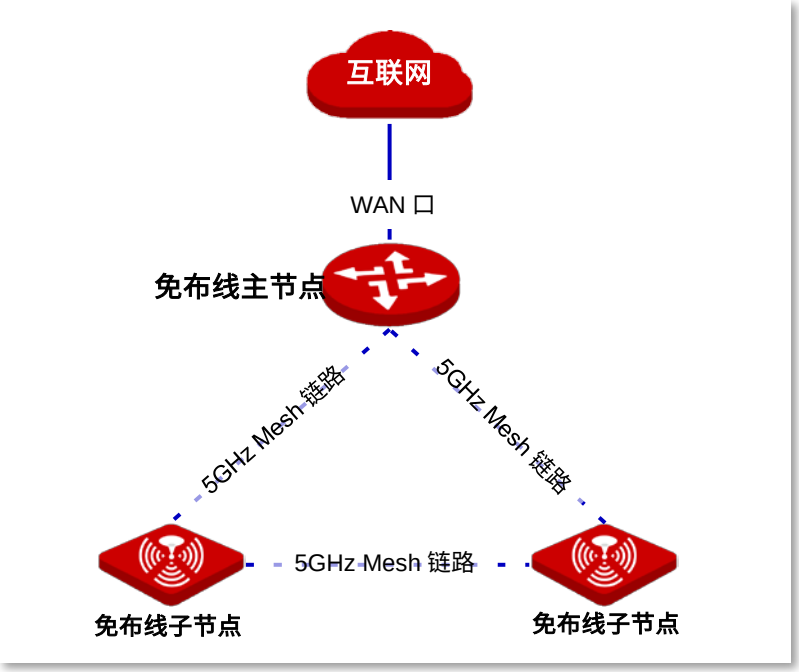
概述

免布线设备支持两种组网方式：无线组网、有线组网。默认采用无线组网方式。

- **无线组网**

使用无线方式组建免布线网络系统，各个免布线设备之间通过无线连接。此时，免布线设备将其中一个 5GHz 无线频段专门用于建立免布线链路，将 2.4GHz 无线频段和另外一个 5GHz 无线频段用于终端设备接入。

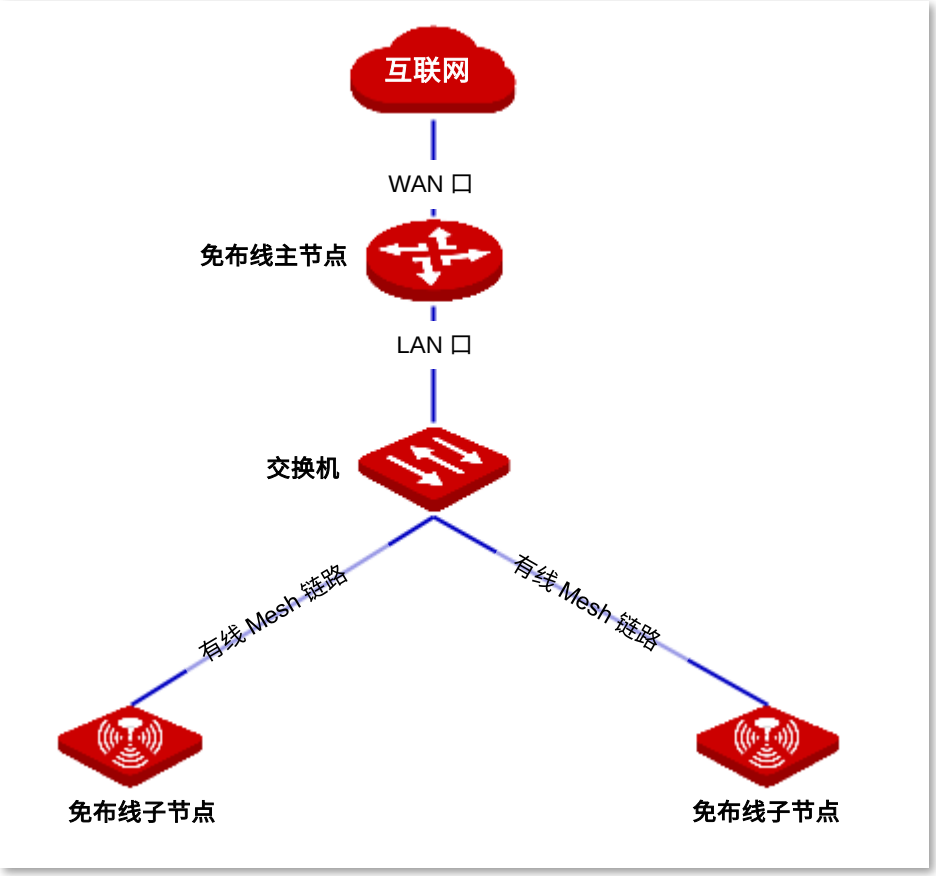
无线组网连接图示如下。



- **有线组网**

使用有线方式组建免布线网络系统，各个免布线设备之间通过网线连接。此时，免布线设备的三个无线频段都用于终端设备接入。

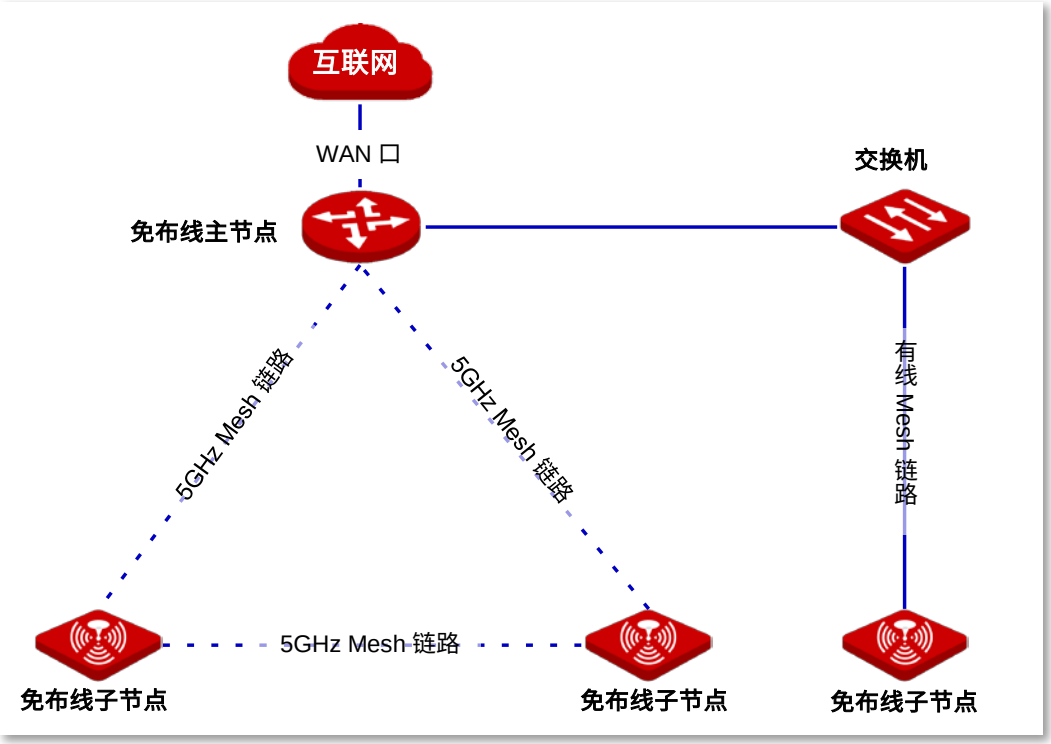
有线组网连接图示如下。



总的来说，无线组网更简单快捷，有线组网对网络布线有一定要求，但它也有以下优势：

- Mesh 链路稳定，速率高，传输距离远
- 无线带机量更高

实际组网中，您也可以根据需要，采用混合组网方式。组网连接图如下图示例。



配置有线组网

提示

开启有线组网后，无线组网功能自动关闭，已通过无线组网的免布线设备将会掉线。

1. 在「智能优化」页面的“有线组网”模块，找到要修改组网方式的节点，点击“有线组网”栏的滑块至。

参数说明

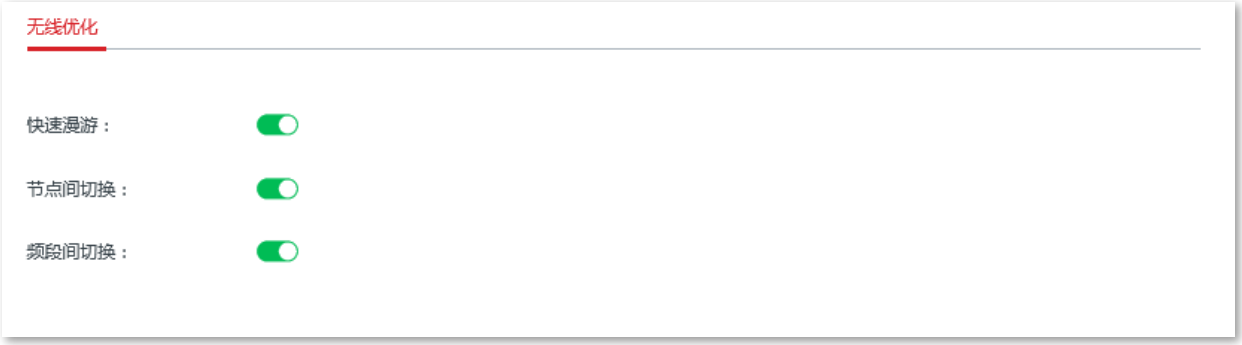
标题项	说明
型号	节点的型号及版本。
备注	节点的备注信息。可以在「节点管理」>「节点维护」页面修改。
IP 地址	节点的 IP 地址。
MAC 地址	节点的物理地址。
状态	有线组网功能的启用状态。
有线组网	开启/关闭节点的有线组网功能。 开启后，节点的组网方式由无线组网转为有线组网，节点的三个无线频段都用于终端接入。

2. 用网线将上述各节点连接起来。

----完成

3.5.2 无线优化

在这里，您可以通过调节快速漫游、节点间切换、频段间切换的启用状态来优化免布线系统的无线体验。



参数说明

标题项	说明
快速漫游	开启后，支持 802.11r 快速漫游协议的客户端在接收到节点无线信号降至其漫游触发临界值时，自动漫游切换到其他节点，这一过程只需毫秒级的时间。开启此功能，可以降低用户在节点之间移动时业务所受的影响。 注意：此功能需要各节点使用相同的无线名称/密码。

标题项	说明
节点间切换	开启后，支持 802.11k、802.11v 协议的客户端能够获得节点的相关网络信息，并根据这些信息判断是否需要切换到其他网络质量更好的节点。开启此功能，可以有效分散客户端使其连接到更合适的节点。 注意：此功能需要各节点使用相同的无线名称/密码。
频段间切换	开启后，当双频客户端连接节点时，节点会根据当前各频段的网络质量情况，引导客户端连接到质量更好的频段。 注意：此功能需要节点的 2.4GHz 频段和 5GHz 使用相同的无线名称/密码。

3.6 静态 IP 分配

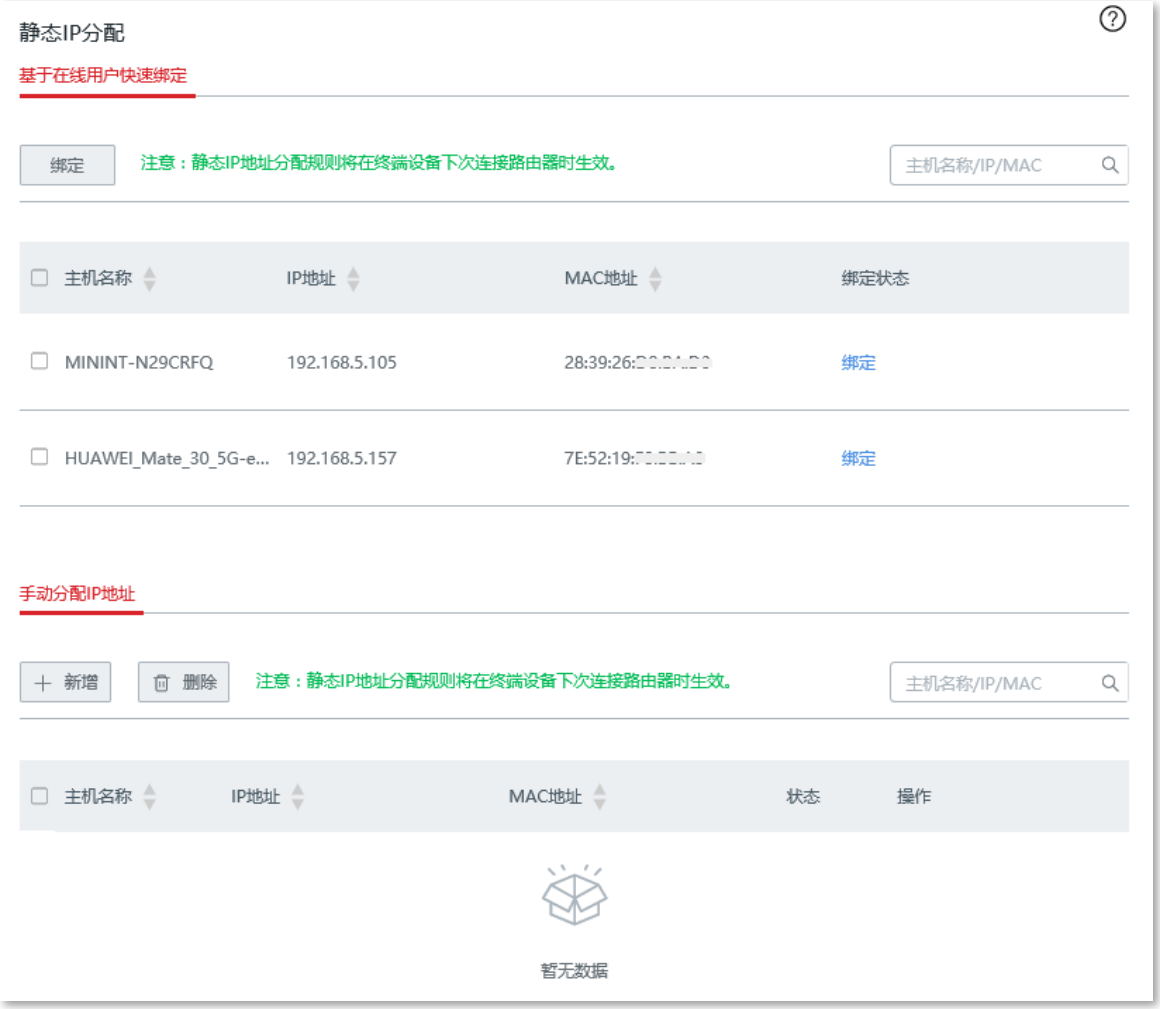
3.6.1 概述

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

本功能仅在节点的“DHCP 服务器”功能开启时生效。节点支持以下两种静态 IP 地址分配方式：

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

进入页面：点击「静态 IP 分配」。



参数说明

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

3.6.2 分配静态 IP 地址

如果要给已连接到免布线网络的客户端分配 IP 地址，推荐在“基于在线用户快速绑定”模块进行设置。客户端未连接到免布线网络时，请在“手动分配 IP 地址”模块进行设置。

基于在线用户快速绑定

绑定单个客户端的 IP 地址：

在「静态 IP 分配」页面的“基于在线用户快速绑定”模块，找到要分配固定 IP 地址的客户端，点击绑定。

同时绑定多个客户端的 IP 地址：

在「静态 IP 分配」页面的“基于在线用户快速绑定”模块，选择多个要分配固定 IP 地址的客户端，点击 绑定 。

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

手动分配 IP 地址

在「静态 IP 分配」页面的“手动分配 IP 地址”模块，点击 + 新增 ，在弹出窗口配置各项参数，然后点击 保存 。

提示

点击 + 可以新增一条规则；点击 - 可以删除未保存的规则。

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

3.7 网速控制

3.7.1 概述

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

进入页面：点击「网速控制」。

参数说明

标题项		说明
WAN 口宽带	上传速率 下载速率	填入您办理的宽带的带宽值。不清楚时，可以咨询您的 ISP。
限速方式	不限速	不对局域网用户的上传/下载速率进行限制。
	自定义限速	网络管理员根据实际环境需要，为连接到免布线网络的用户单独设置最大上传/下载速率，或统一设置最大上传/下载速率。 相较于分组限速来说，自定义限速设置更加灵活。
	自动分配网速	系统根据「网速控制」页面设置的 WAN 口上传/下载速率，平均地给局域网用户分配带宽。
	分组限速	网络管理员根据实际环境需要，分组进行网速控制。

标题项	说明
	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。

3.7.2 自定义限速

- **场景 1：假设要为连接到免布线网络的用户单独设置最大上传/下载速率。**

设置步骤：

1. 点击「网速控制」。
2. 选择“限速方式”为“自定义限速”。
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。
4. 设置对应主机的最大上传/下载速率。
5. 点击页面底端的 保存 。

----完成

参数说明

标题项	说明
主机名称	用户设备的基本信息，包括设备上报的设备名称、连接到免布线网络的方式、IP 地址和 MAC 地址。可根据需要点击 修改主机名称。

标题项	说明
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。当该用户为离线状态时显示此项。
上传速率 下载速率	该用户的实时上传/下载速率。
最大上传速率 最大下载速率	限定该用户使用的最大上传/下载速率。

■ **场景 2：假设要为局域网所有在线用户或离线用户统一设置最大上传/下载速率。**

设置步骤：

1. 点击「网速控制」。
2. 选择“限速方式”为“自定义限速”。
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。
4. 点击 全部限速 。

5. 为局域网所有的在线（或离线）用户设置最大上传速率和下载速率，然后点击 保存 。

----完成

3.7.3 自动分配网速

为连接到免布线网络的在线用户平均分配网速。

设置步骤：

1. 点击「网速控制」。
2. 根据 ISP 提供的带宽，设置对应 WAN 口的上传/下载速率。
3. 选择“限速方式”为“自动分配网速”。
4. 点击页面底端的 保存 。

----完成

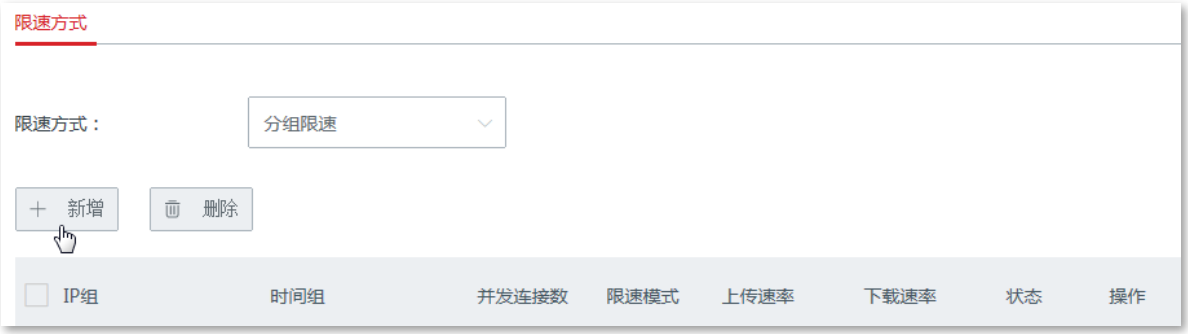
3.7.4 分组限速

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

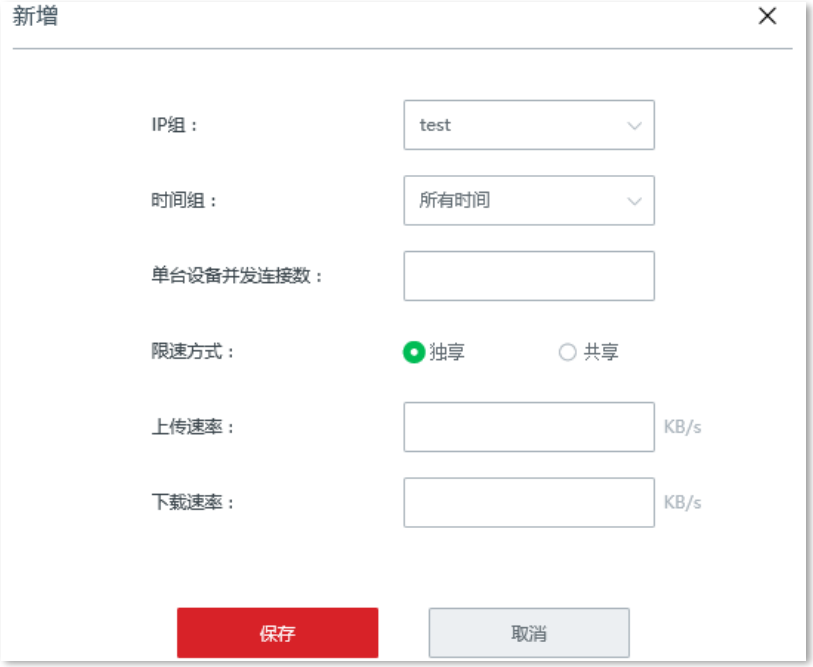
提示

配置分组限速规则前，请先配置好相应的 IP 组和时间组。

1. 点击「网速控制」。
2. 选择“限速方式”为“分组限速”。
3. 点击 + 新增 。



4. 在【新增】窗口配置各项参数。
5. 点击 保存 。



----完成

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

参数说明

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

3.7.5 分组限速配置举例

组网需求

某企业使用免布线设备进行网络搭建。

要求：局域网中采购部（IP 地址为 192.168.5.2~192.168.5.10）的每位员工在星期一到星期五的上班时间（8:00~18:00）都能使用 1Mbps（1Mbps=128KB/s）的固定上下行带宽。对于局域网其他设备，不限制使用带宽。

方案设计

使用“分组限速”功能实现上述需求。假设每台用户设备的并发连接数为 600。

配置步骤

配置流程图：

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。

2. 配置 IP 组。

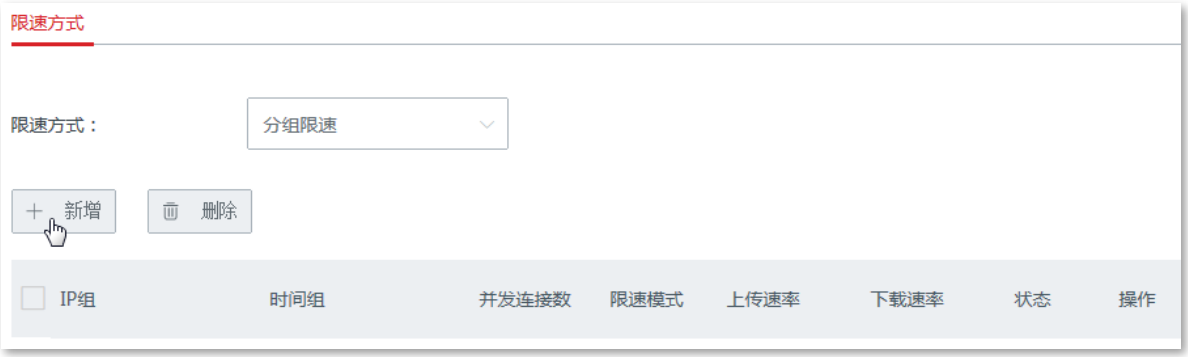
进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

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 。

4. 添加“分组限速”规则。

(1) 进入“网速控制”页面，点击 + 新增 。



(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”。
- 设置单个客户端并发连接数，本例为“600”。
- 选择限速方式，本例为“独享”。
- 设置客户端的最大上传/下载速率，本例均为“128KB/s”。

----完成

验证配置

IP 地址在 192.168.5.2~192.168.5.10 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。

3.8 行为管理

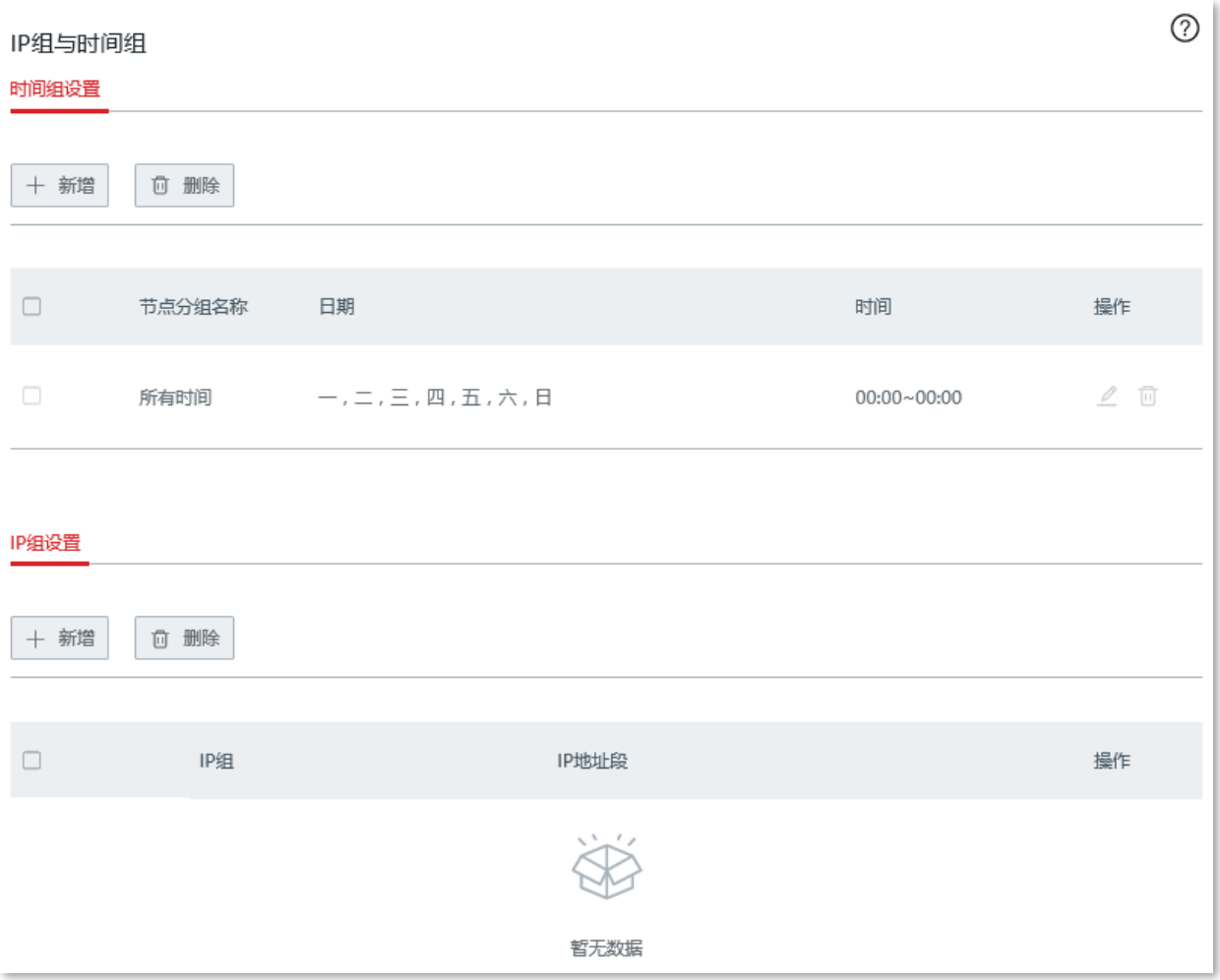
3.8.1 IP 组与时间组

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、网站过滤和分组限速等基于 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。

节点默认已添加 1 条时间组，如下图示。默认时间组不支持删除和编辑操作。



参数说明

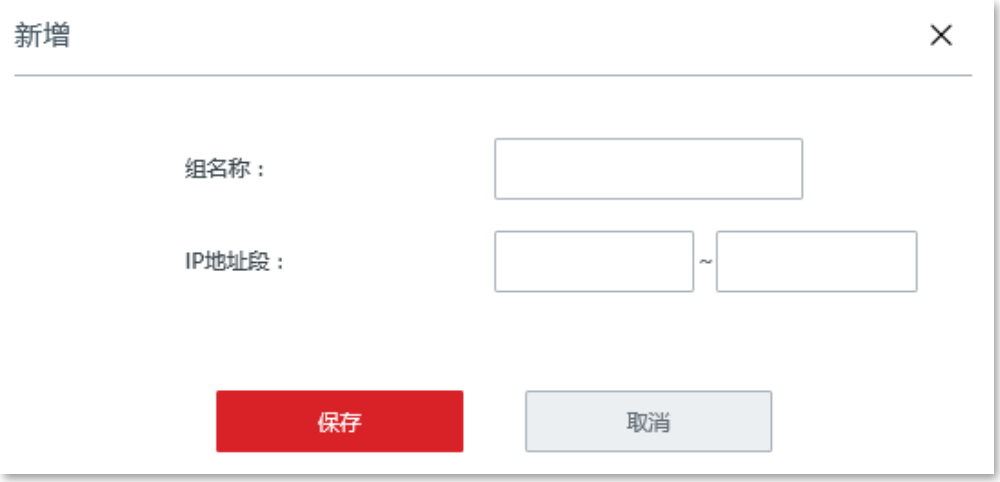
标题项		说明
时间组设置	时间组	时间组的名称。
	日期	时间组所包含的日期。
	时间	时间组的开始~结束时间。00:00~00:00，表示全天。
	操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
IP 组设置	IP 组	IP 组的名称。
	IP 地址段	IP 组的开始~结束 IP 地址。
	操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。

