TP-LINK®

多业务无线控制器

用户手册

1910041056 REV1.0.0

声明

目录

第1章　用户手册简介

本手册第 3~7 章详细介绍如何通过 NMS 平台管理网络，第 8~18 章详细介绍如何配置 AC。请在操作前仔细阅读本手册。

1.1　目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

本书约定

在本手册中，

- 所提到的“AC”、“本产品”等名词，如无特别说明，系指 TP-LINK 多业务无线控制器。
- 全文如无特殊说明，Web 界面以 TL-NAC300-NMS 机型为例。
- 用 >> 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 三级菜单**，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字，表示 Web 界面的按钮名称，如<确定>。
- 正文中出现的“”双引号标记文字，表示 Web 界面出现的除按钮外名词，如“系统升级”界面。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

1.2 产品简介

普联技术有限公司全新开发推出的 TP-LINK 多业务无线控制器，是针对企业级用户推出的具有本地小型局域网集中配置、管理和状态监控、并集成有线设备统一管理的无线控制器产品。在传统无线控制器功能基础上进行了升级，可以统一管理 TP-LINK 所有无线 AP 产品，支持 AP 自动发现、AP 状态查看、AP 统一配置、无线 MAC 地址过滤、AP 软件统一升级等传统无线控制业务；

同时支持网络拓扑、无线智能漫游、连通性诊断、远程故障诊断等整网管理和运维功能，提供高性能、高可靠性、易安装、易维护的高品质无线控制业务。并且增加了集中管理平台的部署方式，简化了用户本地部署的流程及操作。

本手册适用如下型号产品：

产品型号	硬件版本
TL-NAC300-NMS	1.0

第2章　设备初始化

本章介绍如何通过本地 web 界面，商用网络云平台管理 AC。

2.1　通过本地 WEB 管理多功能无线控制器

2.1.1 登录准备

可在机身底部的标贴上查找本产品的 IP，本产品的 IP 为 192.168.1.251/24，第一次登录时，需要确认以下几点：

1. AC 已正常加电启动，任一端口已与管理主机相连。
2. 管理主机已至少安装一种以下浏览器：IE 8.0 或以上版本，最新版本的 FireFox、Chrome 和 Safari 浏览器。
3. 管理主机 IP 地址已设为与交换机端口同一网段，即 192.168.1.X（X 为 2 至 250 之间的任意整数），子网掩码为 255.255.255.0。
4. 为保证能更好地体验 Web 界面显示效果，建议将显示器的分辨率调整到 1024×768 或以上像素。

2.1.2 登录步骤

1. 打开 IE 浏览器，在地址栏中输入无线控制器默认管理地址 http://192.168.1.251 登录无线控制器的 Web 管理界面。

2. 设置用户名和密码，点击<确定>。

3. 再次输入无线控制器管理帐号的用户名和密码，点击<登录>。

4. 首次登录无线控制器可选择“智能开局”功能，通过智能开局，可快速添加全网设备，配置路由器 WAN 口，划分网段，配置交换机端口，并设置无线网络。

交换机设备的用户名将设置为 admin，请为其他待添加设备设置用户名和密码，以增加网络安全性。如待添加设备都已加密，请直接点击<立即开局>。

如无需智能开局功能，请点击网页右下角<跳过智能开局>。

5. 成功登录后将看到无线控制器的 Web 界面首页，如下图所示。

2.1.3 配置 AC 的 IP 地址及网关

无线控制器的默认管理地址为 192.168.1.251/24，可参考如下步骤对无线控制器进行联网配置。

1. 进入首页，点击右上角<AC 模式>，进入 AC 配置界面，AC 配置界面首页如下图所示。

2. 进入页面：网络设置 >> 接口设置，编辑 VLAN ID 为 1 的接口条目，如下图。

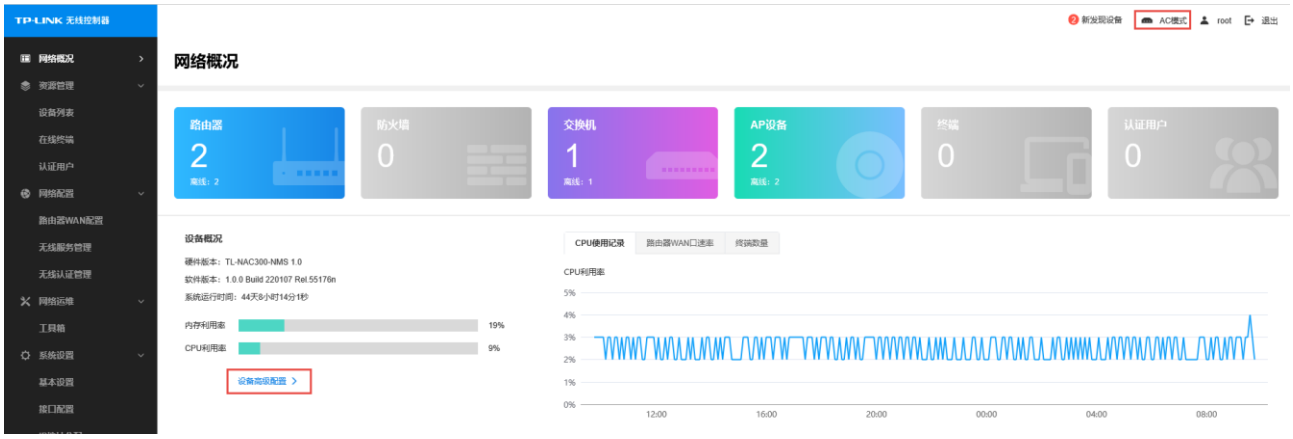
3. 进入页面：系统工具 >> 诊断工具，ping 百度或者其他外网域名，并选择配置网络的接口，如下图，点击<开始>进行网络检测，可收到 reply 数据包即表示能正常联网。

第3章　网络概况

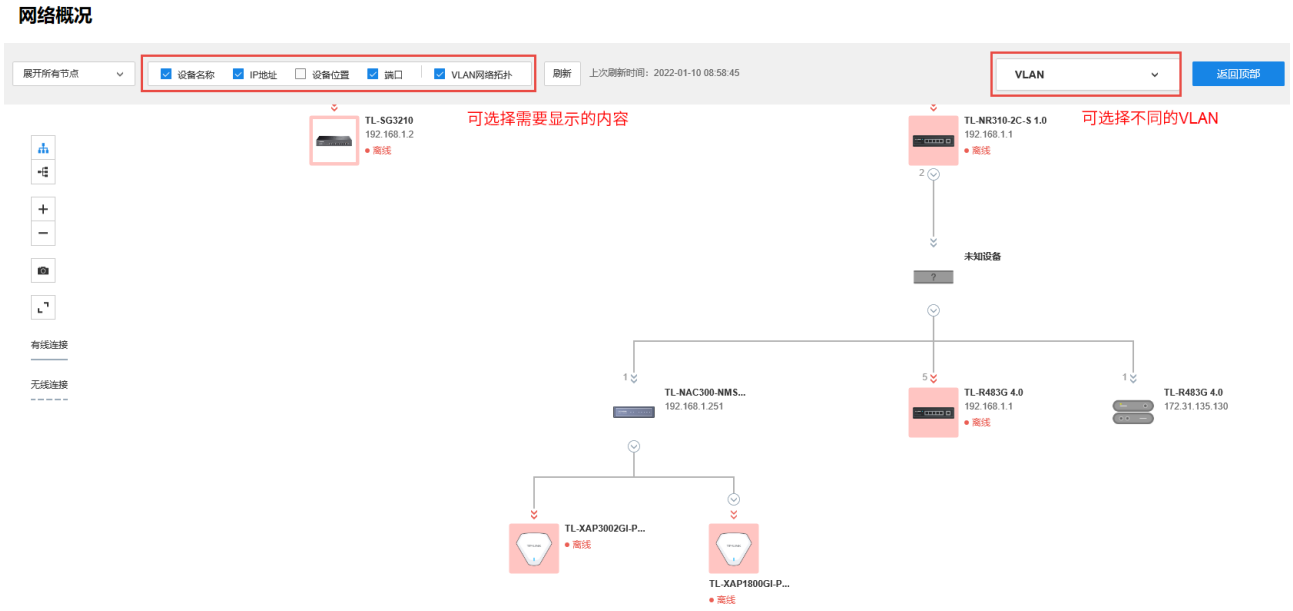
3.1　网络概况

进入无线控制器首页，可查看当前 AC 所在网络的网络概况，如下图。

点击<设备高级配置>或<AC 模式>，可进行详细的 AC 功能配置，AC 详细功能配置见第 8~18 章。



如下界面可查看当前的网络拓扑图。



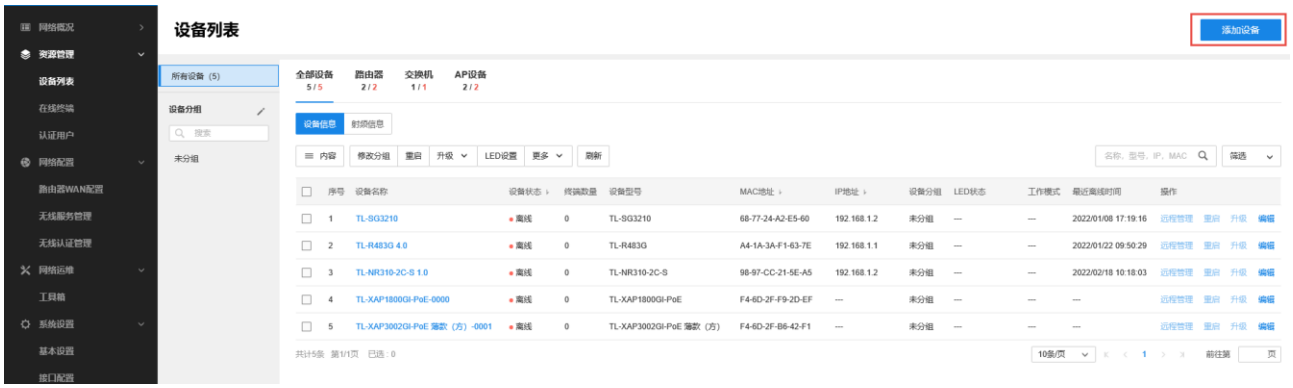
第4章　资源管理

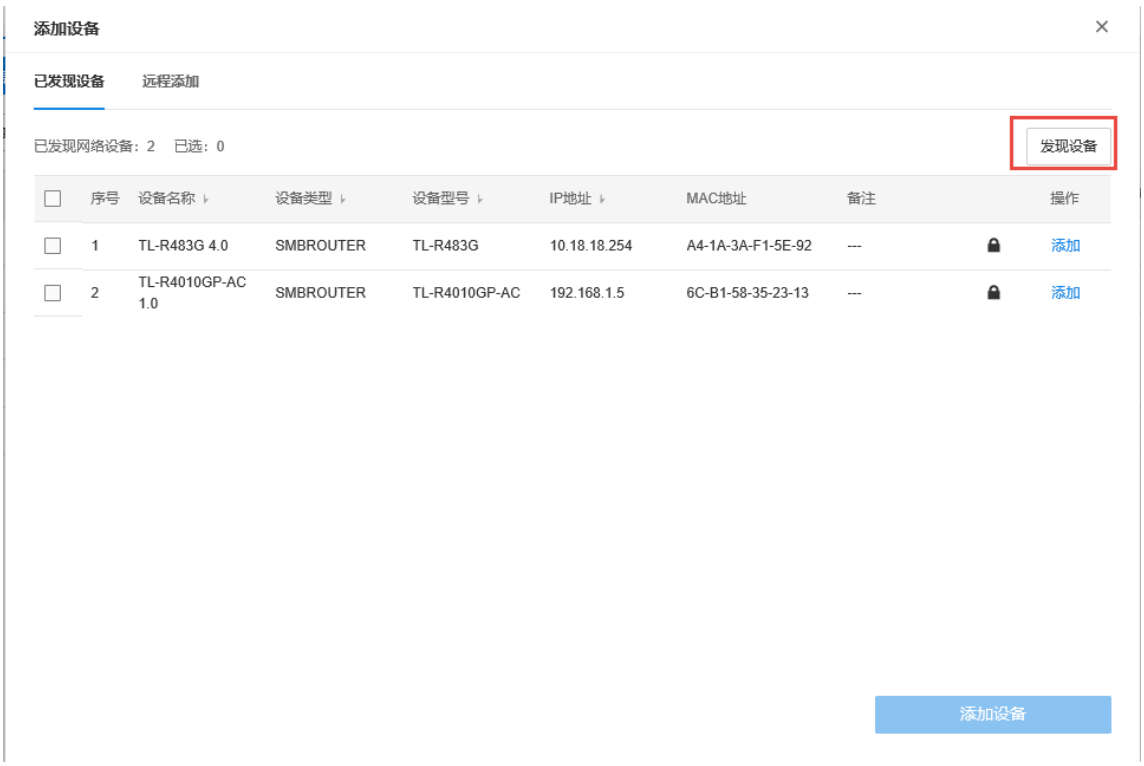
4.1　设备列表

进入页面：资源管理 >> 设备列表，可查看多功能无线控制器当前所连接的设备信息。

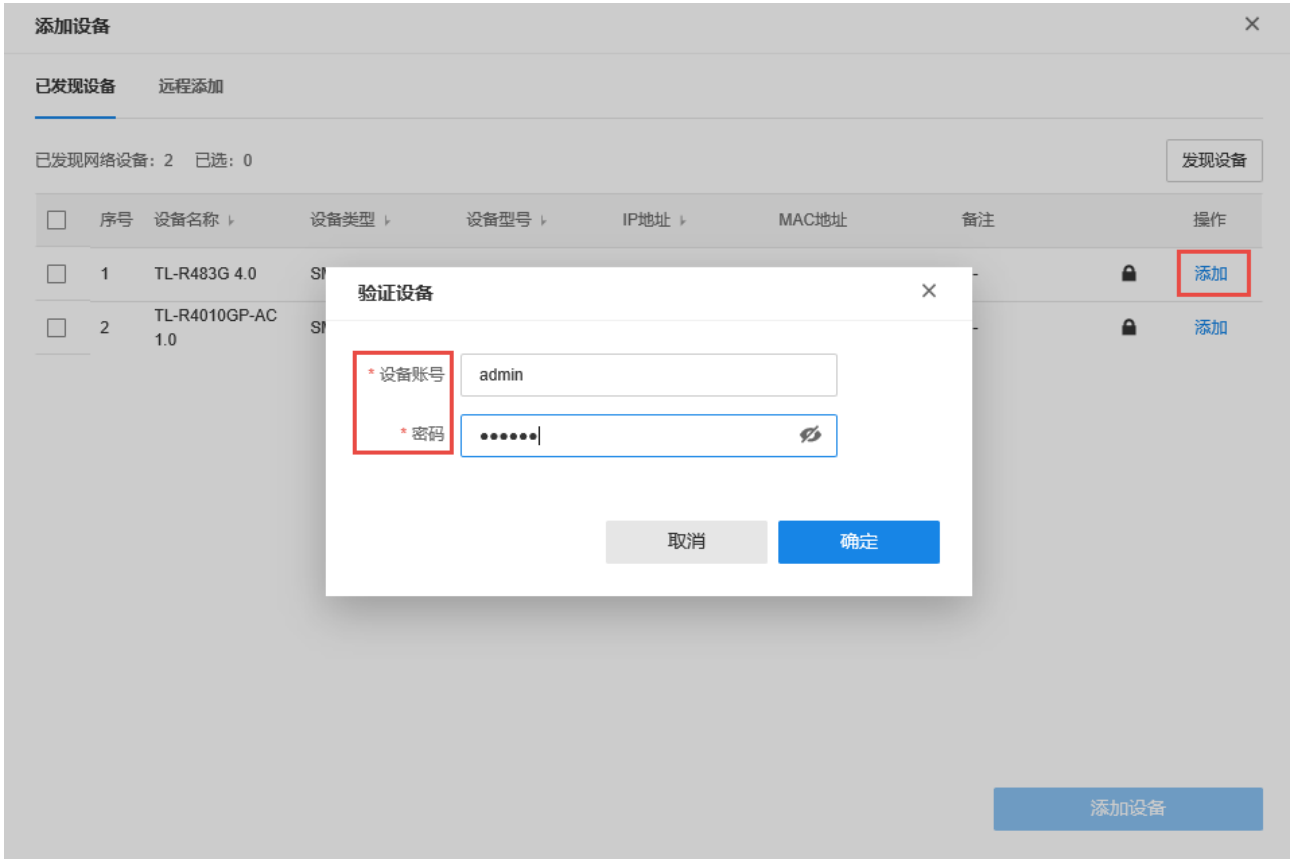
4.1.1 添加设备

进入页面：资源管理 >> 设备列表，点击<添加设备>，无线控制器可自动发现网络中的已连接设备，本产品支持添加路由器、交换机、AP 设备。





点击<添加>，输入需要添加设备的用户名和密码，点击<确定>，即可完成添加。



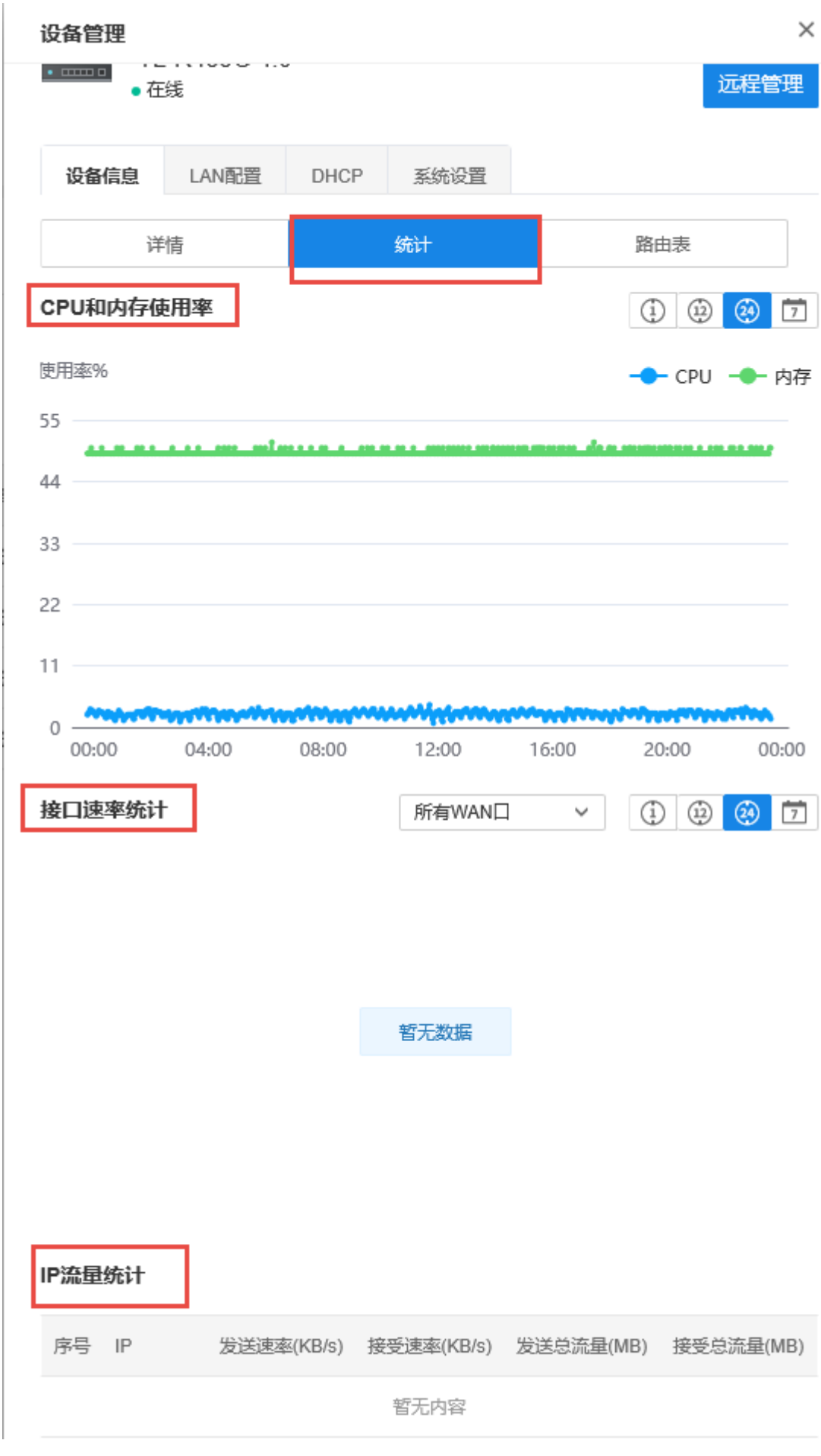
4.1.2 配置路由器

进入页面：资源管理 >> 设备列表，点击“设备名称”或<编辑>，进入路由器配置界面。

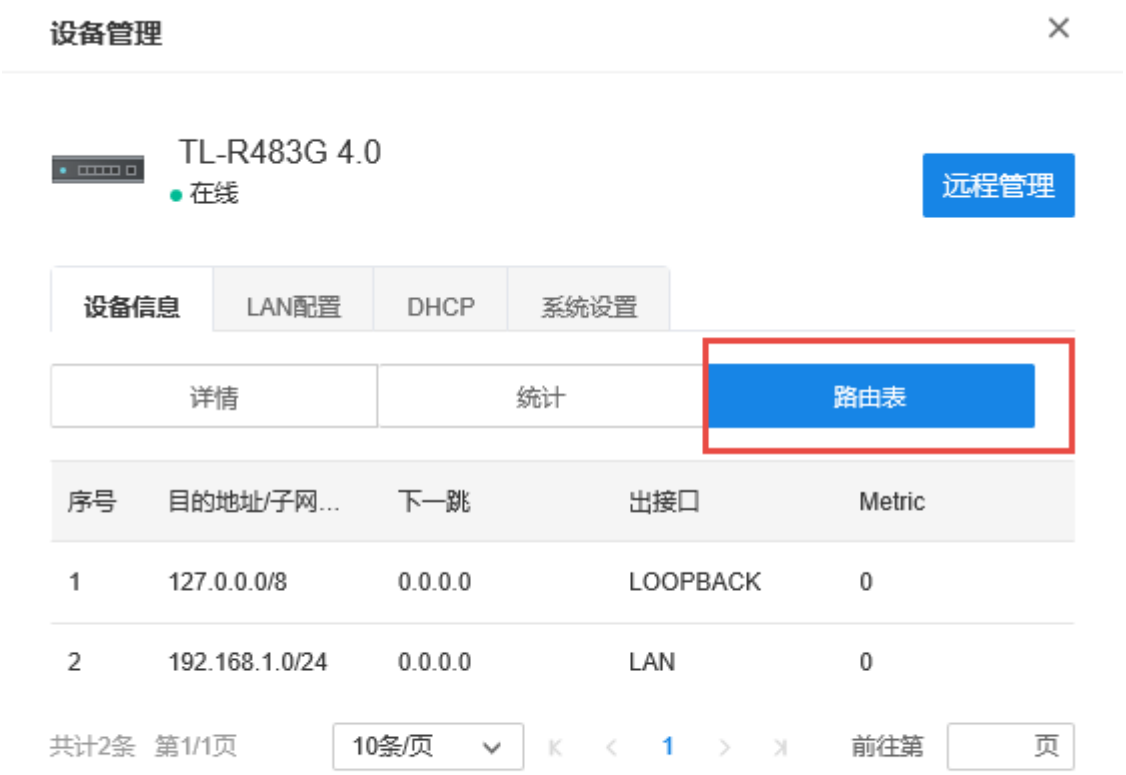
➢ 设备信息

如下界面可编辑路由器的设备名称，并备注路由器的安装位置。

点击<统计>，可查看路由器的“CPU 和内存使用率”，“接口速率统计”，“IP 流量统计”信息。


设备管理
在线
远程管理
设备信息
LAN配置
DHCP
系统设置
详情
统计
路由表
CPU和内存使用率
使用率%
CPU
内存
55
44
33
22
11
0
00:00
04:00
08:00
12:00
16:00
20:00
00:00
接口速率统计
所有WAN口
暂无数据
IP流量统计
序号
IP
发送速率(KB/s)
接受速率(KB/s)
发送总流量(MB)
接受总流量(MB)
暂无内容