新增时间组

在「行为管理」>「IP 组与时间组」页面的“时间组设置”模块，点击 + 新增 ，在弹出的窗口中配置各项参数，然后点击 保存 。

新增 IP 组

在「行为管理」>「IP 组与时间组」页面的“IP 组设置”模块，点击 + 新增 ，在弹出的窗口中配置各项参数，然后点击 保存 。



3.8.2 MAC 地址过滤

概述

通过 MAC 地址过滤功能，可以允许或禁止指定用户通过节点上网。

进入页面：点击「行为管理」>「MAC 地址过滤」。

MAC 地址过滤功能默认关闭，开启后，页面显示如下。

参数说明

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

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

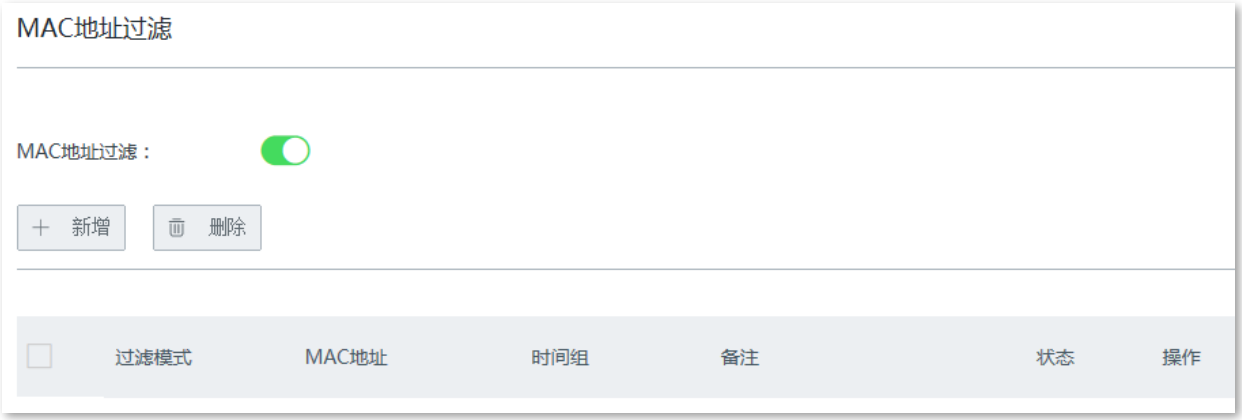
配置 MAC 地址过滤

提示

配置 MAC 地址过滤规则前，请先配置好相应的时间组。

开启 MAC 地址过滤功能

在「行为管理」>「MAC 地址过滤」页面，点击“MAC 地址过滤”滑块至，然后点击页面底端的保存。



新增 MAC 地址过滤规则

在「行为管理」>「MAC 地址过滤」页面点击 + 新增，然后在弹出窗口中配置各项参数，点击 保存。

MAC 地址过滤配置举例

组网需求

某企业使用免布线设备进行网络搭建。

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

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

配置步骤

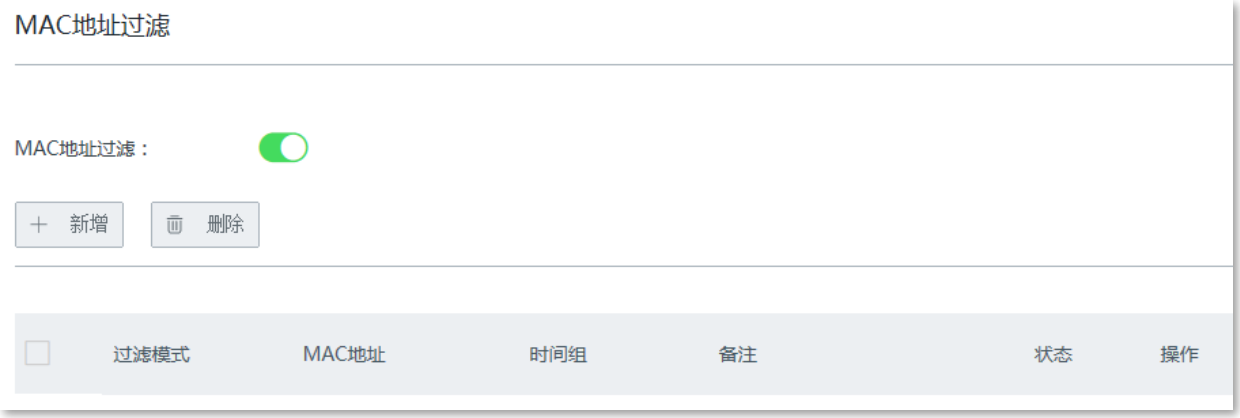
配置流程图：

一、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。

二、开启 MAC 地址过滤功能

在「行为管理」>「MAC 地址过滤」页面，点击“MAC 地址过滤”滑块至，然后点击页面底端的保存。



三、配置 MAC 地址过滤规则

1. 新增 MAC 地址过滤规则。

(1) 在「行为管理」>「MAC 地址过滤」页面，点击 + 新增 。

(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“采购 1”。

2. 禁止未启用规则中的主机和列表外的主机访问互联网。

(1) 取消勾选“允许未启用规则中的主机和列表外的主机访问互联网”。

(2) 点击页面底端的 保存 。

----完成

验证配置

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。

3.8.3 IP 地址过滤

概述

通过 IP 地址过滤功能，可以允许或禁止指定用户通过节点上网。

进入页面：点击「行为管理」>「IP 地址过滤」。

IP 地址过滤功能默认关闭，开启后，页面显示如下。

参数说明

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

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

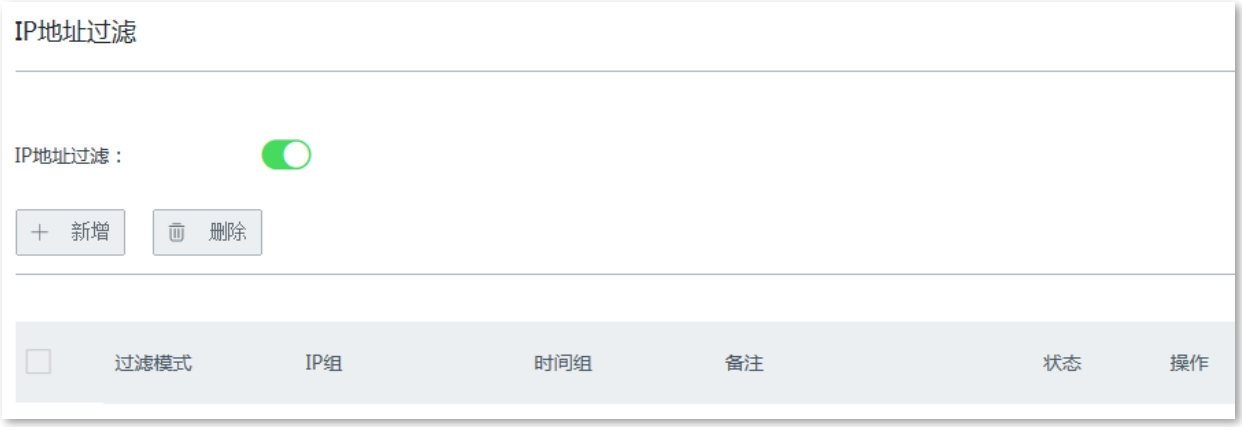
配置 IP 地址过滤

提示

配置 IP 地址过滤规则前，请先配置好相应的 IP 组和时间组。

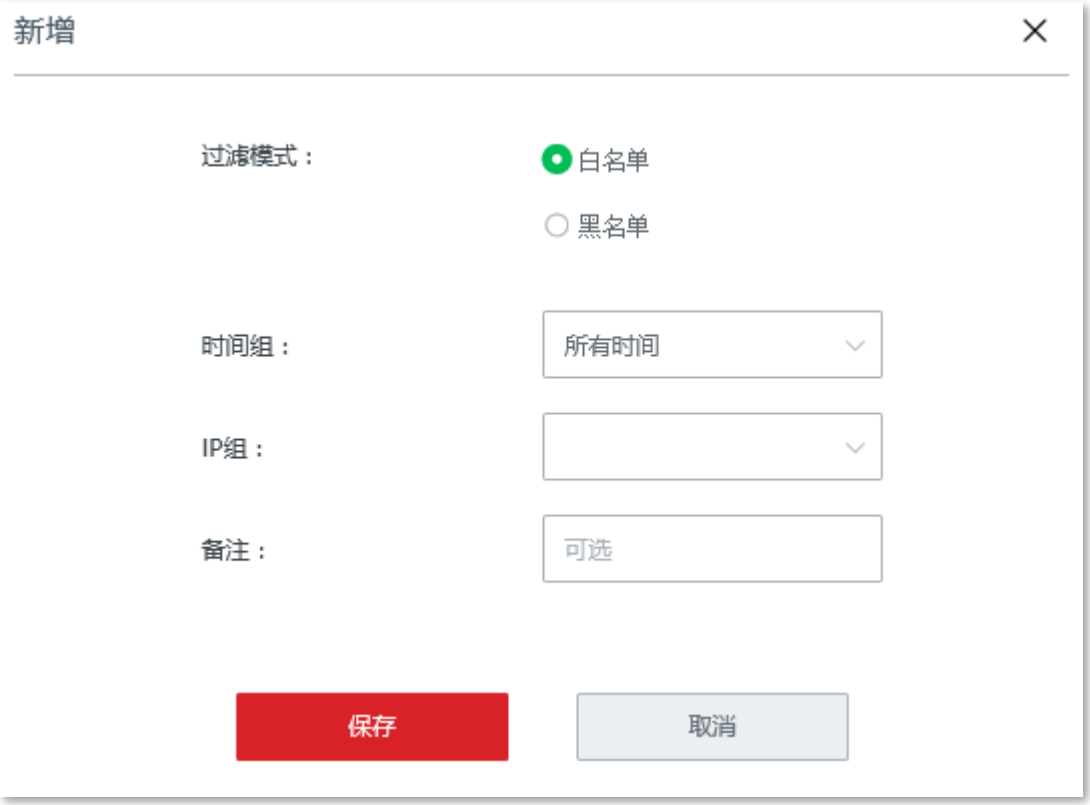
开启 IP 地址过滤功能

在「行为管理」>「IP 地址过滤」页面，点击 IP 地址过滤滑块至，然后点击页面底端的 保存 。



新增 IP 地址过滤规则

在「行为管理」>「IP 地址过滤」页面，点击 + 新增 ，然后在弹出窗口中配置各项参数，点击 保存 。



IP 地址过滤配置举例

组网需求

某企业使用免布线设备进行网络搭建。

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

使用 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 地址范围为 192.168.5.2~192.168.5.10。

配置步骤

配置流程图：

一、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。

二、配置 IP 组

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

三、开启 IP 地址过滤功能

在「行为管理」>「IP 地址过滤」页面，点击 IP 地址过滤滑块至 ，然后点击页面底端的 保存 。

四、配置地址过滤规则

1. 新增 IP 地址过滤规则。

(1) 在「行为管理」>「IP 地址过滤」页面，点击 + 新增 。

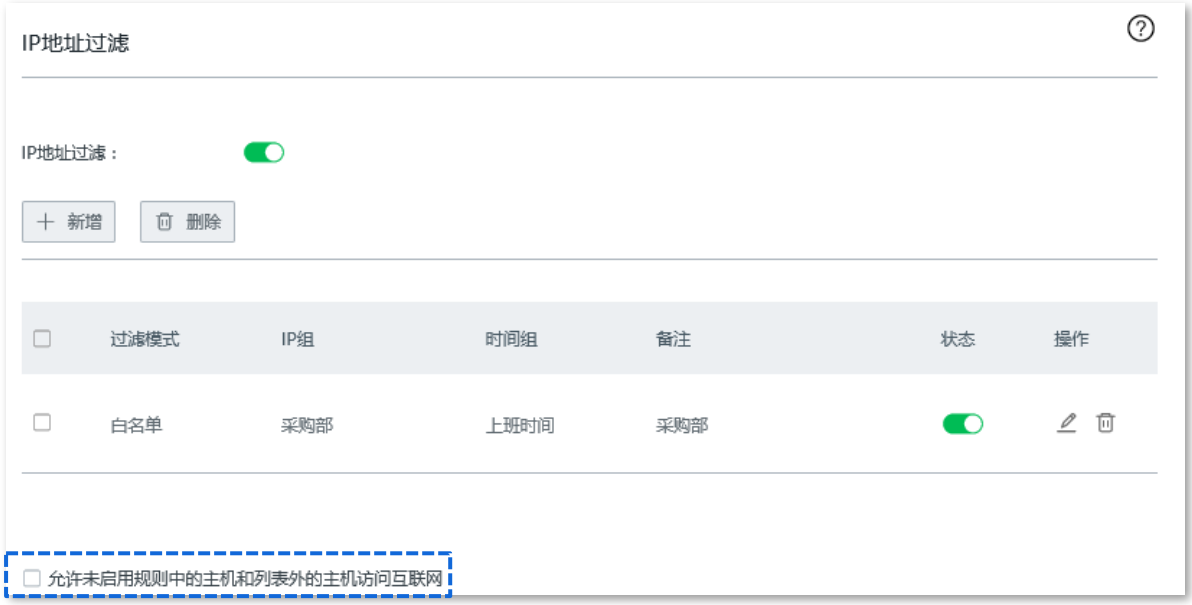
(2) 在【新增】窗口进行如下配置，然后点击 保存 。

- 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“采购部”。

2. 禁止未启用规则中的主机和列表外的主机访问互联网。

(1) 取消勾选“允许未启用规则中的主机和列表外的主机访问互联网”。

(2) 点击页面底端的 保存 。



----完成

验证配置

在星期一到星期五的 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 192.168.5.2~192.168.5.10 范围内）才能访问互联网，使用其他员工的电脑不能访问互联网。

3.8.4 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。

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

进入页面：点击「行为管理」>「端口过滤」。

端口过滤功能默认关闭，开启后，页面显示如下。

参数说明

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

标题项	说明
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	规则的状态，可根据需要开启或关闭。
操作	可对规则进行如下操作： – 点击 可以修改规则。 – 点击 可以删除规则。

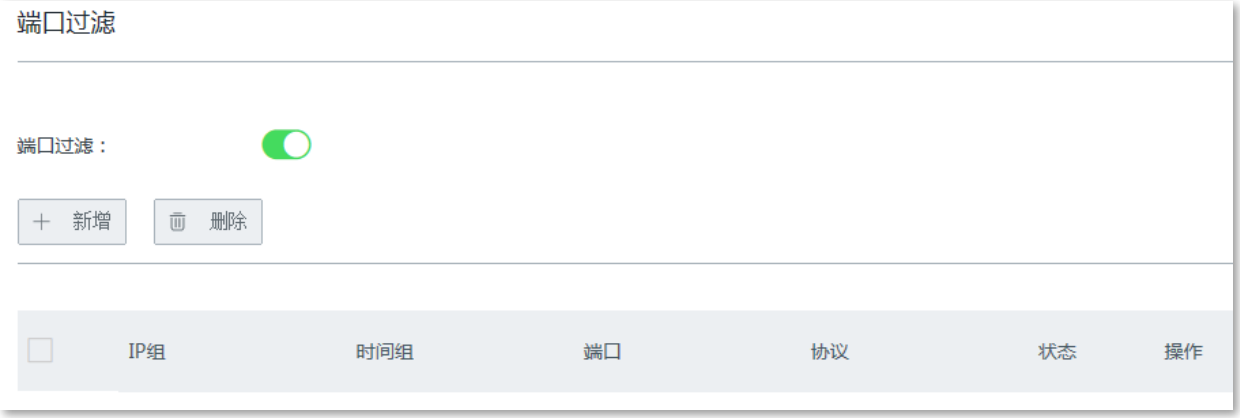
配置端口过滤

提示

配置端口过滤规则前，请先配置好相应的 IP 组和时间组。

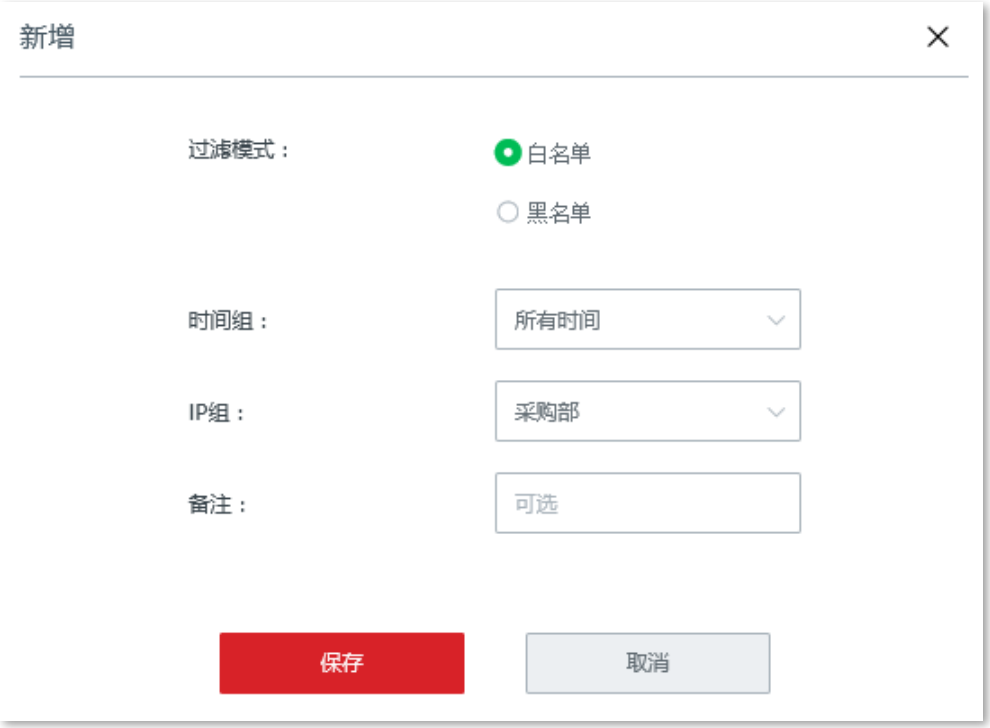
开启端口过滤功能

在「行为管理」>「端口过滤」页面，点击“端口过滤”滑块至，然后点击页面底端的 保存 。



新增端口过滤规则

在「行为管理」>「端口过滤」页面，点击 + 新增 ，在弹出的窗口中配置各项参数，然后点击 保存 。



端口过滤配置举例

组网需求

某企业使用免布线设备进行网络搭建。

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）。

方案设计

使用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 192.168.5.2~192.168.5.10。

配置步骤

配置流程图：

一、设置时间组

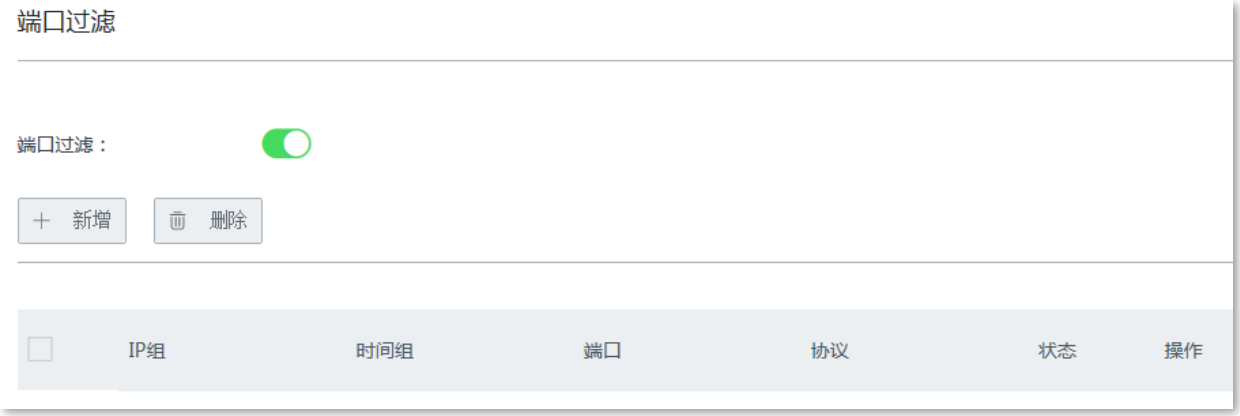
进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

二、设置 IP 组

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

三、开启端口过滤功能

在「行为管理」>「端口过滤」页面，点击“端口过滤”滑块至，然后点击页面底端的 保存 。



四、添加端口过滤规则

1. 在「行为管理」>「端口过滤」页面，点击 + 新增 。

2. 在【新增】窗口进行如下配置，然后点击 保存 。

   (1) 选择规则生效的 IP 组，本例为“财务部”。

   (2) 选择规则生效的时间组，本例为“上班时间”。

   (3) 输入浏览网页服务使用的端口号“80”。

(4) 选择服务使用的协议，建议保持默认“全部”。

添加成功，如下图示。

----完成

验证配置

星期一到星期五的 8:00~18:00，局域网中，IP 地址在 192.168.5.2~192.168.5.10 范围内的电脑不能进行网页浏览服务。

3.8.5 网站过滤

概述

通过网站过滤，允许或禁止用户访问指定类别网址，以规范局域网用户的上网行为。

进入页面：点击「行为管理」>「网站过滤」。

网站过滤功能默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
网站过滤	网站过滤功能开关。表示关闭，表示开启。
过滤模式	网站过滤模式。 – 白名单：即，允许访问互联网。允许 IP 组内的用户在对应时间段内访问指定的网站，不能访问其他网站；在其他时间段内可以访问所有网站。 – 黑名单：即，禁止访问互联网。禁止 IP 组内的用户在对应时间段内访问指定的网站，可以访问其他网站；在其他时间段内可以访问所有网站。
IP 组	规则引用的 IP 组，以指定规则对应的用户。

标题项	说明
	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。
网址	规则对应的网址分类。 网址分类应事先配置好。
状态	规则的状态，可根据需要开启或关闭。
操作	可对规则进行如下操作： - 点击 可以修改规则。 - 点击 可以删除规则。
网址管理	自定义网址分类。 提示 本设备没有内置的默认网址分类，如需快速添加网址分类，请参考特征库本地升级进行设置。

配置网站过滤

开启网站过滤功能

在「行为管理」>「网站过滤」页面，点击网站过滤滑块至，然后点击页面底端的 保存 。

添加自定义网址组

1. 在「行为管理」>「网站过滤」页面，点击 网址管理 。
2. 点击 新增分类 。
3. 在【新增】窗口配置各项参数。
4. 点击 保存 。

----完成

参数说明

标题项	说明
组名称	网址组的名称。组名称不能重复。
网址	填写要限制用户访问的网站的域名 ,或域名关键字。多条域名或域名关键字之间使用英文分号;隔开。
备注	网址组的备注信息。

新增网站过滤规则

提示

配置网站过滤规则前，请先配置好相应的 IP 组、时间组和网址分类。

1. 在「行为管理」>「网站过滤」页面，点击 + 新增 。

2. 在【新增】窗口配置各项参数。
3. 点击 保存 。


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

----完成

网站过滤配置举例

组网需求

某企业使用免布线设备进行网络搭建。

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

方案设计

使用网站过滤功能实现上述需求。假设设计部门人员电脑的 IP 地址为 192.168.5.2~192.168.5.10。

配置步骤

配置流程图：

一、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。

二、配置 IP 组

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

三、开启网站过滤功能

在「行为管理」>「网站过滤」页面，点击“网站过滤”滑块至，然后点击页面底端的 保存 。

四、添加网址组

1. 在「行为管理」>「网站过滤」页面，点击 网址管理 。

2. 点击 新增分类 。

3. 在【新增】窗口进行如下配置，然后点击 保存 。

- 设置网址组名称，如“设计网站”。
- 输入要限制用户访问的网站域名，本例为“zcool.com.cn;huaban.com;sccnn.com”。
- 设置网址组的备注信息，如“设计类”。

五、添加网站过滤规则

(1) 在「行为管理」>「网站过滤」页面，点击 + 新增 。

(2) 在【新增】窗口进行如下配置，然后点击 保存 。

- 选择“过滤模式”为“仅允许访问”。
- 选择需要限制访问网站的 IP 组，本例为“设计部”。
- 选择规则生效的时间组，本例为“上班时间”。
- （可选）设置规则备注信息，可不填。
- 选择要过滤的网址，本例为“设计网站”。


新增
过滤模式：
仅允许访问
仅禁止访问
IP组：
设计部
时间组：
上班时间
备注：
可选
网址：
网址类别
自定义
请选择
全部 反选
搜索
设计网站
保存
取消

添加成功，如下图示。


网站过滤
网站过滤：
新增
删除
过滤模式
IP组
时间组
网址
状态
操作
白名单
设计部
上班时间
设计网站

----完成

验证配置

局域网中 IP 地址在 192.168.5.2~192.168.5.10 范围内的用户在星期一到星期五的 8:00~18:00 只能访问“设计网站”网址组中的网站。

3.9 更多设置

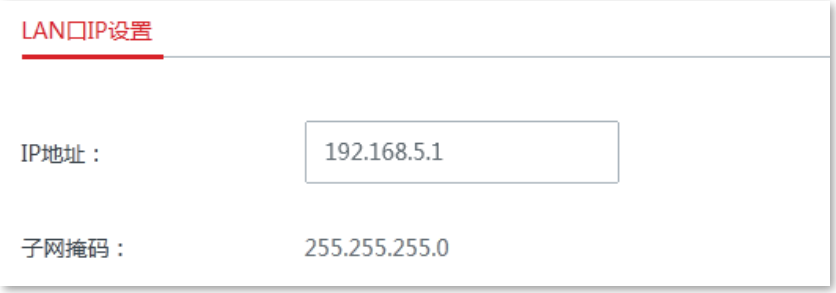
3.9.1 局域网设置

进入页面：点击「更多设置」>「局域网设置」。

在这里，您可以设置节点的 LAN 口 IP 地址和 DHCP 服务器。

LAN 口 IP 设置

LAN 口 IP 地址是节点对局域网的 IP 地址，也是节点的管理 IP 地址。节点默认的 LAN 口 IP 地址为 192.168.5.1，子网掩码为 255.255.255.0。



一般情况下，您无需修改 LAN 口设置，除非遇到 IP 地址冲突，如：节点获得的 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 192.168.5.1。

LAN 口 IP 地址修改成功后，页面将自动跳转到登录页面。如果没有，请确保管理主机的 IP 地址已设置为“自动获得 IP 地址，自动获得 DNS 服务器地址”，之后访问新的 LAN 口 IP 地址重新尝试。

提示

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

DHCP 服务器

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

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

参数说明

标题项	说明
DHCP 服务器	DHCP 服务器功能开关。表示关闭，表示开启。
起始 IP 地址	DHCP 服务器可分配的 IP 地址范围。起始 IP 地址默认为 192.168.5.100，结束 IP 地址默认为 192.168.5.200。
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。 当地址到期后： - 如果设备仍连接在免布线网络，设备将自动续约，继续占用该 IP 地址。 - 如果设备未连接（关机、网线已拔掉、无线已断开等）到免布线网络，节点将释放该 IP 地址。以后若有其它设备请求 IP 地址信息，节点可将该 IP 分配给其它设备。 如无特殊需要，建议保持默认设置。
首选 DNS	DHCP 服务器分配给局域网设备的首选 DNS 服务器 IP 地址。 免布线路由模式节点支持 DNS 代理功能，此模式下，首选 DNS 默认为节点的 LAN 口 IP 地址。 提示 一般情况下，建议保持默认设置。如需修改，为了使局域网设备能够正常上网，请务必确保您设置的首选 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。

3.9.2 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。

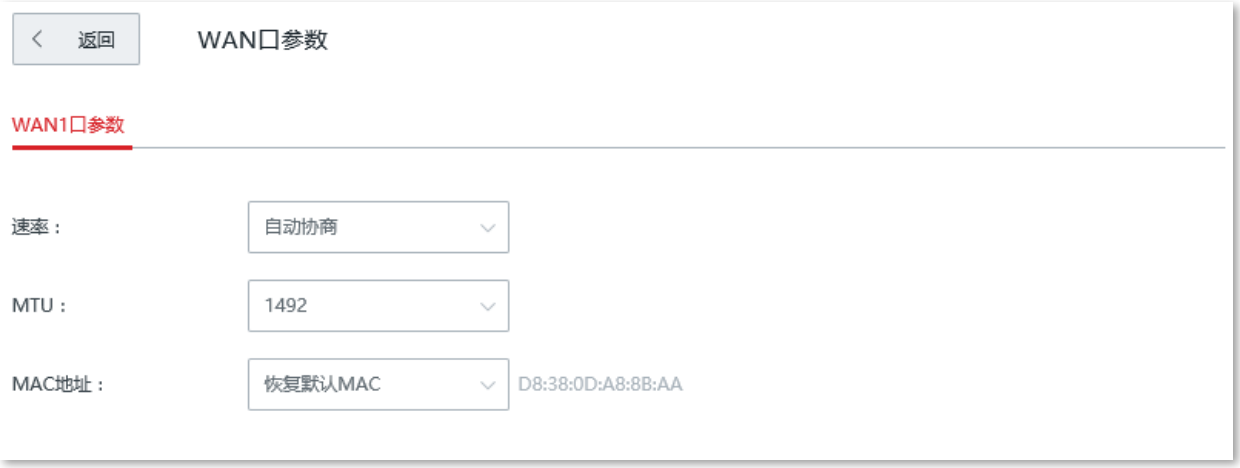
WAN 口速率

如果免布线路由模式节点的 WAN 口已正确连接网线，且网线完好，但 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，可以将该节点的 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”。

MTU

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



一般情况下，建议保持 MTU 值为默认设置，除非您遇到以下情况：

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

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

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

MAC 地址

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

注意

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

方法 1：使用之前能正常上网的电脑进行设置

1. 用网线将之前能正常上网的电脑连接到免布线网络。
2. 登录免布线路由模式节点的管理页面，点击「更多设置」>「WAN 口参数」进入设置页面。
3. 点击 MAC 地址下拉框，选择“克隆当前管理主机 MAC”。
4. 点击页面底端的 保存 。

----完成

方法 2：使用其他设备进行设置

1. 记录正确的 MAC 地址。
2. 登录免布线路由模式节点的管理页面，点击「更多设置」>「WAN 口参数」进入设置页面。
3. 点击“MAC 地址”下拉框，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”）。
4. 点击页面底端的 保存 。

----完成

提示

如果需要将 WAN 口 MAC 地址恢复为出厂 MAC 地址，请在「更多设置」>「WAN 口参数」页面，点击“MAC 地址”下拉框，选择“恢复默认 MAC”，然后点击页面底端的 保存 。

3.9.3 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。

进入页面：点击「更多设置」>「静态路由」。

参数说明

标题项	说明
目标网络	目的网络的 IP 地址。目标网络和子网掩码均为“0.0.0.0”表示默认路由。 提示 当在路由表中找不到与数据包的目的地址精确匹配的路由时，节点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	数据包从节点的接口出去后，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，即该目标网络是节点该接口直连的网络。
接口	数据从节点出去的接口。请根据需要选择相应接口。
操作	点击 可以删除规则。

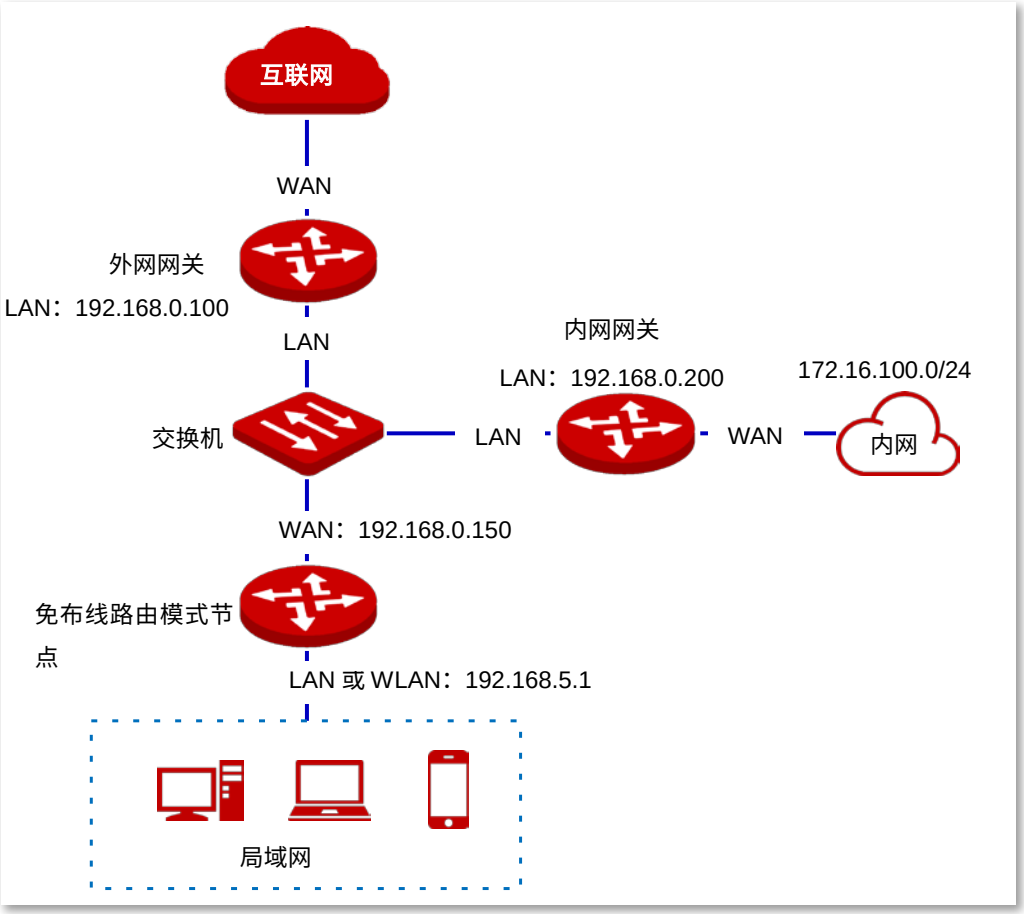
静态路由配置举例

组网需求

某企业使用免布线设备进行网络搭建。互联网、公司内网在不同的网络，节点通过自动获取外网网关分配的 IP 地址接入互联网。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

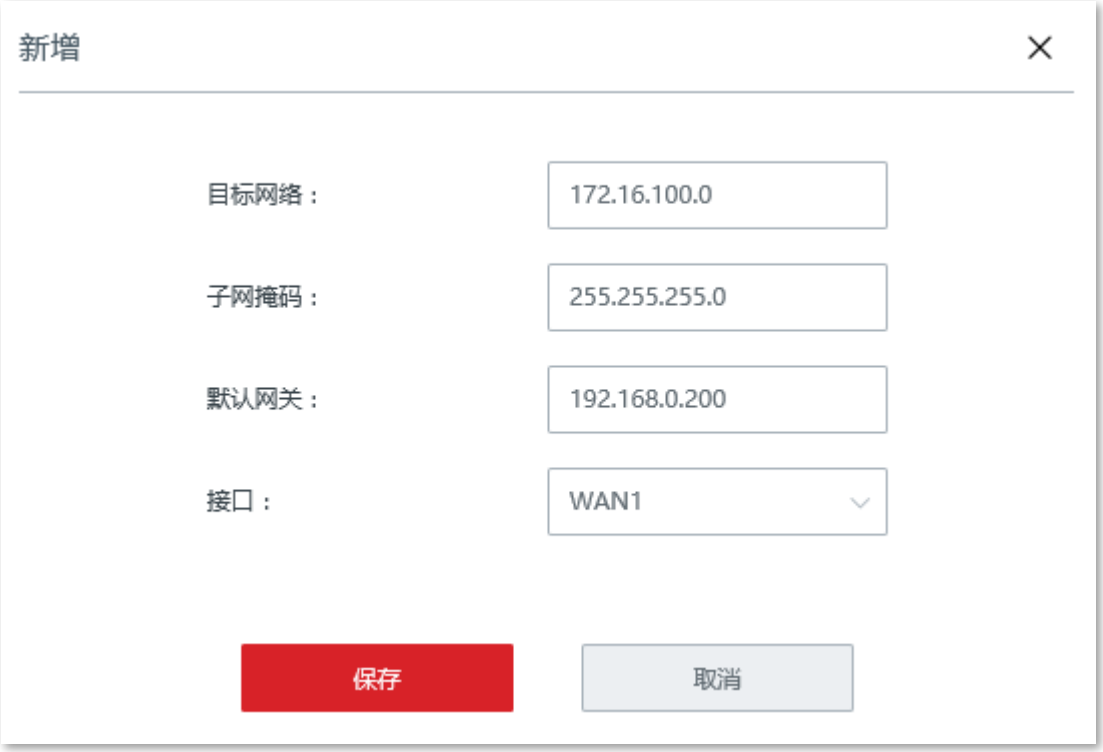
使用静态路由功能实现上述需求。组网图如下。



配置步骤

1. 在「更多设置」>「静态路由」页面，点击 + 新增 。

2. 在【新增】窗口配置下述参数。
   - 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“192.168.0.200”。
   - 选择节点与目标网络通信的接口，本例为“WAN1”。
3. 点击 保存 。



----完成

添加成功。

验证配置

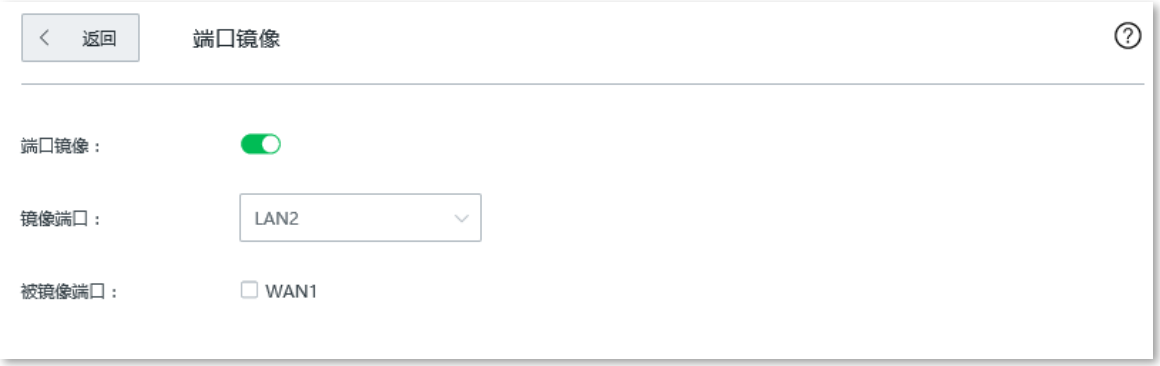
局域网中的用户可以同时访问互联网和公司内网。

3.9.4 端口镜像

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

进入页面：点击「更多设置」>「端口镜像」。

端口镜像默认关闭，开启后，页面显示如下。



参数说明

标题项	说明
端口镜像	端口镜像功能开关。表示关闭，表示开启。
镜像端口	监控端口，该端口下的设备要安装监控软件。镜像端口默认为 LAN2。
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。

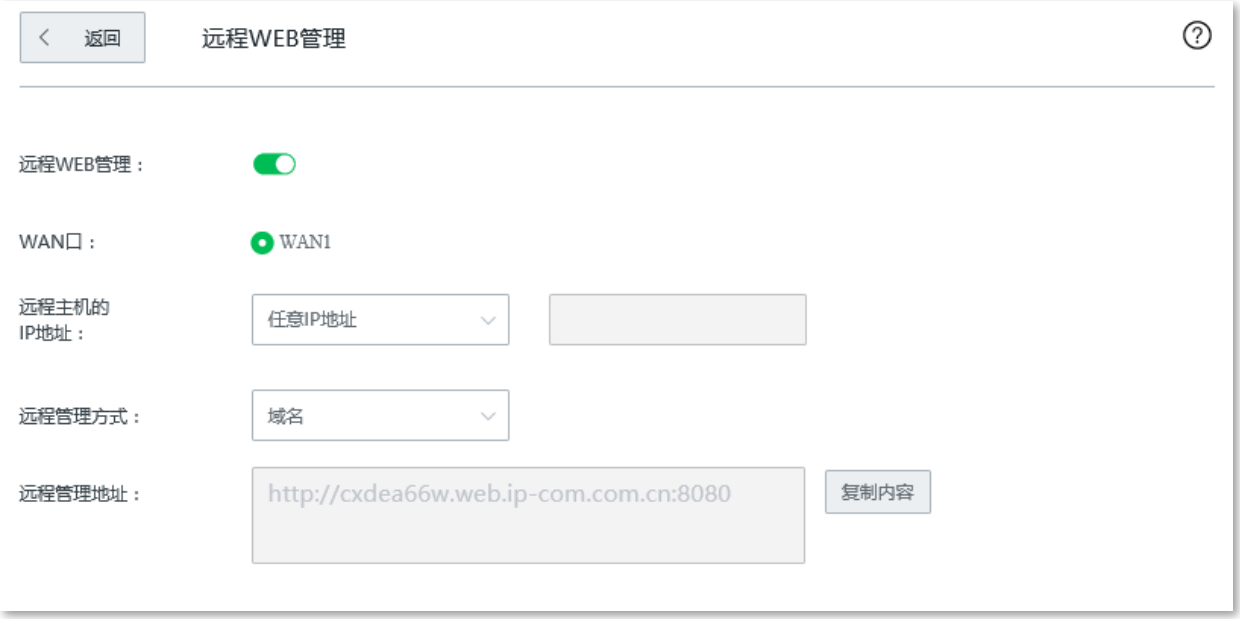
3.9.5 远程 WEB 管理

概述

一般情况下，只有接到节点的 LAN 口或无线网络的设备才能登录节点的管理页面。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 口远程访问节点的管理页面。

进入页面：点击「更多设置」>「远程 WEB 管理」。

远程 WEB 管理默认关闭，开启后，页面显示如下。



参数说明

标题项	说明
远程 WEB 管理	远程 WEB 管理功能开关。表示关闭，表示开启。
WAN 口	节点的 WAN 口，即远程访问节点管理页面时所使用的 WAN 口。
远程主机的 IP 地址	可以远程访问节点管理页面的设备的 IP 地址。 – 任意 IP 地址：互联网上任意 IP 地址的设备都能访问节点的管理页面。为了网络安全，不建议选择此项。 – 特定 IP 地址：只有指定 IP 地址的设备能远程访问节点的管理页面。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）。
远程管理方式	实现远程访问节点管理页面的方式。 – 域名：默认方式。节点自动生成一个唯一的远程管理地址，互联网用户访问该远程管

标题项	说明
	理地址可以登录到节点的管理页面。 – IP 地址：互联网用户通过在浏览器地址栏中输入 **http://节点 WAN 口的 IP 地址:端口号**来访问节点的管理页面。
远程管理地址	远程管理方式为“域名”时有效。 远程管理节点时使用的域名。开启“远程 WEB 管理”，并选择远程管理方式为“域名”后，互联网用户可以访问此域名登录到节点的管理页面。
端口号	远程管理方式为“IP 地址”时有效。 远程管理节点时使用的端口号。默认为 8088，可根据需要修改。 1~1024 端口已被熟知服务占用，为避免端口冲突，强烈建议修改该端口为 1025~65535 范围内的端口。

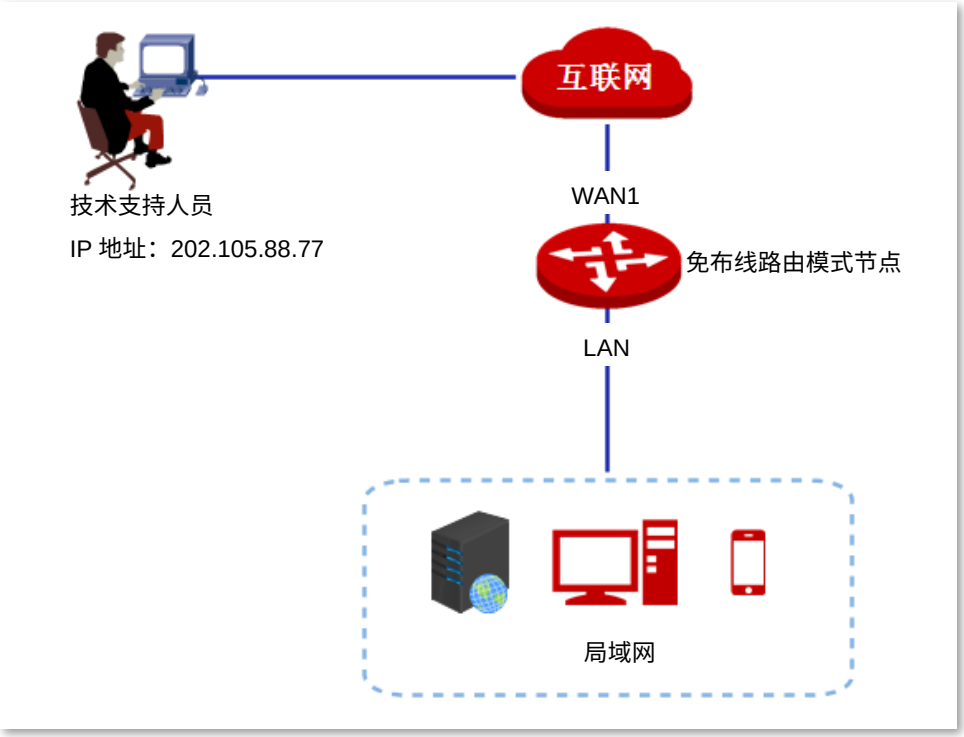
远程 WEB 管理配置举例

组网需求

某企业使用免布线设备进行网络搭建，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本设备管理页面分析并解决。

方案设计

可以采用远程 WEB 管理功能实现上述需求。



配置步骤

1. 点击「更多管理」>「远程 WEB 管理」。
2. 点击“远程 WEB 管理”滑块至。
3. 点击“远程主机的 IP 地址”下拉框，选择“特定 IP 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”。
4. 点击页面底端的 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）上的浏览器访问 **http://cxdea66w.web.ip-com.com.cn:8080**，可以登录此免布线设备的管理页面并对其进行管理。

3.9.6 DDNS

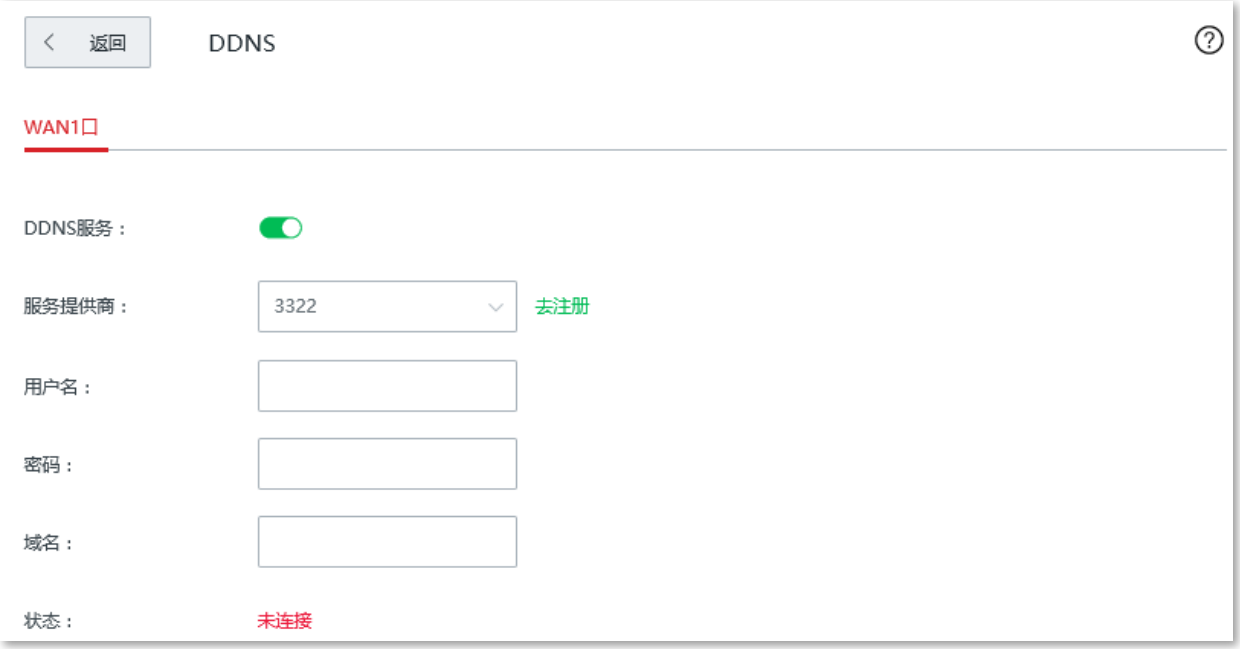
概述

DDNS，Dynamic Domain Name Server，动态域名服务。当服务运行时，节点上的 DDNS 客户端将节点当前的 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，可以将节点动态变化的 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，无需再关注节点的 WAN 口 IP 地址变化。

进入页面：点击「更多设置」>「DDNS」。

DDNS 默认关闭，开启后，页面显示如下。



参数说明

标题项	说明
DDNS 服务	开启/关闭 DDNS 功能。
服务提供商	DDNS 的服务提供商。本设备支持的 DDNS 服务提供商有：3322、88ip、oray（花生壳）、gnway（金万维）。
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。暂时仅支持普通服务。
用户名	登录 DDNS 服务的用户名/密码。

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

DDNS 配置举例

组网需求

某企业使用免布线设备进行网络搭建，该设备已接入互联网，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

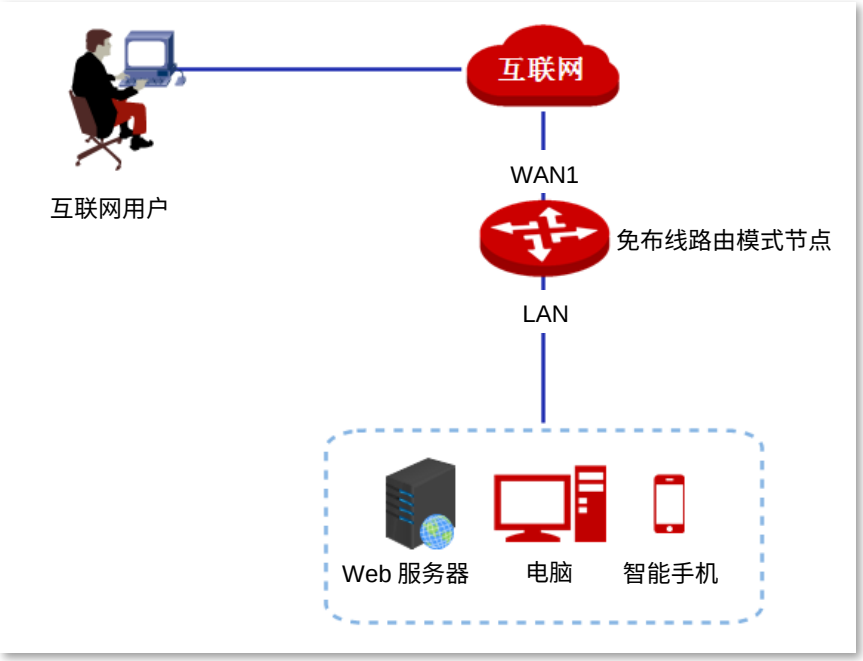
- 使用端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。
- 使用 DDNS 功能让互联网用户可以通过固定域名访问企业内部 Web 服务器，防止因 WAN 口 IP 地址变化导致访问失败。
- 使用静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.5.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999

提示

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



配置步骤

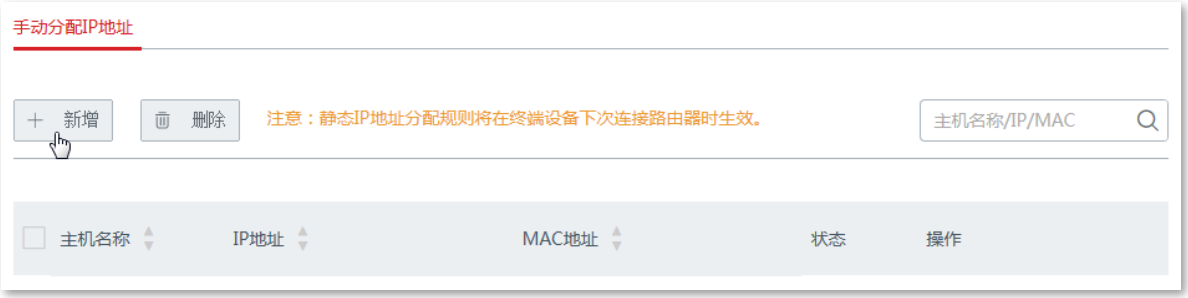
配置流程图：

一、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，可参考配置端口映射。

二、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 。



3. 在【新增】窗口进行如下配置，然后点击 保存 。
   (1) 设置固定分配给服务器主机的 IP 地址，本例为“192.168.5.250”。
   (2) 输入服务器主机的 MAC 地址，本例为“C8:9C:DC:60:54:69”。

固定 IP 地址分配完成，如下图示。

三、配置 DDNS

1. 注册域名。

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

2. 登录到节点的管理页面，设置 DDNS。

   (1) 点击「更多设置」>「DDNS」进入设置页面。

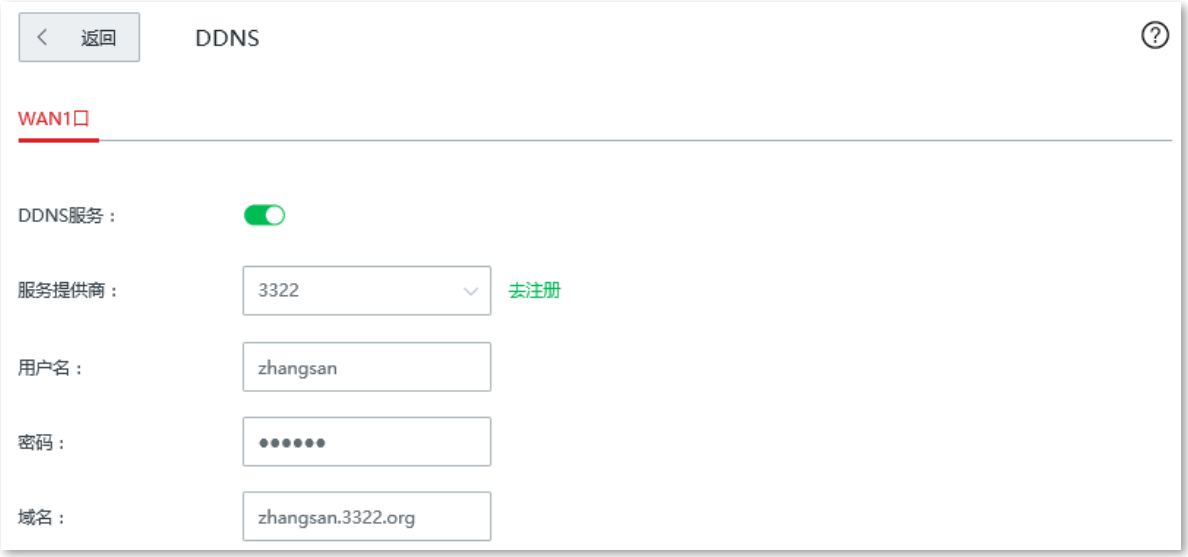
   (2) 点击“DDNS 服务”滑块至开启状态。

   (3) 点击“服务提供商”下拉框，选择您申请域名的 DDNS 提供商，本例为“3322”。

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

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

3. 点击页面底端的 保存 。



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

----完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://WAN 口域名:外网端口”可以成功访问内网服务器。

如果在配置端口映射时，设置的外网端口是内网服务的默认端口号，访问地址可以不添加外网端口号。此时，访问地址为“内网服务应用层协议名称://WAN 口域名”。

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。

3.9.7 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。利用端口映射功能，您可以开放免布线路由模式节点的一个或多个服务端口（TCP 或 UDP），并将这些端口映射到指定的局域网服务器，使节点能够将发送到该端口的服务请求转发到对应的局域网服务器。这样，广域网中的用户就能够访问局域网服务器，局域网也能避免受到侵袭。

进入页面：点击「更多设置」>「端口映射」。

参数说明

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

端口映射配置举例

组网需求

某企业使用免布线设备进行网络搭建，该设备已接入互联网，可以为局域网用户提供上网服务。现需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

方案设计

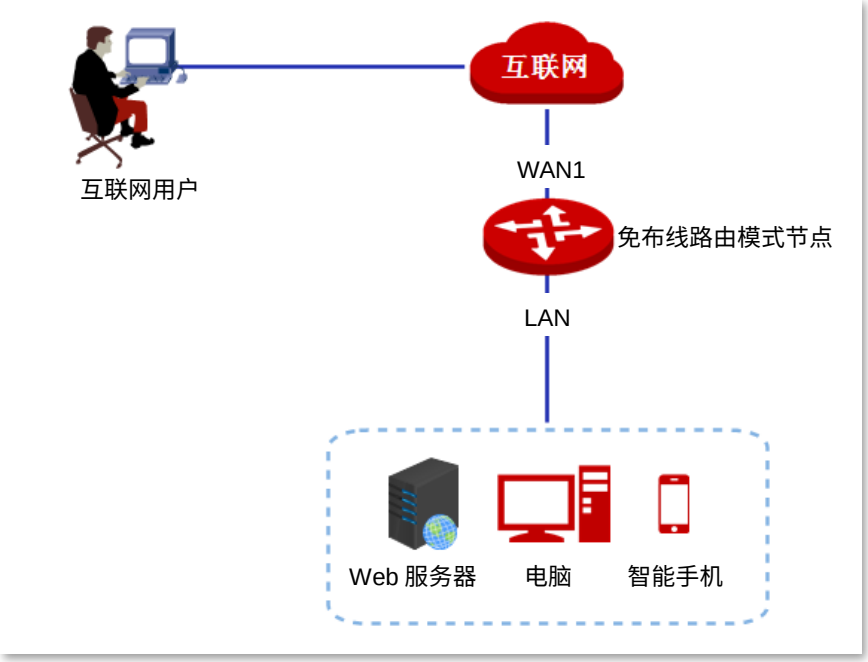
- 使用端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。假设免布线设备开放的外网端口为 9999。
- 使用静态 IP 分配功能防止因 Web 服务器 IP 地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.5.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999

提示

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



配置步骤

配置流程图：

一、配置端口映射

1. 点击「更多设置」>「端口映射」。
2. 点击 + 新增 。

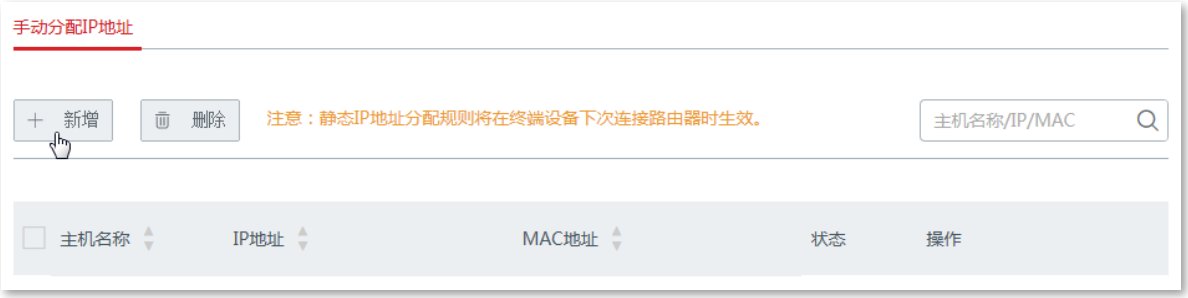
3. 在【新增】窗口进行如下配置，然后点击 保存 。
   (1) 输入 Web 服务器的 IP 地址，本例为“192.168.5.250”。
   (2) 输入内网端口，本例为 Web 服务器使用的端口“9999”。
   (3) 输入外网端口，即节点开放给广域网用户访问的端口，本例为“9999”。

(4) 选择 Web 服务器使用的协议“TCP”。

端口映射规则配置完成，如下图示。

二、给服务器主机分配固定 IP 地址

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



2. 在【新增】窗口进行如下配置，然后点击 保存 。

   (1) 设置固定分配给服务器主机的 IP 地址，本例为“192.168.5.250”。

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

固定 IP 地址分配完成，如下图示。

----完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://WAN 口 IP 地址:外网端口”可以成功访问内网服务

器。

如果在配置端口映射时，设置的外网端口是内网服务的默认端口号，访问地址可以不添加外网端口号。此时，访问地址为“内网服务应用层协议名称://WAN 口 IP 地址”。

本例中，假设 WAN1 IP 地址为 202.105.11.22，则访问地址为“http://202.105.11.22:9999”。

如果 WAN 口开启了 DDNS，还可使用“内网服务应用层协议名称://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。

3.9.8 DMZ 主机

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。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服务器资源时，也可将该局域网服务器设置为 DMZ 主机。

注意

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

进入页面：点击「更多设置」>「DMZ 主机」。

DMZ 主机默认关闭，开启后，页面显示如下。

参数说明

标题项	说明
DMZ 主机	开启/关闭 DMZ 主机功能。
DMZ 主机 IP 地址	要设置为 DMZ 主机的局域网设备的 IP 地址。
VPN 端口过滤	开启/关闭 VPN 端口过滤功能。 开启后，启用 DMZ 功能时，由免布线路由模式节点上的 VPN 服务响应外网的 VPN 请求。 注意 节点已开启 VPN 服务器功能的情况下，开启 DMZ 主机功能时，为了确保节点上的 VPN 服务器有效，请同时开启“VPN 端口过滤”功能。

DMZ 主机配置举例

组网需求

某企业使用免布线设备进行网络搭建，该设备已接入互联网，可以为局域网用户提供上网服务。现需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

方案设计

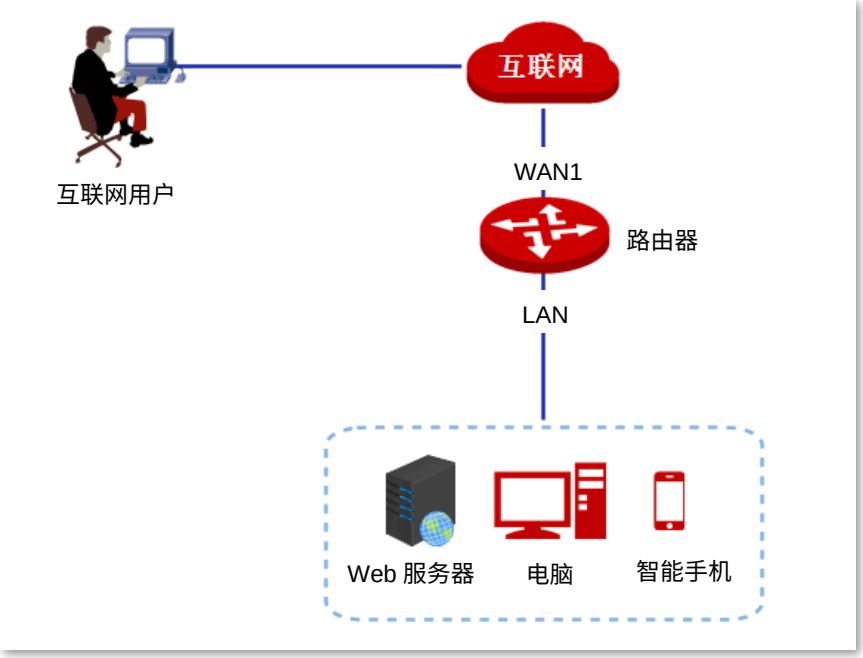
- 使用 DMZ 主机功能实现互联网用户访问企业内部 Web 服务器的需求。
- 使用静态 IP 分配功能防止因 Web 服务器 IP 地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.5.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999

提示

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



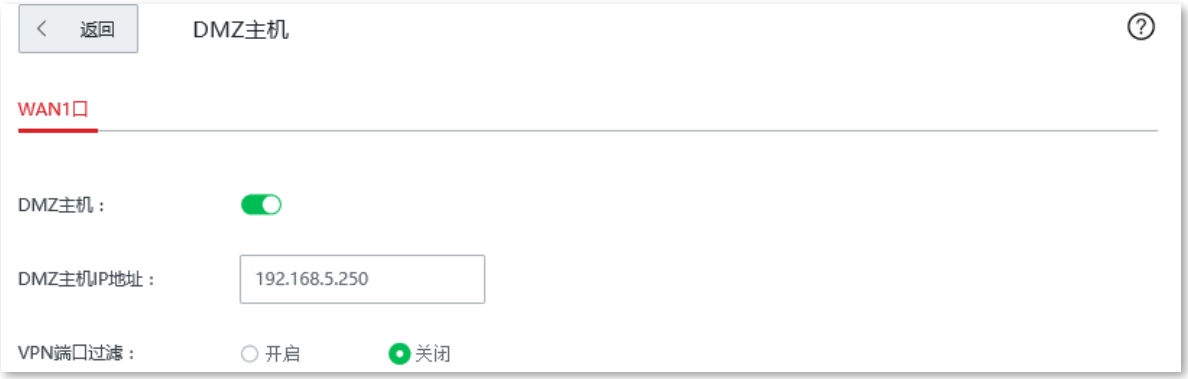
配置步骤

配置流程图：

配置 DMZ 主机 → 给 DMZ 主机分配固定 IP 地址

一、配置 DMZ 主机

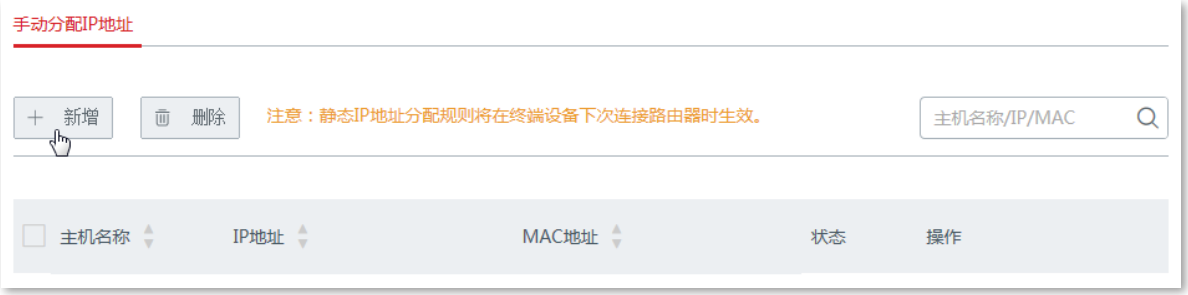
1. 点击「更多设置」>「DMZ 主机」进入配置页面。
2. 点击“DMZ 主机”滑块至。
3. 输入局域网内要设置为 DMZ 主机的设备的 IP 地址，本例为“192.168.5.250”。
4. 点击页面底端的 保存 。



二、给 DMZ 主机分配固定 IP 地址

1. 点击「静态 IP 分配」，找到“手动分配 IP 地址”模块。

2. 点击 + 新增 。



3. 在【新增】窗口进行如下配置，然后点击 保存 。

(1) 设置固定分配给服务器主机的 IP 地址，本例为“192.168.5.250”。

(2) 输入内网服务器所在的主机的 MAC 地址，本例为“C8:9C:DC:60:54:69”。

固定 IP 地址分配完成，如下图示。

----完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://WAN 口 IP 地址:内网服务端口”可以成功访问内网服务器。

如果内网服务使用的是默认端口号，访问地址可以不添加内网服务端口号。此时，访问地址为“内网服务应用层协议名称://WAN 口 IP 地址”。

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

如果 WAN 口开启了 DDNS，还可使用“内网服务应用层协议名称://WAN 口域名”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服务器，可能是 DMZ 主机上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。

3.9.9 UPnP

概述

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

开启 UPnP

在「更多设置」>「UPnP」页面，点击滑块至。

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

UPnP:

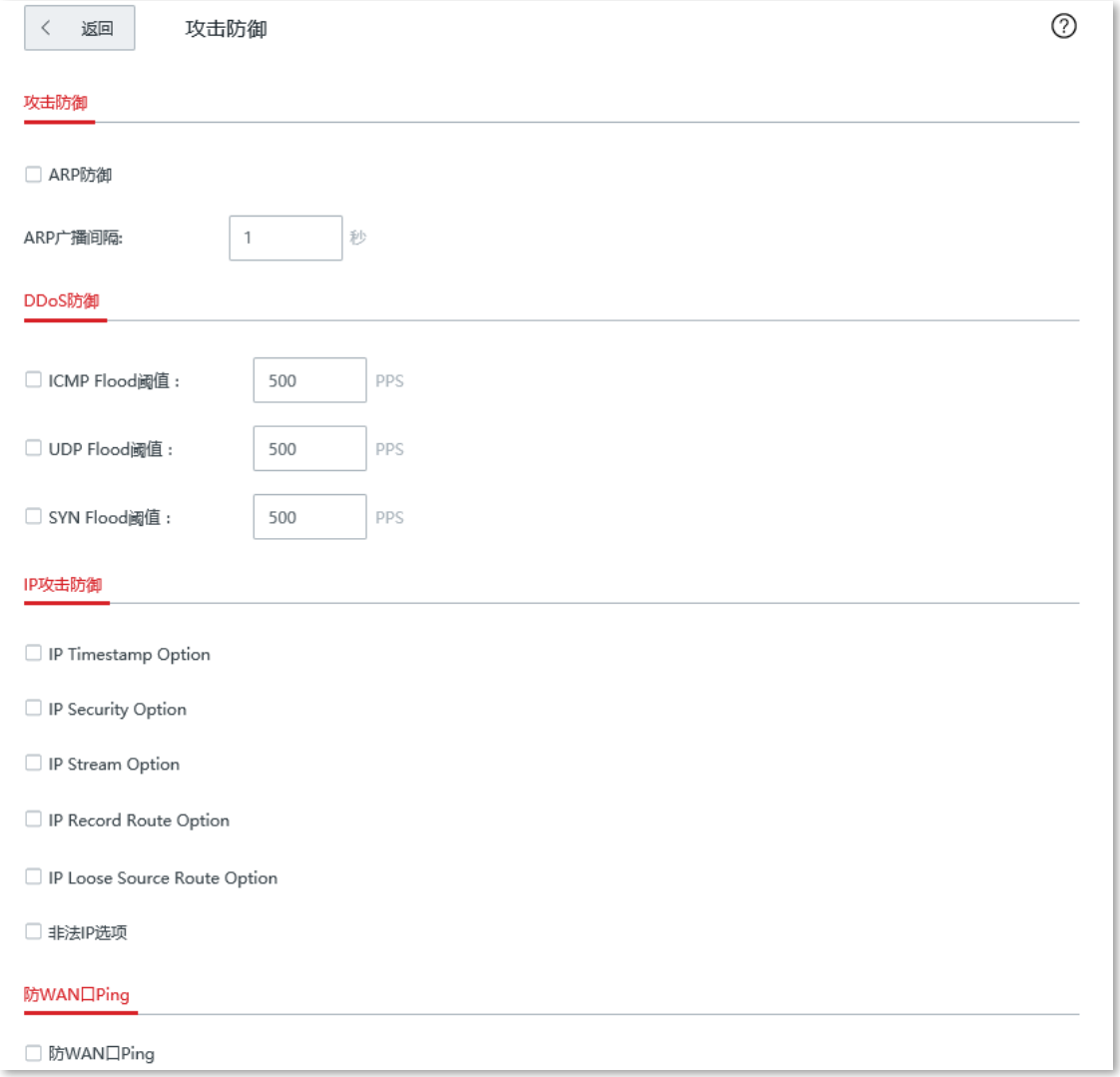
远程主机	外网端口	内网主机	内网端口	协议	备注
anywhere	42094	192.168.5.110	28795	TCP	PTL-D8C4976CAE...
anywhere	28795	192.168.5.110	28795	UDP	PTL-D8C4976CAE...
anywhere	28795	192.168.5.110	28796	TCP	PTL-D8C4976CAE...
anywhere	20741	192.168.5.110	12345	UDP	MiniTP SDK
anywhere	20741	192.168.5.110	54321	TCP	MiniTP SDK

3.9.10 攻击防御

免布线路由模式节点支持的攻击防御类型有：ARP 防御、DDoS 防御、IP 攻击防御和防 WAN 口 Ping。

- ARP 防御：识别局域网中的 ARP 欺骗，并记录攻击者的 MAC 地址。
- DDoS 防御：DDoS 攻击，即分布式拒绝服务（Distributed Denial of Service）攻击。利用 DDoS 攻击，攻击者可以消耗目标系统资源，使该目标系统无法提供正常服务。节点可以防御的 DDoS 攻击类型包括：ICMP Flood、UDP Flood、SYN Flood。
- IP 攻击防御：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：自动忽略广域网主机对节点 WAN 口 IP 地址的 Ping 请求，防止暴露自己，同时防范外部的 Ping 攻击。