点击<路由表>，可查看路由器的路由表信息，包括“目的地址/子网掩码”，“下一跳”，“出接口”，“Metric”。



➢ LAN 配置

如下界面可以配置路由器的 LAN 信息，包括“IP 地址”和“子网掩码”。

➢ DHCP

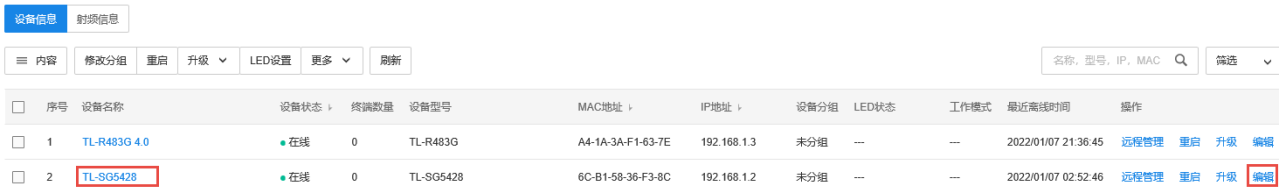
如下界面可以配置路由器的 DHCP 信息，配置“起始地址”，“结束地址”，“地址租期”等参数。具体配置方法可查看相关路由器配置指南。

➢ 系统设置

如下界面可查看路由器的软硬件版本，对路由器进行本地或在线升级，设置备份与导入，对路由器进行重启。

4.1.3 配置交换机

进入页面：资源管理 >> 设备列表，点击“设备名称”或<编辑>，进入交换机配置界面。



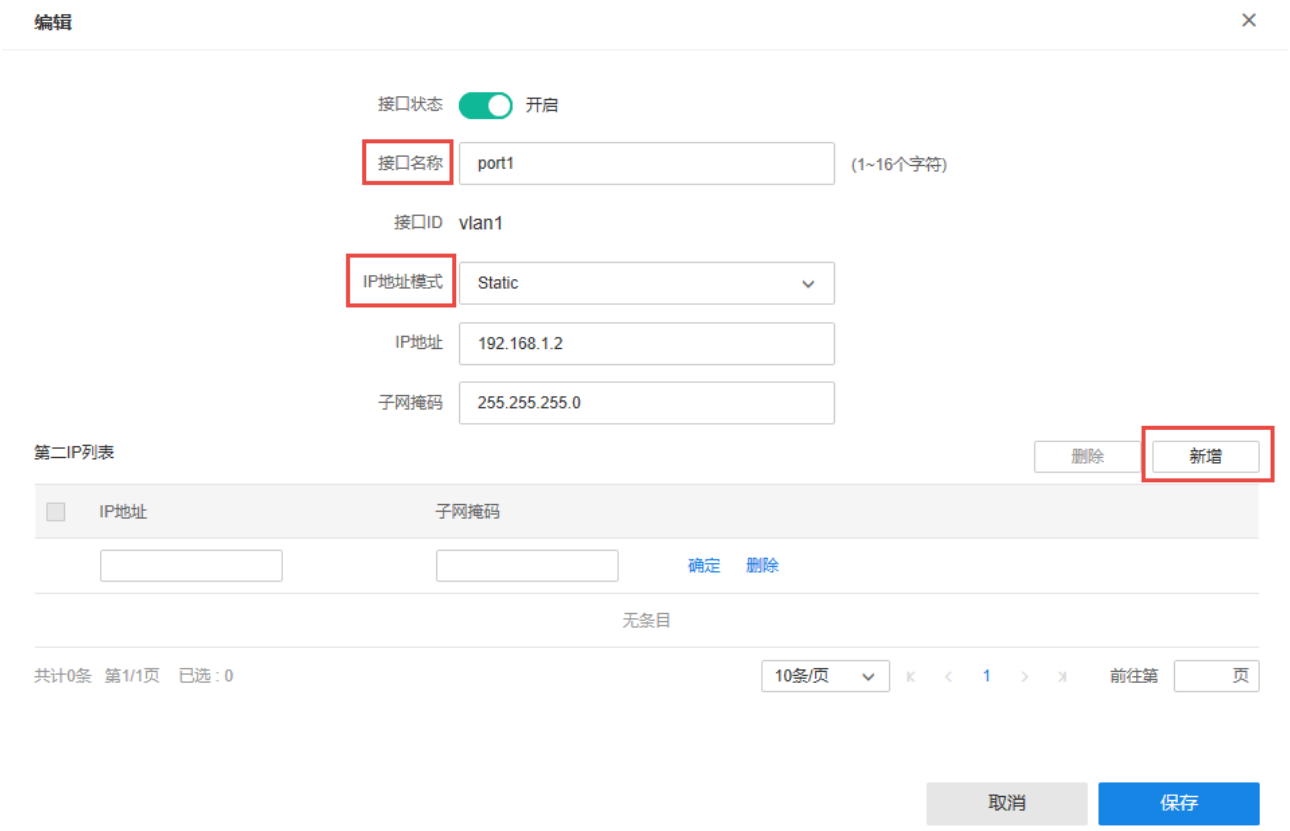
➢ 设备信息

如下界面可编辑交换机的设备名称，查看交换机的地址等信息，并备注交换机的安装位置。在端口处点击需要配置的端口，可以直接跳转的对应端口的配置界面，也可以点击“端口配置”跳转到配置界面。

➢ 接口配置

如下界面可以对交换机的接口进行配置，点击<新增>，可以新增接口，输入下图所示参数。具体配置方法可查看相关交换机配置指南。

选中指定的接口后，点击<编辑>，可以编辑接口的接口状态，接口名称，IP 地址等参数，点击<保存>即可。



➢ 端口配置

如下界面可以配置交换机的端口参数。可通过右上方的分组“unit”进行端口的筛选，选中端口后，点击左上方的<编辑>或直接点击该端口栏目下的<编辑>，即可对相应端口进行编辑操作。

设备管理

TL-SG5428

在线

远程管理

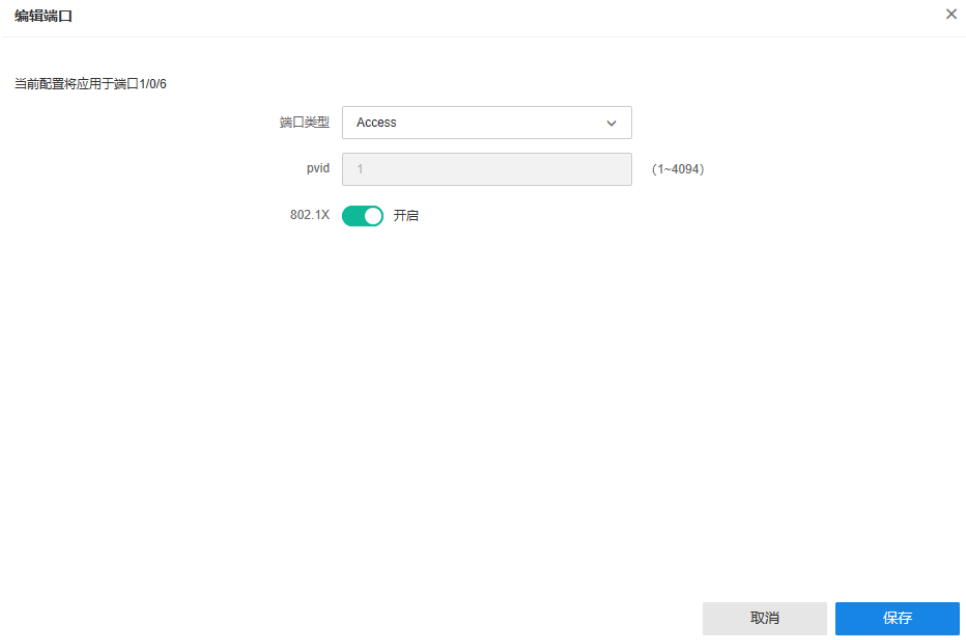
设备信息 | 接口配置 | **端口配置** | VLAN | 网络安全 | 系统设置

编辑

unit1

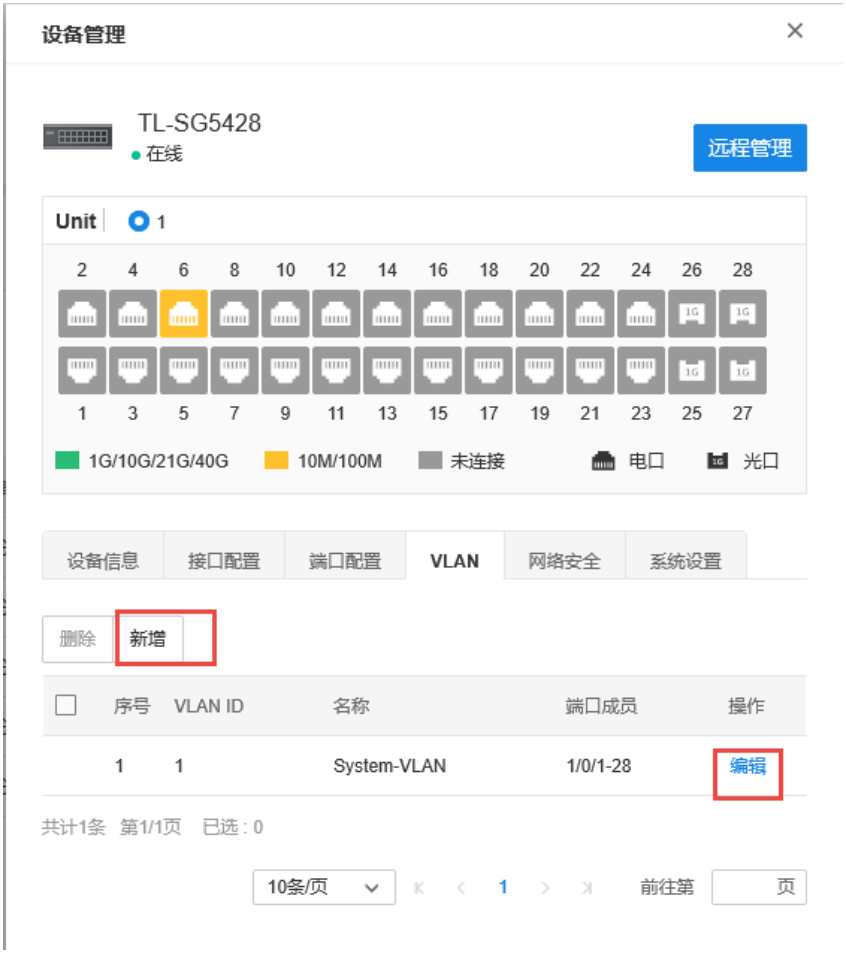
	序号	端口名称	状态	速率	双工	LAG	操作
☑	1	1/0/1	已断开	自协商	自协商	---	编辑
☐	2	1/0/2	已断开	自协商	自协商	---	编辑
☐	3	1/0/3	已断开	自协商	自协商	---	编辑
☐	4	1/0/4	已断开	自协商	自协商	---	编辑
☐	5	1/0/5	已断开	自协商	自协商	---	编辑
☐	6	1/0/6	已连接	自协商	自协商	---	编辑
☐	7	1/0/7	已断开	自协商	自协商	---	编辑
☐	8	1/0/8	已断开	自协商	自协商	---	编辑
☐	9	1/0/9	已断开	自协商	自协商	---	编辑
☐	10	1/0/10	已断开	自协商	自协商	---	编辑

共计28条 第1/3页 已选：1



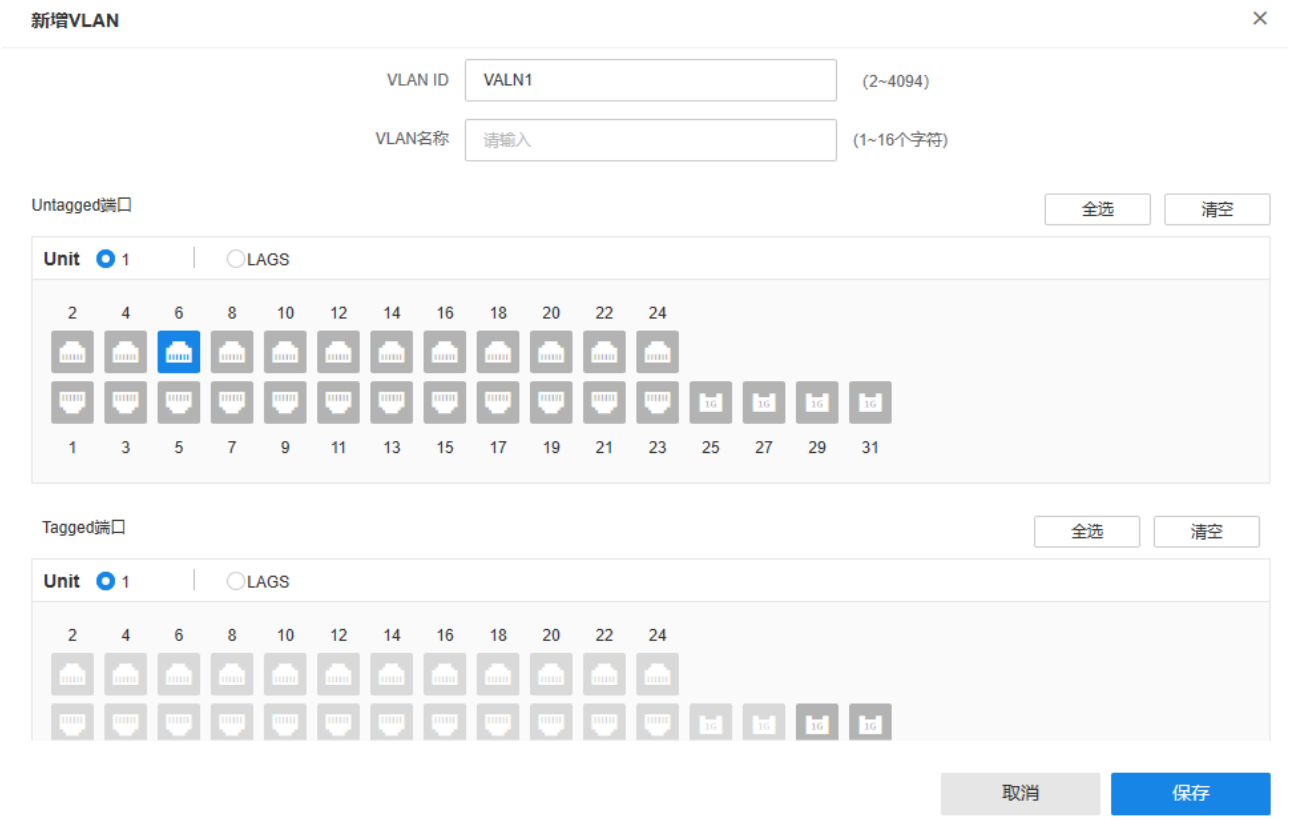
➢ VLAN

如下界面可以配置交换机的 VLAN 参数信息。



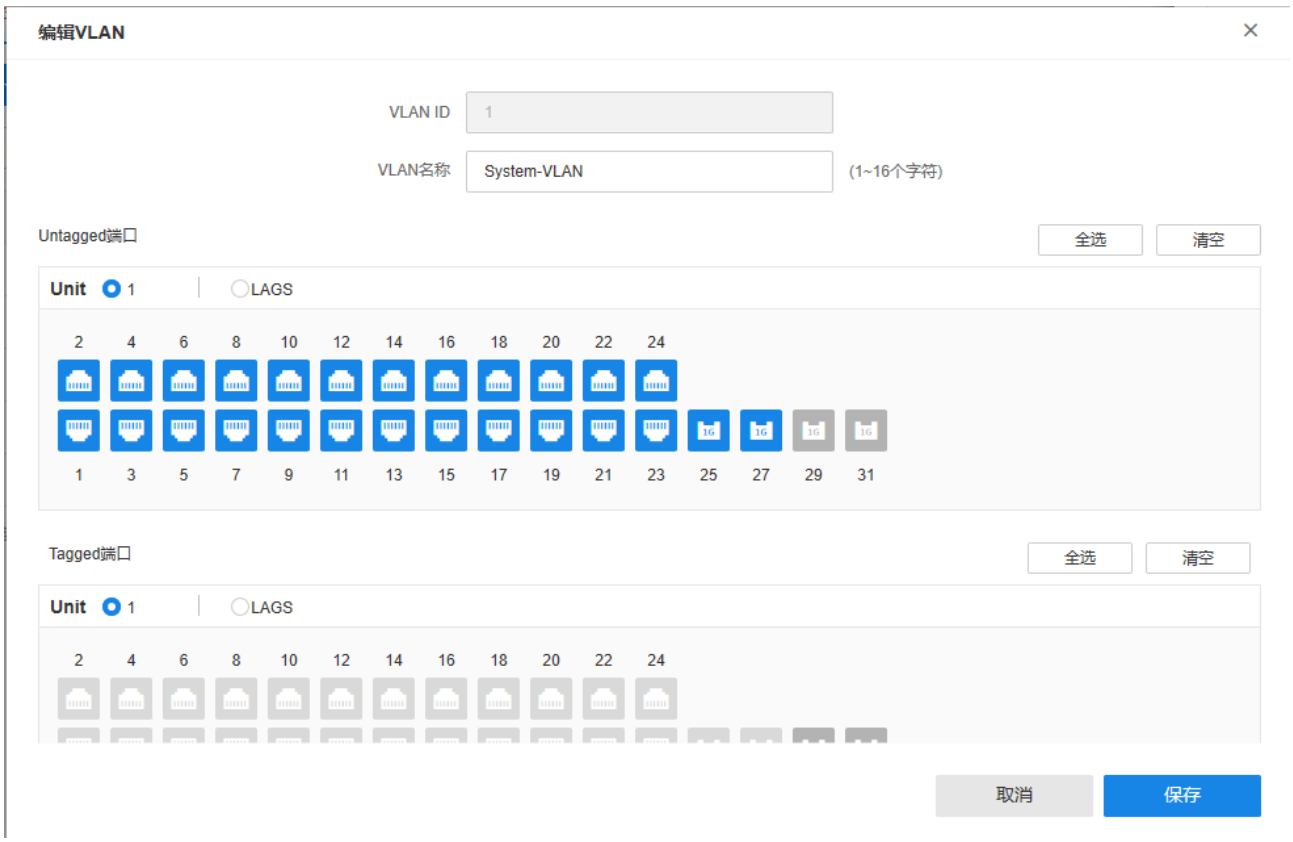
1. 新增 VLAN 条目

在“VLAN”界面下点击<新增>，即可增加 VLAN 条目，设置 VLAN ID 和 VLAN 名称，并选择需要加入该 VLAN 的端口，点击<保存>即可。



2. 编辑 VLAN 条目

在“VLAN”界面下选择需要编辑的 VLAN 条目，点击<编辑>，即可更改该 VLAN 条目的 VLAN 名称和加入的端口，设置完成后点击<保存>即可。



➢ 网络安全

如下界面可以配置交换机的安全信息，可以开启 802.1X 安全保护和 AAA 安全保护。

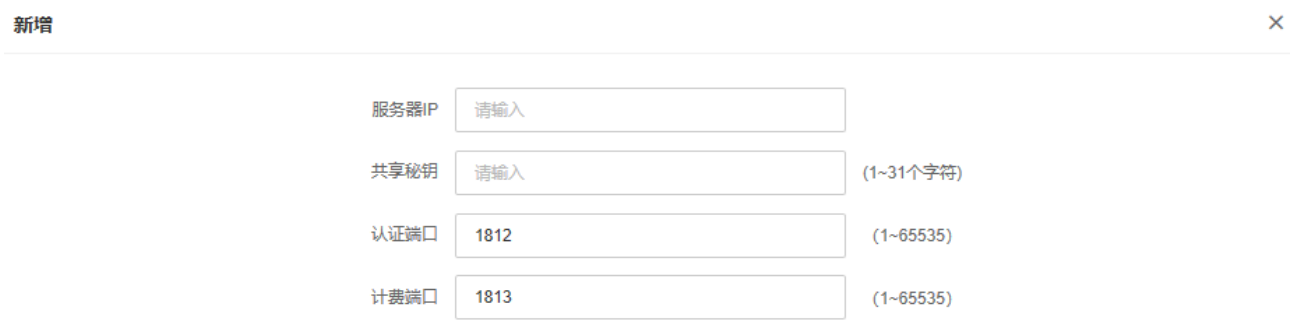
1. 开启 802.1X 安全保护

在“802.1X”界面下点击<开启>，即可开启 802.1X 安全保护。

2. AAA 安全保护

在“AAA”界面下点击<开启>，点击<新增>，输入相关配置参数，即可开启 AAA 安全保护。


设备管理
TL-SG5428
在线
远程管理
Unit 1
2 4 6 8 10 12 14 16 18 20 22 24 26 28
1 3 5 7 9 11 13 15 17 19 21 23 25 27
1G/10G/21G/40G
10M/100M
未连接
电口
光口
设备信息
接口配置
端口配置
VLAN
网络安全
系统设置
802.1X
AAA
AAA
开启
删除
编辑
新增
序号
服务器IP
共享秘钥
认证端口
计费端口
操作
无条目
共计0条 第1/1页 已选：0
10条/页
1
前往第
页