进入页面：点击「更多设置」>「攻击防御」。



参数说明

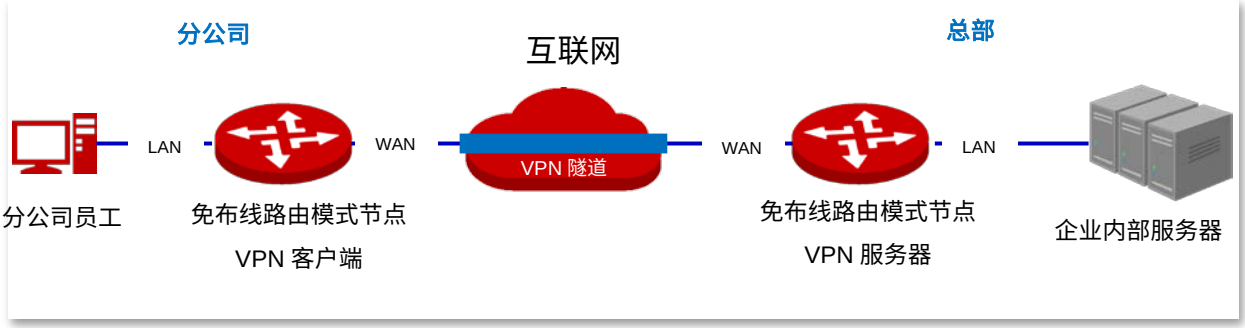
标题项		说明
攻击防御	ARP 防御	启用/禁用 ARP 防御功能。
	ARP 广播间隔	节点发送 ARP 广播报文的间隔。
DDoS 防御	ICMP Flood 阈值	一秒钟内，如果节点收到来自局域网同一主机的 ICMP 请求包超过此阈值，则认为节点正受到 ICMP Flood 攻击。
	UDP Flood 阈值	一秒钟内，如果节点收到来自局域网同一主机的 UDP 包超过此阈值，则认为节点正受到 UDP Flood 攻击。
	SYN Flood 阈值	一秒钟内，如果节点收到来自局域网同一主机的 TCP SYN 包超过此阈值，则认为节点正受到 SYN Flood 攻击。
IP 攻击防御	IP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

3.9.11 VPN 服务器

概述

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

VPN 的典型网络拓扑图如下。



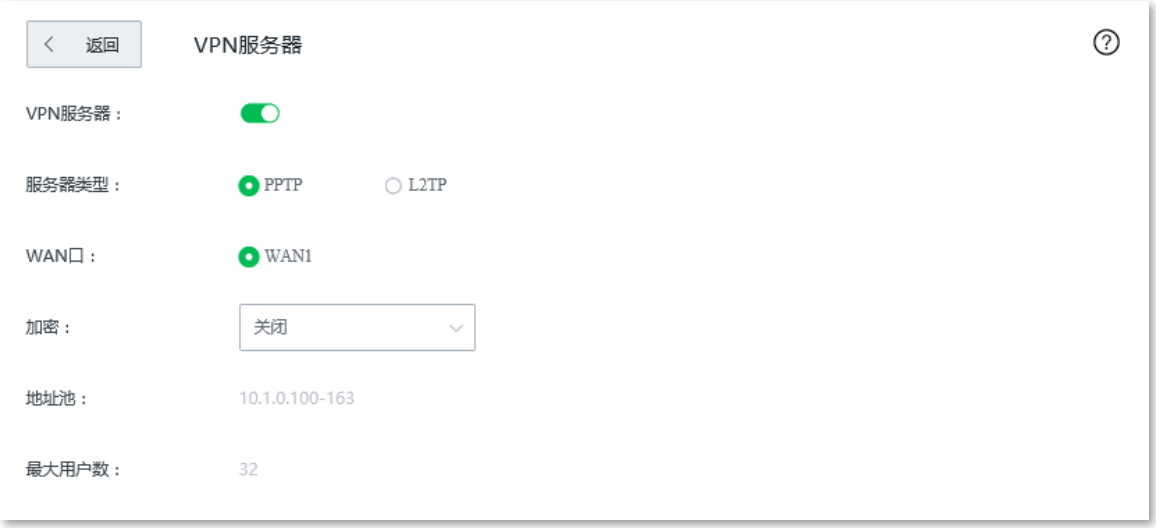
免布线路由模式节点可以作为 PPTP/L2TP 服务器，接受 PPTP/L2TP 客户端的连接。

配置 VPN 服务器

进入页面：点击「更多设置」>「VPN 服务器」。

开启 VPN 服务器

VPN 服务器默认关闭，开启后，页面显示如下。



参数说明

标题项	说明
VPN 服务器	VPN 服务器功能开关。表示关闭，表示开启。 开启后，节点作为 VPN 服务器。
服务器类型	节点使用的 VPN 协议类型，PPTP 或 L2TP。PPTP 和 L2TP 都是二层 VPN 隧道协议，使用 PPP（点到点协议）进行数据封装，并都为数据增添额外首部。 – PPTP：节点作为 PPTP 服务器，接受 PPTP 客户端的连接。 – L2TP：节点作为 L2TP 服务器，接受 L2TP 客户端的连接。
WAN 口	VPN 服务器与客户端建立 VPN 隧道的 WAN 口。 该 WAN 口的 IP 地址或域名是 VPN 客户端的“服务器 IP 地址/域名”。
加密	只有 PPTP VPN 才支持此选项。 根据需要选择是否启用 128 位数据加密。客户端、服务器双方的加密设置需保持一致，否则将不能正常通信。
IPSec 加密	只有 L2TP VPN 才支持此选项。 根据需要选择是否启用 IPSec 加密。如果要进行 IPSec 加密，请选择封装模式为“传输模式”的 IPSec 规则。
地址池	VPN 服务器可分配给 VPN 客户端的 IP 地址范围。
最大用户数	VPN 服务器最多支持的 VPN 客户端数量。系统固定为 32 个。

新增 PPTP/L2TP 用户账号

在「更多设置」>「VPN 服务器」页面的“PPTP/L2TP 用户”模块，点击 + 新增 ，然后在弹出窗口中配置各项参数，点击 保存 。

参数说明

标题项	说明
用户名	VPN 用户账号和密码，即 VPN 用户进行 PPTP/L2TP 拨号（VPN 连接）时需要输入的用户名/密码。
密码	
是否网络	VPN 客户端类型。 - 是：VPN 客户端是一个网络时选择。此时，需要设置 VPN 客户端的“网段”、“子网掩码”参数。 - 否：VPN 客户端是一台主机。
网段	VPN 客户端为一个网络时，在此输入客户端的内网网络号。
子网掩码	VPN 客户端为一个网络时，在此输入客户端内网的子网掩码。
备注	该账号的描述信息。

PPTP/L2TP VPN 服务配置举例

组网需求

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

方案设计

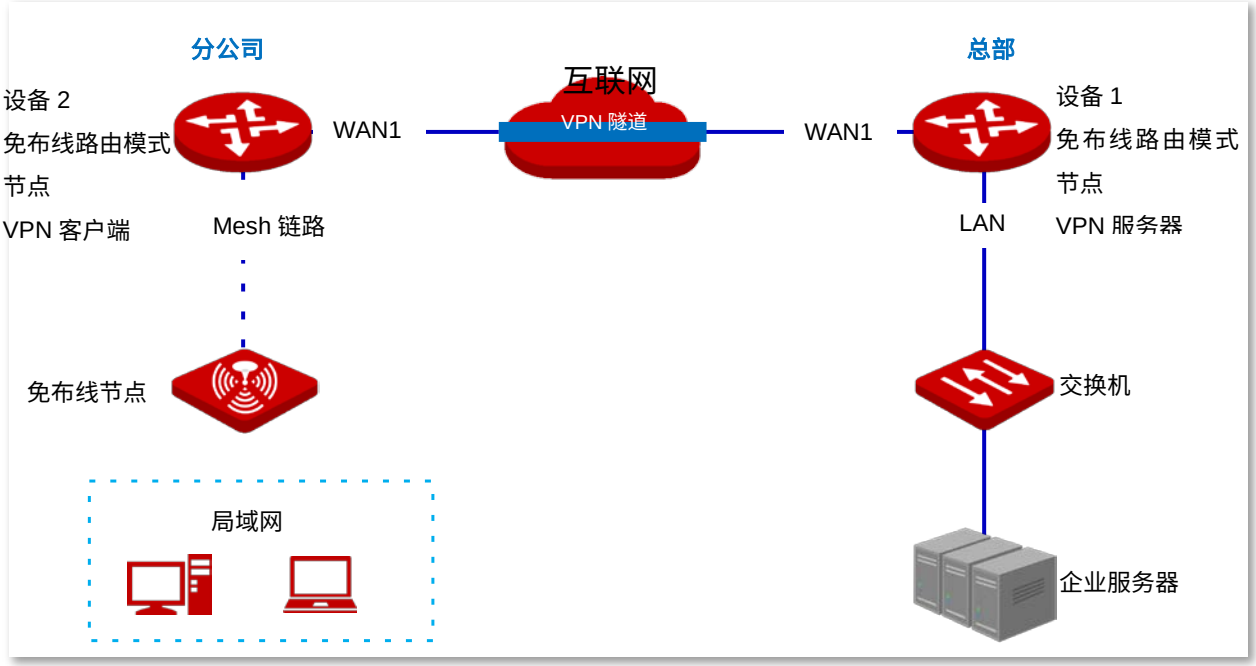
将一台免布线设备设置为 VPN 服务器，另一台设置为 VPN 客户端，实现远端用户经互联网安全访问企业内部局域网的需求。本例以 PPTP VPN 为例说明，L2TP VPN 的设置方法类似。

假设将设备 1 设置为 PPTP 服务器，基本信息如下：

- PPTP 服务器分配的用户名、密码均为 fengongsi1。
- PPTP 服务器 IP 地址为 202.105.11.22。
- PPTP 服务器对数据启用加密。
- PPTP 服务器内网为 192.168.5.0/24。

假设将设备 2 设置为 PPTP 客户端基本信息如下：

PPTP 客户端内网为 192.168.1.0/24。



配置步骤

配置流程图：

设置设备 1 为 VPN 服务器 → 设置设备 2 为 VPN 客户端

一、设置设备 1 为 VPN 服务器

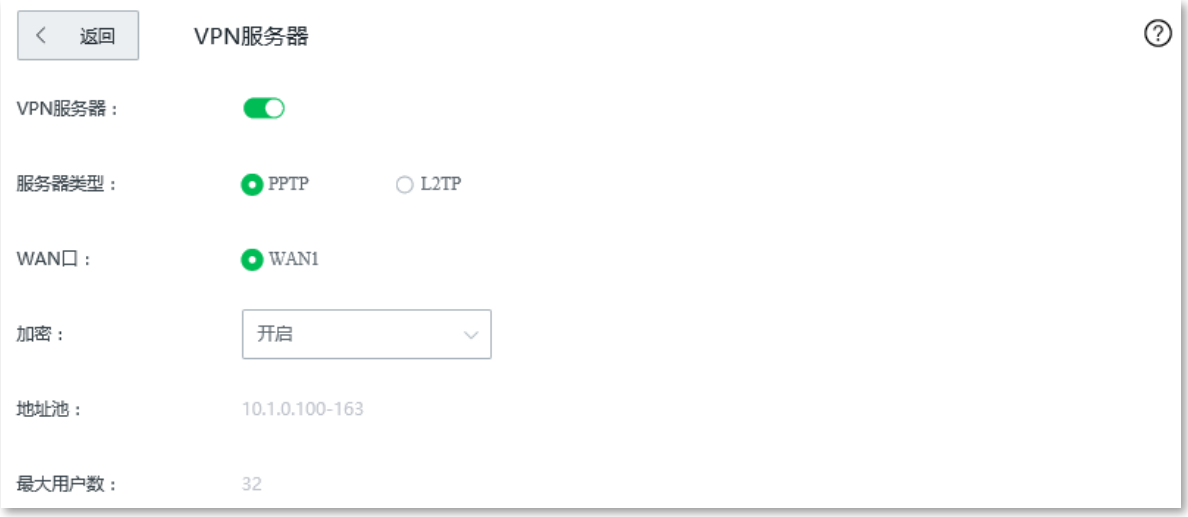
1. 登录设备 1 的 Web 管理界面。
2. 开启 PPTP 服务器。

   (1) 点击「更多设置」>「VPN 服务器」。

   (2) 点击“VPN 服务器”滑块至。

   (3) 进行如下配置，然后点击页面底端的 保存 。

   - 选择 VPN 服务器类型，本例为“PPTP”。
   - 选择“加密”为“开启”。



3. 配置 PPTP/L2TP 用户。

   (1) 在「更多设置」>「VPN 服务器」页面的“PPTP/L2TP 用户”模块，点击 + 新增 。

   (2) 在【新增】窗口进行如下配置，然后点击 保存 。

   - 输入 VPN 客户端进行 VPN 连接时所用的用户名，本例为“fengongsi1”。

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

添加完成，如下图示。

二、设置设备 2 为 VPN 客户端

1. 登录设备 2 的 Web 管理界面，转到「更多设置」>「VPN 客户端」页面。

2. 点击“VPN 客户端”滑块至。

3. 进行如下配置，然后点击 保存 。

   (1) 选择“客户端类型”与 VPN 服务器侧一致，本例为“PPTP”。

   (2) 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”。

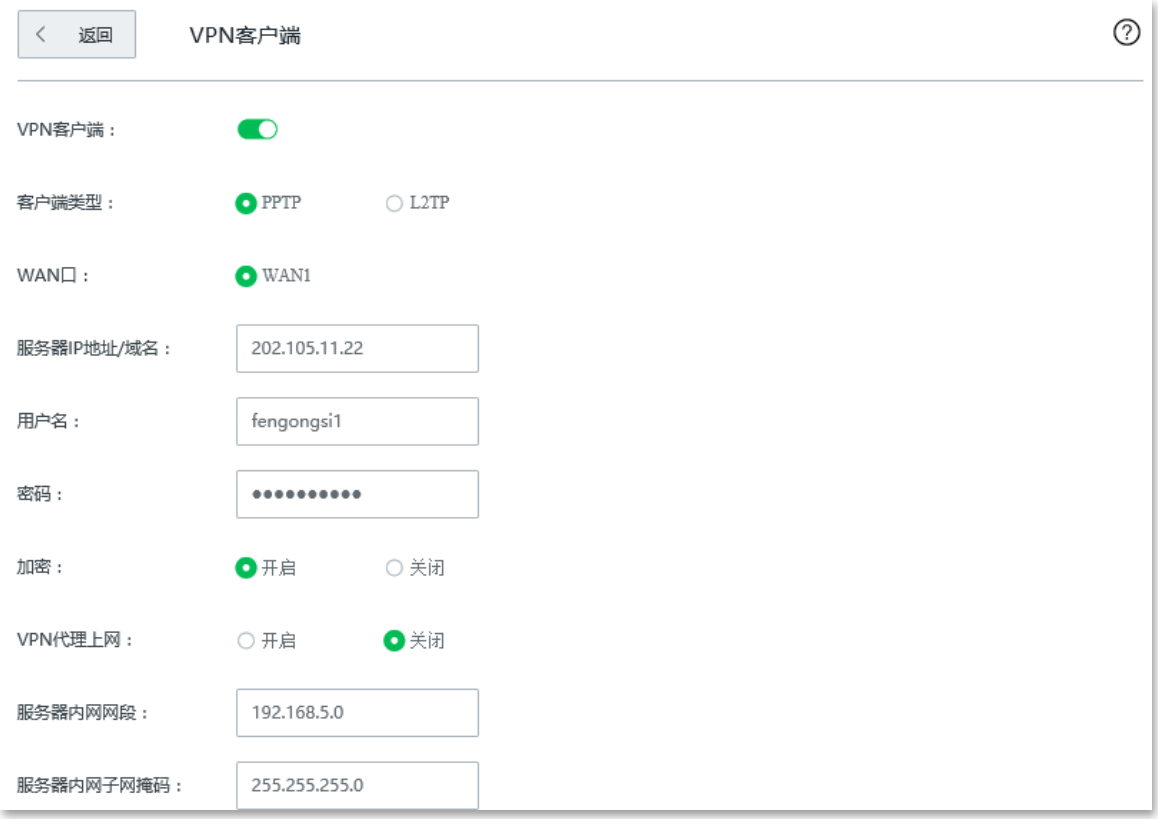
   (3) 输入 VPN 服务器分配的用户名，本例为“fengongsi1”。

   (4) 输入 VPN 服务器分配的用户名对应的密码。

   (5) 选择“加密”为“开启”，与 VPN 服务器侧配置保持一致。

   (6) 输入 VPN 服务器内网的网段，本例为“192.168.5.0”。

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



   当「VPN 客户端」页面的状态显示为“已联网”时，VPN 连接成功。

   ----完成

之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。

验证配置

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

- FTP 服务器 IP 地址为 192.168.5.104

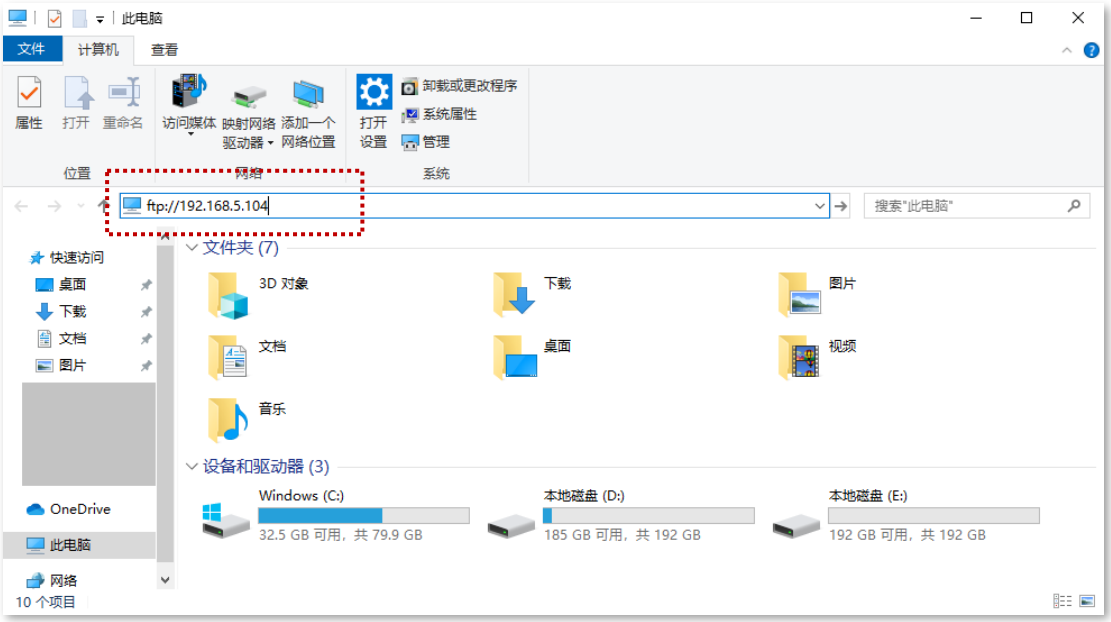
- FTP 服务端口为 21
- FTP 服务器登录用户名和密码均为 zhangsan

当分公司员工访问总部项目资料时，步骤如下：

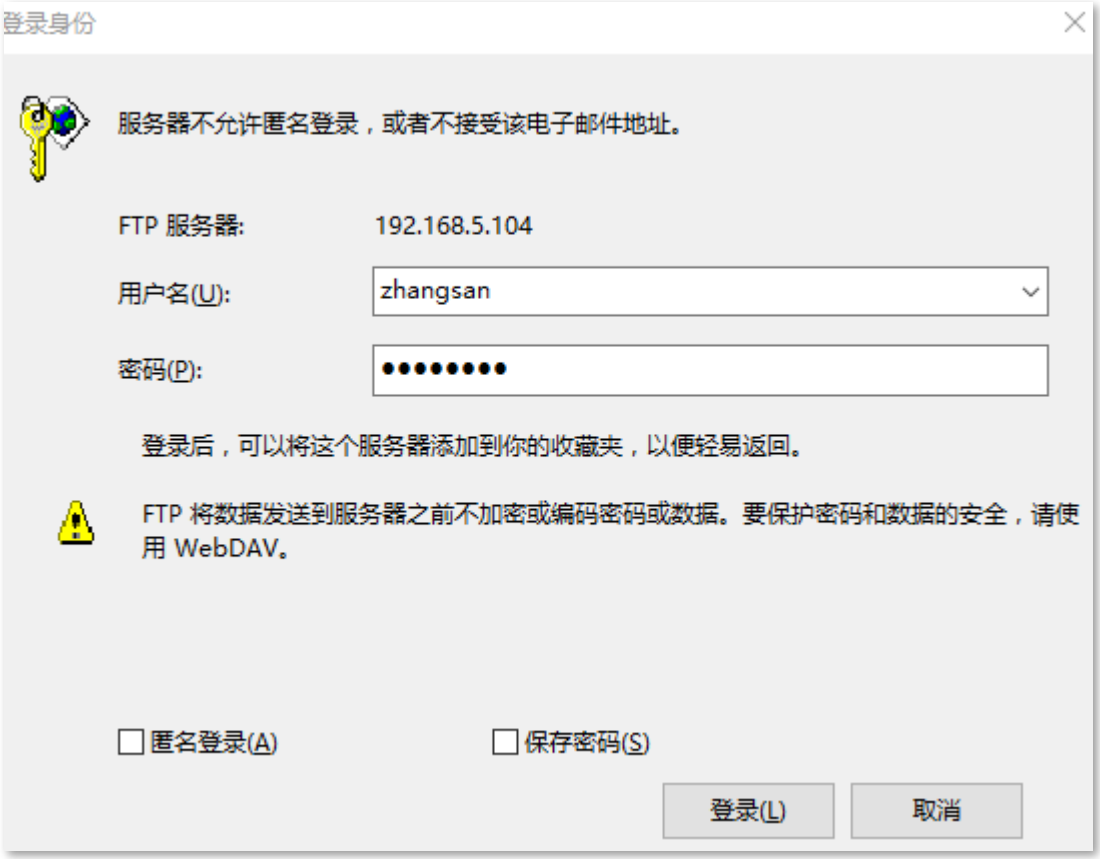
1. 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 ftp://192.168.5.104。

提示

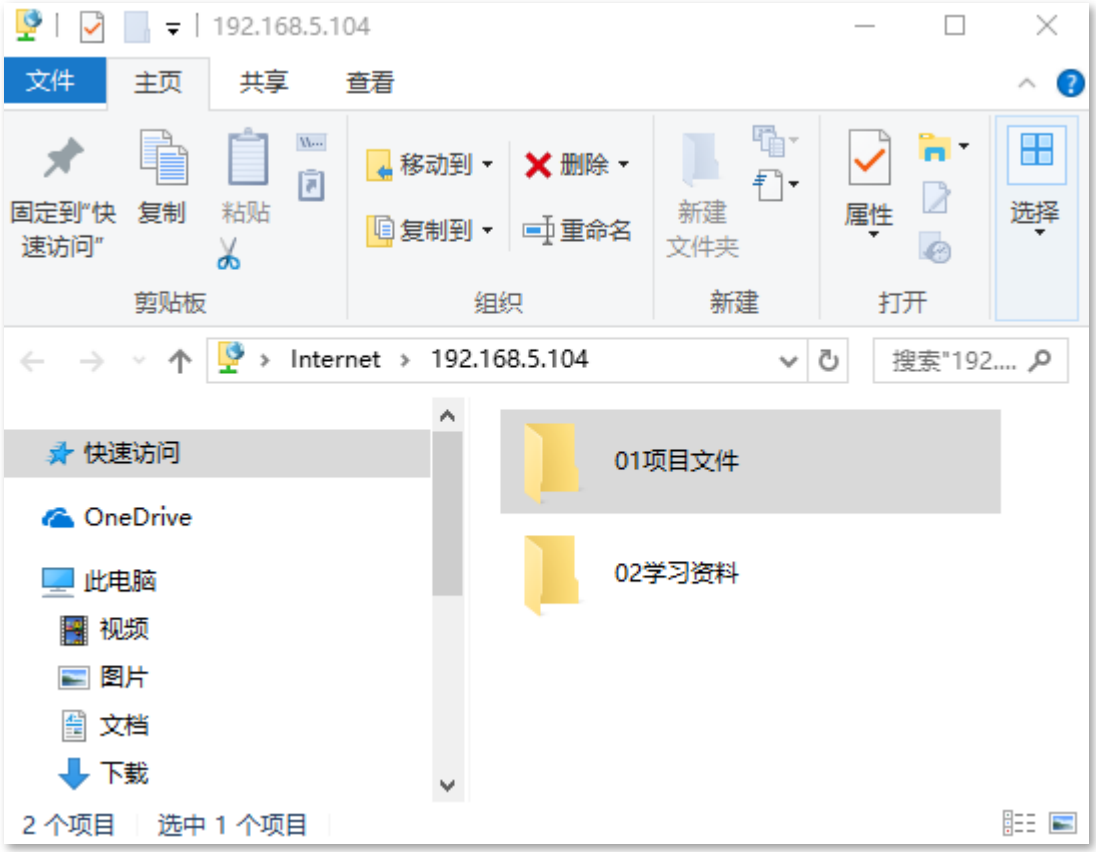
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



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


登录身份
服务器不允许匿名登录，或者不接受该电子邮件地址。
FTP 服务器:
192.168.5.104
用户名(U):
zhangsan
密码(P):
登录后，可以将这个服务器添加到你的收藏夹，以便轻易返回。
FTP 将数据发送到服务器之前不加密或编码密码或数据。要保护密码和数据的安全，请使用 WebDAV。
匿名登录(A)
保存密码(S)
登录(L)
取消

访问成功。

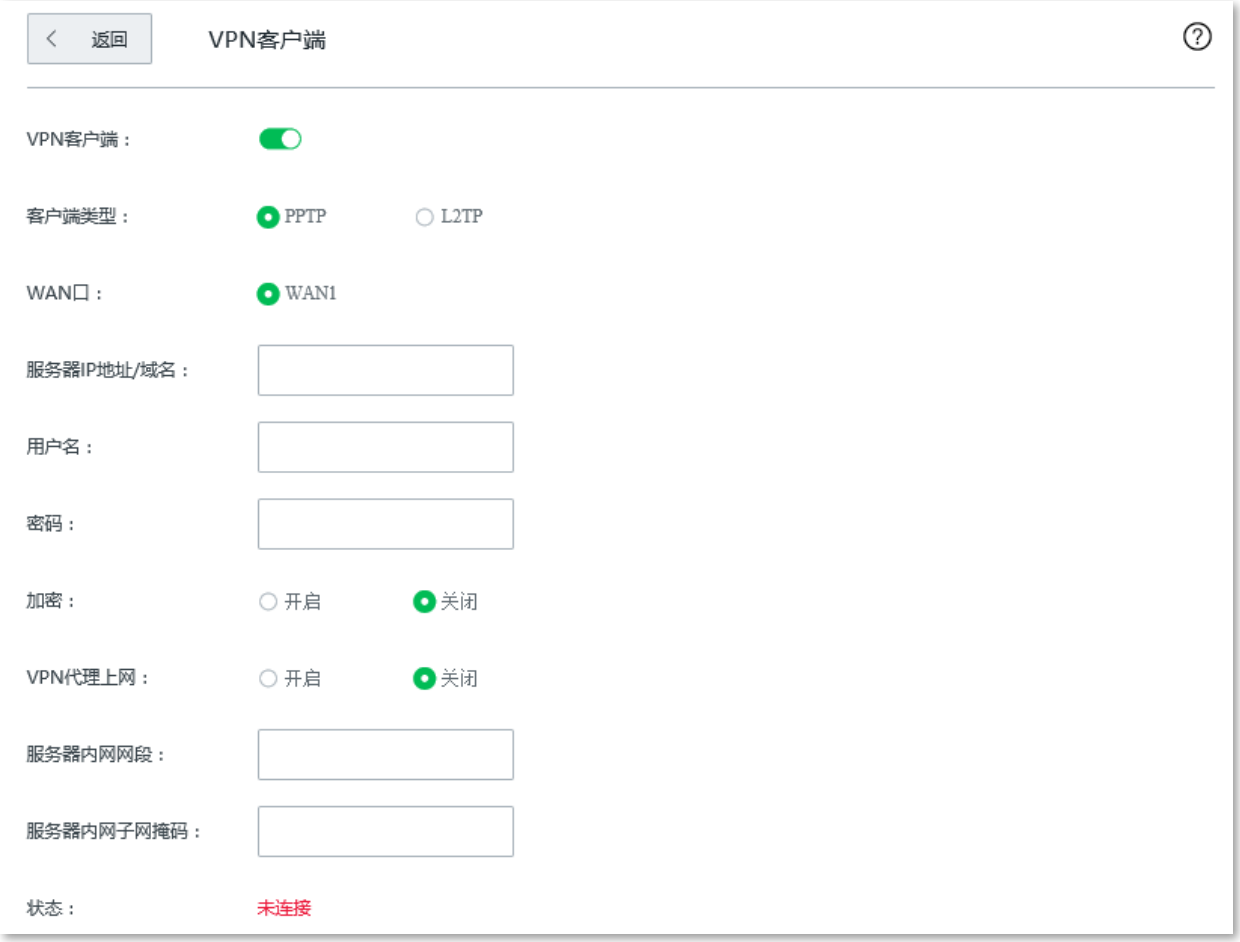

192.168.5.104
文件
主页
共享
查看
固定到"快速访问"
复制
粘贴
剪贴板
移动到
删除
复制到
重命名
组织
新建文件夹
新建
属性
打开
选择
Internet › 192.168.5.104
搜索"192....
快速访问
OneDrive
此电脑
视频
图片
文档
下载
01项目文件
02学习资料
2 个项目
选中 1 个项目

3.9.12 VPN 客户端

免布线路由模式节点可以作为 PPTP/L2TP 客户端连接到 PPTP/L2TP 服务器。

进入页面：点击「更多设置」>「VPN 客户端」。

VPN 客户端默认关闭，开启后，页面显示如下。



参数说明

标题项	说明
VPN 客户端	VPN 客户端功能开关。表示关闭，表示开启。 开启后，节点作为 VPN 客户端。
客户端类型	节点使用的 VPN 协议类型，PPTP 或 L2TP。PPTP 和 L2TP 都是二层 VPN 隧道协议，使用 PPP（点到点协议）进行数据封装，并都为数据增添额外首部。 - PPTP：要连接的 VPN 服务器是 PPTP 服务器时，选择此项。 - L2TP：要连接的 VPN 服务器是 L2TP 服务器时，选择此项。

标题项	说明
WAN 口	节点进行 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。

3.9.13 IPSec

概述

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

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。本设备支持“隧道模式”和“传输模式”两种。

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

- **安全网关**

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

- **IPSec 对等体**

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

- **SA**

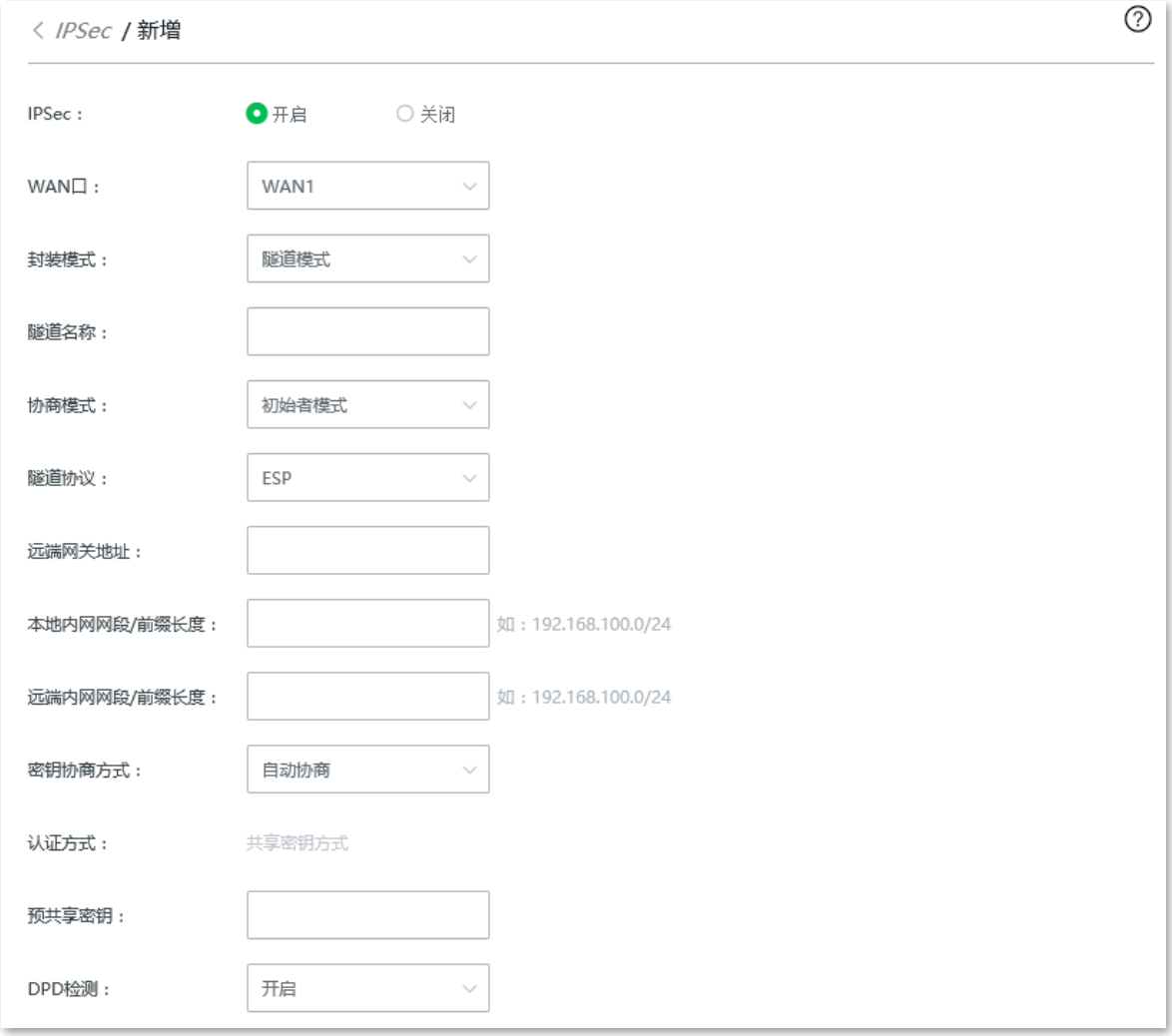
  SA 是通信对等体间对某些要素的约定。如，使用哪种协议（AH、ESP 还是两者结合）、协议的封装模式（传输模式、隧道模式）、加密算法（DES、3DES、AES）、特定流中保护数据的共享密钥以及密钥的生命周期等。SA 具有以下特征：