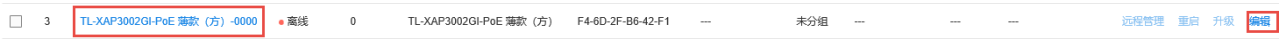
➢ 系统设置

如下界面可以配置交换机的系统信息，对交换机进行升级操作，备份与导入操作以及重启交换机。


设备管理
TL-SG5428
在线
远程管理
Unit 1
2 4 6 8 10 12 14 16 18 20 22 24 26 28
1 3 5 7 9 11 13 15 17 19 21 23 25 27
1G/10G/21G/40G
10M/100M
未连接
电口
光口
设备信息
接口配置
端口配置
VLAN
网络安全
系统设置
软件升级
当前软件版本 1.1.4 Build 20220217 Rel.109660(s)
当前硬件版本 3.0
本地升级
请选择本地文件
选取文件
升级
在线升级
在线升级
备份与导入
导出系统备份
导入本地配置
重启
立即重启

4.1.4 配置 AP 设备

进入页面：资源管理 >> 设备列表，点击“设备名称”或<编辑>，进入 AP 配置界面。



➢ 设备信息

如下界面可编辑 AP 的设备名称，备注 AP 的安装位置，并可配置 AP 的 LED 状态与 LED 开启时间。

➢ 设备管理

1. 2.4G 无线配置

如下界面可以配置 AP 的无线状态。在 2.4G 栏目下，状态选择<开启>，并填写相关参数，点击<保存>即可。具体配置方法可查看相关本配置指南第九章“AP 管理”。

点击<绑定 SSID>，在如下界面选择需要绑定或解绑的 SSID 即可。

2. 5G 无线配置

如下界面可以配置 AP 的无线状态。在 5G 栏目下，状态选择<开启>，并填写相关参数，点击<保存>即可。

其余配置操作同 2.4G。

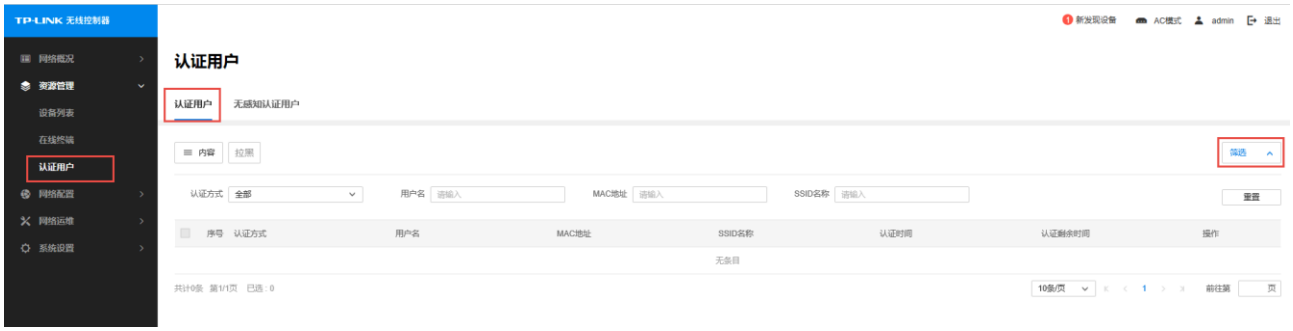
4.2 在线终端

进入页面：资源管理 >> 在线终端，可查看当前网络中在线的终端。

点击<筛选>，可选择查看当前网络中在线的终端。

4.3 认证用户

进入页面：资源管理 >> 认证用户，可查看当前网络中的认证用户。具体配置方法可查看本配置指南第十五章“认证管理”。



进入页面：资源管理 >> 认证用户 >> 无感知认证用户，可查看当前网络中的无感知认证用户。

认证用户

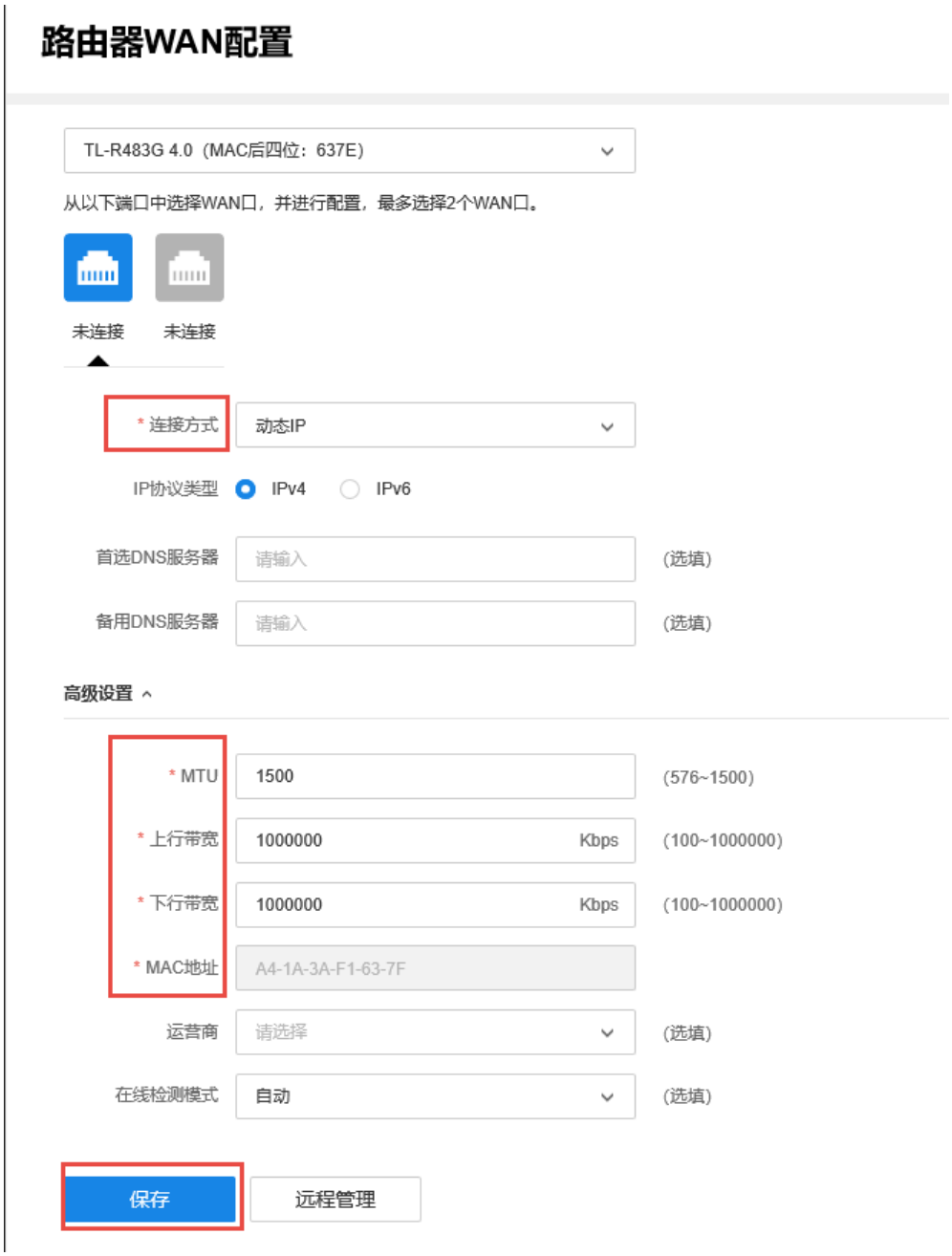

认证用户
无感知认证用户
内容
拉黑
筛选
SSID名称
请输入
MAC地址
请输入
用户名
请输入
密码
请输入
重置
序号
SSID名称
MAC地址
用户名
密码
认证时间
操作
无条目
共计0条 第1/1页 已选：0
10条/页
1
前往第
页

第5章　网络配置

5.1　路由器 WAN 配置

进入页面：网络配置 >> 路由器 WAN 配置，可对当前网络中所连接的路由器的 WAN 进行配置。

如下图所示，选定需要配置的路由器后，设置 WAN 口相关参数，点击<保存>，最多可选择 2 个 WAN 口进行配置。具体配置方法可查看相关路由器配置指南。

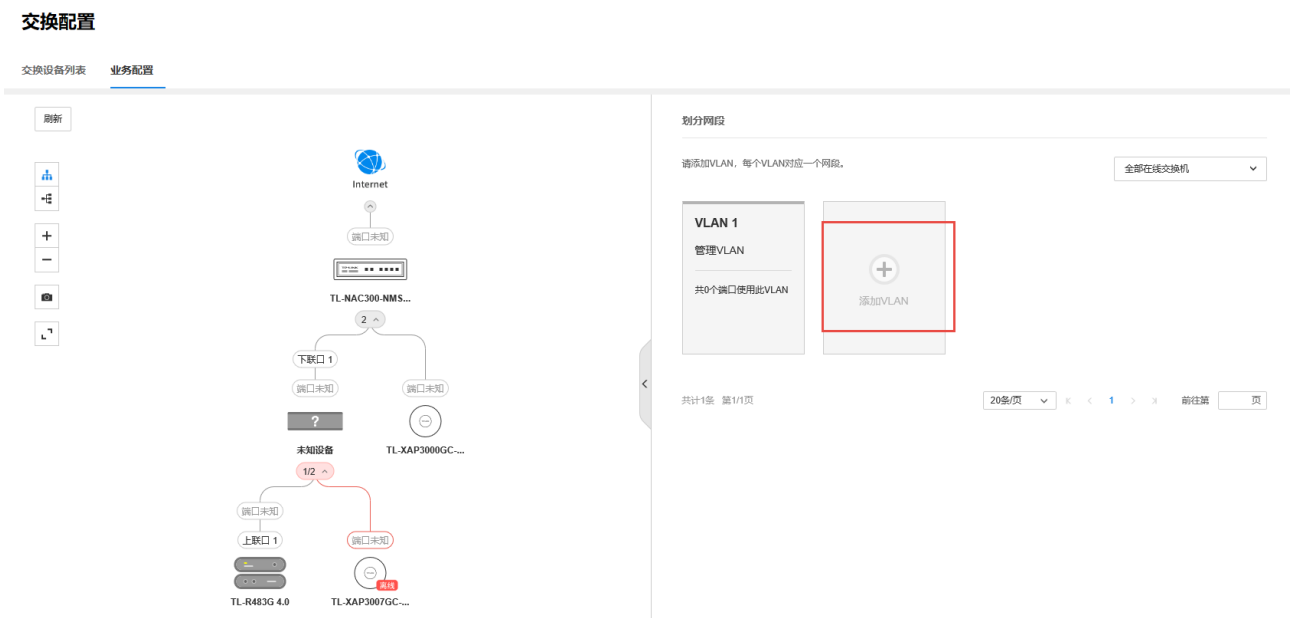


5.2 交换配置

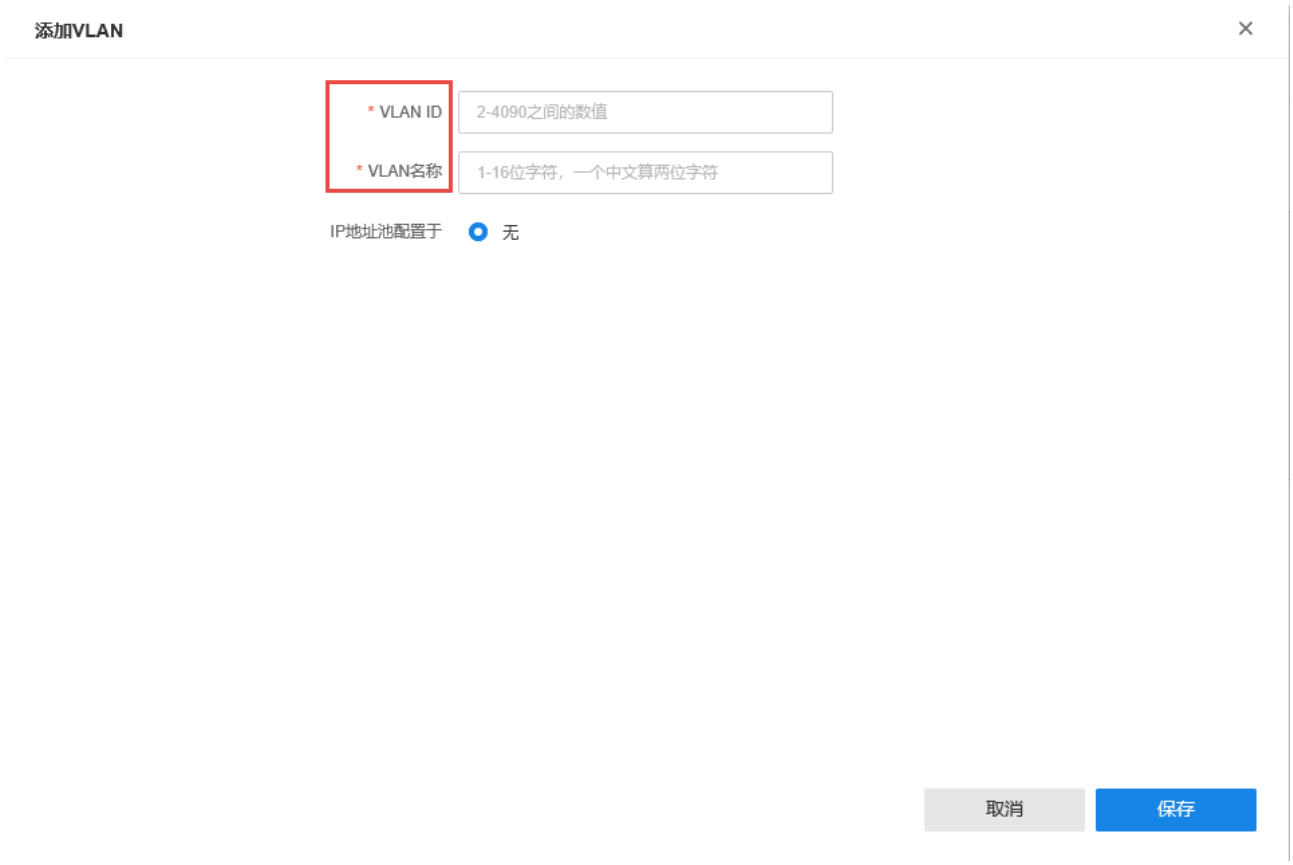
进入页面：网络配置 >> 交换配置，如下图所示，可查看交换设备列表。

5.2.1 业务配置

进入页面：网络配置 >> 交换配置 >> 业务配置，如下图所示，可查看网络拓扑图。点击拓扑中的交换机设备，可以绑定交换机的端口和 VLAN。

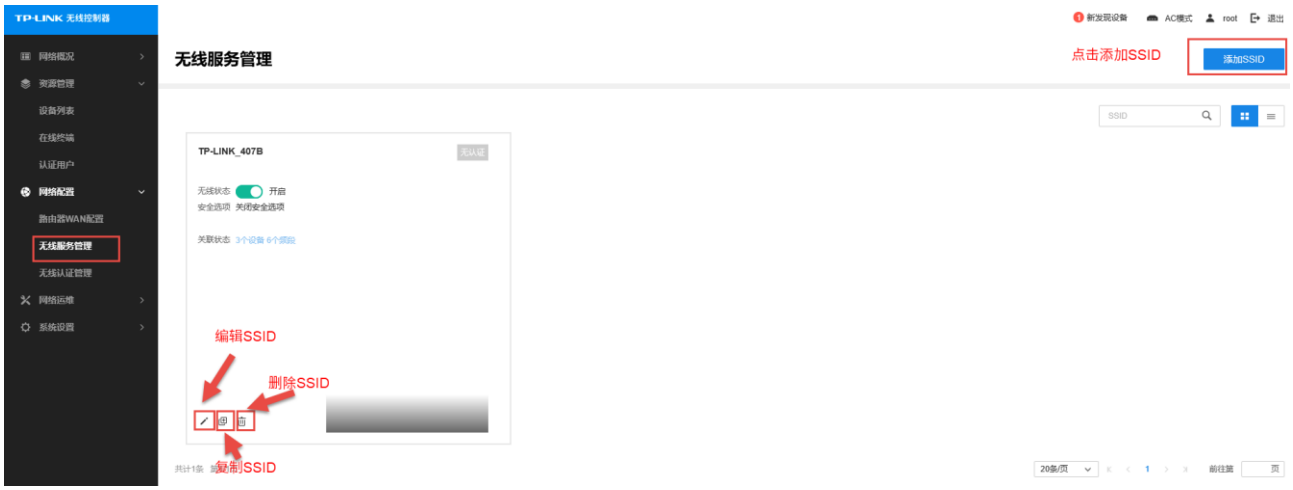


点击“添加 VLAN”，可进行网段划分，每个 VLAN 对应一个网段。



5.3 无线服务管理

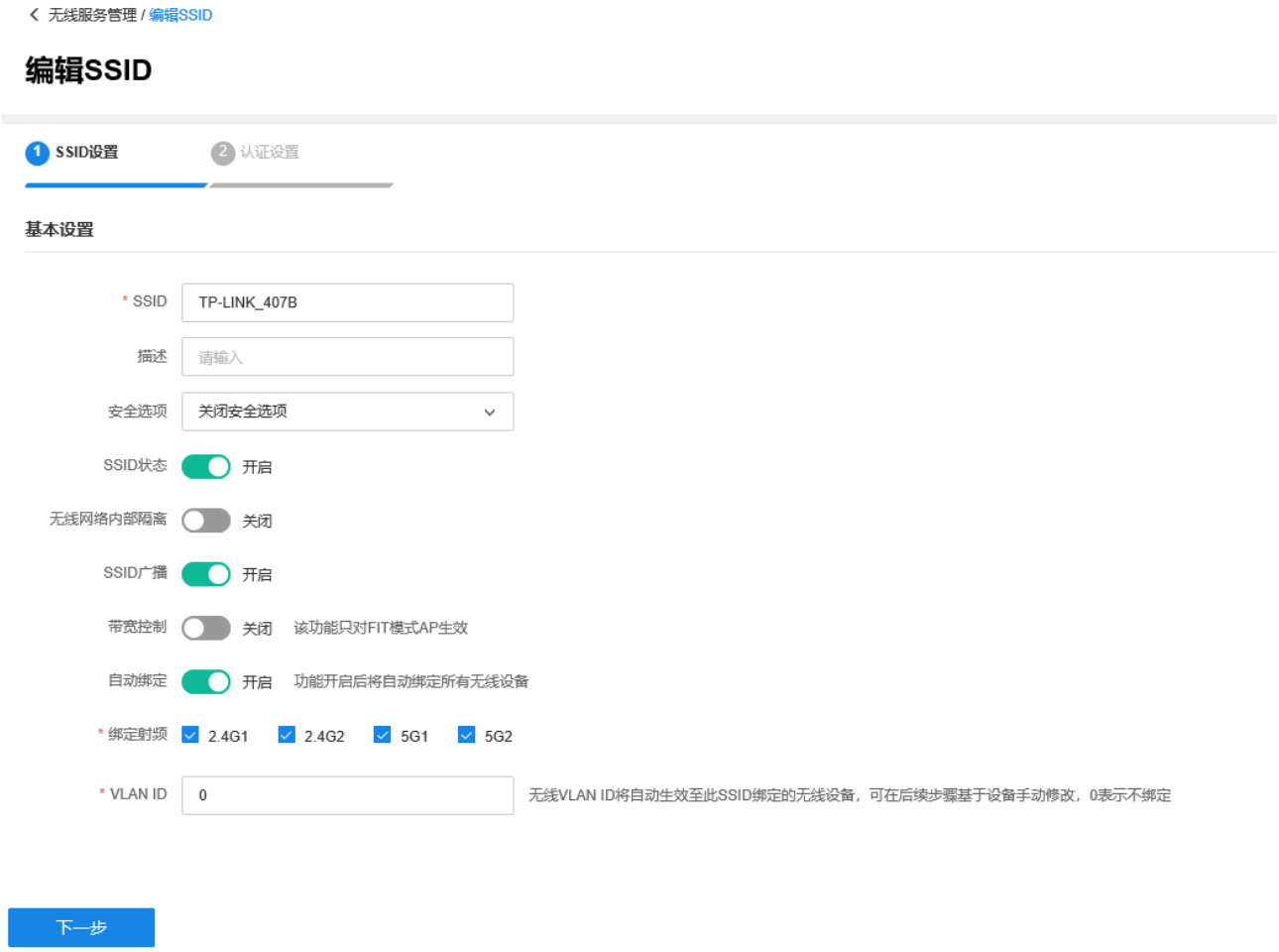
进入页面：网络配置 >> 无线服务管理，如下图所示，可进行添加、编辑、复制、删除 SSID 的操作。