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

配置 IPSec 连接

新建 IPSec 连接

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



参数说明

标题项	说明
IPSec	开启/关闭 IPSec 功能。
WAN 口	IPSec 生效的 WAN 口，IPSec 对端设备的“远端网关地址”需填为此接口的 IP 地址或域名。
封装模式	IPSec 数据的封装模式。 – 隧道模式：通常用于两个安全网关之间的通讯。 – 传输模式：通常用于主机和主机、主机与网关之间的通信。

标题项	说明
隧道名称	该 IPSec 连接的名称。
协商模式	IPSec 隧道的协商模式。 – 初始者模式：主动向对端发起连接。 – 响应者模式：等待对端发起连接。 注意 请勿将 IPSec 隧道两端都设置为“响应者模式”，否则会导致 IPSec 隧道建立失败。
隧道协议	为 IPSec 提供安全服务的协议。 – AH：Authentication Header，鉴别首部。该协议主要提供数据完整性校验功能，若数据报文在传输过程中被篡改，则接收方将在完整性验证时丢弃该报文。 – ESP：Encapsulating Security Payload，封装安全性载荷。该协议可以对数据的完整性进行检查，还对数据进行加密，这样，即使报文在传输过程中被截获，截取方也难以获取到真实信息。 – AH+ESP：同时使用上述两种协议。
远端网关地址	填写 IPSec 隧道对端网关的 IP 地址或域名。
本地内网网段/前缀长度	本设备局域网的网段/前缀长度。例如：本设备的 LAN 口 IP 地址为 192.168.5.1，子网掩码为 255.255.255.0，则本地内网网段/前缀长度可填为 192.168.5.0/24。
远端内网网段/前缀长度	IPSec 隧道对端网关局域网的网段/前缀长度。若对端是一台特定主机，则此参数设置为“该设备的 IP 地址/32”。
密钥协商方式	建立 IPSec 安全隧道的密钥协商方式。默认为“自动协商”。 – 自动协商：通过 IKE 自动建立 SA，并进行动态维护、删除，降低了手工配置的复杂度，简化 IPSec 的使用、管理工作。自动建立的 SA 有生命周期，会定时更新，增强了安全性。 – 手动设置：用户手动设置加密/认证算法及密钥来建立 SA。手动建立的 SA 没有生命周期限制，除非手动删除，否则永不过期，因此有安全隐患。该方式常用于调试阶段。

密钥协商方式--自动协商

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

– ISAKMP：Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议，该协议为交换密钥和 SA 协商提供了一个框架。

– Oakley：密钥确定协议，该协议描述了密钥交换的具体机制。

- SKEME：安全密钥交换机制，该协议描述了与 Oakley 不同的另一种密钥交换机制。

IKE 协商过程分为两个阶段：

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

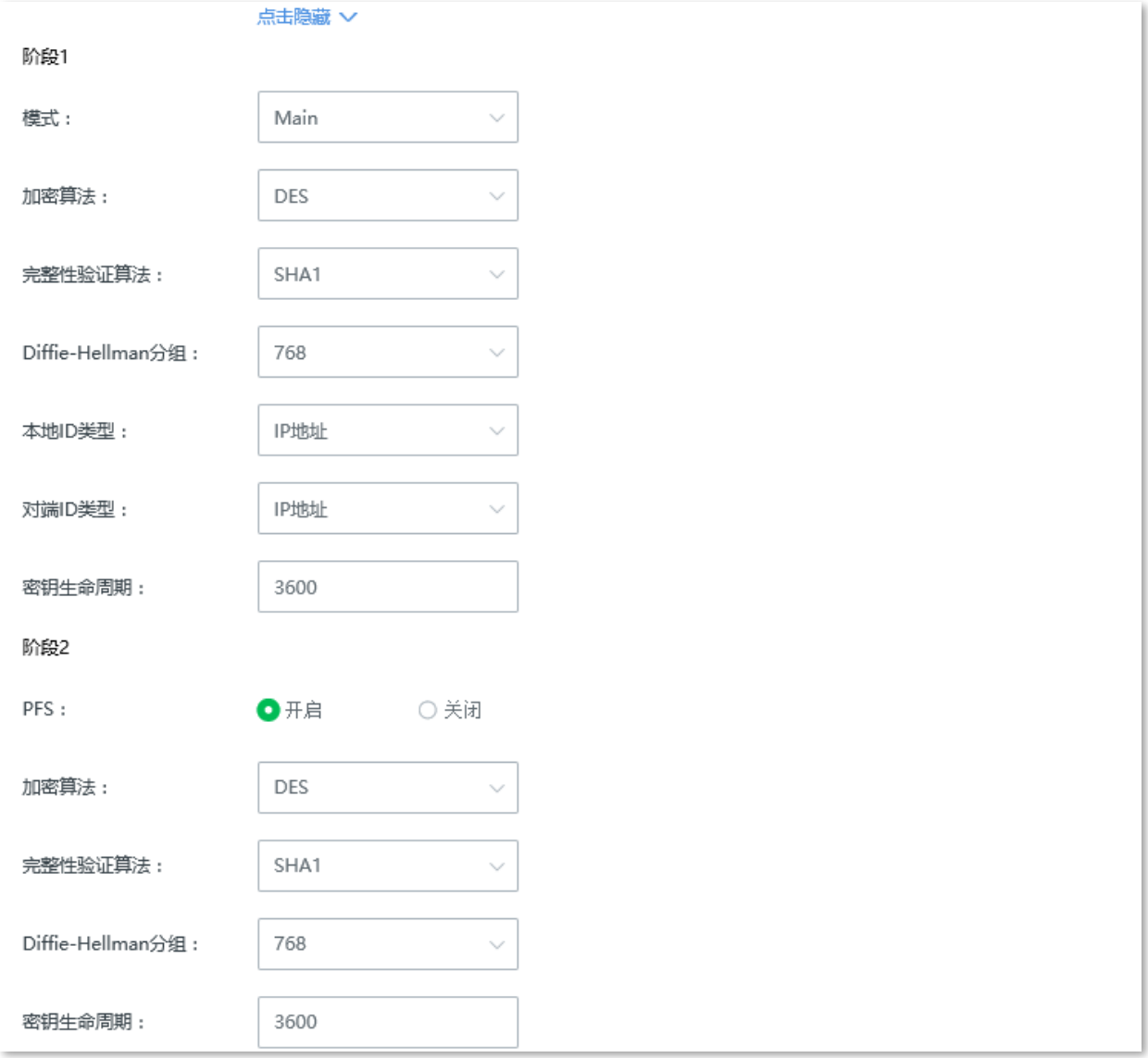
阶段 2：使用阶段 1 中建立的 ISAKMP SA 为 IPSec 的安全性协议协商参数，创建 IPSec SA，用于对双方的通信数据进行保护。

密钥协商方式为“自动协商”时，如下图。

参数说明

标题项	说明
认证方式	显示为“共享密钥方式”，表示 IPSec 双方事先通过某种方式协商好一个双方共享的密钥字符串。
预共享密钥	输入协商时所用的预共享密钥，需要与对端网关设备保持一致。最长为 128 字符。
DPD 检测	开启/关闭对等体检测功能。 通过 DPD 检测可以检测远端的隧道站点是否有效。
DPD 检测周期	发送 DPD 报文的周期。 本设备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。



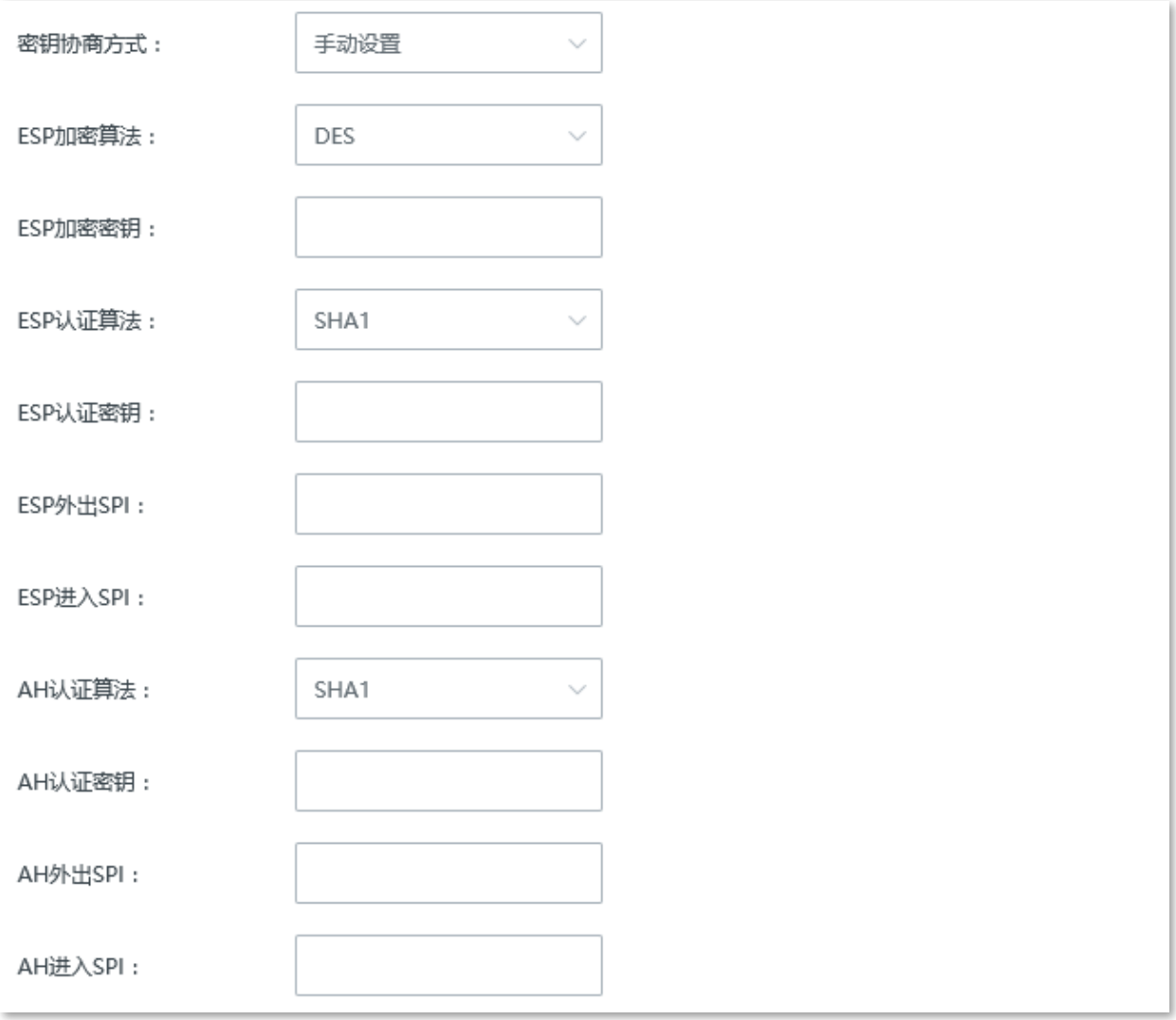
参数说明

标题项	说明
模式	IKE 阶段 1 的交换模式，该交换模式必须与对端设置相同。 - Main：主模式，此模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。 - Aggressive：野蛮模式，又称主动模式，此模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。
加密算法	应用于 IKE 会话的加密算法。本设备支持以下加密算法： - DES（Data Encryption Standard，数据加密标准）：使用 56 位的密钥对 64 位数据进行加密，64 位的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56 位的密钥进行加密。 - AES（Advanced Encryption Standard，高级加密标准）：AES 128/192/256 表示使用长度为 128/192/256 位的密钥进行加密。

标题项	说明
完整性验证算法	应用于 IKE 会话的验证算法。本设备支持以下验证算法： – MD5：Message Digest Algorithm，消息摘要算法。对一段消息产生 128 位的消息摘要，防止消息被篡改。 – SHA1：Secure Hash Algorithm，安全散列算法。对一段消息产生 160 位的消息摘要，比 MD5 更难破解。
Diffie-Hellman 分组	Diffie-Hellman 算法的组信息，用于产生加密 IKE 隧道的会话密钥。
本地 ID 类型	本地网关标识。 – IP 地址：本设备使用 WAN 口 IP 地址与对端网关协商。 – FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“本地 ID”输入框中输入任意字符串，用于与对端网关协商。“本地 ID”与远端网关的“对端 ID”必须相同。 注意 “本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）。
对端 ID 类型	对端网关标识。 – IP 地址：本地网关默认对端网关使用其 WAN 口 IP 地址进行协商。 – FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“对端 ID”输入框中输入任意字符串，用于与本地网关协商。“对端 ID”与远端网关的“本地 ID”必须相同。 注意 “本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）。
密钥生命周期	ISAKMP SA 的生存时间。
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）特性使得 IKE 阶段 2 协商生成一个新的密钥材料，该密钥材料与阶段 1 协商生成的密钥材料没有任何关联，这样即使 IKE1 阶段 1 的密钥被破解，阶段 2 的密钥仍然安全。 如果没有使用 PFS，阶段 2 的密钥将根据阶段 1 生成的密钥材料来产生，一旦阶段 1 的密钥被破解，用于保护通信数据的阶段 2 密钥也岌岌可危，这将严重威胁到双方的通信安全。
密钥生命周期	IPSec SA 的生存时间。

密钥协商方式-手动设置

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



参数说明

标题项	说明
ESP 加密算法	当选择隧道协议为“ESP”时需设置 ESP 加密算法。本设备支持以下加密算法： – DES：使用 56 位的密钥对 64 位数据进行加密，64 位的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56 位的密钥进行加密。 – AES：AES128/192/256 表示使用长度为 128/192/256 位的密钥进行加密。
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	当选择隧道协议为“ESP”时，需设置 ESP 认证算法；当选择隧道协议为“AH”时，需设置 AH 认证算法。本设备支持以下验证算法： – MD5：对一段消息产生 128 位的消息摘要，防止消息被篡改。

标题项	说明
	– SHA1：对一段消息产生 160 位的消息摘要，比 MD5 更难破解。
ESP/AH 认证密钥	当选择隧道协议为“ESP”时，需设置 ESP 认证密钥；当选择隧道协议为“AH”时，需设置 AH 认证密钥。 IPSec 通信双方设置需保持一致。
ESP/AH 外出 SPI	设置外出 SPI 参数。 SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“进入 SPI”值相同。
ESP/AH 进入 SPI	设置进入 SPI 参数。 SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“外出 SPI”值相同。

修改 IPSec 连接

在「更多设置」>「IPSec」页面，点击操作栏的，可以修改对应 IPSec 连接。

删除 IPSec 连接

在「更多设置」>「IPSec」页面，点击操作栏的，可以删除对应 IPSec 连接。

IPSec VPN 配置举例

组网需求

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

方案设计

在 2 台免布线设备上均建立 IPSec 隧道，实现远端用户经互联网安全访问企业内部局域网的需求。

假设将设备 1 部署在总部，基本信息如下：

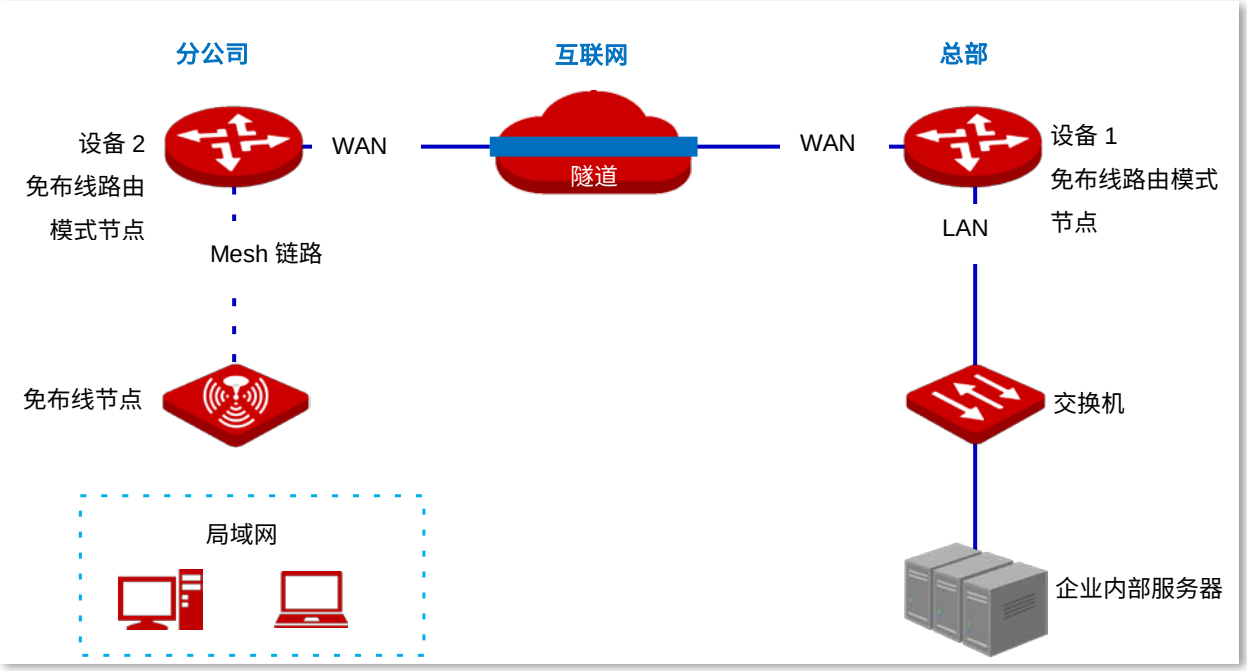
- WAN IP 地址为 202.105.11.22。
- 局域网网络为 192.168.5.0/24。

假设将设备 2 部署在分公司，基本信息如下：

- WAN IP 地址为 202.105.88.77。
- 局域网网络为 192.168.1.0/24。

假设两台路由器的 IPSec 连接基本信息如下：

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



配置步骤

注意

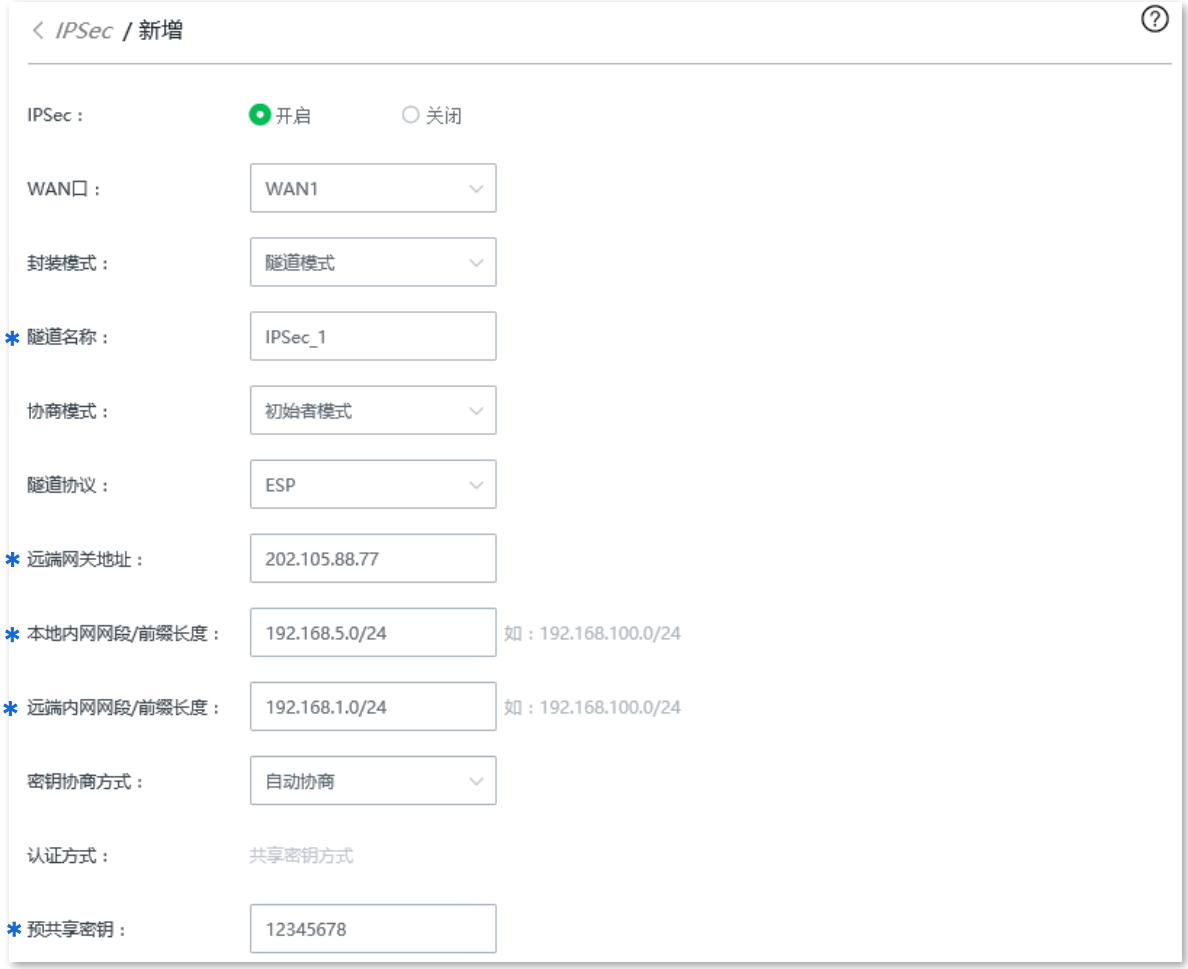
配置过程中，如果需要设置 IPSec 连接的高级选项，请保持两台设备的设置参数一致。

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，设备 1 的外出 SPI 与设备 2 的进入 SPI 一致，设备 1 的进入 SPI 与设备 2 的外出 SPI 一致。

一、设置设备 1

1. 登录免布线设备 1 的 Web 管理界面，点击「更多设置」>「IPSec」。
2. 点击 + 新增 。

3. 在“新增”页面进行下述配置，然后点击页面底端的 保存 。
   (1) 为本条隧道设置一个名称，如“IPSec_1”。
   (2) 输入对端设备上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.88.77”。
   (3) 输入本端设备内网的网段/前缀长度，本例为“192.168.5.0/24”。
   (4) 输入对端设备内网的网段/前缀长度，本例为“192.168.1.0/24”。
   (5) 设置双方协商时所用的预共享密钥，本例为“12345678”。



添加完成，如下图示。

二、设置设备 2

1. 登录免布线设备 2 的 Web 管理界面，点击「更多设置」>「IPSec」。
2. 点击 新增 。

3. 在“新增”页面进行下述配置，然后点击页面底端的 保存 。

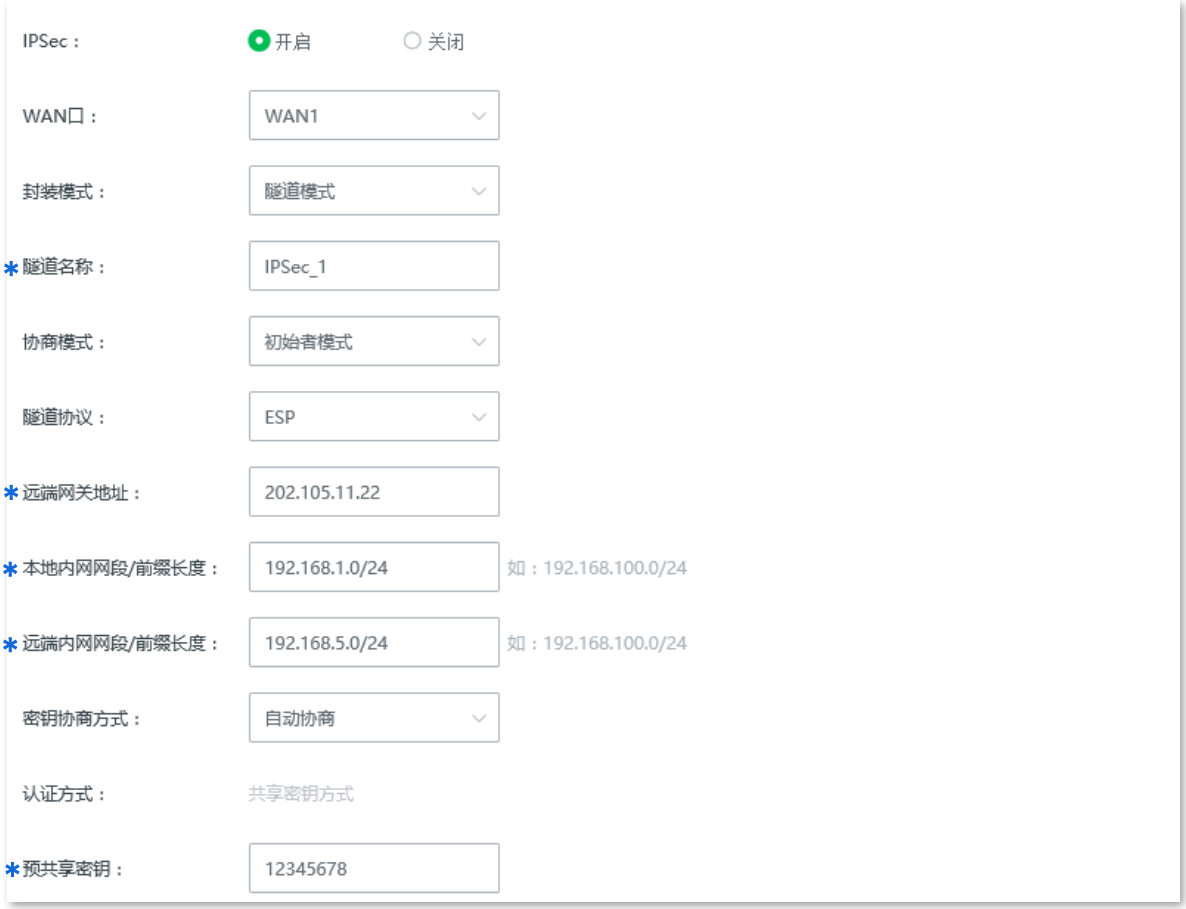
(1) 为本条隧道设置一个名称，如“IPSec_1”。

(2) 输入对端设备上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.11.22”。

(3) 输入本端设备内网的网段/子网掩码，本例为“192.168.1.0/24”。

(4) 输入对端设备内网的网段/子网掩码，本例为“192.168.5.0/24”。

(5) 输入双方协商时所用的预共享密钥，本例为“12345678”。



添加完成，如下图示。

----完成

验证配置

当“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。

3.10 系统维护

3.10.1 重启

当您设置的某项参数不能正常生效时，可以尝试重启免布线设备解决问题。

进入页面：点击「系统维护」>「重启」。

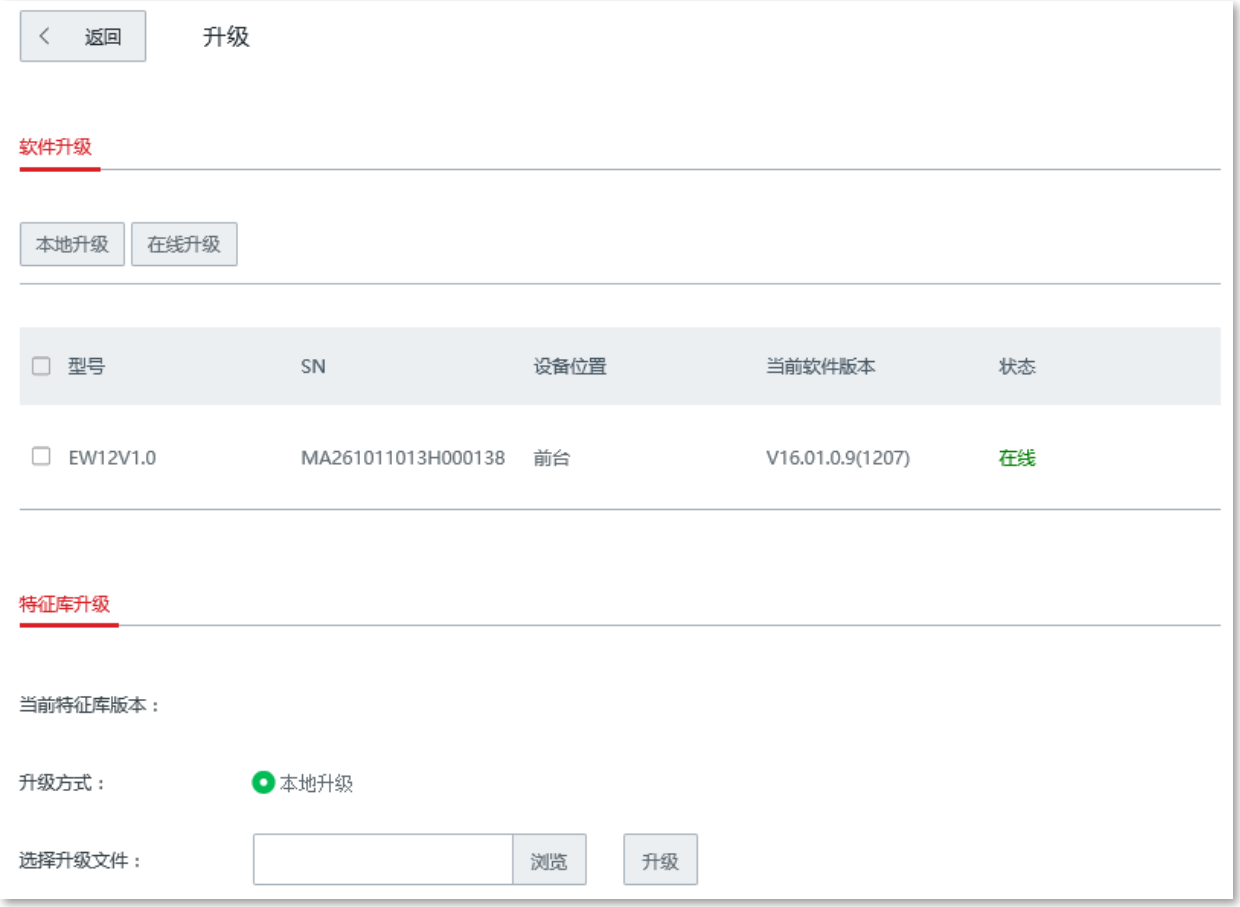
3.10.2 升级

概述

进入页面：点击「系统维护」>「升级」。

在这里，您可以对免布线设备进行软件升级和特征库升级。

- 软件升级：通过升级软件，可以体验更多功能，获得更好的用户体验。本设备支持“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：更新免布线设备行为管理模块的 URL 特征库。升级特征库不会对本设备的软件产生影响。本设备暂仅支持“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。

标题项	说明
在线升级	仅“软件升级”支持。需设备已联网。 方法：勾选要进行在线升级的设备，然后点击 在线升级 ，系统将自动下载升级文件，并进行升级。

软件本地升级

注意

为了确保升级正确，避免免布线设备损坏，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，不要断开免布线设备电源。

1. 访问 IP-COM 官网 www.ip-com.com.cn，下载对应型号的免布线设备升级软件到本地电脑并解压。
2. 登录免布线设备 Web 管理页面，进入「系统维护」>「升级」页面，找到“软件升级”模块。
3. 选择待升级的免布线设备，点击 本地升级 。
4. 点击 浏览 选择升级文件，然后点击 升级 。

提示

不同浏览器的文件加载按钮会有所不同，具体请以实际使用的浏览器为准。此处以 IE 浏览器为例。

----完成

等待进度条走完。之后，您可重新登录免布线设备，在“软件升级”或“系统状态”页面查看设备当前的软件版本号来确认是否升级成功。

提示

为了更好地体验高版本软件的稳定性及增值功能，升级完成后，建议将免布线设备恢复出厂设置，然后重新配置。

特征库本地升级

注意

为了确保升级正确，避免免布线设备损坏，请：

- 使用正确的升级文件进行升级。一般情况下，特征库升级文件的文件后缀为.cfg。
- 升级过程中，不要断开免布线设备电源。

1. 访问 IP-COM 官方网站 www.ip-com.com.cn，下载对应型号的免布线设备最新的特征库文件并存放到本地电脑。
2. 登录免布线设备的 Web 管理页面，进入「系统维护」>「升级」页面，找到“特征库升级”模块。
3. 点击 浏览 选择升级文件，然后点击 升级 。

提示

不同浏览器的文件加载按钮会有所不同，具体请以实际使用的浏览器为准。此处以 IE 浏览器为例。

----完成

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

3.10.3 复位

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；或您需要登录免布线设备的管理页面，但是却忘记登录密码时，可以将免布线设备复位后重新设置。

免布线设备支持软件复位和硬件复位两种方式。

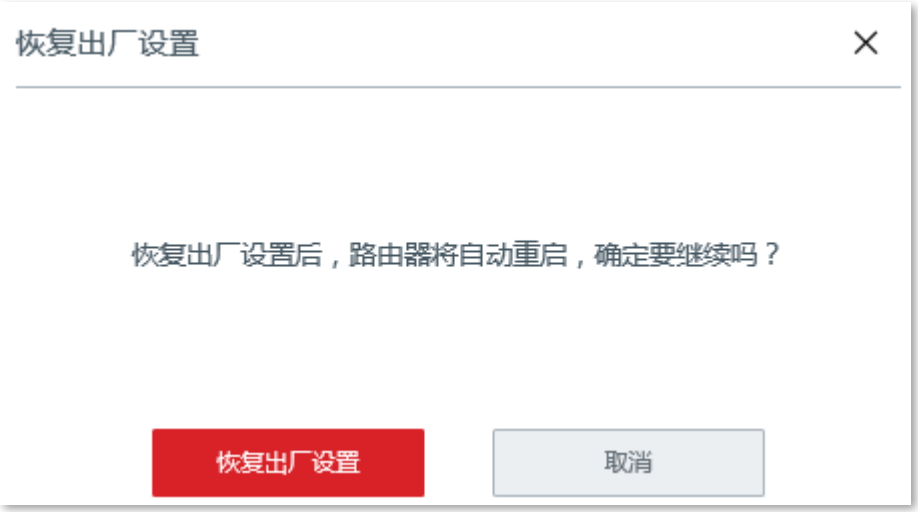
复位后，免布线设备的默认 LAN 口 IP 地址为 192.168.5.1。

注意

- 复位后，免布线设备的所有设置将会恢复到出厂状态，您需要重新设置免布线设备才能上网。请谨慎使用复位操作。
- 为避免损坏免布线设备，复位过程中，请确保该设备供电正常。

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 。



硬件复位

使用此方式时，您无需进入免布线设备管理页面就可以将其复位。操作方法如下：

免布线设备系统已启动的状态下（SYS 灯闪烁），用尖状物按住复位按钮（RESET）约 8 秒，当 SYS 灯长亮时松开，设备将会恢复出厂设置。当 SYS 灯重新闪烁时，恢复出厂设置完成。

3.10.4 密码管理

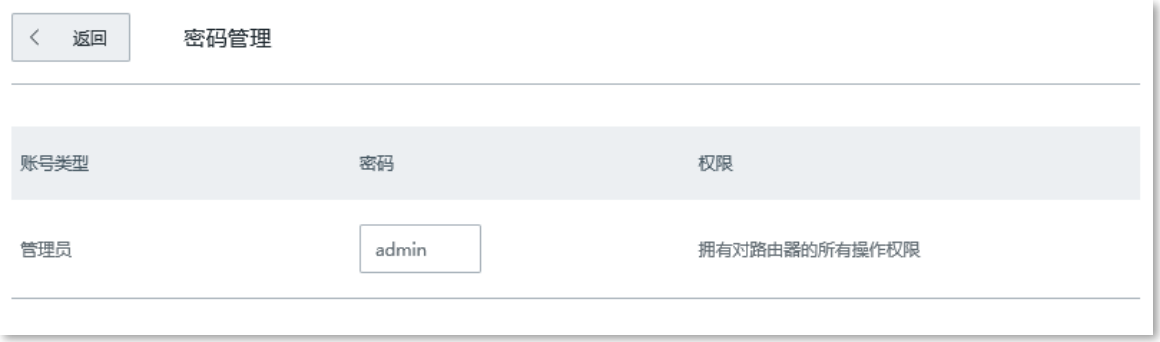
概述

进入页面：点击「系统维护」>「密码管理」。

在这里，您可以修改免布线设备的管理员密码。首次使用免布线设备时，需要设置管理员密码。

修改登录密码

在「系统维护」>「密码管理」页面，在对应账号类型的密码输入框中修改登录密码，然后点击页面底端的 保存 。



保存修改后，页面将会跳转到登录页面，输入刚才设置的密码可以重新登录到免布线设备的管理页面。

3.10.5 自定义重启

概述

进入页面：点击「系统维护」>「定时重启」。

在这里，您可以设置免布线设备周期性地定时自动重启，预防免布线设备长时间运行导致其出现性能下降、不稳定等现象。

自定义重启支持两种方式：循环重启、定时重启。

- 循环重启：免布线设备每隔指定的间隔时间就自动重启一次。
- 定时重启：免布线设备在指定的日期和时间自动重启。

设置设备循环重启

1. 点击「系统维护」>「自定义重启」。
2. 点击滑块至。
3. 选择“维护方式”为“循环重启”。
4. 设置自动重启的间隔时间。
5. 点击页面底端的 保存 。

----完成

设置完成后，每间隔指定的重复时间，免布线设备即自动重启一次。

设置设备定时重启

提示

定时重启时间以免布线设备的系统时间为准，为避免重启时间出错，请确保免布线设备的系统时间准确。

1. 点击「系统维护」>「定时重启」。
2. 点击滑块至。
3. 选择免布线设备自动重启的时间点，如“凌晨 3 点”。
4. 设置自动重启的日期，如“每天”。
5. 点击页面底端的 保存 。

----完成

如上图设置完成后，每天的凌晨 3 点，免布线设备将自动重启。

3.10.6 备份与恢复

概述

进入页面：点击「系统维护」>「备份与恢复」。

使用备份功能，可以将免布线设备当前的配置信息保存到本地电脑；使用恢复功能，可以将免布线设备的配置还原到之前备份的配置。

如，当您对免布线设备进行了大量的配置，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。当您对免布线设备进行了升级、复位等操作后，可以恢复免布线设备原有的配置文件。

备份配置

1. 点击「系统维护」>「备份与恢复」。
2. 点击 备份 ，之后按页面提示选择备份文件的存储路径。

----完成

浏览器将下载文件名为 RouterCfm.cfg 的配置文件。

恢复配置

1. 点击「系统维护」>「备份与恢复」。
2. 点击 浏览 选择之前备份的配置文件，然后点击 恢复 。

提示

不同浏览器的文件加载按钮会有所不同，具体请以实际使用的浏览器为准。此处以 IE 浏览器为例。

----完成

页面出现重启进度提示，请耐心等待。免布线设备重启后配置恢复完成。

3.10.7 系统日志

进入页面：点击「系统维护」>「系统日志」。

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

日志记录时间以免布线设备的系统时间为准，为确保日志记录时间准确，请先准确设置免布线设备的系统时间。

注意

- 免布线设备仅记录其最近一次启动后的事件信息。
- 断电后重新通电、软件升级、备份/恢复设置、复位等操作都会导致免布线设备重启。

3.10.8 诊断工具

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：用于检测数据包从本设备到目标主机所经过的路由。

执行 Ping

假设要检测免布线设备到百度服务器的链路是否畅通。

设置步骤：

1. 点击「系统维护」>「诊断工具」。
2. 选择“诊断工具”为“Ping”。
3. 输入目的 IP 地址或域名，本例为“www.baidu.com”。
4. 设置 ping 发送的数据包的个数，建议保持默认设置。
5. 设置 ping 发送的数据包的大小，建议保持默认设置。
6. 点击 开始 。

----完成

稍后，诊断结果将显示在页面下方。如下图示。

执行 Traceroute

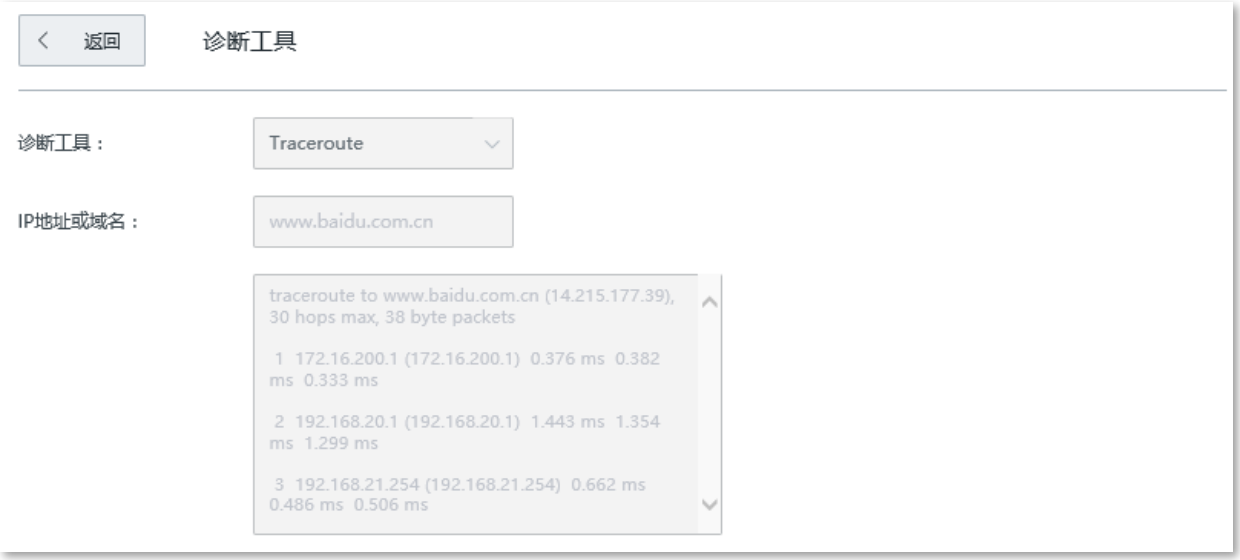
假设要检测免布线设备到百度服务器所经过的路由。

设置步骤：

1. 点击「系统维护」>「诊断工具」。
2. 选择“诊断工具”为“Traceroute”。
3. 输入目的 IP 地址或域名，本例为“www.baidu.com”。
4. 点击 开始 。

----完成

稍后，诊断结果将显示在页面下方。如下图示例。


返回
诊断工具
诊断工具：
Traceroute
IP地址或域名：
www.baidu.com.cn
traceroute to www.baidu.com.cn (14.215.177.39), 30 hops max, 38 byte packets
1 172.16.200.1 (172.16.200.1) 0.376 ms 0.382 ms 0.333 ms
2 192.168.20.1 (192.168.20.1) 1.443 ms 1.354 ms 1.299 ms
3 192.168.21.254 (192.168.21.254) 0.662 ms 0.486 ms 0.506 ms

3.10.9 系统时间

为了保证免布线设备基于时间的功能正常生效，需要确保免布线设备的系统时间准确。免布线设备支持网络校时和手动设置两种时间设置方式，默认为“网络校时”。

进入页面：点击「系统维护」>「系统时间」。

网络校时

使用此方式时，系统时间自动同步互联网上的时间服务器。只要免布线设备成功连接至互联网就能自动校准其系统时间。

设置完成后，您可以进入系统状态页面查看免布线设备的系统时间是否校对准确。

参数说明

标题项	说明
系统时间	选择系统时间的设置方式，支持网络校时和手动设置。
校时周期	免布线设备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	选择免布线设备当前所在地区的标准时区。

手动设置

手动设置免布线设备的系统时间。使用此方式时，免布线设备每次重启后，您都需要重新设置系统时间。选择“手动设置”时，页面展开的相关参数如下图所示。

参数说明

标题项	说明
系统时间	选择系统时间的设置方式，支持网络校时和手动设置。
日期	可以直接在此处输入正确的时间，也可以点击 复制管理主机时间 将正在管理免布线设备的电脑的时间同步到免布线设备。
时间	

设置完成后，您可以进入系统状态页面，查看免布线设备的系统时间是否校对准确。

3.10.10 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，您可以查看免布线设备当前已启用、未启用的功能列表。点击该功能可以跳转到其配置页面。

系统时间

为了保证免布线设备基于时间的功能正常生效，需要确保免布线设备的系统时间准确。免布线设备支持网络校时和手动设置两种时间设置方式，默认为“网络校时”。

进入页面：点击「系统维护」>「系统时间」。

网络校时

使用此方式时，系统时间自动同步互联网上的时间服务器。只要免布线设备成功连接至互联网就能自动校准其系统时间。

设置完成后，您可以进入系统状态页面查看免布线设备的系统时间是否校对准确。

参数说明

标题项	说明
系统时间	选择系统时间的设置方式，支持网络校时和手动设置。
校时周期	免布线设备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	选择免布线设备当前所在地区的标准时区。

手动设置

手动设置免布线设备的系统时间。使用此方式时，免布线设备每次重启后，您都需要重新设置系统时间。选择“手动设置”时，页面展开的相关参数如下图所示。

参数说明

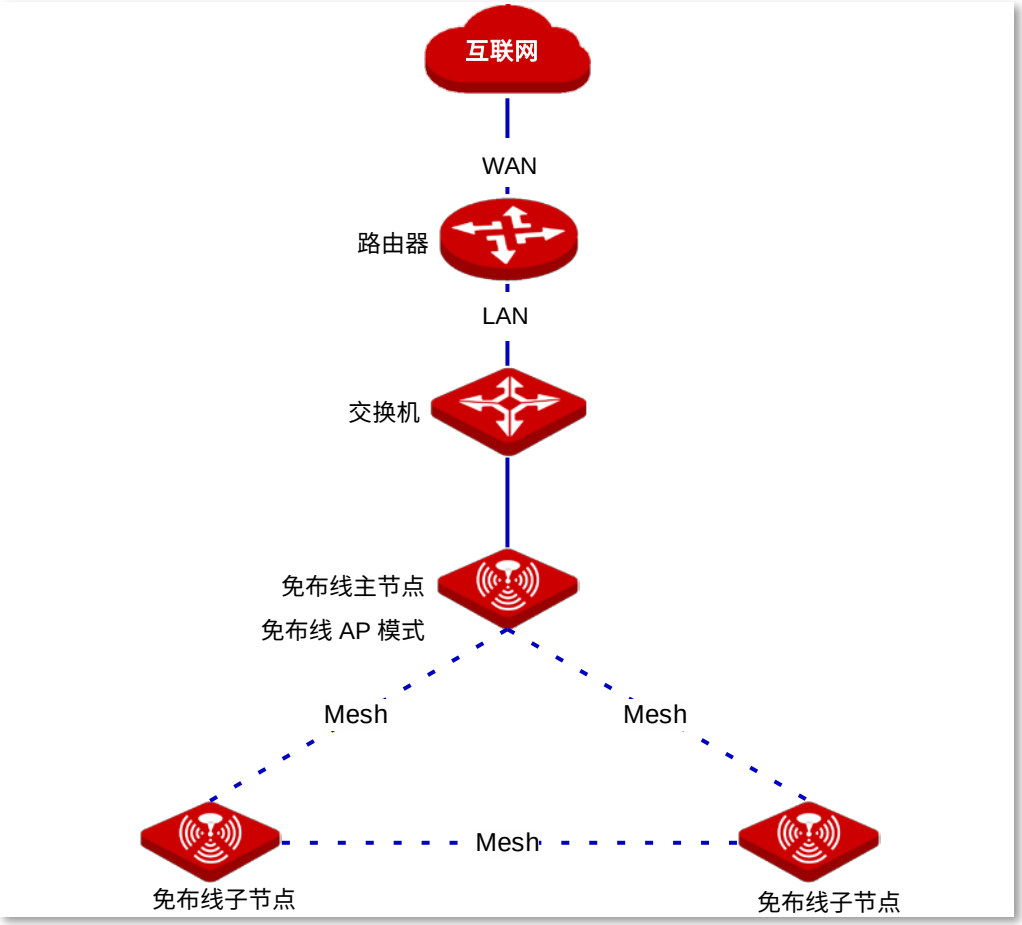
标题项	说明
系统时间	选择系统时间的设置方式，支持网络校时和手动设置。
日期	可以直接在此处输入正确的时间，也可以点击 复制管理主机时间 将正在管理免布线设备的电脑的时间同步到免布线设备。
时间	

设置完成后，您可以进入系统状态页面，查看免布线设备的系统时间是否校对准确。

4 免布线 AP 模式

免布线设备工作在免布线 AP 模式时，作为一个无线接入点，可与其他免布线设备进行 Mesh 组网，提供无线网络覆盖。

应用拓扑图如下：



提示

免布线 AP 模式节点的“PoE WAN/LAN1”口为 LAN 口，通常连接到上级交换机或路由器，以连接到互联网。

4.1 系统状态

在「系统状态」模块，您可以：

- 添加免布线子节点
- 查看设备信息
- 查看在线用户
- 查看无线网络射频状态

进入页面：点击「系统状态」。

4.1.1 添加免布线子节点

免布线主节点可以自动发现已通电并处于出厂设置状态的其他免布线设备，您可根据需要添加这些设备为免布线网络子节点。

添加免布线设备：

如果系统已自动发现新的免布线设备，直接在“系统状态”页面点击“详情”添加即可。如果系统没有发现新的免布线设备，请按以下步骤操作。

1. 在「系统状态」页面，点击“添加”。

2. 输入要添加的免布线设备的 SN（见设备底面贴纸）。
3. 点击 添加 。

----完成

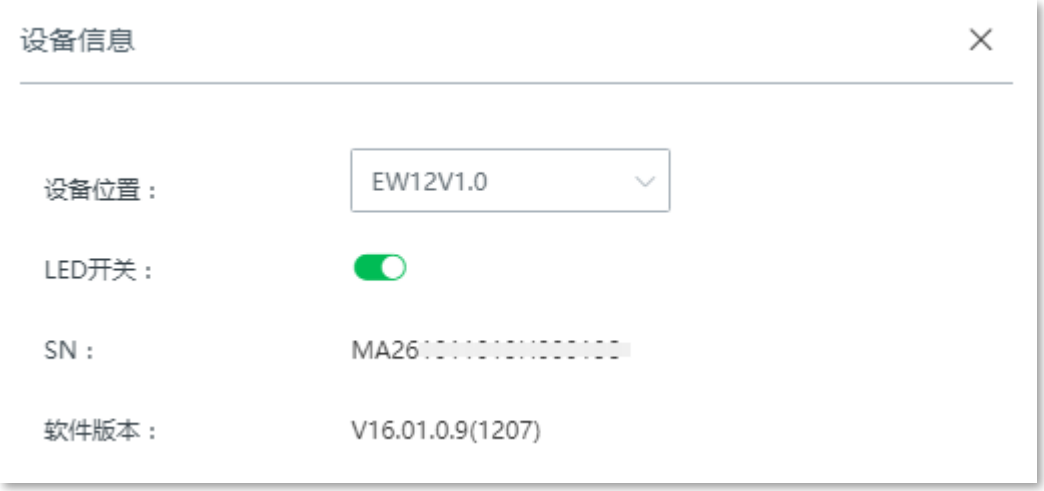
免布线设备添加成功后，可以点击“系统状态”模块右侧的“免布线设备”查看该设备详情。

4.1.2 查看设备信息

查看免布线主节点信息

点击“系统状态”页面中与互联网直连的免布线设备，进入设备信息窗口。在这里，您可以查看免布线主节点的设备基本信息、运行状态和 LAN 口状态。

基本信息



参数说明

标题项	说明
设备位置	节点的位置信息。 建议设置为节点的安装位置描述，方便在管理时，快速定位节点。

标题项	说明
LED 开关	开启/关闭节点的指示灯。 开启后，您可根据指示灯判断节点的工作状态。默认为“开启”。
SN	节点的序列号。
软件版本	节点系统软件的版本号。

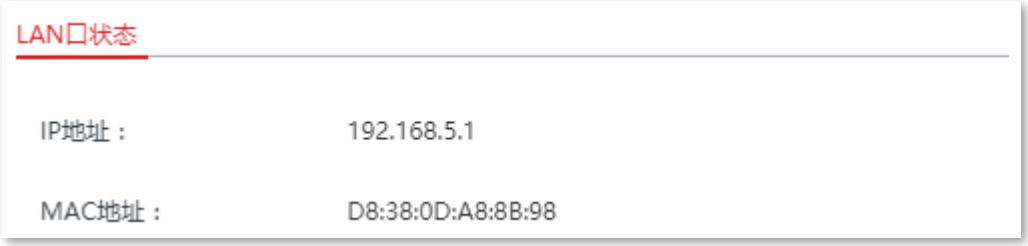
运行状态

参数说明

标题项	说明
工作模式	节点当前的工作模式。 - 免布线主节点：节点作为免布线网络的主节点，上联到有线网络，是免布线网络中唯一访问外部网络的出口，实现 Mesh 网络和有线网络的数据转换。 - 免布线节点：节点作为免布线网络的子节点，通过 Mesh 自组网，扩展现有免布线网络的覆盖范围。 提示 免布线子节点的 PoE WAN/LAN1 口为 LAN 口。
已连接终端	当前连接到免布线网络的终端数量。
系统时间	节点当前的系统时间。
运行时间	节点最近一次启动后连续运行的时长。

标题项	说明
CPU 使用率	节点当前的 CPU 使用率。
内存使用率	节点当前的内存使用率。

LAN 口状态

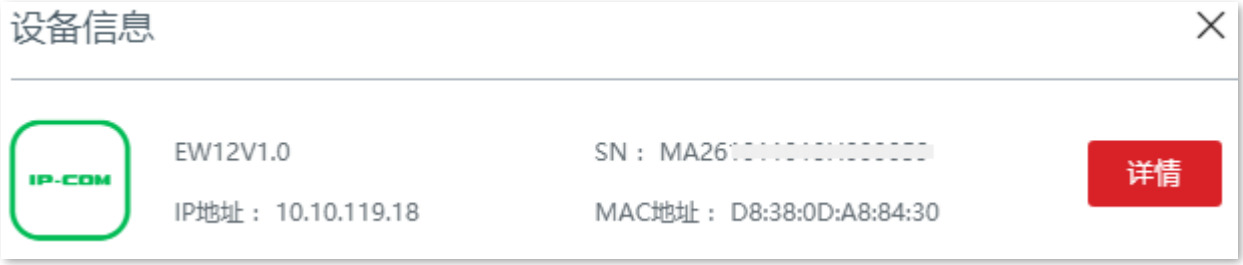


参数说明

标题项	说明
IP 地址	节点的 LAN 口 IP 地址，也是节点的管理 IP 地址，局域网用户可访问该 IP 地址登录到节点的管理页面。 主节点的 LAN 口 IP 地址默认为“192.168.5.1”。子节点的 LAN 口 IP 地址从局域网中的 DHCP 服务器自动获取。 提示 免布线 AP 模式下，如果网络中有 DHCP 服务器，节点会从 DHCP 服务器自动获取 IP 地址。下次登录节点的管理页面前，您必须到 DHCP 服务器的客户端列表中查看节点获得的 IP 地址，再用该 IP 地址进行登录。
MAC 地址	节点 LAN 口的物理地址。

查看免布线子节点信息

点击“系统状态”页面中用户设备旁的免布线设备，在出现的窗口中，您可以查看免布线子节点的设备信息。



如需了解更多信息，请点击对应节点后的 详情 展开页面。

在这里，您可以查看或设置节点的基本信息，查看运行状态、LAN 口状态、免布线链路信息，重启或删除节点。

免布线链路信息

参数说明

标题项	说明
上级节点的 MAC 地址	Mesh 自组网链路上级节点用于组建 Mesh 链路的接口的物理地址。
免布线链路质量	免布线链路的连接质量。
与上级链接方式/强度	本节点与上级节点的组网方式/本节点接收到的上级节点的信号强度。

重启节点

点击 重启 ，可以立即重启该节点。

删除节点

点击 删除节点 ，可以将该节点从免布线网络中移除。从免布线网络中移除的节点，配置会恢复到出厂状态。

4.1.3 查看在线用户

进入页面：点击「系统状态」。

在这里，您可以点击“用户设备”查看所有的在线终端。

4.1.4 查看无线网络射频状态

在“系统状态”页面的“无线网络射频状态”模块，可以查看节点各无线网络的名称、MAC 地址和网络启用状态。

无线网络射频状态

射频	无线名称	MAC	启用状态
2.4GHz网络	IP-COM_A88B98	D8:38:0D:A8:8B:99	已启用
5GHz网络	IP-COM_A88B98	D8:38:0D:A8:8B:A0	已启用
2.4GHz网络	IP-COM_A88B99	--	未启用
5GHz网络	IP-COM_A88B99	--	未启用
2.4GHz网络	IP-COM_A88B9A	--	未启用
5GHz网络	IP-COM_A88B9A	--	未启用
2.4GHz网络	IP-COM_A88B9B	--	未启用
5GHz网络	IP-COM_A88B9B	--	未启用

4.2 无线设置

在这里，您可以修改免布线主节点的无线接入相关设置。

本设备最多支持三频无线网络。默认情况下，设备采用无线方式组建免布线网络，其中一个 5GHz 无线频段专用于建立免布线链路，2.4GHz 无线频段和另外一个 5GHz 无线频段用于终端设备接入。当设备采用有线方式组建免布线网络时，设备的三个无线频段都用于终端设备接入。

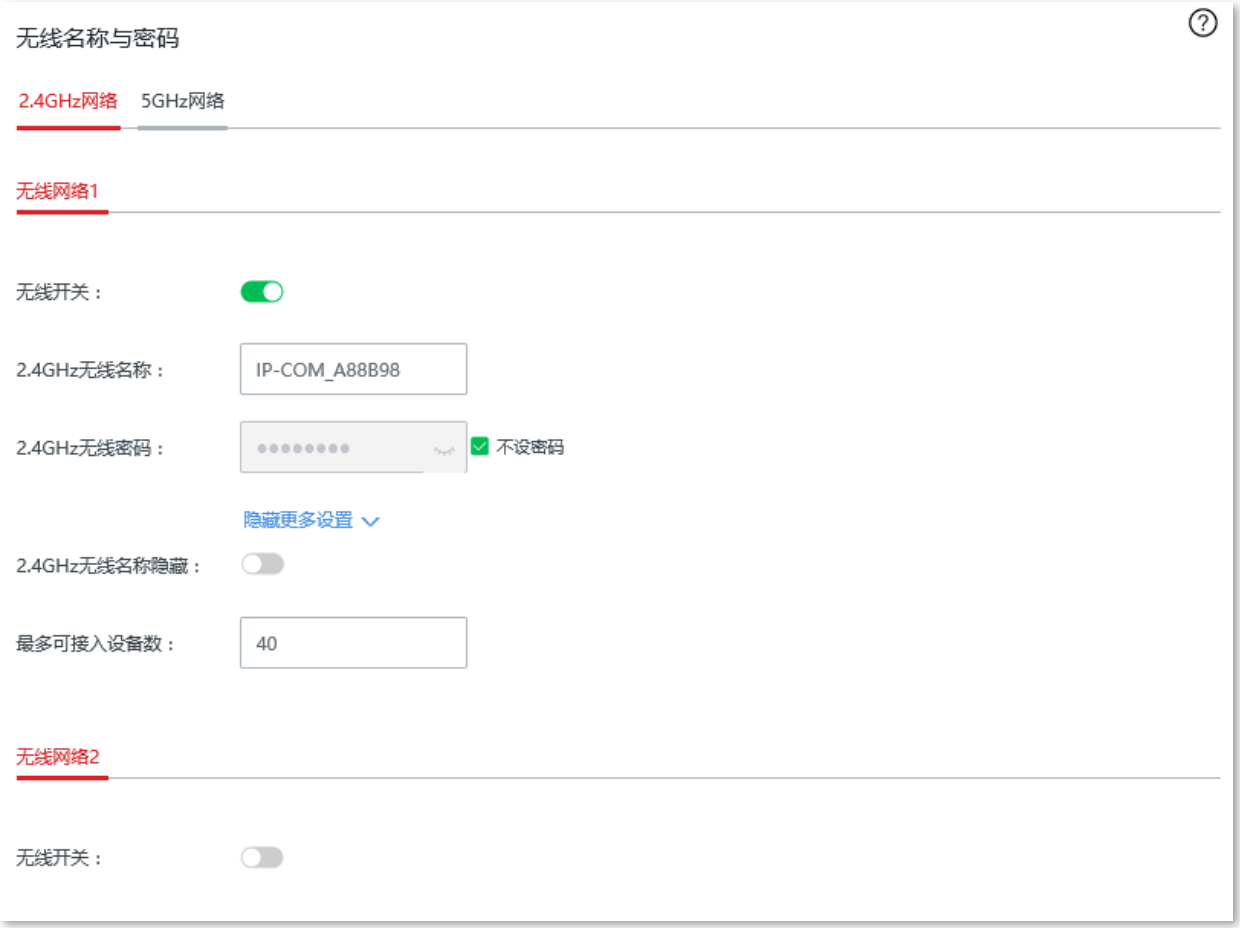
提示

本模块的配置会同步应用到免布线网络中的其他节点。

4.2.1 无线名称与密码

进入页面：点击「无线设置」>「无线名称与密码」。

在这里，您可以设置无线基本参数，包括开启/关闭无线网络、修改无线名称、设置无线密码等。



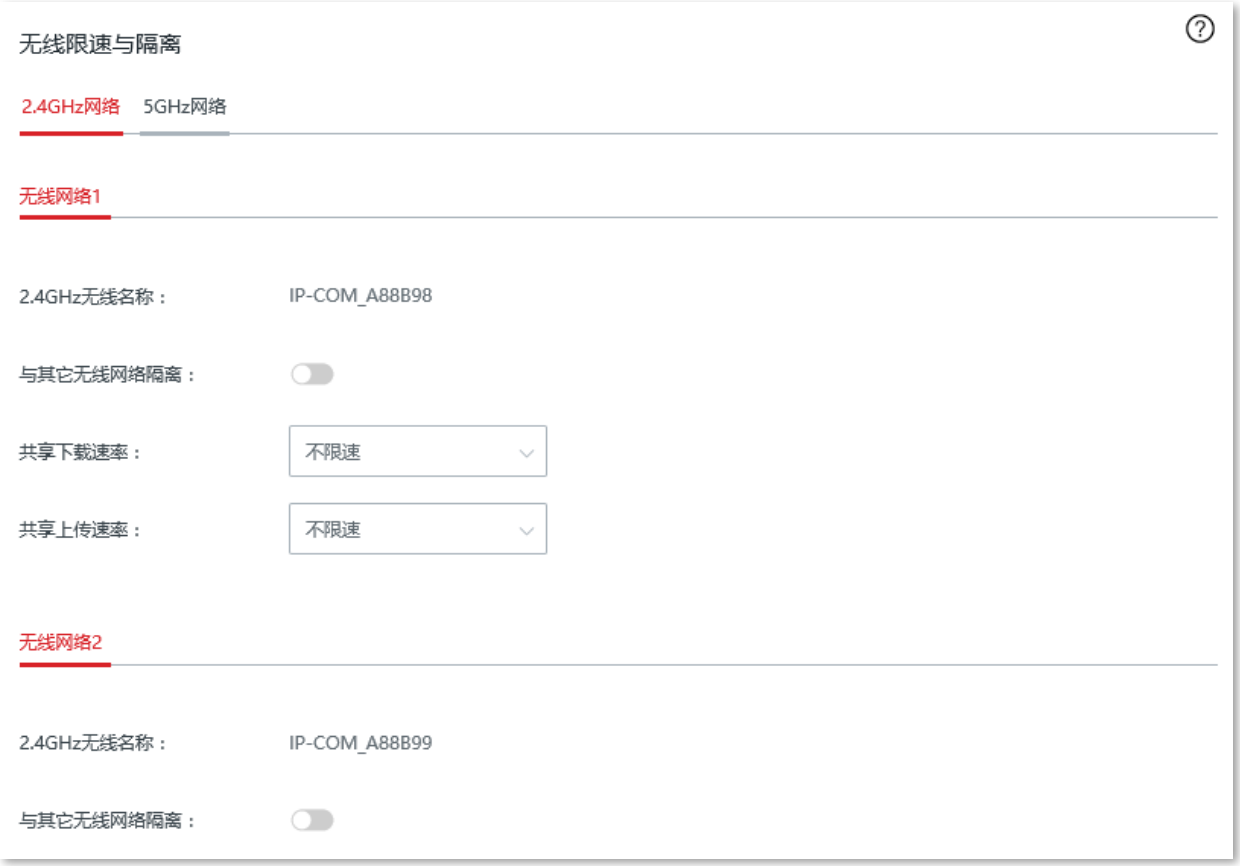
参数说明

标题项	说明
无线网络 1/2/3	节点每个频段均支持 4 个无线网络，默认只开启无线网络 1。
无线开关	开启/关闭对应无线网络的无线功能。
无线名称	节点的无线网络名称。
无线密码	无线网络密码。为了无线网络安全，强烈建议设置无线密码。
不设密码	不设置无线密码，此时对应的无线网络为不加密状态。
无线名称隐藏	开启后，无线网络名称会隐藏，该无线网络不会出现在终端设备（如手机）的可用无线网络列表中，一定程度上增强了无线网络的安全性。 如果要连接隐藏的无线网络，用户需要在终端设备上手动输入该无线网络名称。
最多可接入设备数	无线网络最多允许接入的无线设备数量。 若接入无线网络的无线设备达到此值，除非某些设备断开连接，否则新的无线设备不能接入该无线网络。