5.3.1 编辑 SSID

➢ 编辑 SSID

点击相应图标，即可编辑无线控制器的 SSID，具体参数如下图所示，设置完成后点击<下一步>。



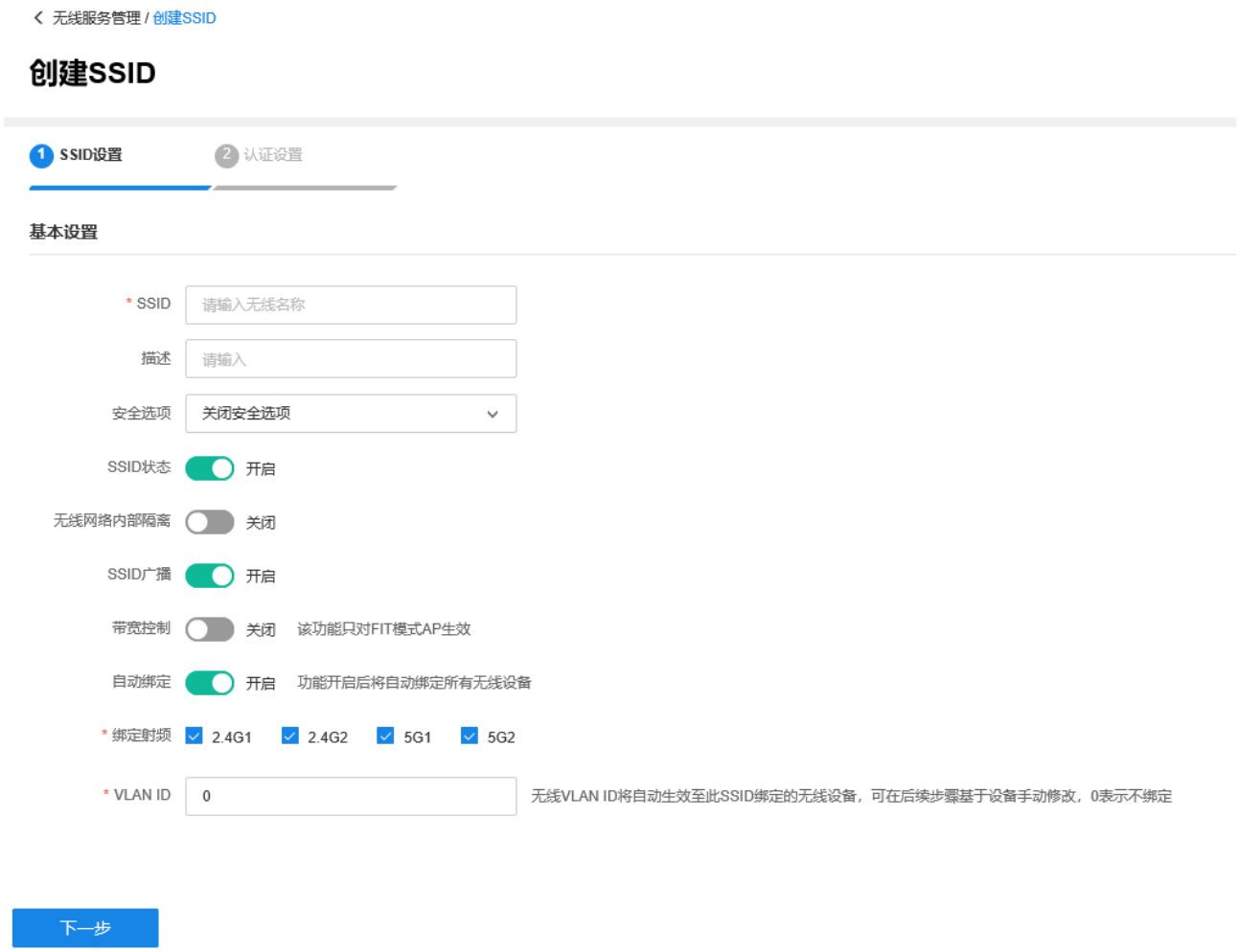
➢ 认证设置

认证设置界面可设置无线控制器的认证方式，具体参数如下图所示，可选择“一键上网”，“Web 认证”，“短信认证”，“远程 Portal”四种认证方式，设置完成后点击<保存>即可。

5.3.2 创建 SSID

➢ 创建 SSID

点击相应图标，即可创建无线控制器的 SSID，具体参数如下图所示，设置完成后点击<下一步>，认证设置步骤同编辑 SSID 操作中的认证设置。

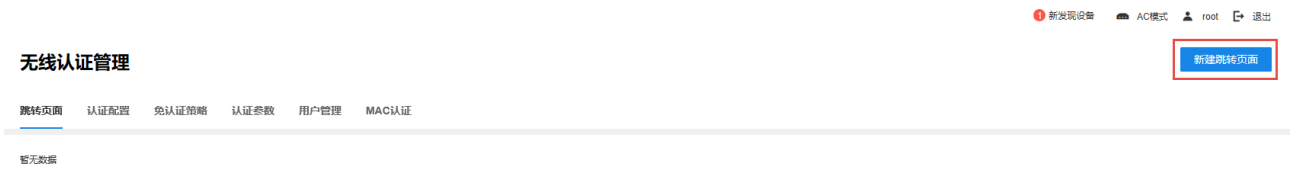


5.4 无线认证管理

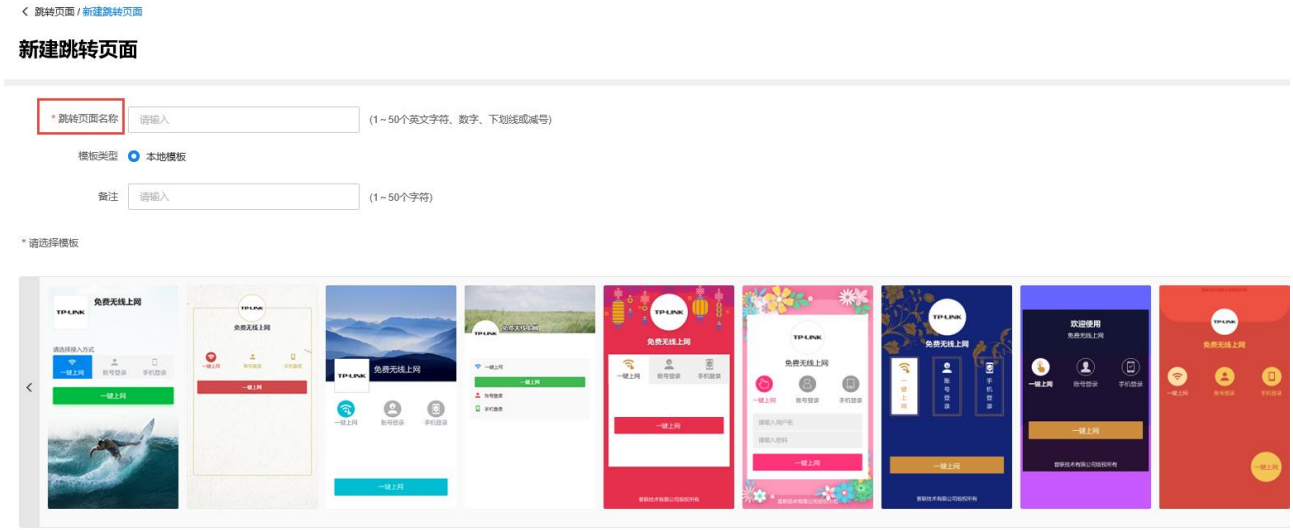
进入页面：网络配置 >> 无线认证管理，如下图所示，可设置“跳转页面”、“认证配置”、“免认证策略”、“认证参数”、“用户管理”和“MAC”认证。

5.4.1 跳转页面

进入页面：网络配置 >> 无线认证管理 >> 跳转页面，如下图所示，点击<新建跳转页面>。

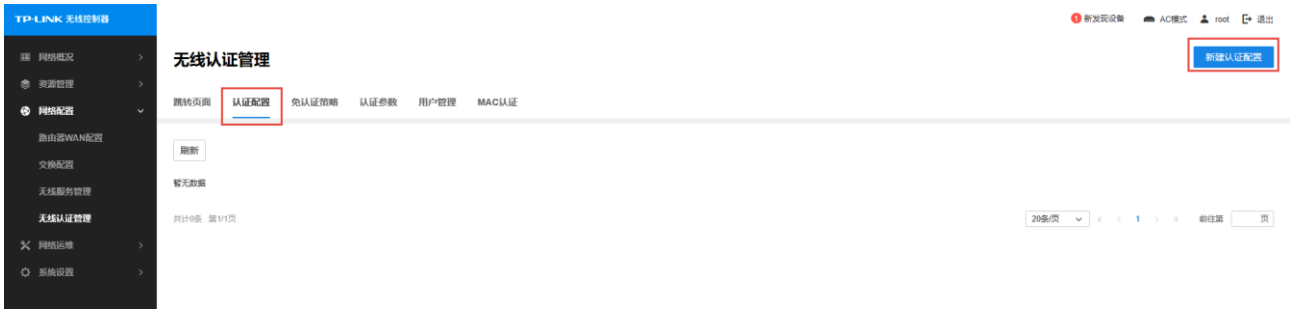


在如下界面中选择需要的跳转页面，输入跳转页面名称和备注，点击<保存>即可。



5.4.2 认证配置

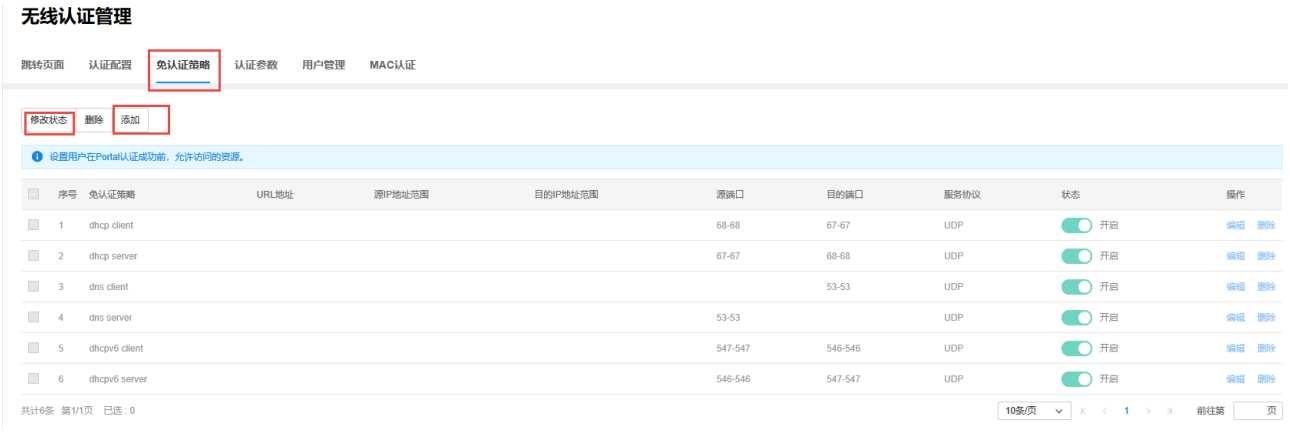
进入页面：网络配置 >> 无线认证管理 >> 认证配置，如下图所示，点击<新建认证配置>。



在如下界面中填写认证设置名称和认证方式等信息，点击<保存>即可

5.4.3 免认证策略

进入页面：网络配置 >> 无线认证管理 >> 免认证策略，如下图所示，可修改/删除已有的免认策略，或者添加新的免认证策略。



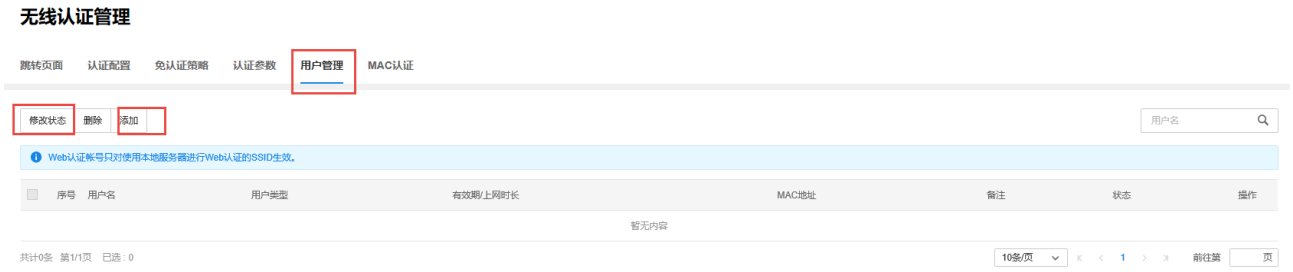
点击<添加>，输入免认证策略的相关配置信息，点击<确定>即可。

5.4.4 认证参数

进入页面：网络配置 >> 无线认证管理 >> 认证参数，如下图所示，可开启“认证老化”功能，设置“认证老化时间”和“Portal 认证端口”，点击<保存>即可。

5.4.5 用户管理

进入页面：网络配置 >> 无线认证管理 >> 用户管理，如下图所示，可修改或添加认证用户。



➢ 添加正式用户

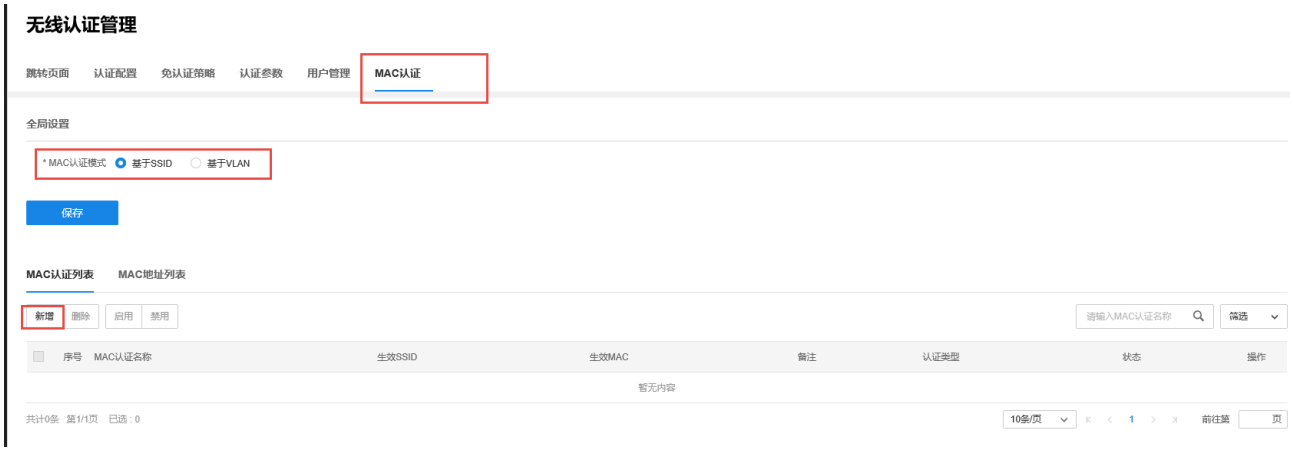
点击<添加>，选择“正式用户”，输入相应信息，点击<确定>即可。

➢ 添加免费用户

点击<添加>，选择“免费用户”，输入相应信息，点击<确定>即可。

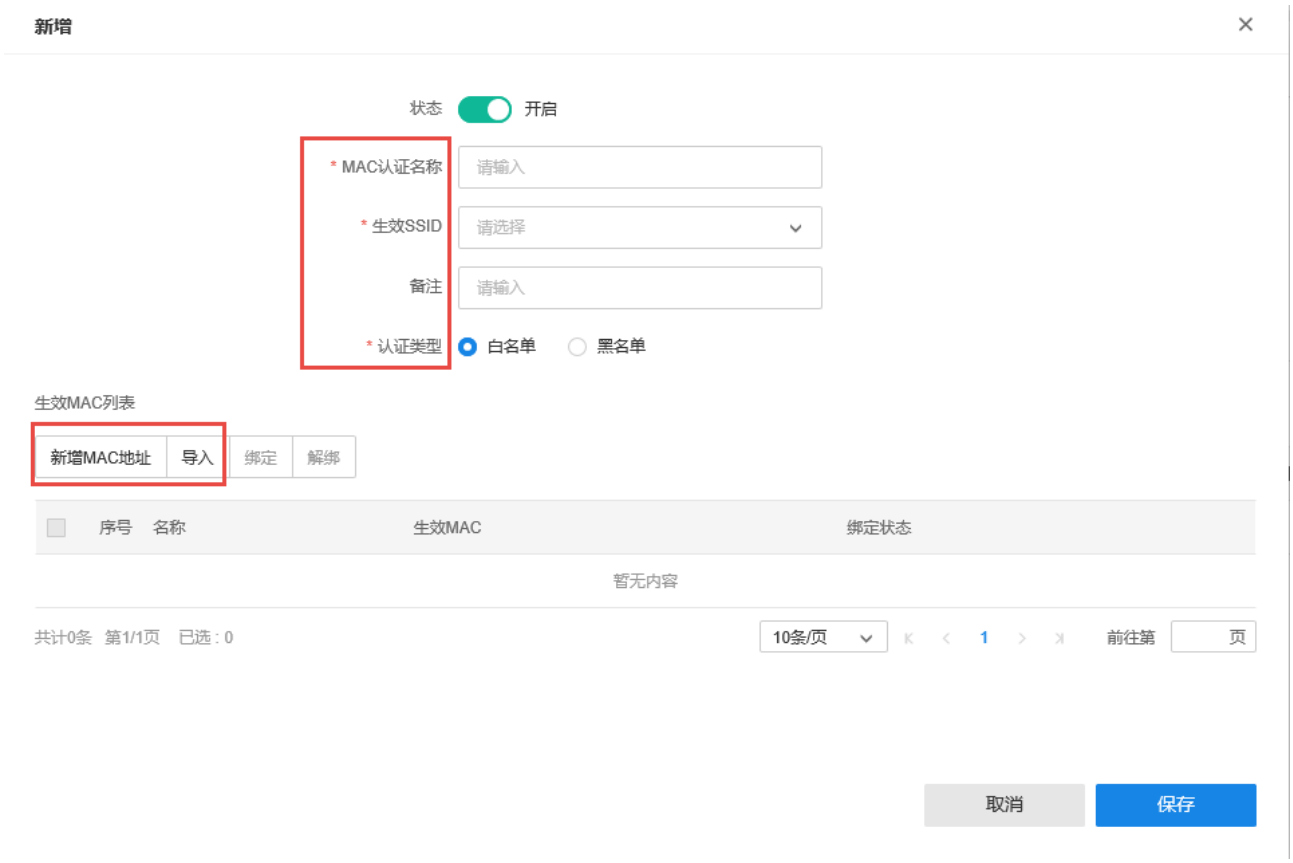
5.4.6 MAC 认证

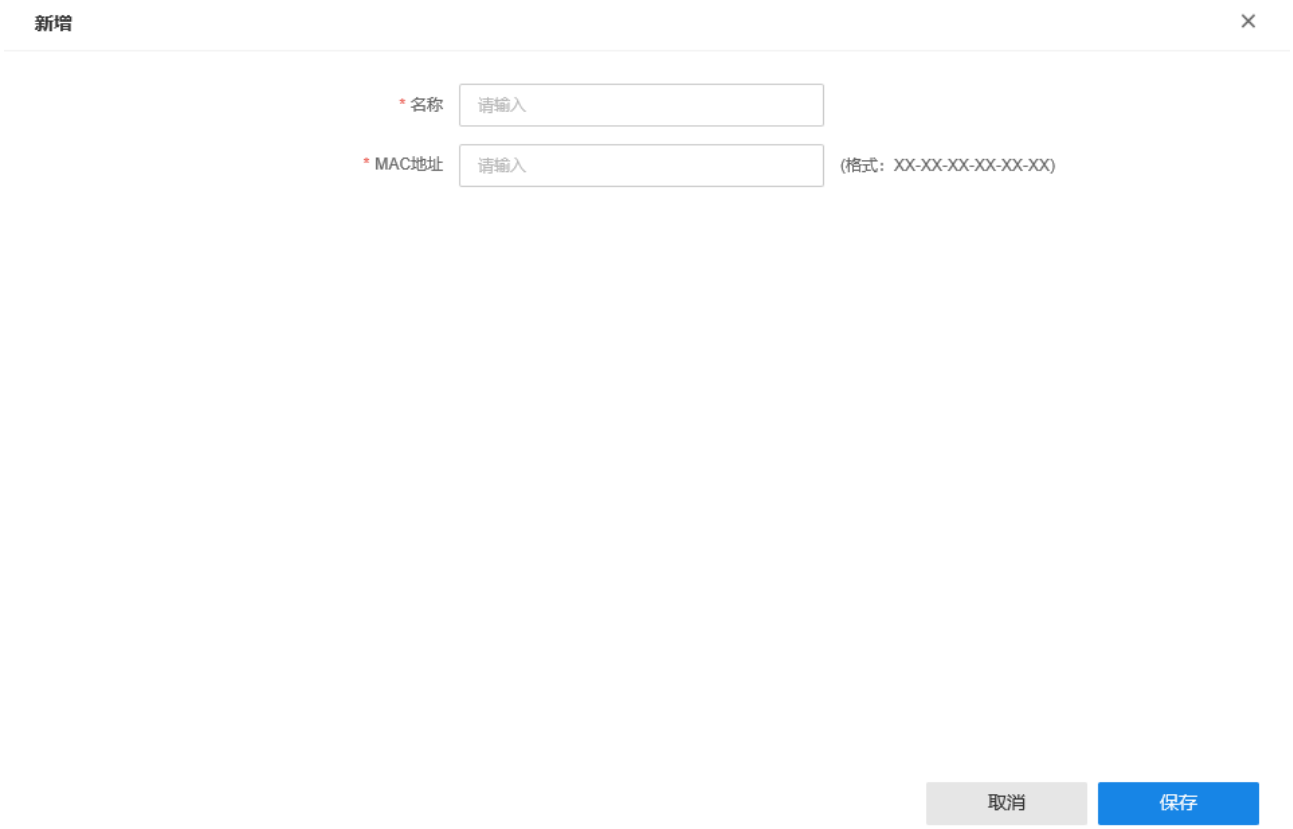
进入页面：网络配置 >> 无线认证管理 >> MAC 认证，如下图所示，可设置“MAC 认证模式”，查看 MAC 地址列表，并新增 MAC 认证。



➢ 新增 MAC 认证

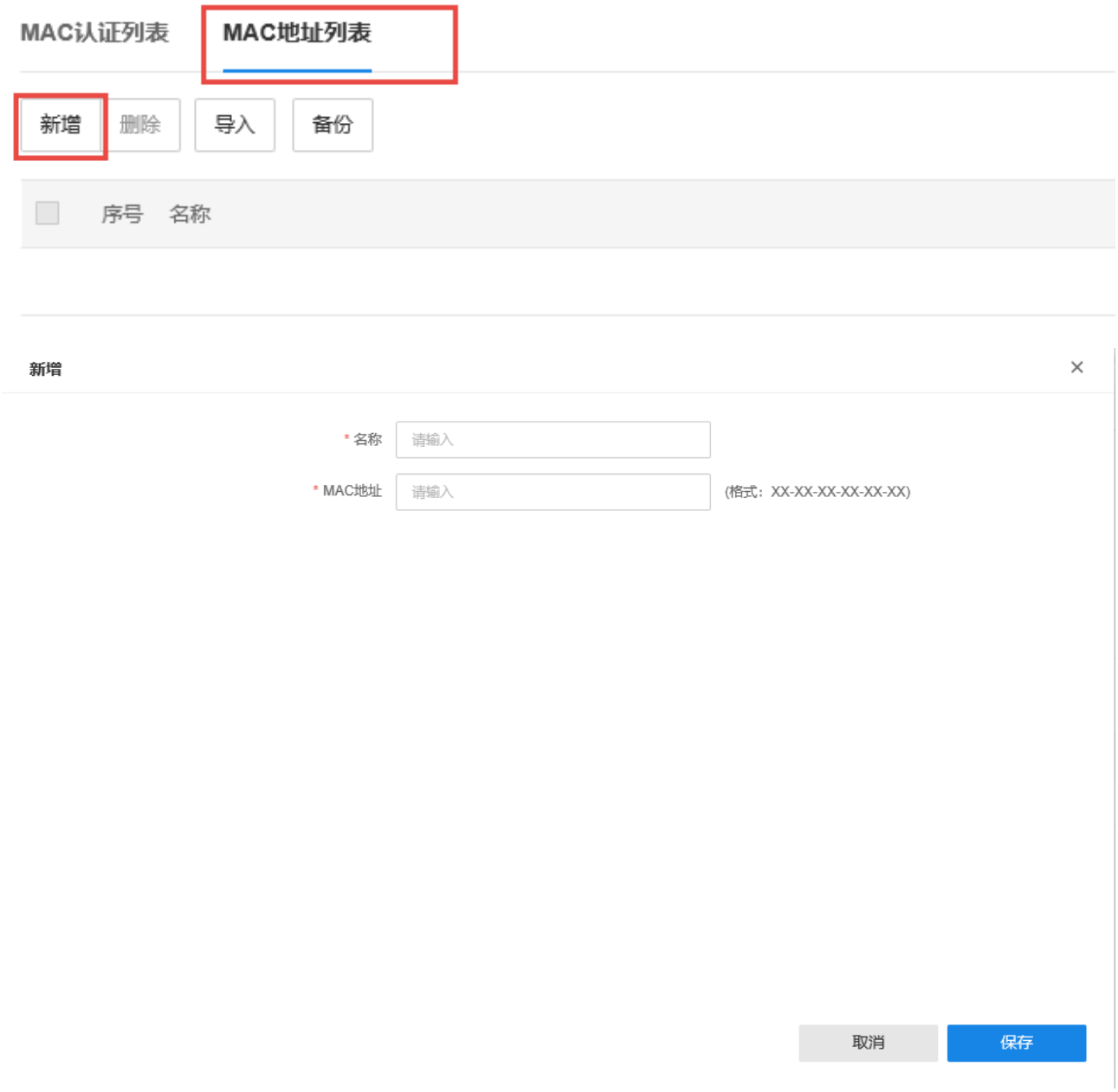
在 MAC 认证列表栏目下，点击<新增>，输入 MAC 认证相应信息，输入或批量导入新增的 MAC 地址，点击<保存>即可。