4.2.2 无线限速与隔离

进入页面：点击「无线设置」>「无线隔离」。

在这里，您可以设置无线网络限速与隔离。本功能默认关闭。



参数说明

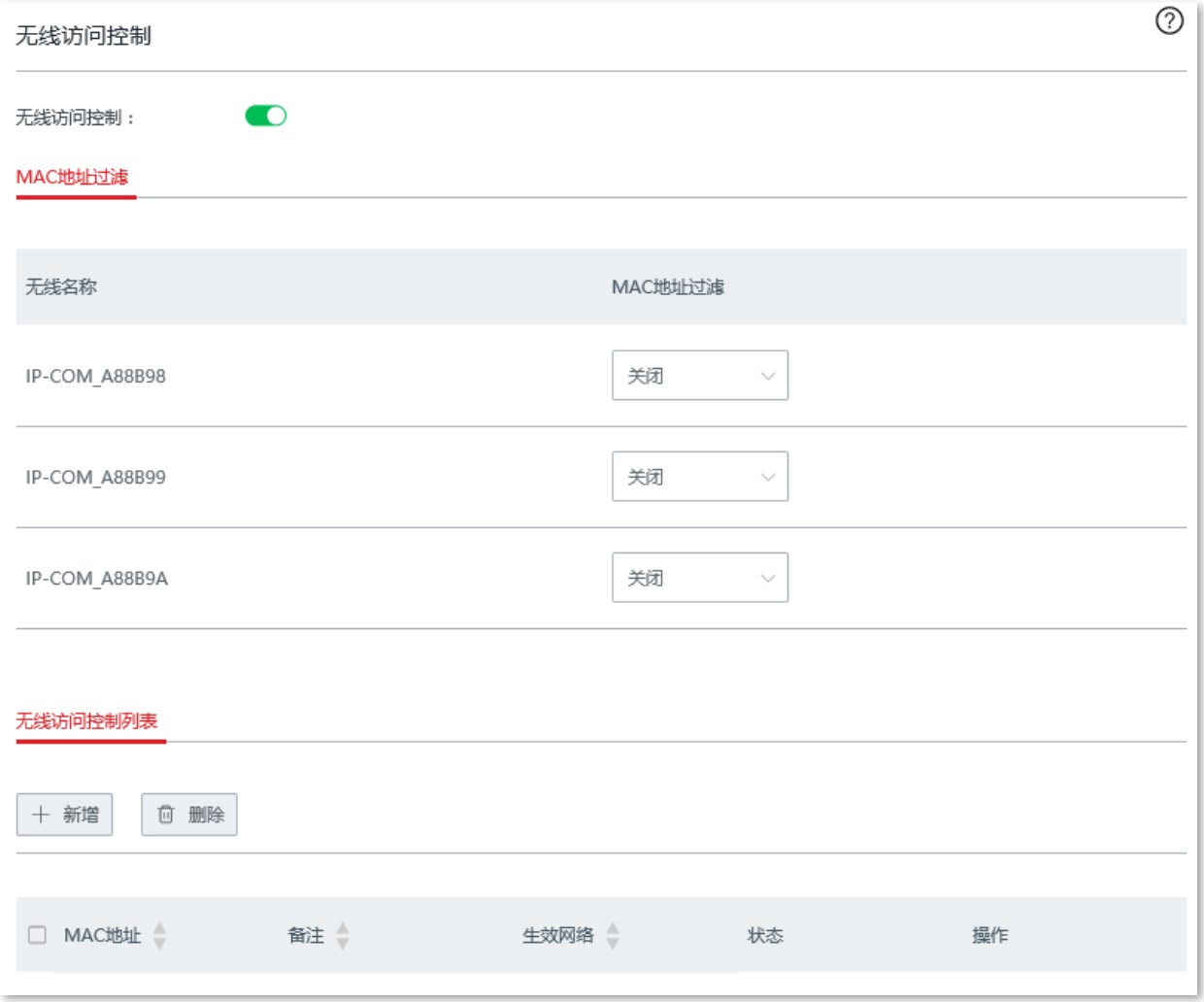
标题项	说明
无线名称	节点的无线网络名称。
与其它无线网络隔离	开启后，连接到该无线网络的用户与连接到免布线系统其他无线网络的用户之间不能互相通信，可增强无线网络的安全性。
共享下载/上传速率	连接到该无线网络的用户共享的最大下载/上传速率。 不限制：不限制该无线网络的最大下载/上传速率。

4.2.3 无线访问控制

概述

进入页面：点击「无线设置」>「无线访问控制」。

在这里，您可以通过设置无线访问控制规则，允许或禁止指定设备连接到对应的无线网络。无线访问控制功能默认关闭，开启后，页面显示如下。



参数说明

标题项		说明
无线访问控制		无线访问控制功能开关。表示关闭，表示开启。
MAC 地址过滤	无线名称	节点当前启用的无线网络的名称。

标题项		说明
	MAC 地址过滤	MAC 地址过滤模式。 – 关闭：该无线网络不启用 MAC 地址过滤功能，允许所有无线客户端连接。 – 仅允许：仅允许无线访问控制列表中指定的无线客户端连接到该无线网络。 – 仅禁止：仅禁止无线访问控制列表中指定的无线客户端连接到该无线网络，其他无线客户端可以连接到该无线网络。
无线访问控制列表	MAC 地址	无线客户端的 MAC 地址。
	备注	MAC 地址的备注信息。
	生效网络	规则生效的无线网络。
	状态	规则的状态，可根据需要开启或关闭。
	操作	可对规则进行如下操作： – 点击 可以修改规则。 – 点击 可以删除规则。

配置无线访问控制

开启无线访问控制功能

在「无线设置」>「无线访问控制」页面，点击滑块至，然后点击页面底端的 保存 。

设置 MAC 地址过滤模式

在「无线设置」>「无线访问控制」页面，根据需要选择无线网络的“MAC 地址过滤”模式，然后点击页面底端的 保存 。

添加无线访问控制规则

1. 在「无线设置」>「无线访问控制」页面，点击 + 新增 进入配置窗口。
2. 设置无线访问控制规则。
   (1) 输入要限制连接无线网络的无线客户端的 MAC 地址。
   (2) （可选）设置该 MAC 地址的备注信息。
   (3) 选择规则生效的无线网络。

提示

点击 + ，可同时添加多条访问控制规则，点击 – 可删除未保存的访问控制规则。

3. 点击 保存 。

----完成

您可以在「无线设置」>「无线访问控制」页面看到新增的无线访问控制规则。

无线访问控制配置举例

组网需求

某企业使用免布线设备进行网络搭建。

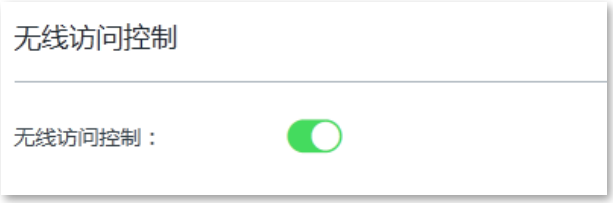
要求：仅允许某一采购人员连接免布线主节点 WiFi（caigou）访问互联网，其他员工禁止连接。

方案设计

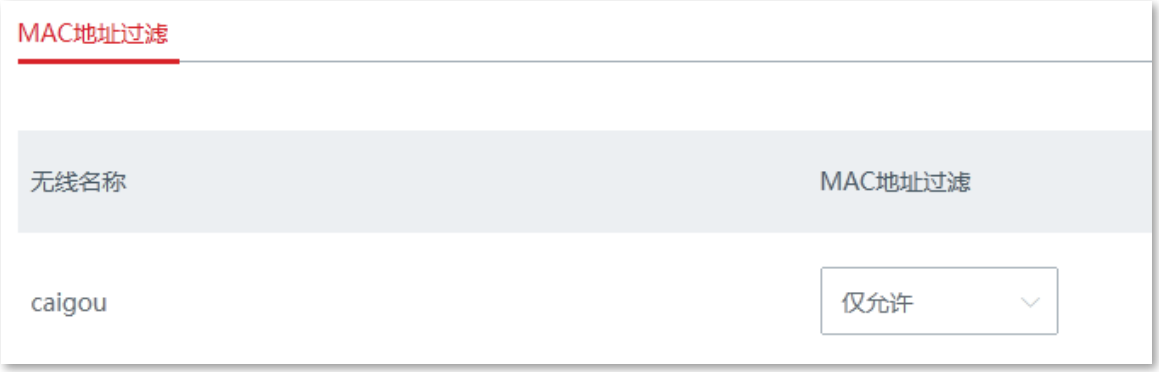
使用无线访问控制功能实现上述需求。假设该采购人员电脑的物理地址为 CC:3A:61:71:1B:6E。

配置步骤

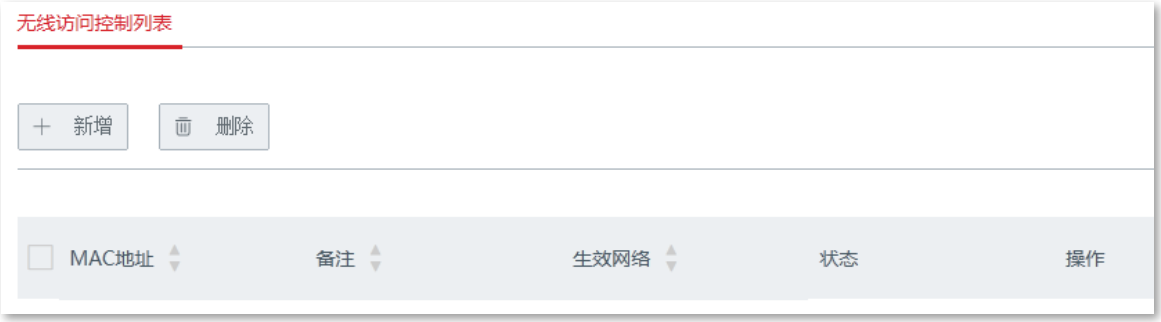
1. 点击「无线设置」>「无线访问控制」进入配置页面。
2. 开启无线访问控制功能。
   (1) 点击滑块至。
   (2) 点击页面底端的 保存 。



3. 设置 MAC 地址过滤模式。
   (1) 选择无线网络“caigou”的“MAC 地址过滤”模式，本例为“仅允许”。
   (2) 点击页面底端的 保存 。

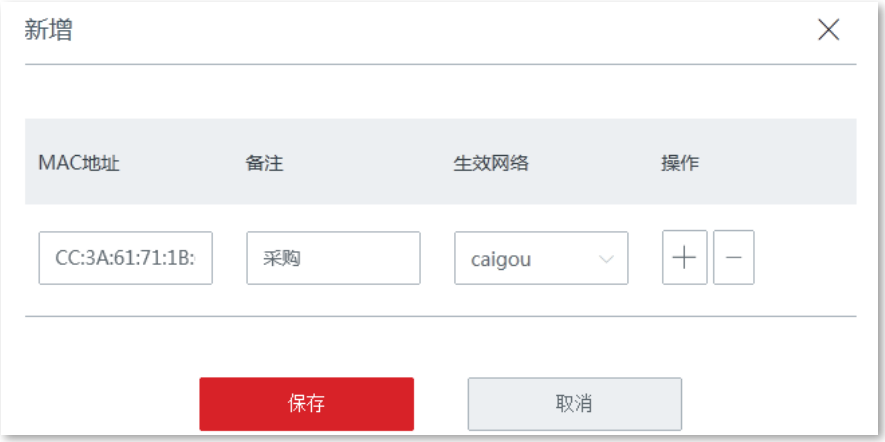


4. 添加无线访问控制规则。
   (1) 点击 + 新增 。

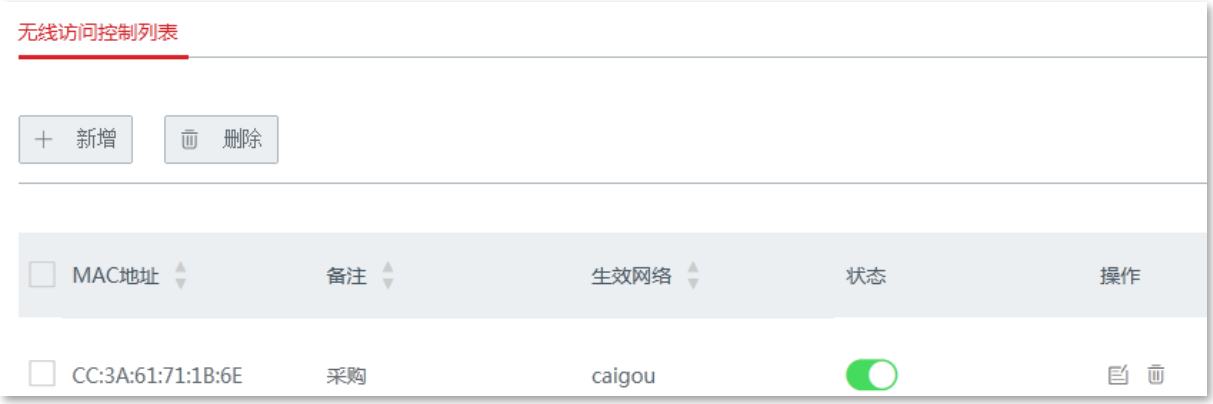


(2) 在【新增】窗口进行如下配置，然后点击 保存 。

- 输入采购人员电脑的 MAC 地址（物理地址），本例为“CC:3A:61:71:1B:6E”。
- （可选）设置本规则的备注，如“采购”。
- 选择规则生效的无线网络，本例为“caigou”。



添加成功，如下图示。



----完成

验证配置

只有上述 1 台无线设备可以接入无线网络“caigou”，其他设备无法连接到该网络。

4.2.4 无线高级设置

进入页面：点击「无线设置」>「无线高级设置」。

在这里，您可以设置无线高级参数，包括发射功率、网络模式、信道、信道带宽等。

参数说明

标题项	说明
2.4GHz/5GHz 网络	开启/关闭对应无线频段的无线功能。
发射功率	节点对应频段的无线发射功率。 发射功率越大，无线覆盖范围越广。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。
国家或地区	选择节点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。
网络模式	节点对应频段的无线网络模式。 2.4GHz 包括 11b、11g、11b/g、11b/g/n，默认工作在 n+256QAM。

标题项	说明
	- 11b：此模式下，仅允许 802.11b 无线设备接入节点的 2.4GHz 无线网络。 - 11g：此模式下，仅允许 802.11g 无线设备接入节点的 2.4GHz 无线网络。 - 11b/g：此模式下，802.11b、802.11g 的无线设备可以接入节点的 2.4GHz 无线网络。 - 11b/g/n：此模式下，802.11b、802.11g 以及工作在 2.4GHz 的 802.11n 无线设备可以接入节点的 2.4GHz 无线网络。 - n+256QAM：802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备可以接入节点的 2.4GHz 无线网络。 QAM，Quadrature Amplitude Modulation，正交幅度调制。QAM 是一种在两个正交载波上进行幅度调制的调制方式，它利用正弦波和余弦波的正交性，同时调制两路信号，提高了调制效率。n+256QAM 是在 2.4GHz 频段，让 IEEE 802.11n 标准改用 IEEE 802.11ac 的 256-QAM 调制模式，单流速率也从 IEEE 802.11n 标准的 150Mbps 提升至 IEEE 802.11ac 标准的 200Mbps。 需要注意的是，这种提升只有在 2.4GHz 频段且发射端和接收端均支持的情况下才有效，任何一方不支持 n+256QAM，那 2.4GHz 频段下单流速率最高仍然是 150Mbps。而且在调制模式改为 n+256QAM 后，网络的稳定度及抗干扰性都比其他模式下要逊色。 5GHz 包括 11a、11ac、11a/n，默认工作在 11ac。 - 11a：此模式下，仅允许 802.11a 无线设备接入节点的 5GHz 无线网络。 - 11ac：此模式下，仅允许 802.11ac 无线设备接入节点的 5GHz 无线网络。 - 11a/n：此模式下，802.11a 以及工作在 5GHz 的 802.11n 无线设备可以接入节点的 5GHz 无线网络。
信道	节点无线数据传输的通道。可选择范围由当前选择的国家或地区、无线工作频段来决定。 自动：节点自动检测各信道利用率，并据此选择合适的工作信道。 如果使用节点无线网络时，经常出现掉线、卡顿或网速慢现象，可以尝试修改节点的信道来解决问题。您可以通过工具软件（如 WiFi 分析仪）获得周边较少用到、干扰较小的信道。
信道带宽	节点无线信道的频带宽度。高信道带宽下，更容易获得较高的传输速率，但穿透性稍差，传输距离近。 - 20MHz：节点使用 20MHz 的信道带宽。 - 40MHz：节点使用 40MHz 的信道带宽。 - 20MHz/40MHz：仅适用于 2.4GHz。节点根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。 - 80MHz：仅适用于 5GHz。节点使用 80MHz 的信道带宽。
接入信号强度限制	节点对应频段可接受的最低无线信号强度，信号强度低于此值的设备将无法接入节点。 当环境中存在多个节点时，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节点。

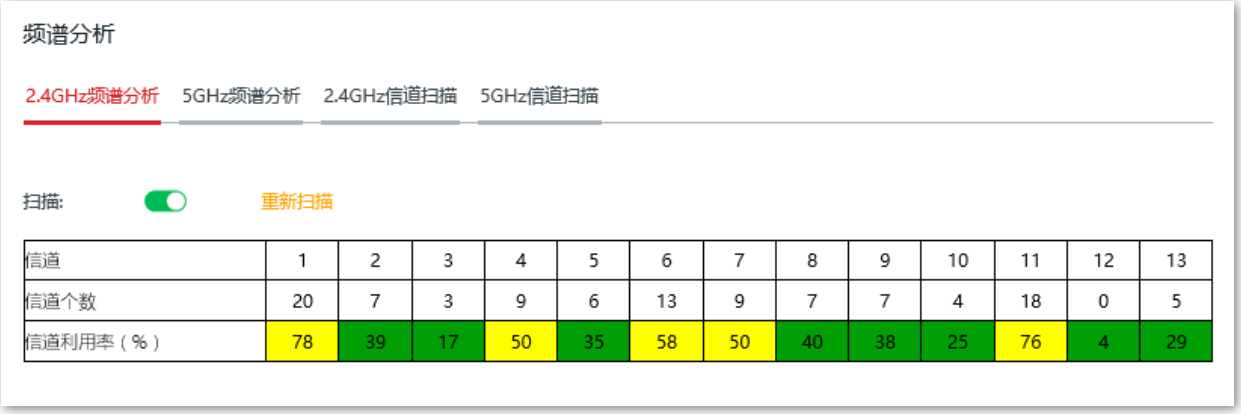
4.2.5 频谱分析

频谱分析

通过频谱分析，您可以查看各个信道的无线网络个数及信道利用率，然后选择一个利用率较低的信道来作为节点的工作信道，以提升无线传输效率。

进入页面：点击「无线设置」>「频谱分析」>「频谱分析」。

以下图示以 2.4GHz 频段为例。



信道	1	2	3	4	5	6	7	8	9	10	11	12	13
信道个数	20	7	3	9	6	13	9	7	7	4	18	0	5
信道利用率（%）	78	39	17	50	35	58	50	40	38	25	76	4	29

- 信道利用率的底色为绿色，代表信道情况良好。
- 信道利用率的底色为黄色，代表信道拥挤。
- 信道利用率的底色为红色，代表信道非常拥挤，基本不可用。

信道扫描

通过信道扫描，您可以查看节点周围环境中其他无线网络的基本情况，例如无线名称、MAC 地址、信道带宽和信号强度等信息。

进入页面：点击「无线设置」>「频谱分析」>「信道扫描」。

以下图示以 2.4GHz 频段为例。


频谱分析
2.4GHz频谱分析
5GHz频谱分析
2.4GHz信道扫描
5GHz信道扫描
扫描:
重新扫描
序号
无线名称
MAC地址
信道带宽
信道
信号强度
1
888888
d8:38:0d:86:70:06
40
9
-37dBm
2
office
d8:38:0d:a8:8b:09
20
6
-48dBm
3
hu
d8:38:0d:ad:8d:11
20
3
-50dBm

4.3 智能优化

通过智能优化功能，您可以对整个免布线网络系统进行优化，以获得更好的用户体验。

进入页面：点击「智能优化」。

4.3.1 有线组网

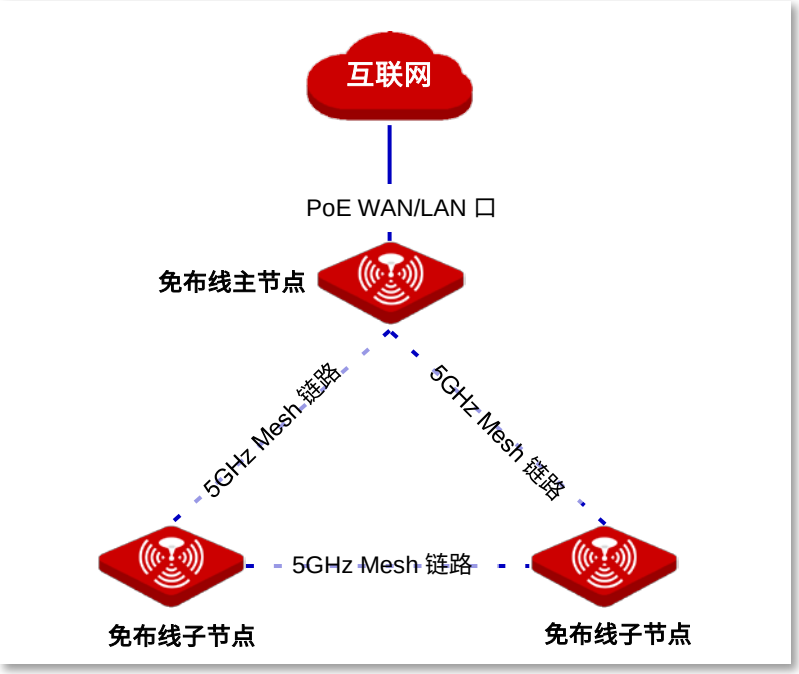
概述

免布线设备支持两种组网方式：无线组网、有线组网。默认采用无线组网方式。

- **无线组网**

使用无线方式组建免布线网络系统，各个免布线设备之间通过无线连接。此时，免布线设备将其中一个 5GHz 无线频段专门用于建立免布线链路，将 2.4GHz 无线频段和另外一个 5GHz 无线频段用于终端设备接入。

无线组网连接图示如下。

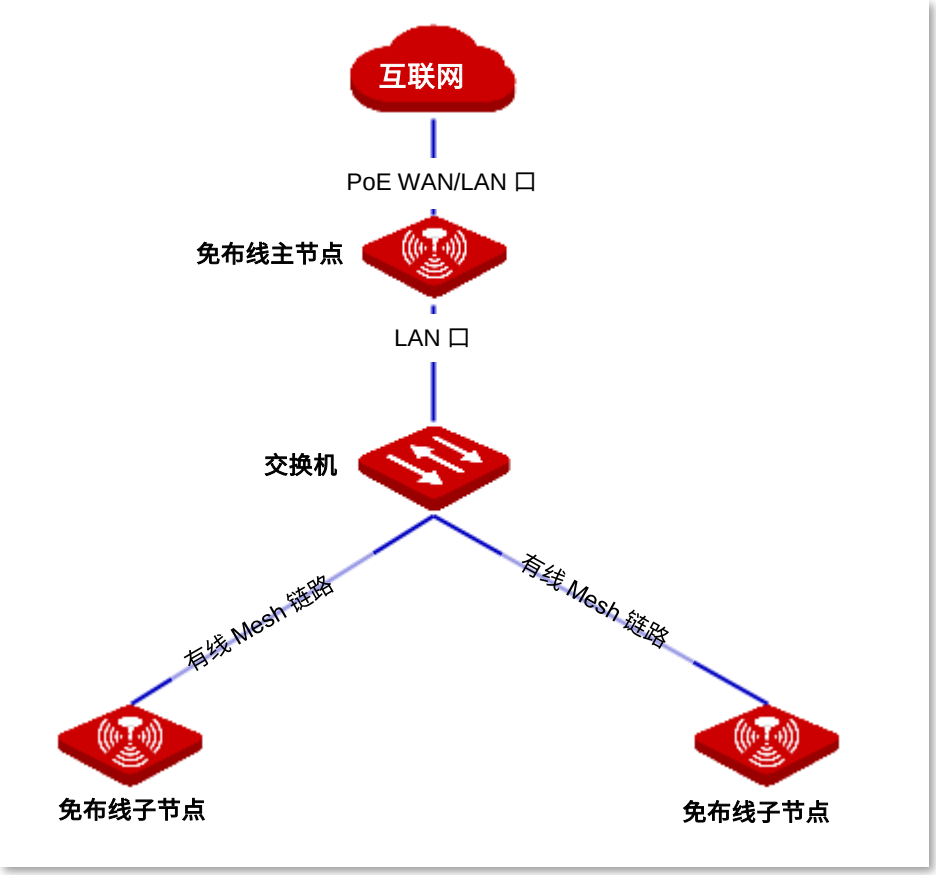


- **有线组网**

使用有线方式组建免布线网络系统，各个免布线设备之间通过网线连接。此时，免布线设备的三个无

线频段都用于终端设备接入。

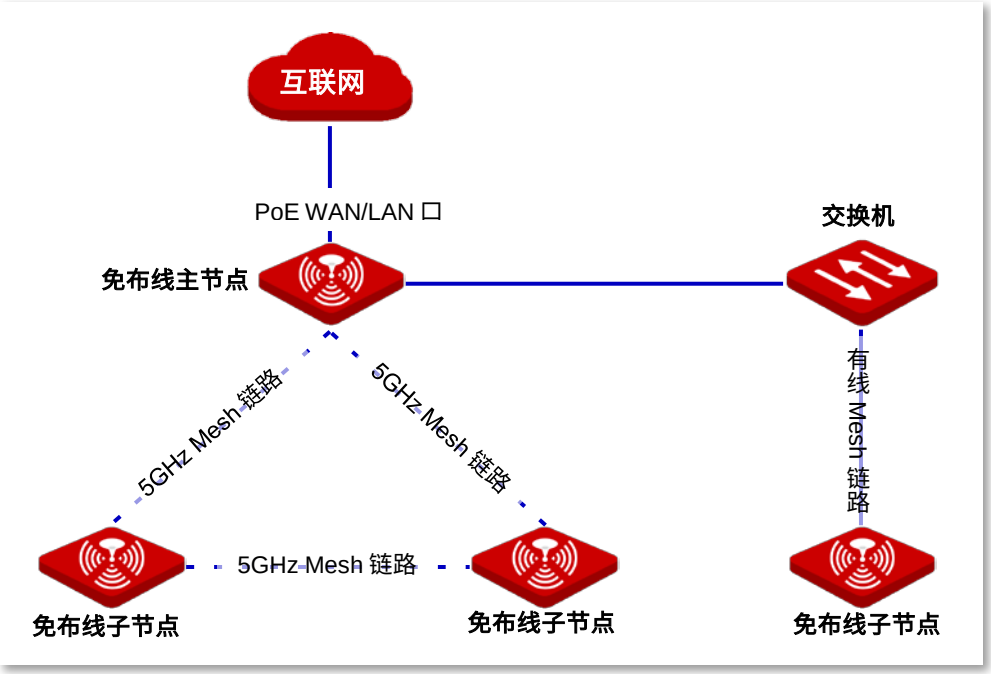
有线组网连接图示如下。



总的来说，无线组网更简单快捷，有线组网对网络布线有一定要求，但它也有以下优势：

- Mesh 链路稳定，速率高，传输距离远
- 无线带机量更高

实际组网中，您也可以根据需要，采用混合组网方式。组网连接图如下图示例。



配置有线组网

提示

开启有线组网后，无线组网功能自动关闭，已通过无线组网的免布线设备将会掉线。

1. 在「智能优化」页面的“有线组网”模块，找到要修改组网方式的节点，点击“有线组网”栏的滑块至。

参数说明

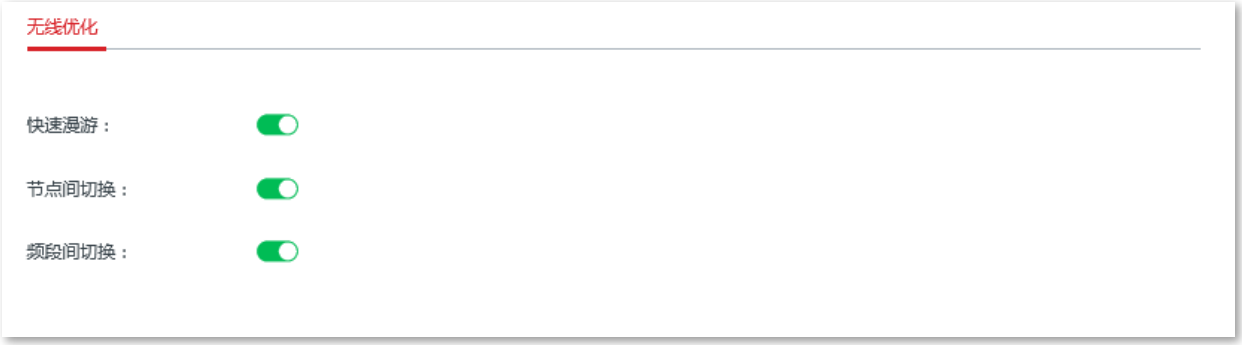
标题项	说明
型号	节点的型号及版本。
备注	节点的备注信息。可以在「节点管理」>「节点维护」页面修改。
IP 地址	节点的 IP 地址。
MAC 地址	节点的物理地址。
状态	有线组网功能的启用状态。
有线组网	开启/关闭节点的有线组网功能。 开启后，节点的组网方式由无线组网转为有线组网，节点的三个无线频段都用于终端接入。

2. 用网线将上述各节点连接起来。

----完成

4.3.2 无线优化

在这里，您可以通过调节快速漫游、节点间切换、频段间切换的启用状态来优化免布线系统的无线体验。



参数说明

标题项	说明
快速漫游	开启后，支持 802.11r 快速漫游协议的客户端在接收到节点无线信号降至其漫游触发临界值时，自动漫游切换到其他节点，这一过程只需毫秒级的时间。开启此功能，可以降低用户在节点之间移动时业务所受的影响。 注意：此功能需要各节点使用相同的无线名称/密码。

标题项	说明
节点间切换	开启后，支持 802.11k、802.11v 协议的客户端能够获得节点的相关网络信息，并根据这些信息判断是否需要切换到其他网络质量更好的节点。开启此功能，可以有效分散客户端使其连接到更合适的节点。 注意：此功能需要各节点使用相同的无线名称/密码。
频段间切换	开启后，当双频客户端连接节点时，节点会根据当前各频段的网络质量情况，引导客户端连接到质量更好的频段。 注意：此功能需要节点的 2.4GHz 频段和 5GHz 使用相同的无线名称/密码。

4.4 更多设置

4.4.1 局域网设置

进入页面：点击「更多设置」>「局域网设置」。

在这里，您可以设置节点的 LAN 口 IP 地址和 DHCP 服务器。

LAN 口 IP 设置

LAN 口 IP 地址是节点对局域网的 IP 地址，也是节点的管理 IP 地址。节点默认的 LAN 口 IP 地址为 192.168.5.1，子网掩码为 255.255.255.0。

一般情况下，您无需修改 LAN 口设置，除非遇到 IP 地址冲突，如：局域网内，有其它设备的 IP 地址也为 192.168.5.1。

LAN 口 IP 地址修改成功后，页面将自动跳转到登录页面。如果没有，请确保管理主机的 IP 地址已设置为与节点新的 LAN 口 IP 地址在同一网段的其他 IP 地址，之后访问新的 LAN 口 IP 地址重新尝试。

参数说明

标题项	说明
IP 地址	节点的 IP 地址，也是节点的管理 IP 地址，局域网用户可访问该 IP 地址登录到节点的管理页面。

标题项	说明
子网掩码	节点的子网掩码，用于定义设备网段的地址空间。
默认网关	节点的默认网关。 如果节点需要接入互联网，一般设置网关地址为出口路由器的 LAN 口 IP 地址。
首选 DNS	节点的首选 DNS 服务器地址。 如果出口路由器有 DNS 代理功能，此处可填入出口路由器的 LAN 口 IP 地址。否则，请填入正确的 DNS 服务器的 IP 地址。
备用 DNS	节点的备用 DNS 服务器地址，该选项可选填。 若有两个 DNS 服务器 IP 地址，可将另一个 IP 地址填在此处。

DHCP 服务器

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

免布线 AP 模式下，默认禁用了 DHCP 服务器。

开启 DHCP 服务器后，页面显示如下。

参数说明

标题项	说明
DHCP 服务器	DHCP 服务器功能开关。表示关闭，表示开启。

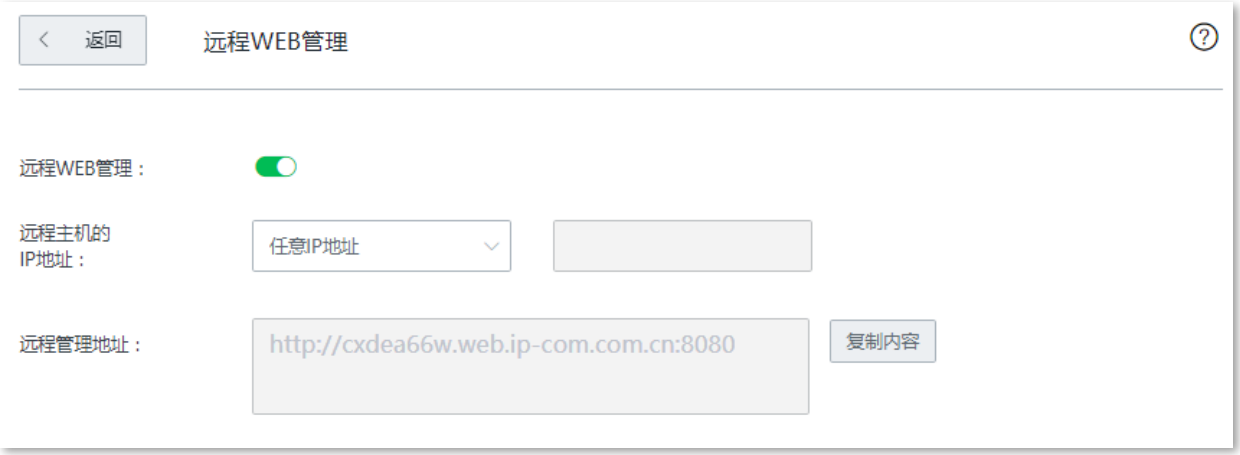
标题项	说明
起始 IP 地址	DHCP 服务器可分配的 IP 地址范围。起始 IP 地址默认为 192.168.5.100，结束 IP 地址默认为 192.168.5.200。 提示 修改 LAN 口 IP 地址后，如果新的 LAN 口 IP 地址与原 LAN 口 IP 地址不在同一网段，系统将自动匹配修改 DHCP 地址池，使其和新的 LAN 口 IP 地址在同一网段。
结束 IP 地址	
租约时间	DHCP 服务器分配给局域网设备的 IP 地址的有效时间，默认为 30 分钟。 当地址到期后： - 如果设备仍连接在免布线网络，设备将自动续约，继续占用该 IP 地址。 - 如果设备未连接（关机、网线已拔掉、无线已断开等）到免布线网络，节点将释放该 IP 地址。以后若有其它设备请求 IP 地址信息，节点可将该 IP 分配给其它设备。 如无特殊需要，建议保持默认设置。
首选 DNS	DHCP 服务器分配给局域网设备的首选 DNS 服务器 IP 地址。默认为节点的 LAN 口 IP 地址。 提示 开启 DHCP 服务器的情况下，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。