新增
状态
开启
* MAC认证名称
请输入
* 生效SSID
请选择
备注
请输入
* 认证类型
白名单
黑名单
生效MAC列表
新增MAC地址
导入
绑定
解绑
序号
名称
生效MAC
绑定状态
暂无内容
共计0条 第1/1页 已选：0
10条/页
1
前往第
页
取消
保存


新增
* 名称
请输入
* MAC地址
请输入
(格式：XX-XX-XX-XX-XX-XX)
取消
保存

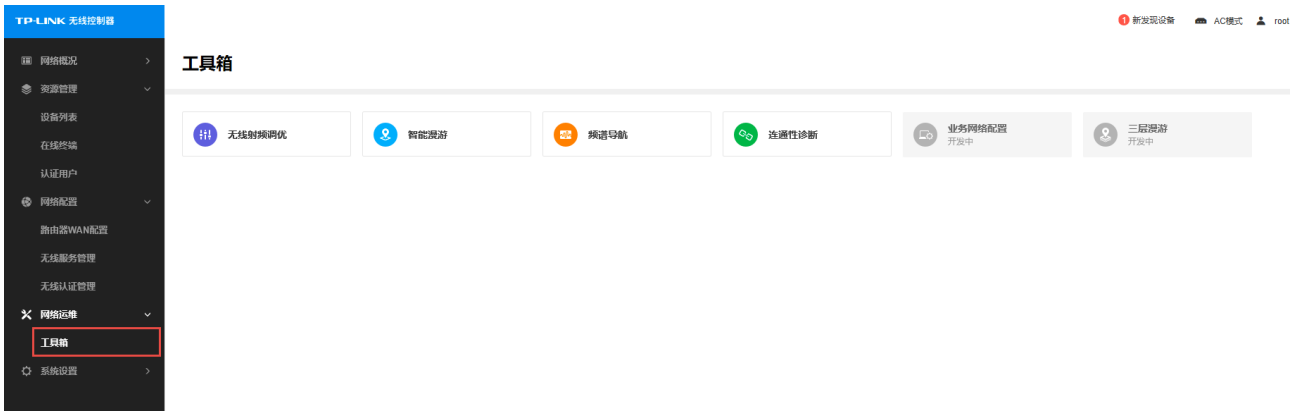
➢ 新增 MAC 地址

在 MAC 地址列表栏目下，点击<新增>，输入新增的 MAC 地址，点击<保存>即可。



第6章　网络运维

进入页面：网络运维 >> 工具箱，可开启并设置“无线射频调优”，“智能漫游”，“频谱导航”和“连通性诊断”功能。

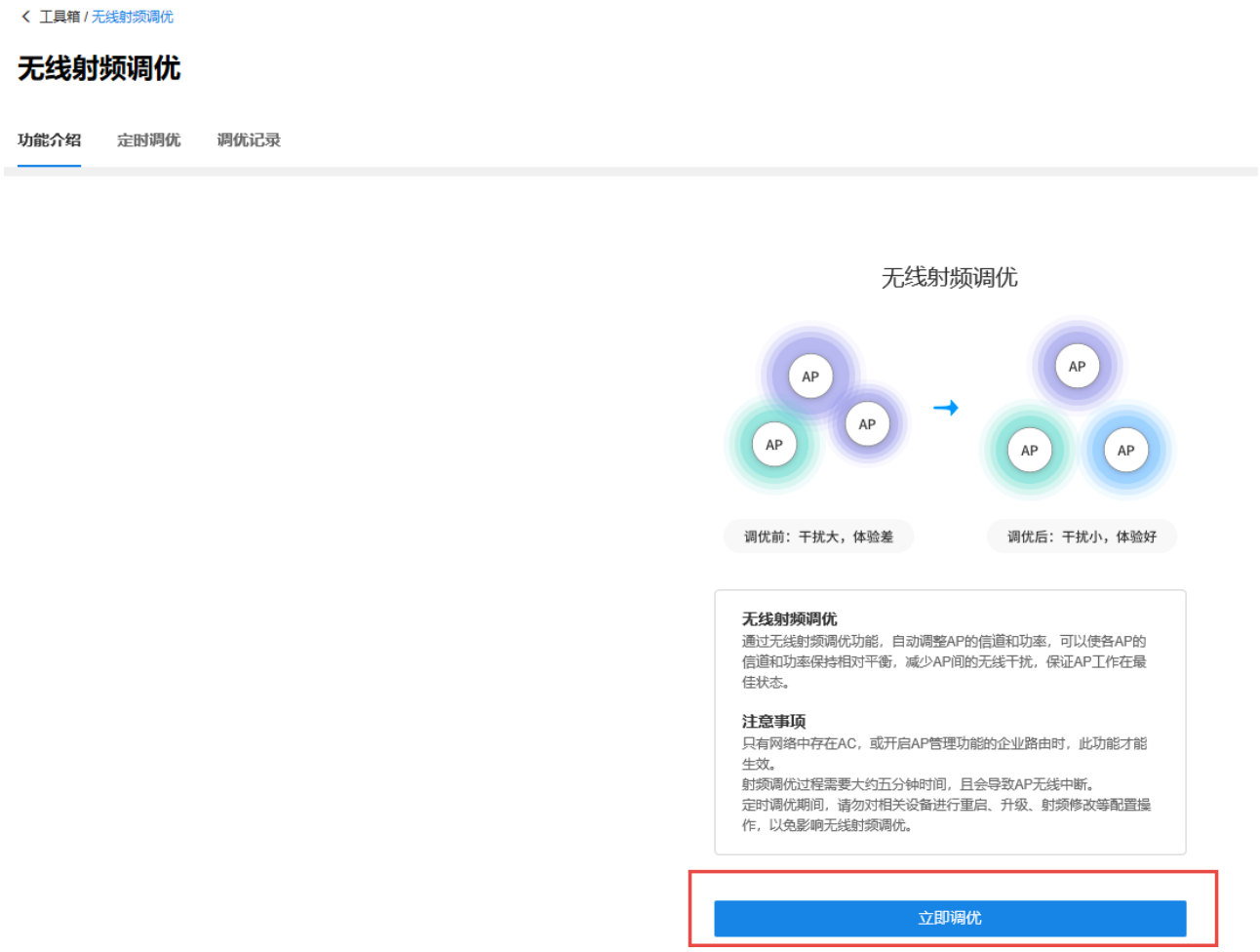


6.1　无线射频调优

进入页面：网络运维 >> 工具箱 >> 无线射频调优，在此页面下可设置 AC 的无线射频调优功能。具体配置方法可查看本配置指南第十一章“射频设置”。

➢　功能介绍

进入“功能介绍”页面，点击<立即调优>，进入射频调优设置。



➢ 定时调优

在定时调优页面，可设置固定时间进行射频调优，设置 2.4G 和 5G 信道调优参数，并可开启功率调优功能。

➢ 功率调优

点击开启功率调优功能，设置功率调优参数，点击<保存>即可。

➢ 调优记录

如下界面可选择查看一定时间内的调优记录，如下图。

6.2 智能漫游

进入页面：网络运维 >> 工具箱 >> 智能漫游，在此页面下可设置 AC 的智能漫游功能。具体配置方法可查看本配置指南第十章第四节“智能漫游”。

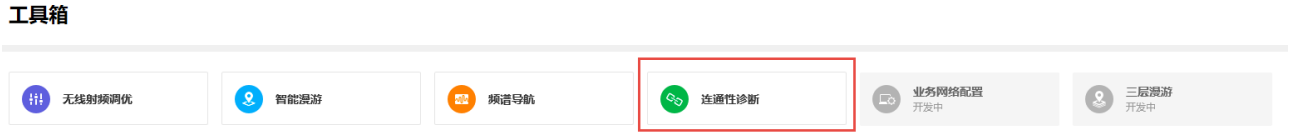
点击开启 802.11k/v/r 快速漫游功能，并设置 2.4G 和 5G 的漫游参数，可选择“基于信号强度”或“基于速率百分比”的智能漫游，点击<保存>即可。

6.3 频谱导航

进入页面：网络运维 >> 工具箱 >> 频谱导航，在此页面下可设置频谱导航参数，如下图。具体配置方法可查看本配置指南第十一章第三节“频谱导航”。

6.4 连通性诊断

进入页面：网络运维 >> 工具箱 >> 连通性诊断，在此页面下可进行网络的连通性诊断，如下图。



可输入目的 IP/域名，点击<开始检测>，检测设备的网络是否联通。

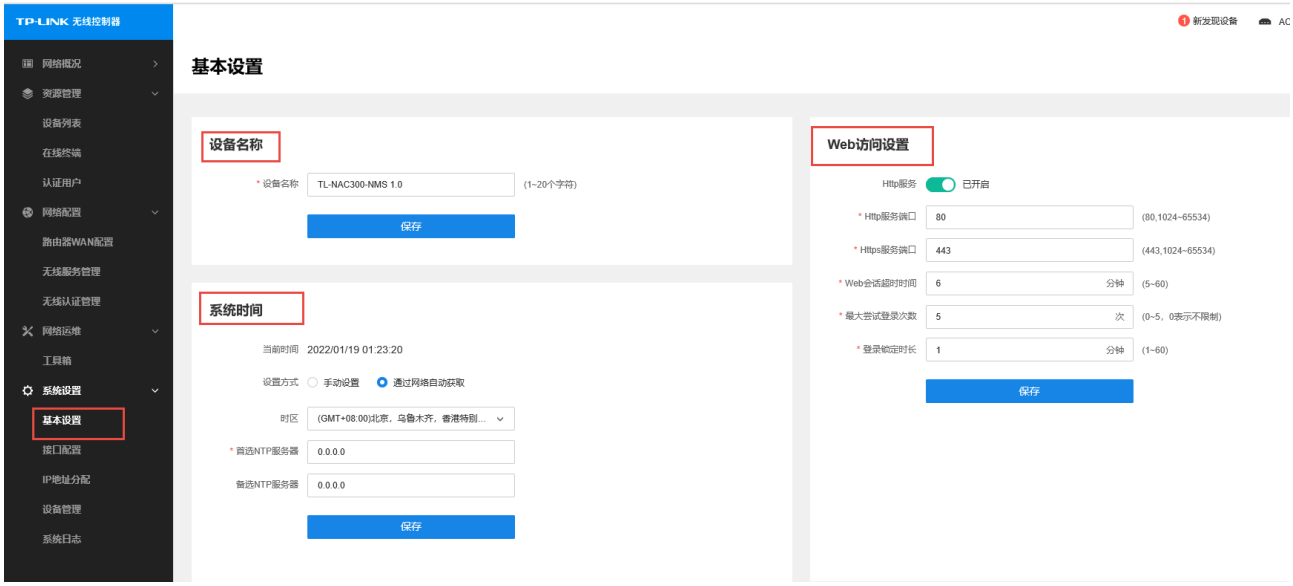
➢ 诊断记录

进入页面：网络运维 >> 工具箱 >> 连通性诊断 >> 诊断记录，可以查看最近 10 次的连通性诊断记录。

第7章　系统设置

7.1　基本设置

进入页面：系统设置 >> 基本设置 ，可以更改设备名称，设置系统时间，设置 Web 访问参数，点击<保存>即可，如下图。



7.2　接口配置

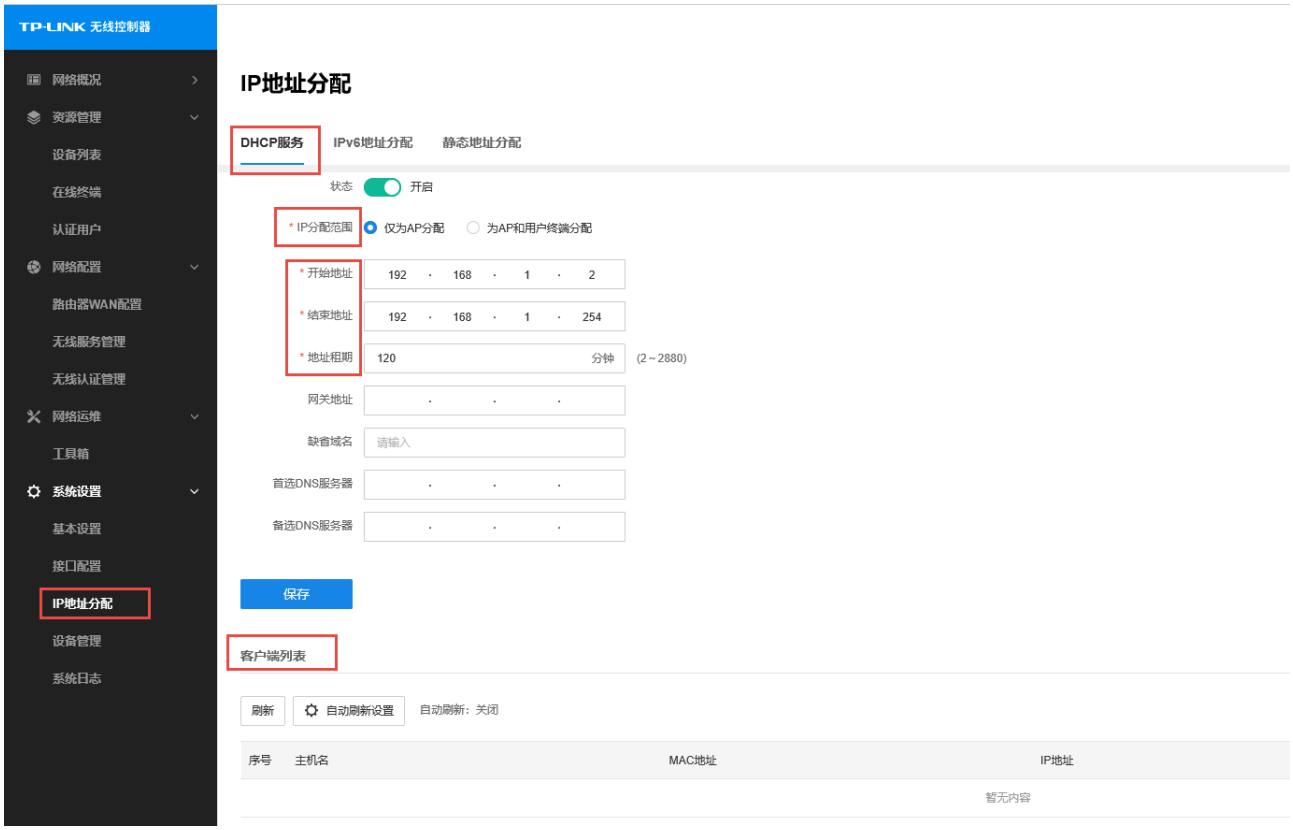
进入页面：系统设置 >> 接口配置 ，可以设置 IP 地址，子网掩码，MTU 等参数，点击<保存>即可，如下图。

➢ IPv6 接口配置

进入页面：系统设置 >> 接口配置 >>IPv6 接口配置，可以设置 IPv6 地址，子网掩码，MTU 等参数，点击<保存>即可，如下图。

7.3 IP 地址分配

进入页面：系统设置 >> IP 地址分配 >> DHCP 服务，可以设置 IP 地址分配范围，地址租期等参数，并可查看客户端列表，点击<保存>即可，如下图。

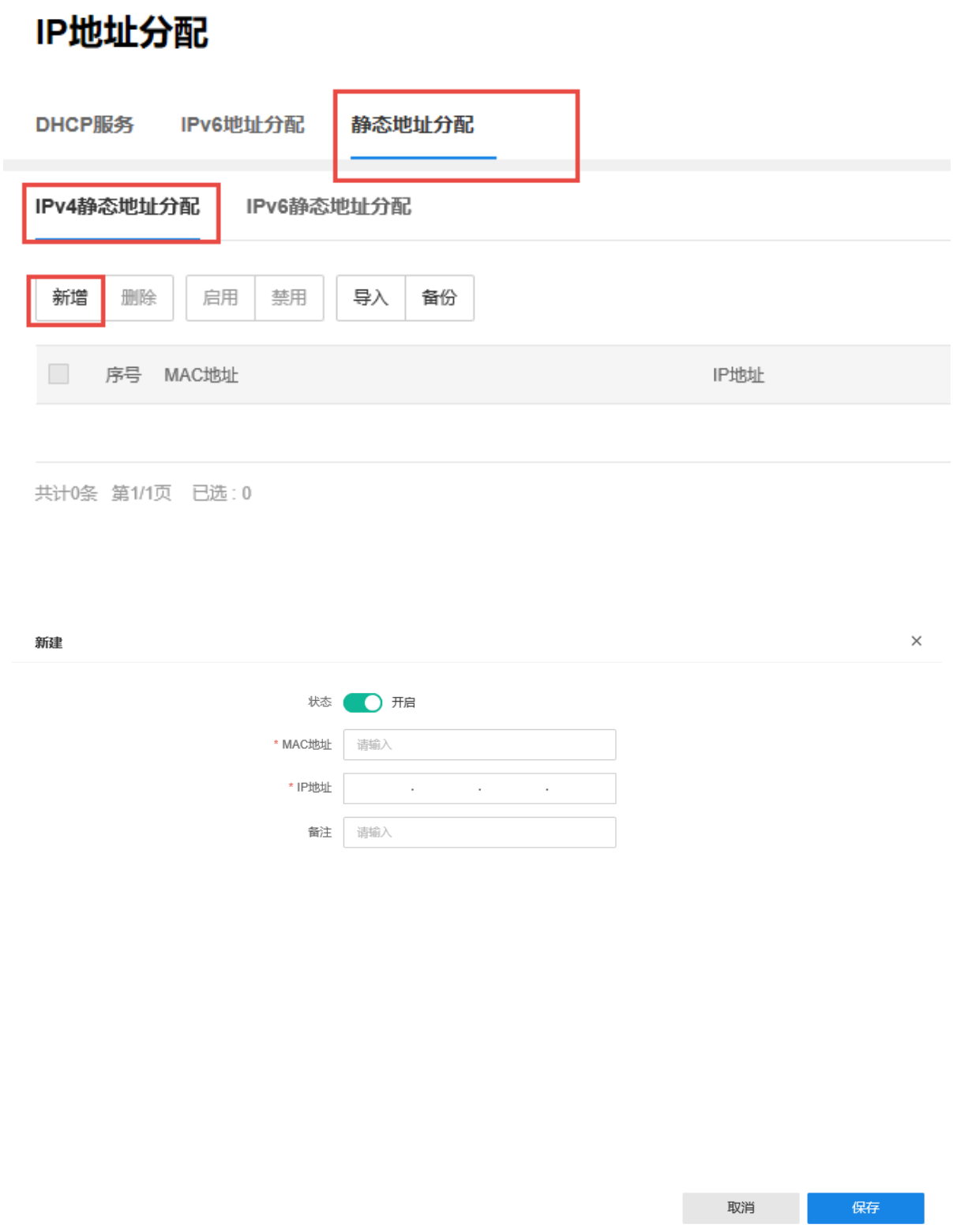


➢ IPv6 地址分配

进入页面：系统设置 >> IP 地址分配 >> IPv6 地址分配，可以设置 IPv6 地址分配范围，地址租期等参数，并可查看客户端列表，点击<保存>即可，如下图。

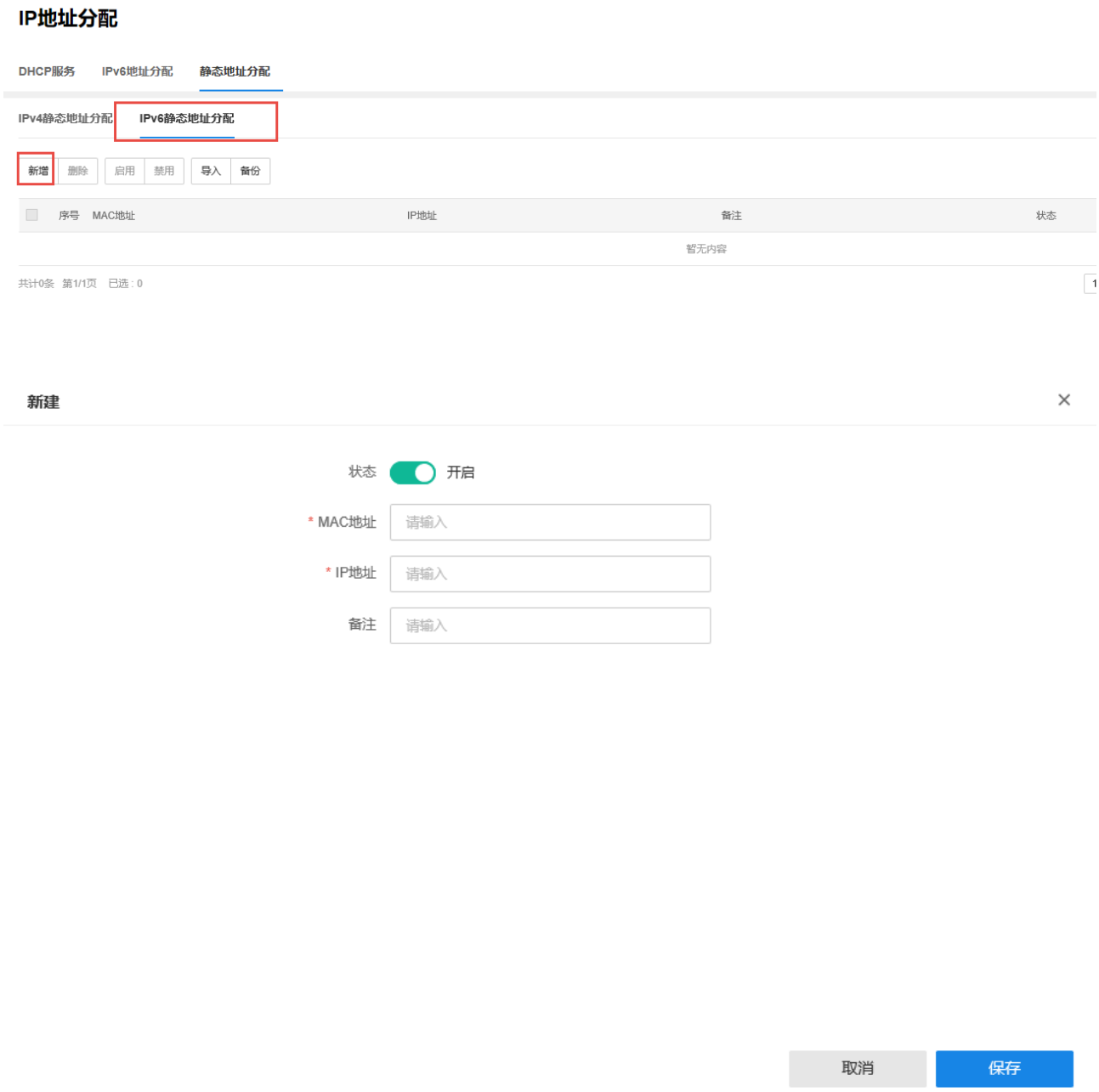
➢ 静态 IPv4 地址分配

进入页面：系统设置 >> IP 地址分配 >> 静态 IPv4 地址分配，点击<新增>，可以手动添加 MAC 地址及 IP 地址，点击<保存>即可，如下图。



➢ 静态 IPv6 地址分配

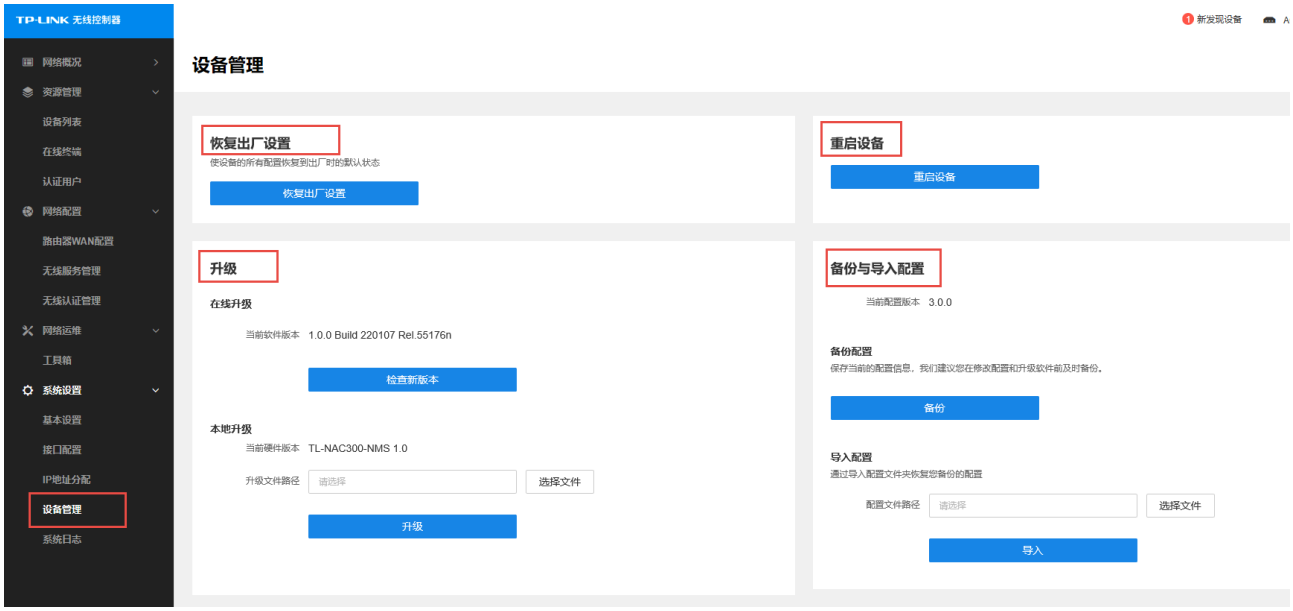
进入页面：系统设置 >> IP 地址分配 >> 静态 IPv6 地址分配，点击<新增>，可以手动添加 MAC 地址及 IPv6 地址，点击<保存>即可，如下图。