4.4.2 远程 WEB 管理

一般情况下，只有接到节点的 LAN 口或无线网络的设备才能登录节点的管理页面。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），可以从互联网远程访问节点的管理页面。

进入页面：点击「更多设置」>「远程 WEB 管理」。

远程 WEB 管理默认关闭，开启后，页面显示如下。



参数说明

标题项	说明
远程 WEB 管理	远程 WEB 管理功能开关。表示关闭，表示开启。
远程主机的 IP 地址	可以远程访问节点管理页面的设备的 IP 地址。 - 任意 IP 地址：互联网上任意 IP 地址的设备都能访问节点的管理页面。为了网络安全，不建议选择此项。 - 特定 IP 地址：只有指定 IP 地址的设备能远程访问节点的管理页面。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	远程管理节点时使用的域名。 开启“远程 WEB 管理”后，互联网用户可以访问此域名登录到节点的管理页面。

4.4.3 QVLAN

概述

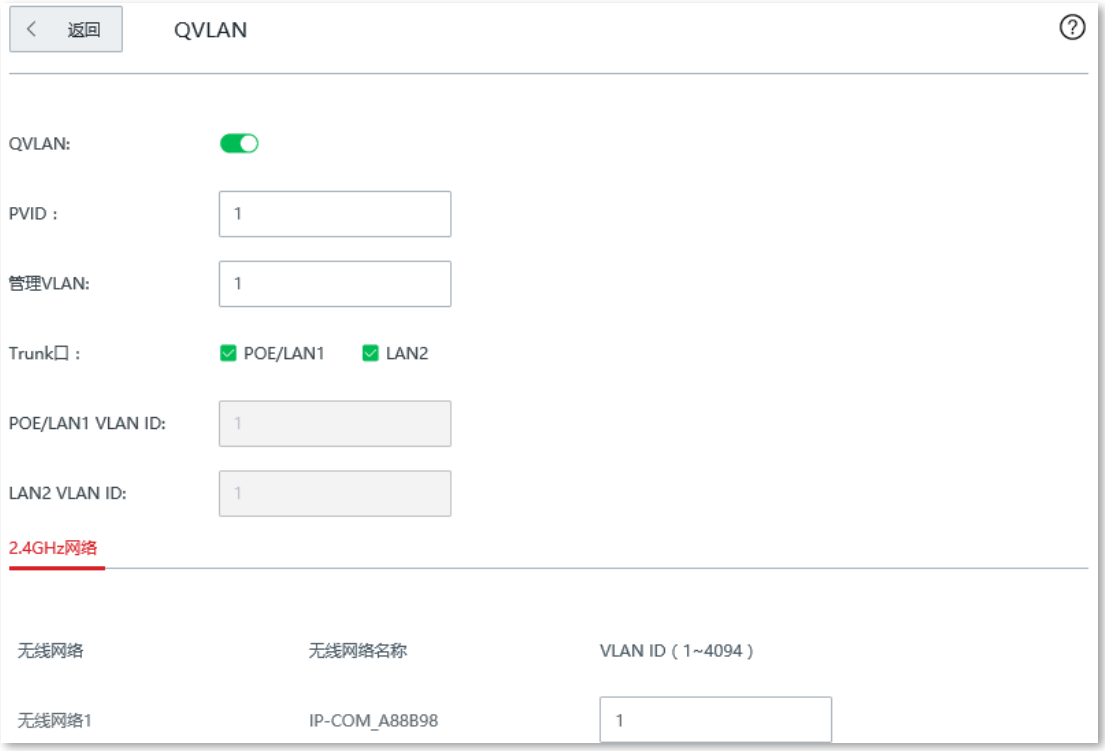
免布线 AP 模式节点支持 IEEE 802.1q VLAN，可以在划分了 QVLAN 的网络环境使用。默认情况下，节点关闭了 QVLAN 功能。

启用 QVLAN 后，对于进入端口的 Tag 数据，按数据中的 VID 转发到相应 VLAN 的其他端口；对于进入端口的 Untag 数据，按该端口的 PVID 转发到相应 VLAN 的其他端口。各链路类型端口对数据的接收和发送处理方式详见下表：

<table>
<tr><th rowspan="2">端口链路类型</th><th colspan="2">接收数据处理</th><th rowspan="2">发送数据处理</th></tr>
<tr><th>接收 Tag 数据</th><th>接收 Untag 数据</th></tr>
<tr><td>Access</td><td rowspan="2">按 Tag 中的 VID 转发到相应 VLAN 的其他端口。</td><td rowspan="2">按该端口的 PVID 转发到相应 VLAN 的其他端口。</td><td>去掉报文的 Tag 再发送。</td></tr>
<tr><td>Trunk</td><td>VID ＝ 端口 PVID，去掉 Tag 发送。
VID ≠ 端口 PVID，保留 Tag 发送。</td></tr>
</table>

配置 QVLAN

点击「更多设置」>「QVLAN」进入设置页面。



参数说明

标题项	说明
QVLAN	QVLAN 功能开关。表示关闭，表示开启。
PVID	节点的 Trunk 口默认所属的 VLAN 的 ID。
管理 VLAN	节点的管理 VLAN ID。 更改管理 VLAN 后，管理主机需要重新连接到新的管理 VLAN，才能管理节点。
Trunk 口	选择作为节点的 Trunk 口的以太网口（有线 LAN 口）。默认为“POE/LAN1”和“LAN2”。Trunk 口允许所有 VLAN 通过。 注意 启用 QVLAN 功能时，至少要选择一个 LAN 口作为 Trunk 口。如果节点只有一个以太网口，则默认将该以太网口作为 Trunk 口。
POE/LAN1 VLAN ID LAN2 VLAN ID	若以太网口未被设为 Trunk 口，则视作 Access 口，可以在此处设置其 VLAN ID。
无线网络 VLAN ID	节点 2.4GHz/5GHz 频段当前已启用的无线网络，以及各无线网络对应的 VLAN。 提示 启用 VLAN 后，无线网络相当于一个 Access 口，其 PVID 与 VLAN ID 相同。

QVLAN 配置举例

组网需求

某酒店使用免布线设备进行无线覆盖，已设置免布线设备工作在免布线 AP 模式，且已接入互联网。现需求如下：

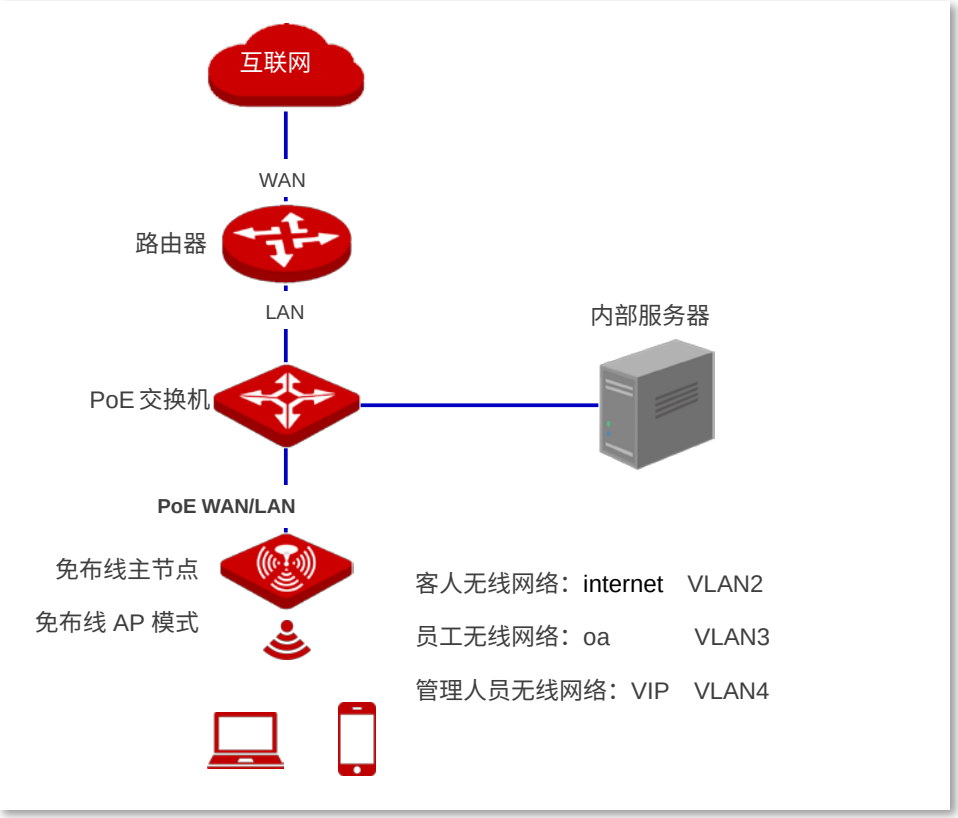
- 酒店客人接入无线网络后，只能访问互联网。
- 酒店员工接入无线网络后，只能访问酒店内网。
- 酒店管理人员接入无线网络后，既能访问互联网，也能访问酒店内网。

方案设计

为客人、员工、管理人员分配不同的无线网络，并划分 VLAN，使所有用户均获得自身对应的访问权限。

假设：

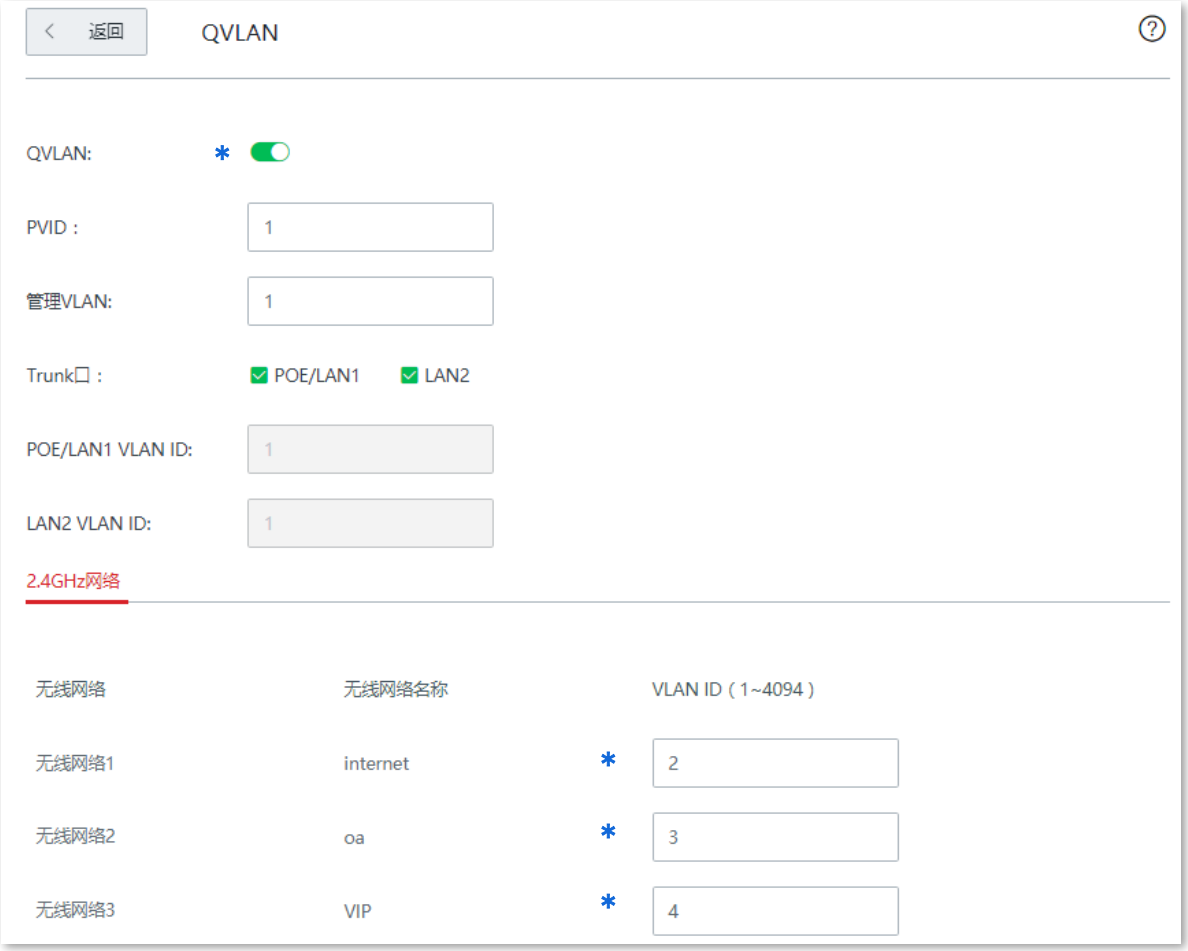
- 使用 2.4GHz 频段部署无线网络。
- 客人无线网络为“internet”，属于 VLAN 2。
- 员工无线网络为“oa”，属于 VLAN 3。
- 管理人员无线网络为“VIP”，属于 VLAN 4。



配置步骤

一、配置免布线设备

1. 登录到免布线设备的 Web 管理页面，点击「更多设置」>「QVLAN」进入设置页面。
2. 点击“QVLAN”滑块至 。
3. 修改 2.4GHz 频段各无线网络的 VLAN ID，其中，internet 的 VLAN ID 为“2”，oa 的 VLAN ID 为“3”，VIP 的 VLAN ID 为“4”。
4. 点击 保存 。



二、配置交换机

在交换机上划分 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
免布线主节点	1,2,3,4	Trunk	1
内部服务器	3,4	Trunk	1

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
路由器	2,4	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、配置路由器和内部服务器

为保证接入到免布线设备的无线客户端能正常上网，路由器和内部服务器需要支持并进行 QVLAN 配置。具体如下。

路由器：

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
交换机	2,4	Trunk	1

内部服务器：

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
交换机	3,4	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

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；连接到“VIP”的用户既能访问互联网也能访问酒店内网。

4.5 系统维护

4.5.1 重启

当您设置的某项参数不能正常生效时，可以尝试重启免布线设备解决问题。

进入页面：点击「系统维护」>「重启」。

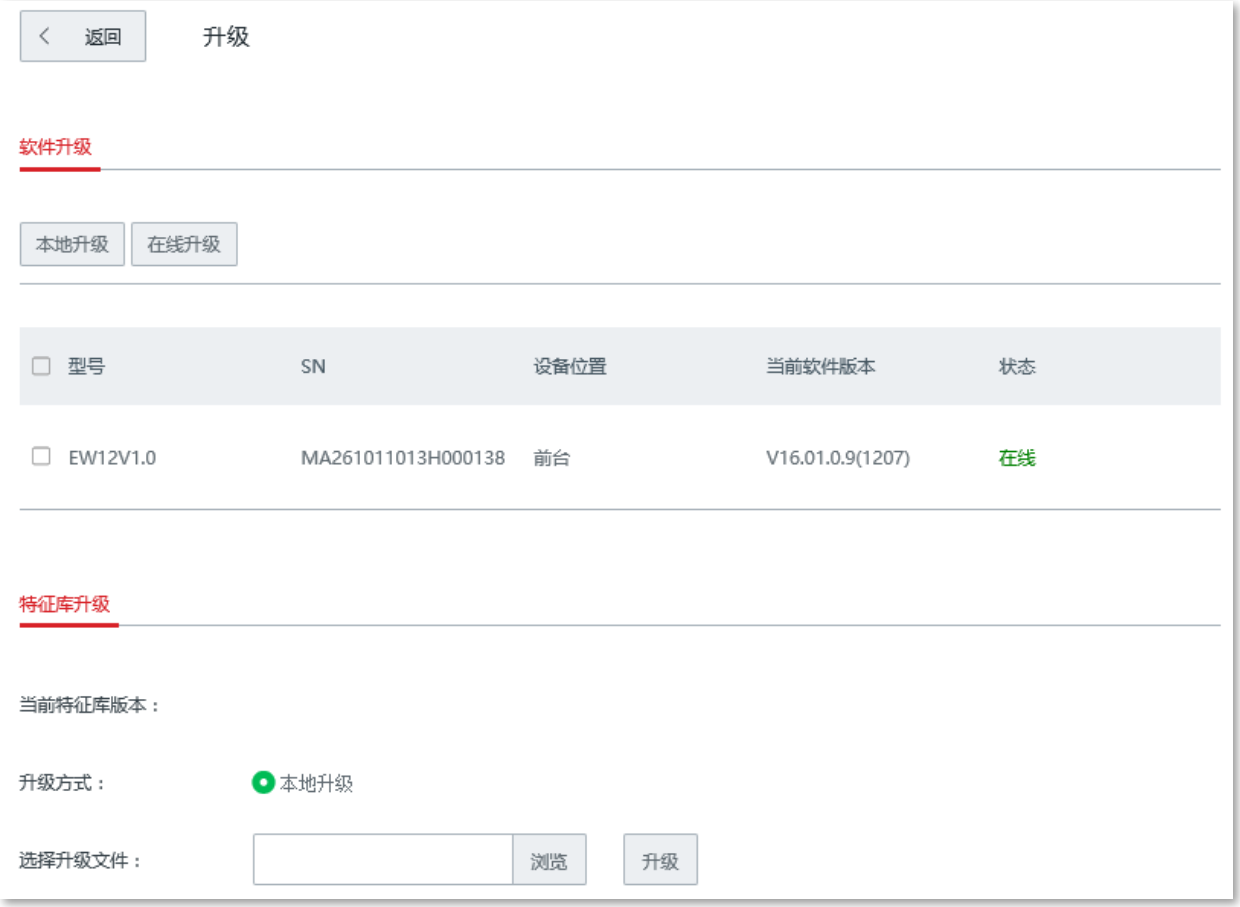
4.5.2 升级

概述

进入页面：点击「系统维护」>「升级」。

在这里，您可以对免布线设备进行软件升级和特征库升级。

- 软件升级：通过升级软件，可以体验更多功能，获得更好的用户体验。本设备支持“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：更新免布线设备行为管理模块的 URL 特征库。升级特征库不会对本设备的软件产生影响。本设备暂仅支持“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。

标题项	说明
在线升级	仅“软件升级”支持。需设备已联网。 方法：勾选要进行在线升级的设备，然后点击 在线升级 ，系统将自动下载升级文件，并进行升级。

软件本地升级

注意

为了确保升级正确，避免免布线设备损坏，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，不要断开免布线设备电源。

1. 访问 IP-COM 官网 www.ip-com.com.cn，下载对应型号的免布线设备升级软件到本地电脑并解压。
2. 登录免布线设备 Web 管理页面，进入「系统维护」>「升级」页面，找到“软件升级”模块。
3. 选择待升级的免布线设备，点击 本地升级 。
4. 点击 浏览 选择升级文件，然后点击 升级 。

提示

不同浏览器的文件加载按钮会有所不同，具体请以实际使用的浏览器为准。此处以 IE 浏览器为例。

----完成

等待进度条走完。之后，您可重新登录免布线设备，在“软件升级”或“系统状态”页面查看设备当前的软件版本号来确认是否升级成功。

提示

为了更好地体验高版本软件的稳定性及增值功能，升级完成后，建议将免布线设备恢复出厂设置，然后重新配置。

特征库本地升级

注意

为了确保升级正确，避免免布线设备损坏，请：

- 使用正确的升级文件进行升级。一般情况下，特征库升级文件的文件后缀为.cfg。
- 升级过程中，不要断开免布线设备电源。

1. 访问 IP-COM 官方网站 www.ip-com.com.cn，下载对应型号的免布线设备最新的特征库文件并存放到本地电脑。
2. 登录免布线设备的 Web 管理页面，进入「系统维护」>「升级」页面，找到“特征库升级”模块。
3. 点击 浏览 选择升级文件，然后点击 升级 。

提示

不同浏览器的文件加载按钮会有所不同，具体请以实际使用的浏览器为准。此处以 IE 浏览器为例。

----完成

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

4.5.3 复位

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；或您需要登录免布线设备的管理页面，但是却忘记登录密码时，可以将免布线设备复位后重新设置。

免布线设备支持软件复位和硬件复位两种方式。

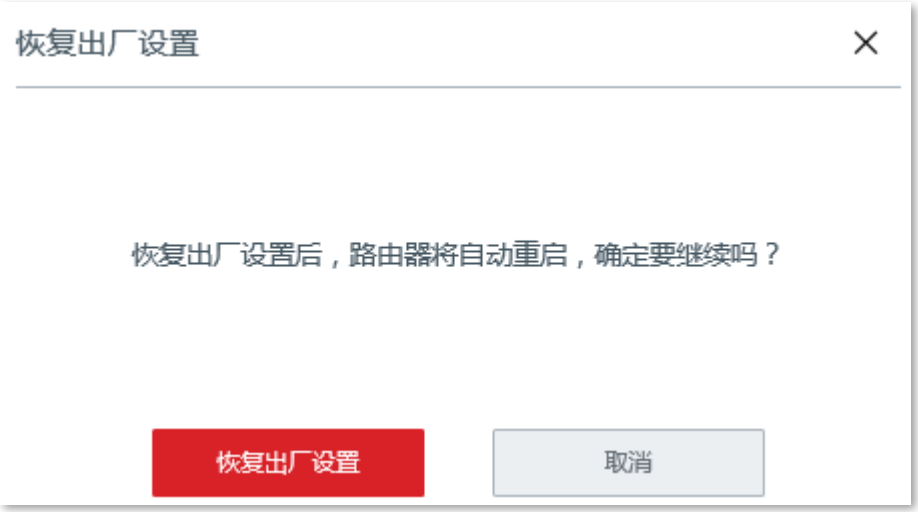
复位后，免布线设备的默认 LAN 口 IP 地址为 192.168.5.1。

注意

- 复位后，免布线设备的所有设置将会恢复到出厂状态，您需要重新设置免布线设备才能上网。请谨慎使用复位操作。
- 为避免损坏免布线设备，复位过程中，请确保该设备供电正常。

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 。



硬件复位

使用此方式时，您无需进入免布线设备管理页面就可以将其复位。操作方法如下：

免布线设备系统已启动的状态下（SYS 灯闪烁），用尖状物按住复位按钮（RESET）约 8 秒，当 SYS 灯长亮时松开，设备将会恢复出厂设置。当 SYS 灯重新闪烁时，恢复出厂设置完成。

4.5.4 密码管理

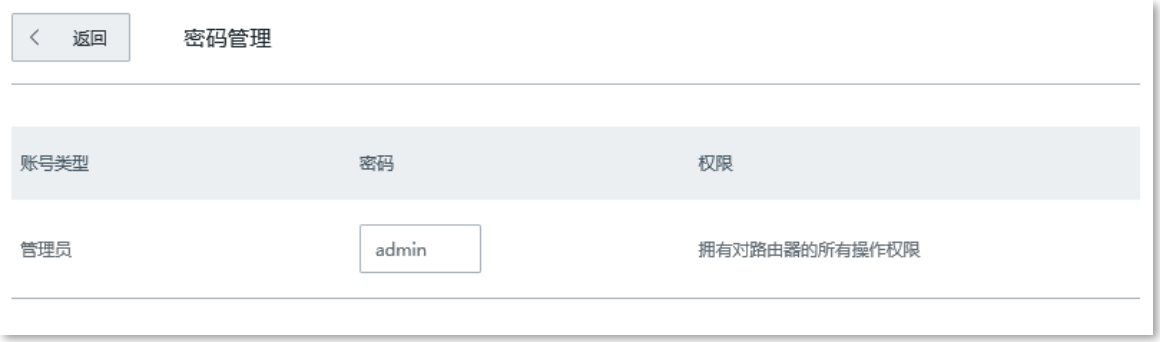
概述

进入页面：点击「系统维护」>「密码管理」。

在这里，您可以修改免布线设备的管理员密码。首次使用免布线设备时，需要设置管理员密码。

修改登录密码

在「系统维护」>「密码管理」页面，在对应账号类型的密码输入框中修改登录密码，然后点击页面底端的 保存 。



保存修改后，页面将会跳转到登录页面，输入刚才设置的密码可以重新登录到免布线设备的管理页面。

4.5.5 自定义重启

概述

进入页面：点击「系统维护」>「定时重启」。

在这里，您可以设置免布线设备周期性地定时自动重启，预防免布线设备长时间运行导致其出现性能下降、不稳定等现象。

自定义重启支持两种方式：循环重启、定时重启。

- 循环重启：免布线设备每隔指定的间隔时间就自动重启一次。
- 定时重启：免布线设备在指定的日期和时间自动重启。

设置设备循环重启

1. 点击「系统维护」>「自定义重启」。
2. 点击滑块至。
3. 选择“维护方式”为“循环重启”。
4. 设置自动重启的间隔时间。
5. 点击页面底端的 保存 。

----完成

设置完成后，每间隔指定的重复时间，免布线设备即自动重启一次。

设置设备定时重启

提示

定时重启时间以免布线设备的系统时间为准，为避免重启时间出错，请确保免布线设备的系统时间准确。

1. 点击「系统维护」>「定时重启」。
2. 点击滑块至。
3. 选择免布线设备自动重启的时间点，如“凌晨 3 点”。
4. 设置自动重启的日期，如“每天”。
5. 点击页面底端的 保存 。

----完成

如上图设置完成后，每天的凌晨 3 点，免布线设备将自动重启。

4.5.6 备份与恢复

概述

进入页面：点击「系统维护」>「备份与恢复」。

使用备份功能，可以将免布线设备当前的配置信息保存到本地电脑；使用恢复功能，可以将免布线设备的配置还原到之前备份的配置。

如，当您对免布线设备进行了大量的配置，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。当您对免布线设备进行了升级、复位等操作后，可以恢复免布线设备原有的配置文件。

备份配置

1. 点击「系统维护」>「备份与恢复」。
2. 点击 备份 ，之后按页面提示选择备份文件的存储路径。

----完成

浏览器将下载文件名为 RouterCfm.cfg 的配置文件。

恢复配置

1. 点击「系统维护」>「备份与恢复」。
2. 点击 浏览 选择之前备份的配置文件，然后点击 恢复 。

提示

不同浏览器的文件加载按钮会有所不同，具体请以实际使用的浏览器为准。此处以 IE 浏览器为例。

----完成

页面出现重启进度提示，请耐心等待。免布线设备重启后配置恢复完成。

4.5.7 系统日志

进入页面：点击「系统维护」>「系统日志」。

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

日志记录时间以免布线设备的系统时间为准，为确保日志记录时间准确，请先准确设置免布线设备的系统时间。

注意

- 免布线设备仅记录其最近一次启动后的事件信息。
- 断电后重新通电、软件升级、备份/恢复设置、复位等操作都会导致免布线设备重启。

4.5.8 诊断工具

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：用于检测数据包从本设备到目标主机所经过的路由。

执行 Ping

假设要检测免布线设备到百度服务器的链路是否畅通。

设置步骤：

1. 点击「系统维护」>「诊断工具」。
2. 选择“诊断工具”为“Ping”。
3. 输入目的 IP 地址或域名，本例为“www.baidu.com”。
4. 设置 ping 发送的数据包的个数，建议保持默认设置。
5. 设置 ping 发送的数据包的大小，建议保持默认设置。
6. 点击 开始 。

   ----完成

稍后，诊断结果将显示在页面下方。如下图示。

执行 Traceroute

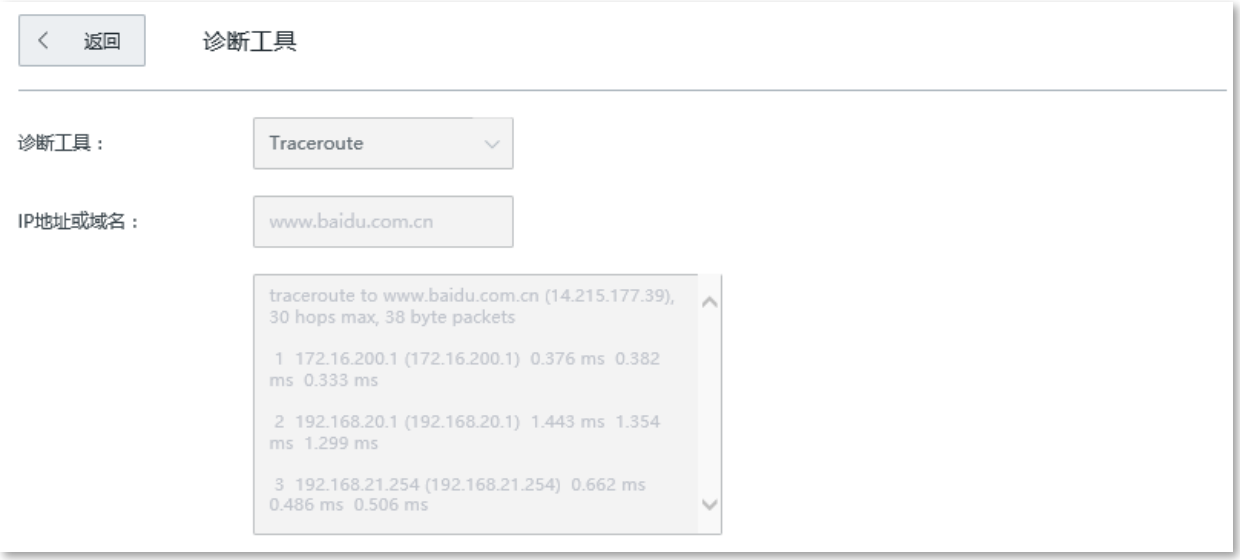
假设要检测免布线设备到百度服务器所经过的路由。

设置步骤：

1. 点击「系统维护」>「诊断工具」。
2. 选择“诊断工具”为“Traceroute”。
3. 输入目的 IP 地址或域名，本例为“www.baidu.com”。
4. 点击 开始 。

----完成

稍后，诊断结果将显示在页面下方。如下图示例。


返回
诊断工具
诊断工具：
Traceroute
IP地址或域名：
www.baidu.com.cn
traceroute to www.baidu.com.cn (14.215.177.39), 30 hops max, 38 byte packets
1 172.16.200.1 (172.16.200.1) 0.376 ms 0.382 ms 0.333 ms
2 192.168.20.1 (192.168.20.1) 1.443 ms 1.354 ms 1.299 ms
3 192.168.21.254 (192.168.21.254) 0.662 ms 0.486 ms 0.506 ms

4.5.9 系统时间

为了保证免布线设备基于时间的功能正常生效，需要确保免布线设备的系统时间准确。免布线设备支持网络校时和手动设置两种时间设置方式，默认为“网络校时”。

进入页面：点击「系统维护」>「系统时间」。

网络校时

使用此方式时，系统时间自动同步互联网上的时间服务器。只要免布线设备成功连接至互联网就能自动校准其系统时间。

设置完成后，您可以进入系统状态页面查看免布线设备的系统时间是否校对准确。

参数说明

标题项	说明
系统时间	选择系统时间的设置方式，支持网络校时和手动设置。
校时周期	免布线设备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	选择免布线设备当前所在地区的标准时区。

手动设置

手动设置免布线设备的系统时间。使用此方式时，免布线设备每次重启后，您都需要重新设置系统时间。选择“手动设置”时，页面展开的相关参数如下图所示。

参数说明

标题项	说明
系统时间	选择系统时间的设置方式，支持网络校时和手动设置。
日期	可以直接在此处输入正确的时间，也可以点击 复制管理主机时间 将正在管理免布线设备的电脑的时间同步到免布线设备。
时间	

设置完成后，您可以进入系统状态页面，查看免布线设备的系统时间是否校对准确。

附录

默认参数

参数		默认设置
设备登录	管理域名	www.ipcwifi.com
	管理 IP 地址	192.168.5.1
	登录密码	无
工作模式		免布线路由模式
Mesh 组网方式		无线组网
LAN 口设置	IP 地址	192.168.5.1
	子网掩码	255.255.255.0
DHCP 服务器	DHCP 服务器	开启
	起始 IP 地址	192.168.5.100
	结束 IP 地址	192.168.5.200
	租约时间	30 分钟
	首选 DNS	192.168.5.1
无线设置	主无线网络	开启主无线网络 2.4/5GHz 无线名称一致 无线名称：IP-COM_XXXXXX。其中，XXXXXX 为免布线设备 LAN 口 MAC 后六位 无线密码：不设密码
	访客网络	关闭

参数	默认设置
节点管理	开启
系统时间	网络校时

缩略语

缩略语	全称
AES	高级加密标准（Advanced Encryption Standard）
AH	鉴别首部 Authentication Header）
AP	无线接入点（Access Point）
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）
DMZ	非军事化区（Demilitarized Zone）
DNS	域名系统（Domain Name System）
DPD	失效对等体检测（Dead Peer Detection）
ERP	企业资源计划（Enterprise Resource Planning）
FQDN	完全合格域名（Fully Qualified Domain Name）
FTP	文件传输协议（File Transfer Protocol）
GI	保护间隔（Guard Interval）
ESP	封装安全载荷（Encapsulating Security Payload）
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）
IPsec	互联网安全协议（Internet Protocol Security）

缩略语	全称
ISP	互联网服务提供商（Internet Service Provider）
ISAKMP	Internet安全联盟密钥管理协议（Internet Security Association Key Management Protocol）
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）
MTU	最大传输单元（Maximum Transmission Unit）
NAT	网络地址转换（Network Address Translation）
OA	办公自动化（Office Automation）
ID	身份标识号码（Identity Document）
PFS	完善的前向安全性（Perfect Forward Secrecy）
PoE	以太网供电（Power over Ethernet）
POP	邮局协议（Post Office Protocol）
PPP	点对点协议（Point to Point Protocol）
PPTP	点对点隧道协议（Point to Point Tunneling Protocol）
PSK	预共享密钥（Preshared Key）
PVID	端口的虚拟局域网标识号（Port-base VLAN ID）
QAM	正交幅度调制（Quadrature Amplitude Modulation）
SA	安全联盟（Security Association）
SHA	安全散列算法（Secure Hash Algorithm）
SMTP	简单邮件传输协议(Simple Mail Transfer Protocol)
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）
SYN	同步序列编号（Synchronize Sequence Numbers）
TCP	传输控制协议（Transmission Control Protocol）

缩略语	全称
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）
VID	虚拟局域网标识号（VLAN Identity Document）
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）
WLAN	无线局域网（Wireless Local Area Network）
WMM	无线多媒体（Wi-Fi multi-media）