7.4 设备管理

进入页面：系统设置 >> 设备管理，可以进行“恢复出厂设置”，“重启设备”，“在线及本地升级”，“备份

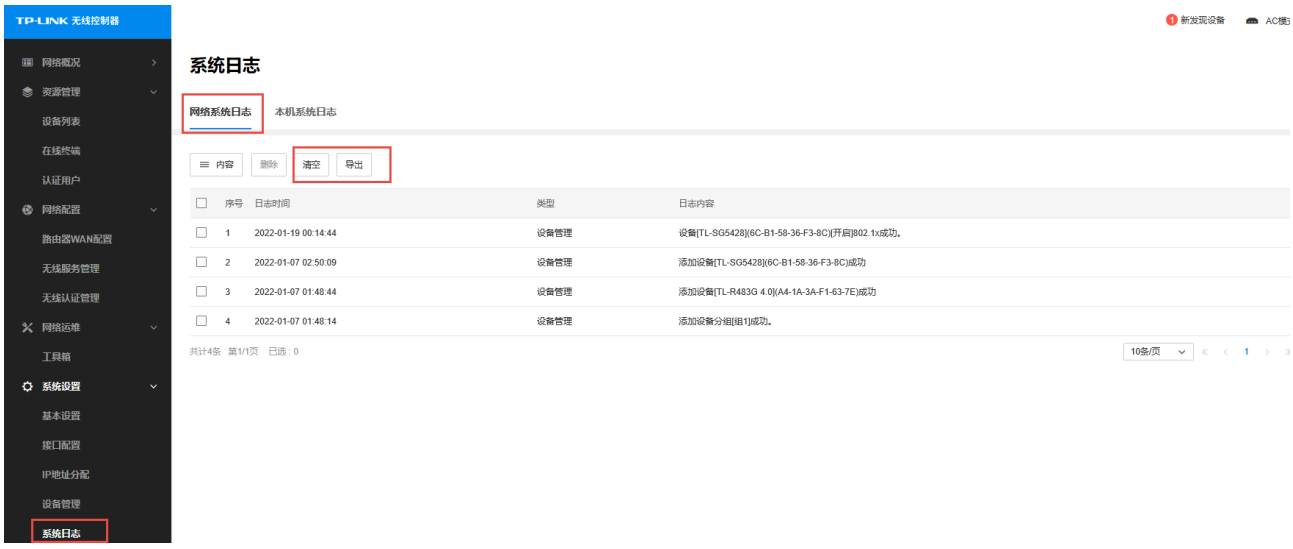
与导入配置” 操作，如下图。



7.5 系统日志

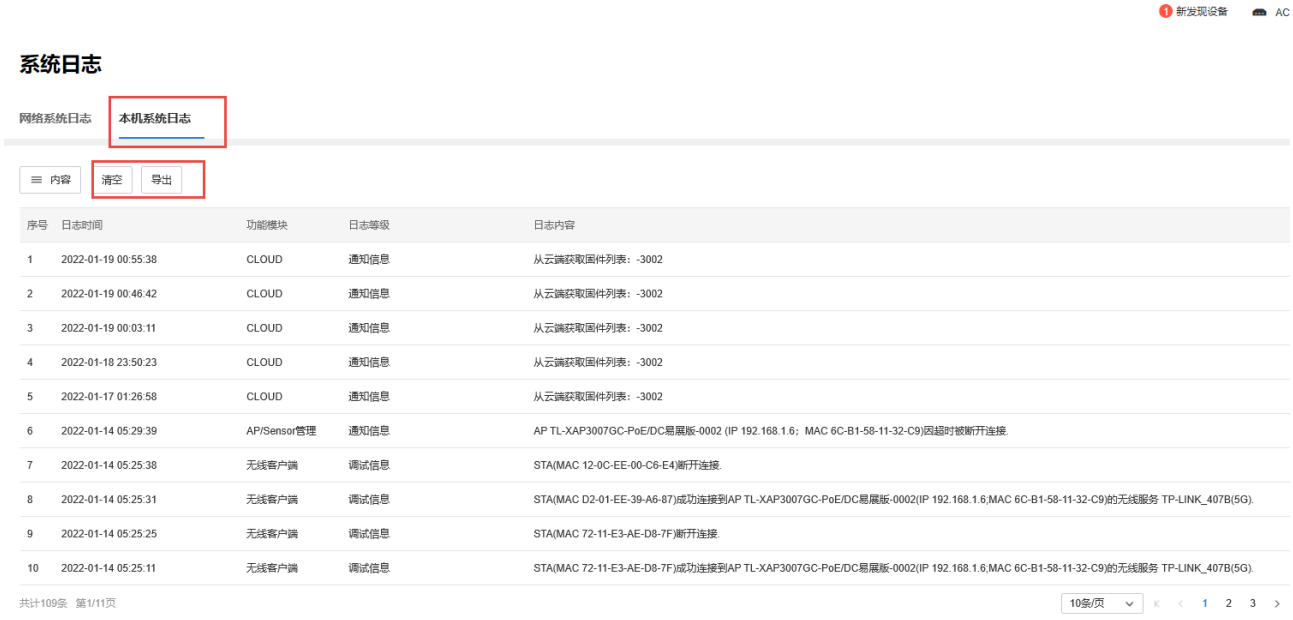
7.5.1 网络系统日志

进入页面：系统设置 >> 系统日志 >> 网络系统日志，查看网络系统日志，并可进行“清空”与“导出”操作，如下图。



7.5.2 本机系统日志

进入页面：系统设置 >> 系统日志 >> 本机系统日志，查看网络系统日志，并可进行“清空”与“导出”操作，如下图。

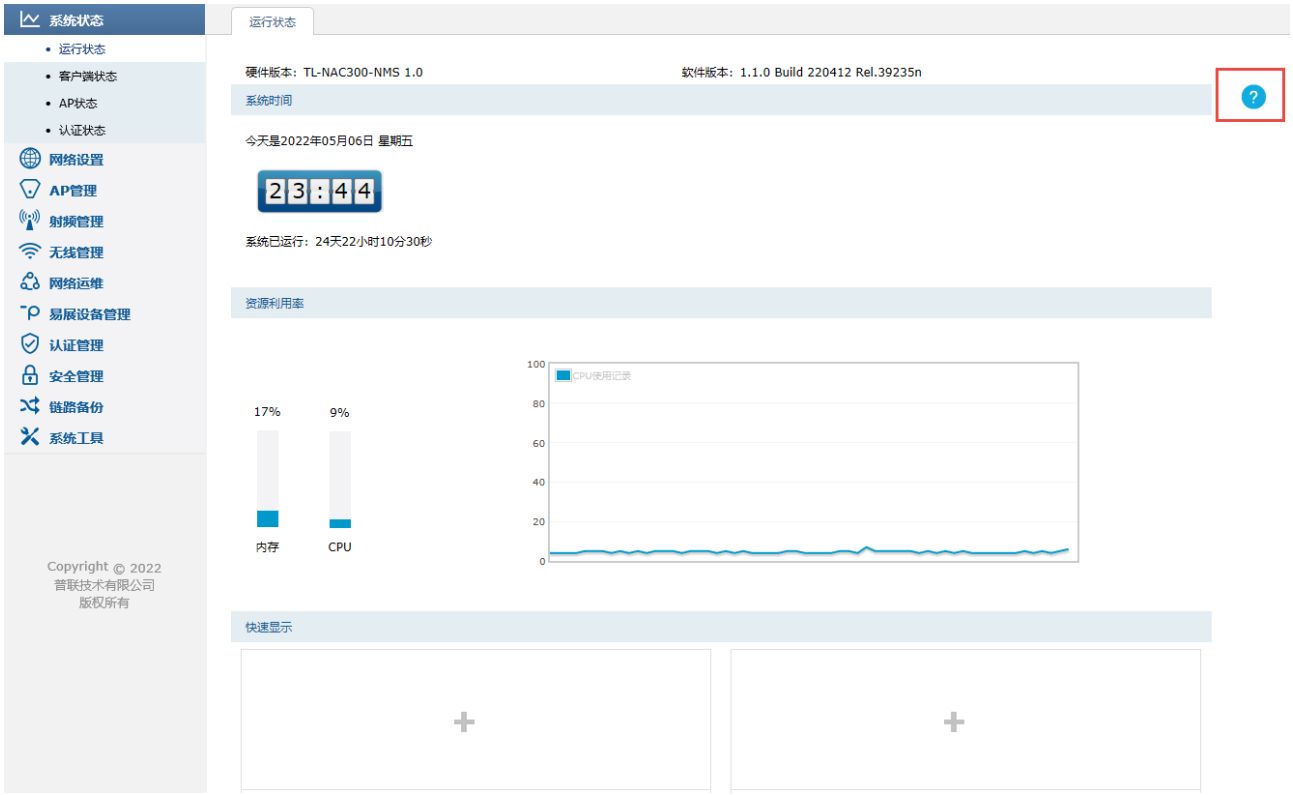


第8章　系统状态

8.1　运行状态

点击<设备高级配置>或<AC 模式>，可进行详细的 AC 功能配置。在第 8~18 章配置章节中，点击页面右上角 ，可获取到更多参数信息。

进入页面：系统状态 >> 运行状态，可查看设备的软硬件版本、系统时间和运行时间、资源利用率，并可在快速显示一栏添加需要显示的端口状态，如下图。



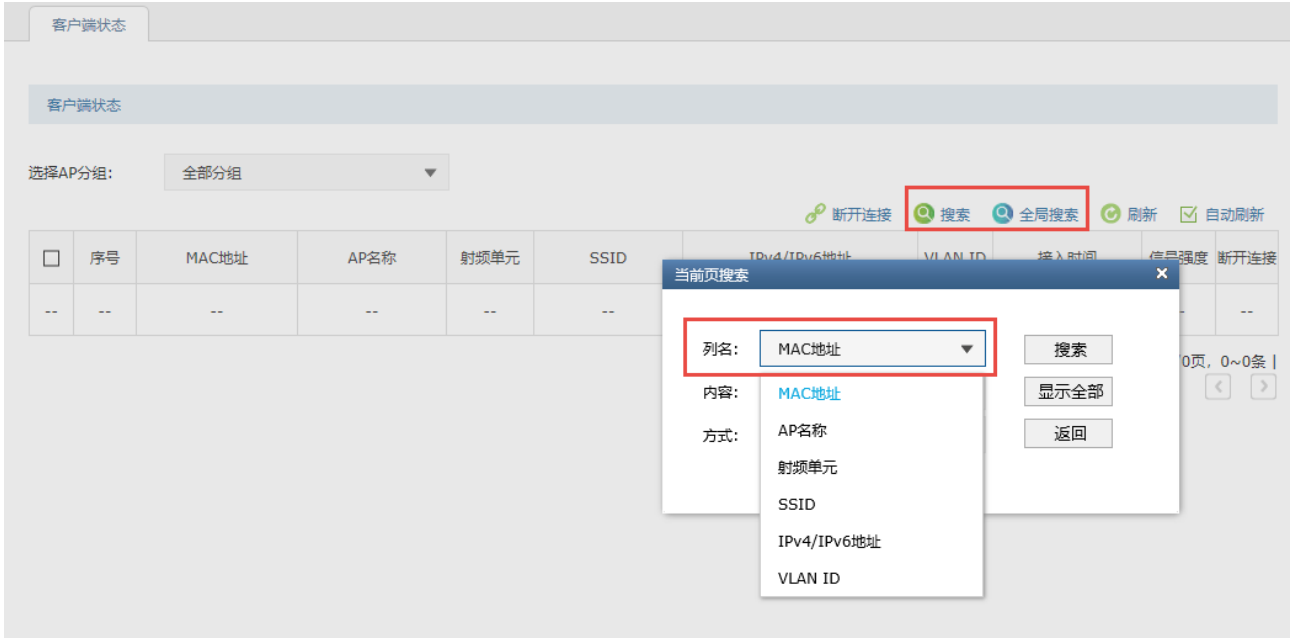
8.2　客户端状态

8.2.1 查看客户端状态

进入页面：系统状态 >> 客户端状态，选择 AP 分组，可查看该分组下的客户端状态，具体栏目如下图。

8.2.2 搜索/断开客户端

点击<搜索/全局搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定条目的客户端，如下图。

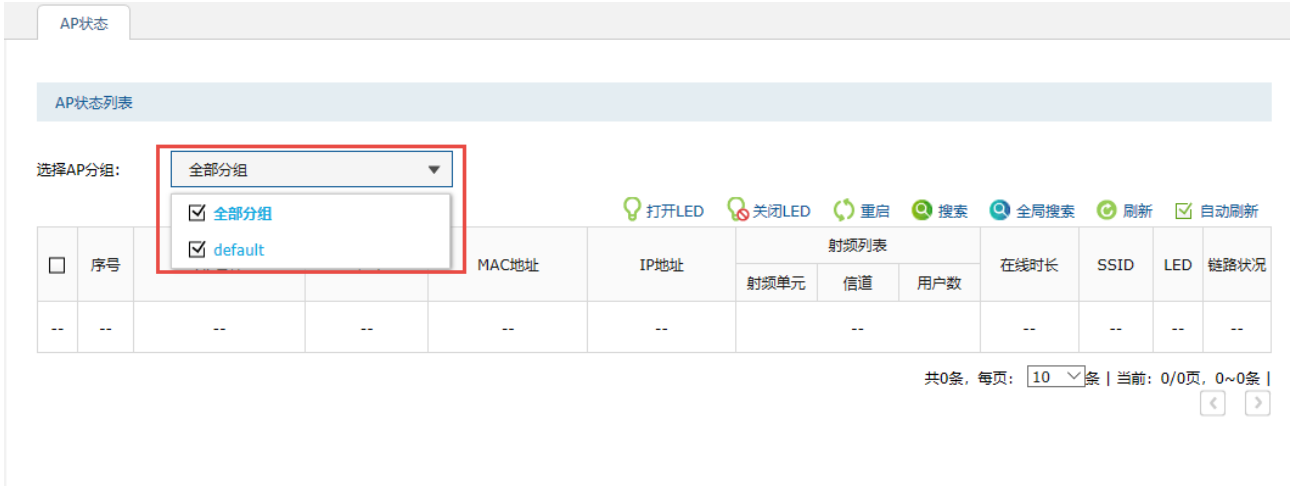


选中客户端条目，点击<断开连接>，即可断开所选客户端，如下图。

8.3 AP 状态

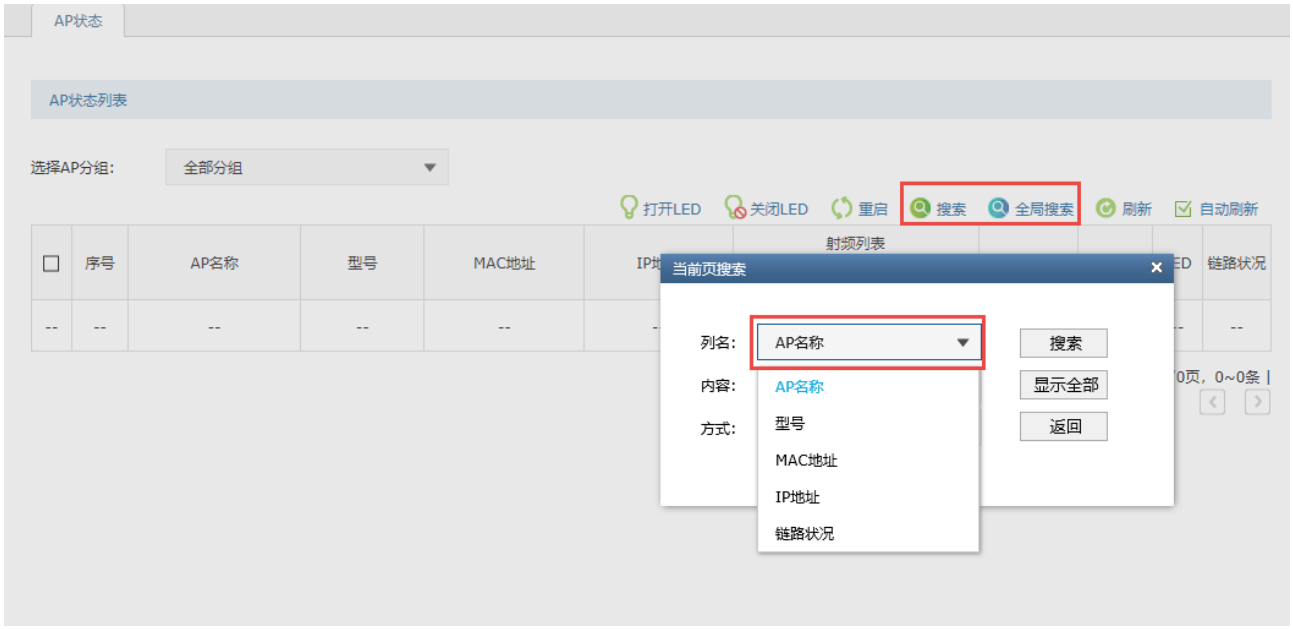
8.3.1 查看 AP 状态

进入页面：系统状态 >> AP 状态，选择 AP 分组，可查看该分组下的客户端状态，具体栏目如下图。



8.3.2 搜索 AP

点击<搜索/全局搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定条目的 AP，如下图。



8.3.3 打开/关闭 LED

选中 AP 条目，点击<打开/关闭 LED>，即可打开或关闭选中 AP 的 LED 灯。

8.4 认证状态

8.4.1 认证状态

- 查看登录用户的认证状态

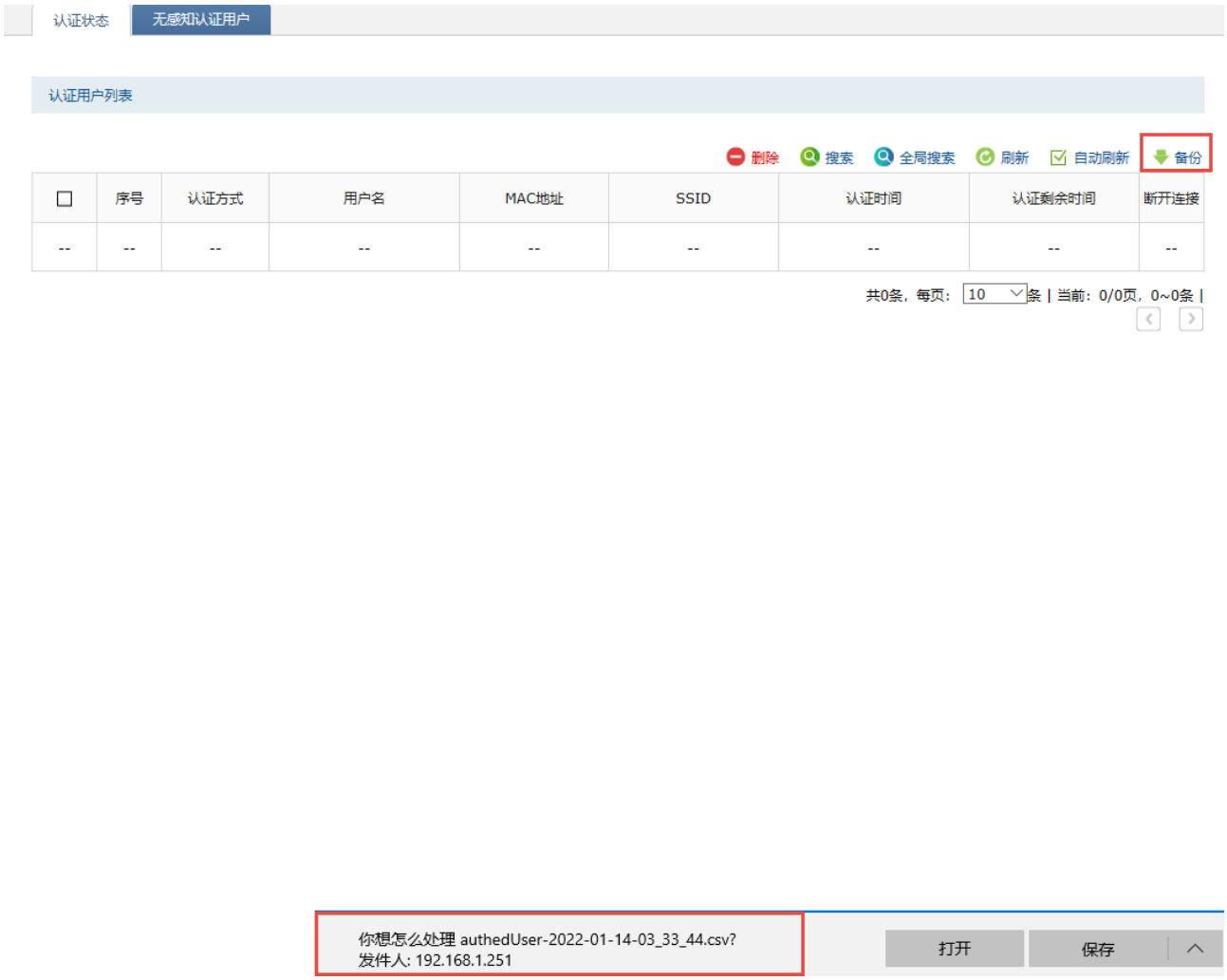
进入页面：系统状态 >> 认证状态，可查看当前登录用户的各条目信息，如下图。

➢ **搜索指定登录用户**

点击<搜索/全局搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定条目的登录用户，如下图。

➢ **备份登录用户**

点击<备份>，即可备份所有认证用户条目至 ANSI 编码格式的 CSV 文件中，如下图。



8.4.2 无感知认证用户

无感知认证是指用户使用一台设备上网时,只有首次登录需要进行 web 认证,再次登录时无需输入用户名和密码的认证方式。

- **查看登录用户的认证状态**

进入页面:系统状态 >> 认证状态>> 无感知认证用户,可查看当前登录的无感知认证用户的各条目信息,如下图。

➢ **搜索指定登录用户**

点击<搜索/全局搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定条目的登录用户，如下图。

第9章　网络设置

9.1　接口设置

9.1.1 查看接口信息

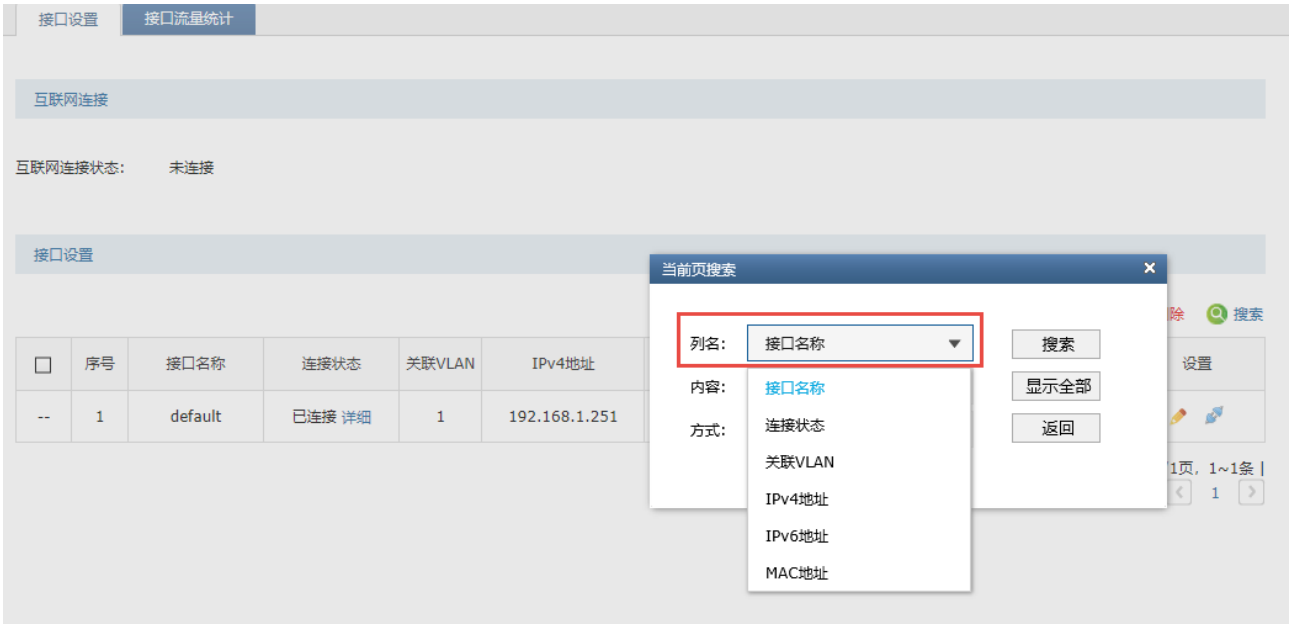
进入页面：网络设置 >> 接口设置，可查看设备的互联网连接状态以及物理接口下的所有接口，并对接口进行相关操作，如下图。

➢　查看接口详细信息

点击接口连接状态旁的<详细>按键，即可查看接口的详细状态信息，如下图。

➢ **搜索指定接口**

点击<搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定接口，如下图。



9.1.2 配置接口

进入页面：网络设置 >> 接口设置，点击<新增>，填写接口名称、IP 地址等信息，点击<确定>，如下图，

目前仅支持静态 IP 连接方式。

可选择 IPv6 连接，如下图，“IP 协议类型”选择“IPv6”，填写相应参数即可：

9.1.3 接口流量统计

进入页面：网络设置 >> 接口设置>> 接口流量统计，可查看设备各接口的流量信息，如下图。

➢ **搜索指定接口**

点击<搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定接口，如下图。

9.2 路由设置

9.2.1 路由功能介绍

路由是指安全网关根据数据包的目的 IP 地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程。

在一次路由过程中选择最优路径是安全网关需要完成的最重要的工作。安全网关通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。路由表中的每一个路由条目基本都包含如下四种基本属性,路由转发时将根据数据包的目的 IP 地址查找最优路径：

1) 目的网络地址：用于标识该条路由条目所指向的目标网络。

2) 子网掩码：用于标识目标网络的子网掩码。

3) 下一跳地址：用于指定通往目标网络的下一跳路由节点，安全网关将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过 ping 工具测试是否可达。

4) 下一跳接口：用于标识数据从本地发出的出接口。

安全网关根据路由表进行数据转发，而路由条目的来源有三种，分别为直连路由、静态路由和动态路由，以下是三种路由的特点。

- 直连路由：通过数据链路层协议发现的，通常指向与安全网关直接连接的网络，如 VLAN。
- 静态路由：由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。
- 动态路由：通过相互连接的安全网关之间交换彼此的路由信息，然后通过路由选择协议计算出自身的路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。常用的动态路由选择协议有 RIP、OSPF 和 BGP 等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。

无线控制器支持静态路由。

9.2.2 静态路由

静态路由是由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模

较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。

进入页面：网络设置 >> 路由设置>> 静态路由，可设置静态路由条目，当数据包与静态路由匹配成功时，将按指定的转发方式进行转发，如下图。

➢ 配置路由条目

点击<新增>，输入规则名称、目的地址、子网掩码、下一跳、出接口等信息，如下图。

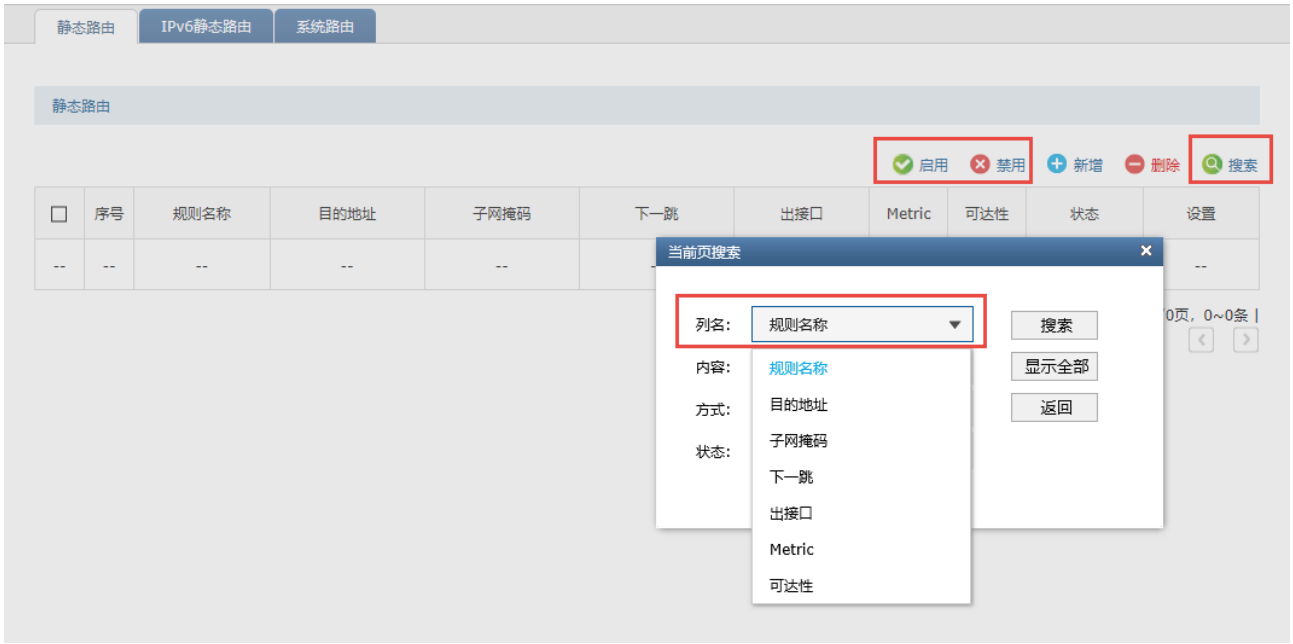
目的地址/子网掩码	设置目的地址和子网掩码，确定路由生效的网段。
下一跳	数据包将发往的下一个路由点。
出接口	设置数据包出接口
Metric	静态路由规则的度量值，数值越小优先级越高，默认为 0

点击页面  ，查看更多页面设置参数信息。

- **启用/禁用/搜索路由条目**

点击<搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定路由条目。

选中路由条目，点击<启用/禁用>，即可设置路由条目生效或不生效，如下图。



9.2.3 静态路由配置实例

组网介绍：

某企业使用无线控制器接入核心交换机，交换机划分了 VLAN，需要实现无线控制器可以连接核心交换机下的 VLAN1 网段的 AP，示意网络拓扑如下：

配置步骤：

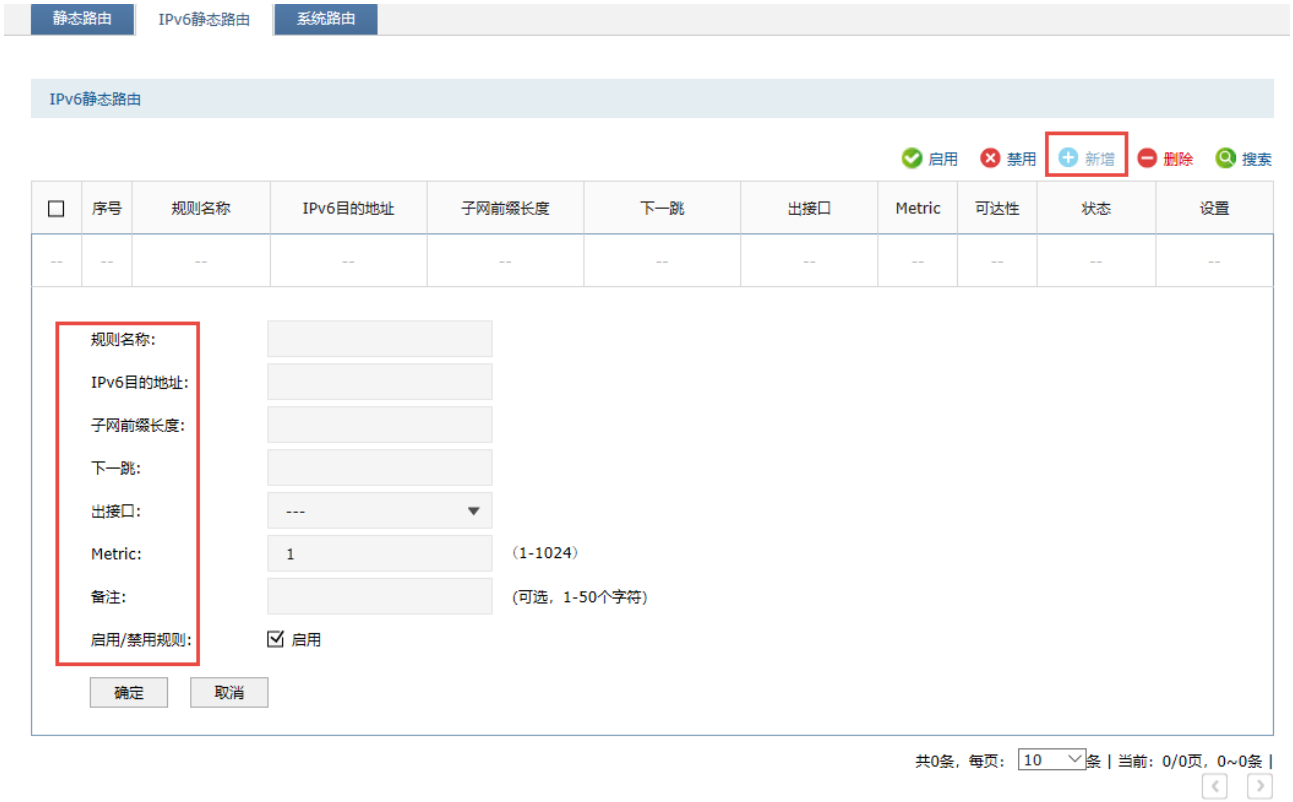
网络设置 >> 路由设置 >> 静态路由，点击<新增>，输入规则名称、目的地址、子网掩码、下一跳、出接口等信息，如下图。

9.2.4 IPv6 静态路由

进入页面：网络设置 >> 路由设置>>IPv6 静态路由，可设置 IPv6 静态路由条目，当数据包与静态路由匹配成功时，将按指定的转发方式进行转发，如下图。

➢ **配置 IPv6 路由条目**

点击<新增>，输入规则名称、IPv6 目的地址、子网前缀长度、下一跳、出接口等信息，点击<确定>如下图。



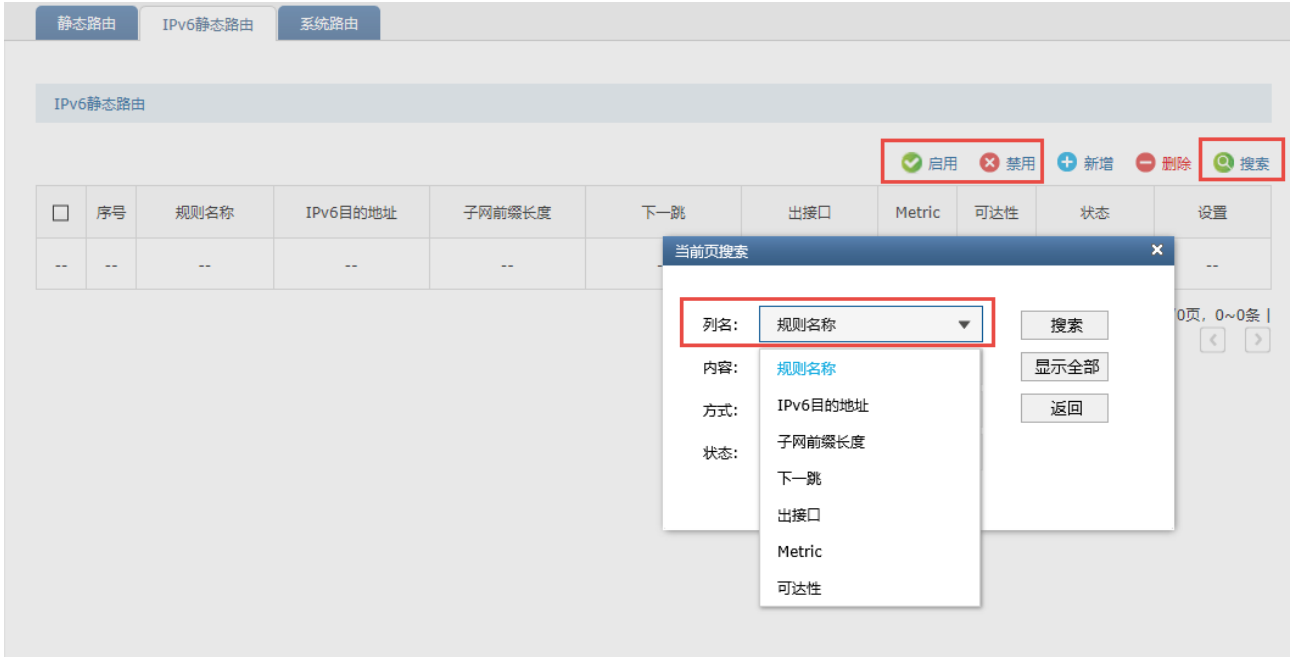
IPv6 目的地址/子网前缀长度	设置 IPv6 目的地址和子网前缀长度，确定路由生效的网段。
下一跳	数据包将发往的下一个路由点。
出接口	设置数据包出接口
Metric	静态路由规则的度量值，数值越小优先级越高，默认为 1

点击页面  ，查看更多页面设置参数信息。

- **启用/禁用/搜索 IPv6 路由条目**

点击<搜索>，选择搜索列名后，输入需要搜索的内容，点击<搜索>，即可搜索指定 IPv6 路由条目。

选中 IPv6 路由条目，点击<启用/禁用>，即可设置 IPv6 路由条目生效或不生效，如下图。



9.2.5 系统路由

进入页面：网络设置 >> 路由设置>>系统路由，可查看当前的系统路由表，如下图。

9.3 IP 地址分配

9.3.1 DHCP 服务

DHCP 服务器能够自动给局域网中的设备分配 IP 地址。

进入页面：网络设置 >> IP 地址分配 >> DHCP 服务，可选择仅为 AP 分配 IP 地址或为 AP 和用户终端分配 IP 地址，选择完成后点击<设置>，如下图。

在“DHCP 服务列表”，点击<新增>，填入配置信息后，点击<确定>应用配置，如下图。

DHCP 服务器	网关的 DHCP 服务器默认开启。 若网络中已经有其他的 DHCP 服务器需要关闭该路由器的 DHCP 服务器，请禁用该条目；
开始/结束地址	设置 IP 地址池，DHCP 服务器开启状态下，路由器自动从地址池（默认为 192.168.1.2~192.168.1.254）中给局域网中的设备分配 IP 地址。

9.3.2 客户端列表

进入页面：网络设置 >> IP 地址分配 >> 客户端列表，可查看 DHCP 的客户端相关信息，如下图。

服务接口	客户端主机所属的服务接口。
主机名	通过 DHCP 获得 IP 地址的主机的名称，可用于识别不同的接入设备。
MAC 地址	分配到 IP 地址的客户端主机的 MAC 地址。
IP 地址	DHCP 服务器分配给客户端主机的 IP 地址。
剩余租期	DHCP 服务器所分配 IP 地址的剩余有效使用时间，超时将重新分配。

9.3.3 静态地址分配

可根据接入设备的 MAC 地址手动分配 IP 地址。当对应的客户端设备请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将自动为其分配指定的 IP 地址。

进入页面：网络设置 >> IP 地址分配 >> 静态地址分配。点击<新增>，输入对应的 MAC 地址和 IP 地址，点击<确定>。

9.3.4 DHCPv6 服务

进入页面：网络设置 >> IP 地址分配 >> DHCPv6 服务，可选择仅为 AP 分配 IP 地址或为 AP 和用户终端分配 IP 地址，选择完成后点击<设置>，如下图。

在“DHCPv6 服务列表”，点击<新增>，填入配置信息后，点击<确定>应用配置，如下图。

DHCP 服务器	网关的 DHCP 服务器默认开启。 若网络中已经有其他的 DHCP 服务器需要关闭该路由器的 DHCP 服务器，请选择关，并点击保存；
开始/结束地址	设置 IP 地址池，DHCP 服务器开启状态下，路由器自动从地址池中给局域网中的设备分配 IP 地址。

9.3.5 SLAAC

SLAAC（Stateless address autoconfiguration），无状态地址自动配置，网关为客户端指定网络前缀和前缀长度，客户端使用前缀和前缀长度自行创建 IPv6 地址。当部分客户端设备不支持 DHCPv6 服务器时，可选择使用 SLAAC。使用前请开启 IPv6 功能。

进入页面：网络设置 >> IP 地址分配 >> SLAAC。点击<新增>，选择 DNS 配置方式。配置完成后，点击<确定>，如下图。

9.3.6 IPv6 客户端列表

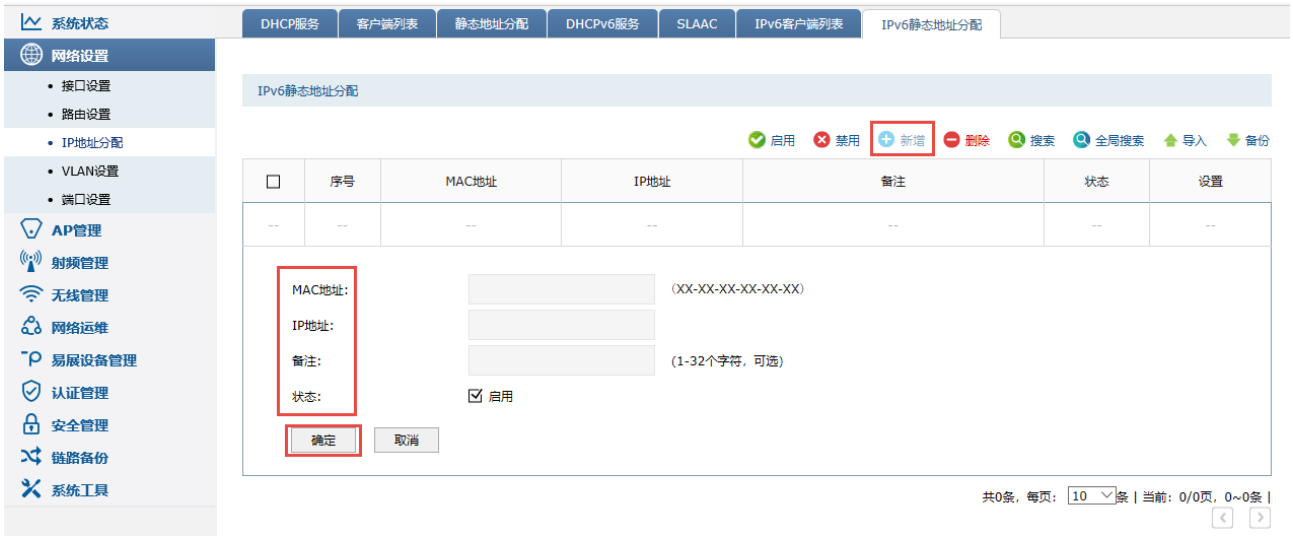
客户端列表显示已由 DHCP 分配 IP 参数的客户端信息。

进入页面：网络设置 >>IP 地址分配设置 >>IPv6 客户端列表。点击<刷新>，可获取最新列表信息，如下图。

9.3.7 IPv6 静态地址分配

可根据接入设备的 MAC 地址手动分配 IP 地址。当对应的客户端设备请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将自动为其分配指定的 IP 地址。

进入页面：网络设置 >>IP 地址分配 >>IPv6 静态地址分配。点击<新增>，输入对应的 MAC 地址和 IP 地址，点击<确定>，如下图。

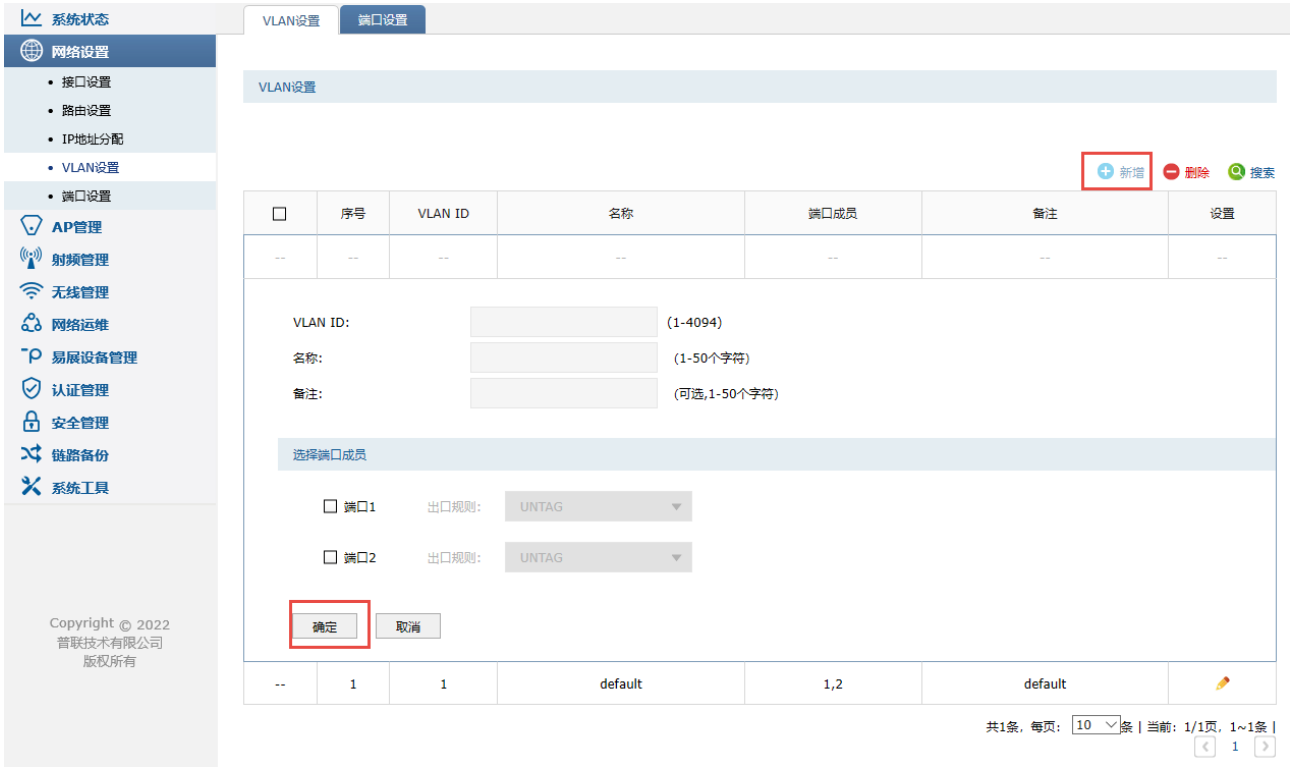


9.4 VLAN 设置

9.4.1 VLAN 设置

通过 VLAN 设置页面可以设置和查看 802.1Q VLAN 条目。802.1Q VLAN 是基于 IEEE 802.1Q 协议的 VLAN 划分方法，它使用 VLAN ID(VID)来区分不同的 VLAN，所有属于同一 VLAN 的数据帧均限制在该 VLAN 中传播。

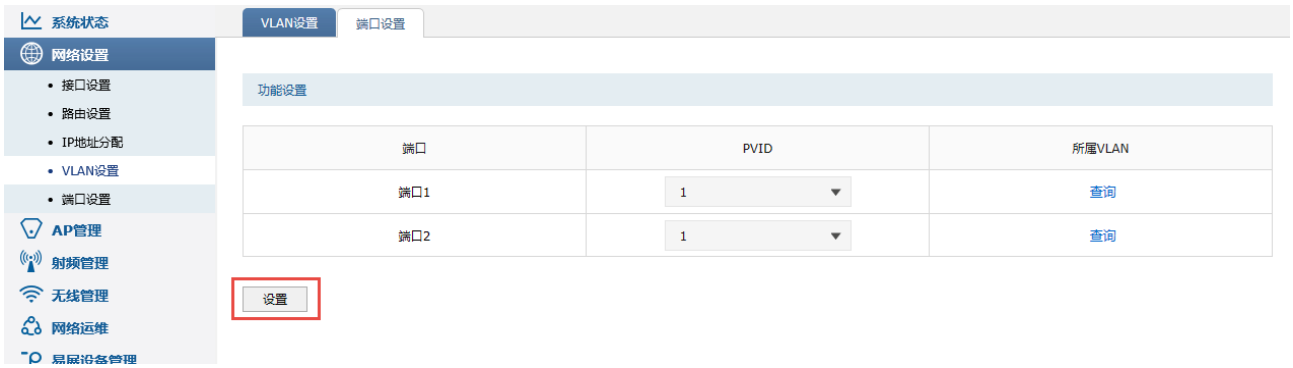
进入页面：网络设置 >> VLAN 设置，可将端口加入不同的 VLAN，完成设置后点击<确定>，如下图。



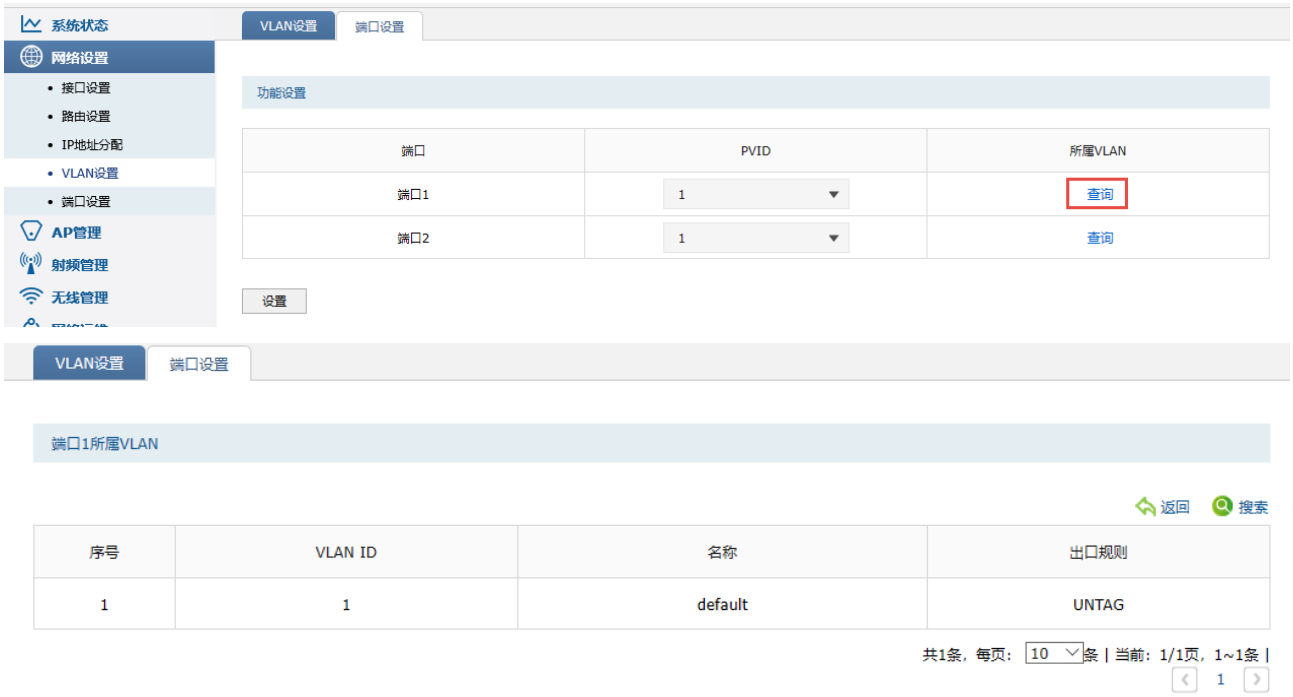
端口成员	显示 VLAN 的端口成员，带't'标识表示该端口的出口规则为 TAG。
出口规则	选择 VLAN 端口成员的出口规则：TAG 表示输出的数据帧带有 tag 信息；UNTAG 表示输出的数据帧不带 tag 信息。

9.4.2 端口设置

进入页面：网络设置 >> VLAN 设置 >> 端口设置，设置和查看端口的 PVID，选择完成后点击<设置>，如下图。



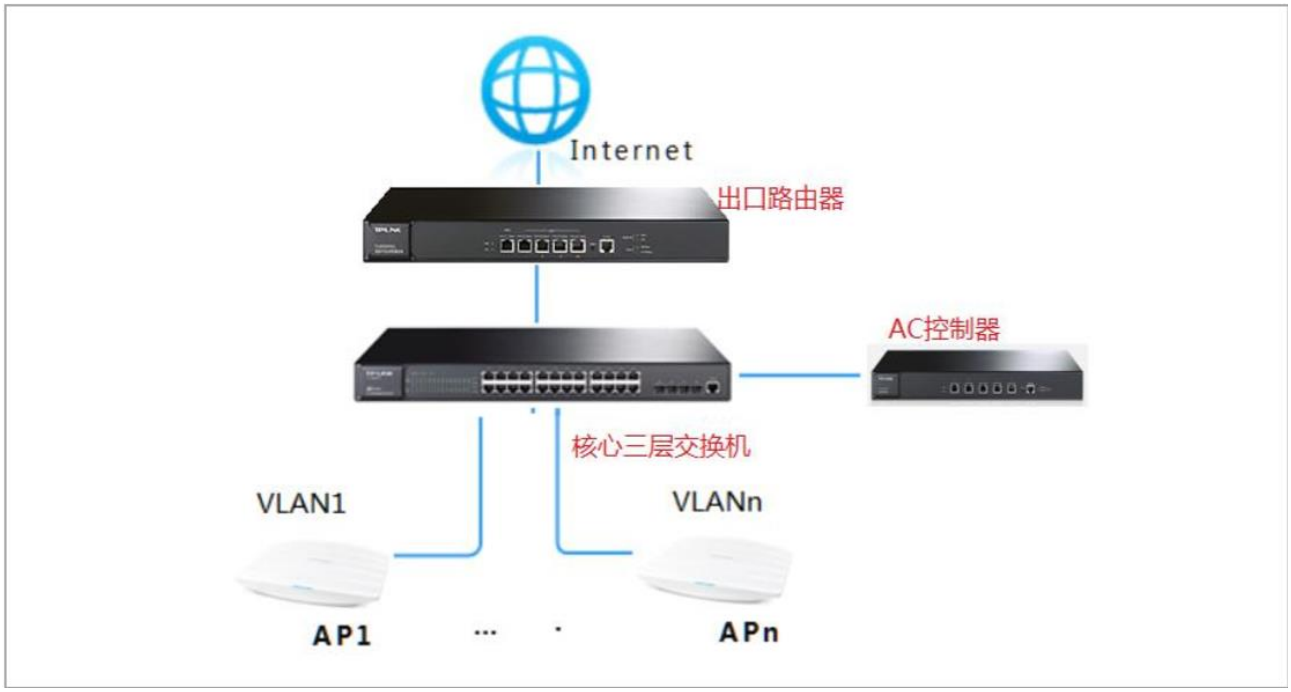
点击端口所属 VLAN 下的<查询>按键，即可查询端口的具体 VLAN 信息，如下图。



9.4.3 VLAN 配置实例

需求介绍：

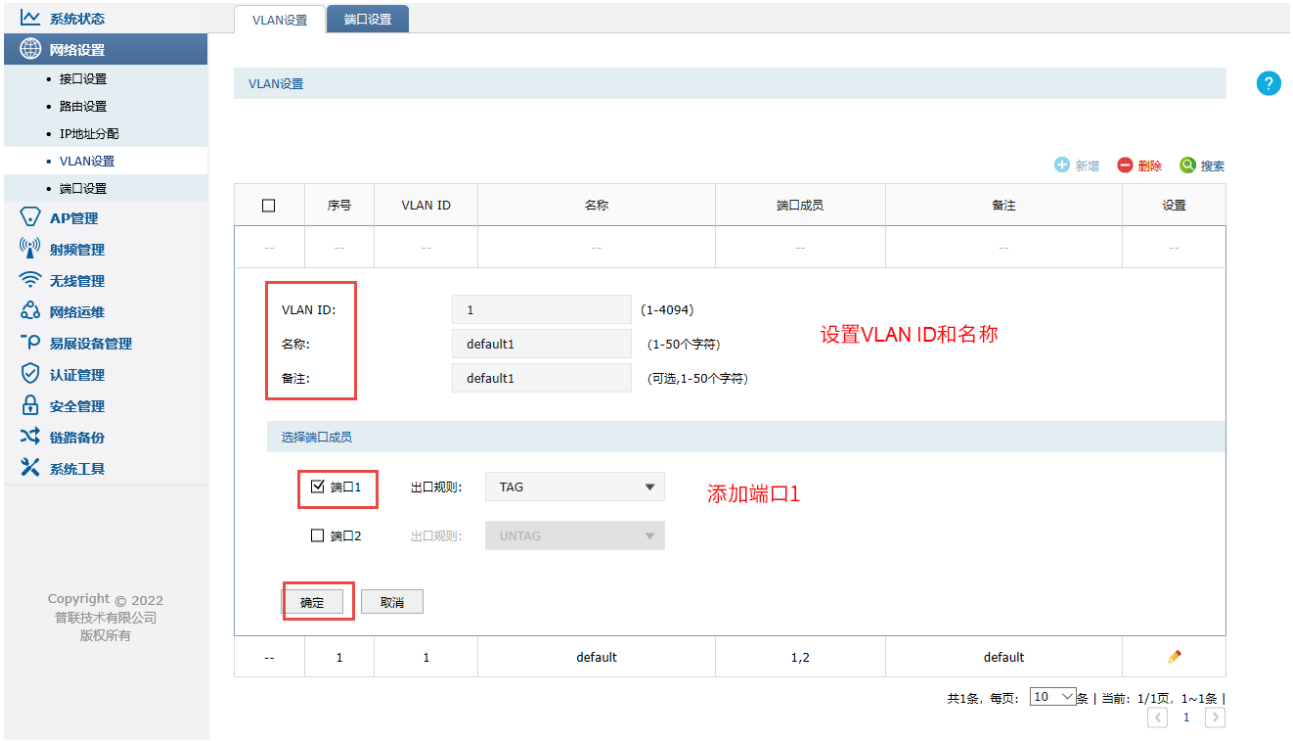
大型网络环境中，使用三层交换机将网络分为多个不同的网段。这种情况下，AC 控制器与 AP 如果处于不同网段，则需要跨三层交换机进行管理。



配置步骤：

将 AC 的连接到核心交换机的有线接口加入到 AP 所在的 VLAN，假设 AC 的管理 IP 为 192.168.1.254，如下图所示（本例中在 VLAN1、2 中有需要管理的 AP）：

1. 进入页面：网络设置 >> VLAN 设置，点击<新增>，将 AC 连接到核心交换机的有线接口（本例使用 AC 的端口 1），选择完成后点击<确定>，如下图。



2. 重复以上设置将 AC 的端口 1 加入到 VLAN2 中。

3. 将 AC 连接到核心交换机中，核心交换机连接 AC 的接口类型需要为 TRUNK 接口，且该接口需要加入到所有 AP 所在的 VLAN 中。做了以上配置 AC 即可实现跨三层交换机发现不同VLAN中的AP。

9.5 端口设置

9.5.1 端口监控

端口监控有下面三种监控模式：

- 输出输入监控：流入流出被监控端口的数据帧将被复制到监控端口。
- 输入监控：流入被监控端口的数据帧将被复制到监控端口。
- 输出监控：流出被监控端口的数据帧将被复制到监控端口

进入页面：网络设置 >> 端口设置 >> 端口监控，可开启端口监控功能，选择监控端口和被监控端口，完成后点击<设置>，如下图。

注意：

- 一个端口不能同时作为监控端口和被监控端口。
- 只能设置一个监控端口。

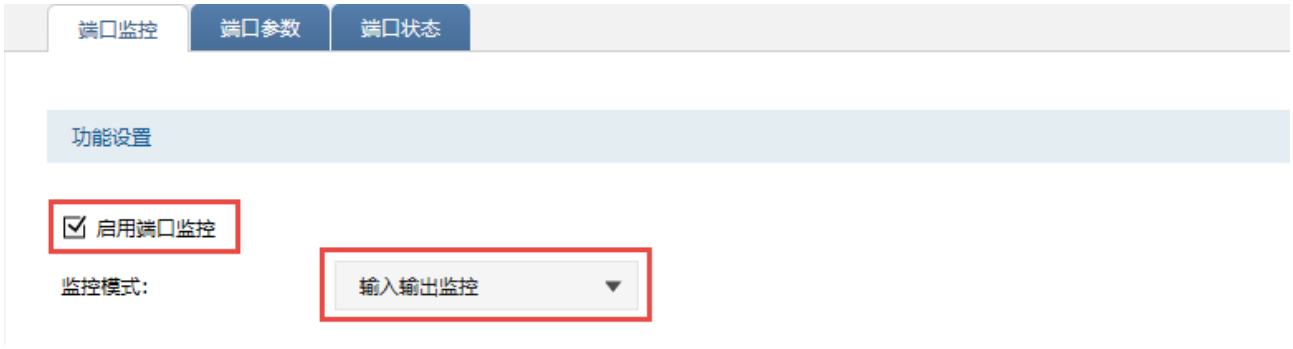
9.5.2 端口监控配置实例

需求介绍：

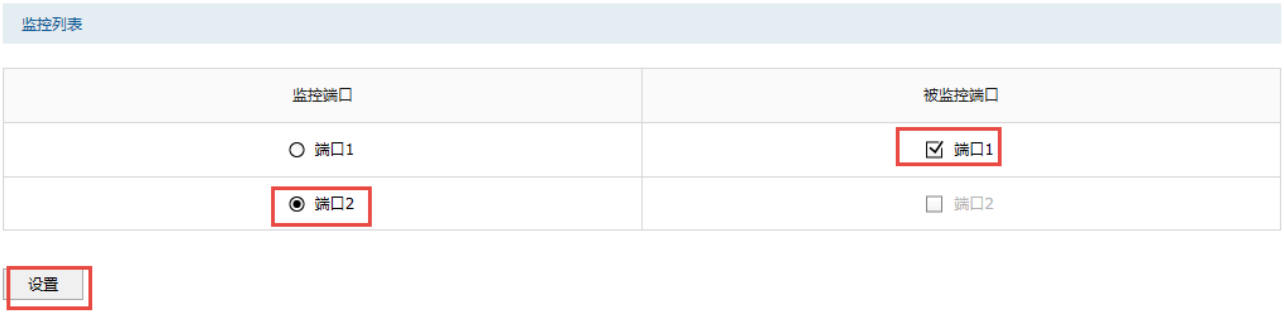
现需要对无线控制器的端口 1 中输入输出数据进行监控，将其复制到监控端口 2。

配置步骤：

1. 进入端口设置 >> 端口监控，启用“启用端口监控”，选择监控模式为 “输入输出监控”。



2. 选择端口 2 为监控端口，端口 1 为被监控端口，点击<设置>

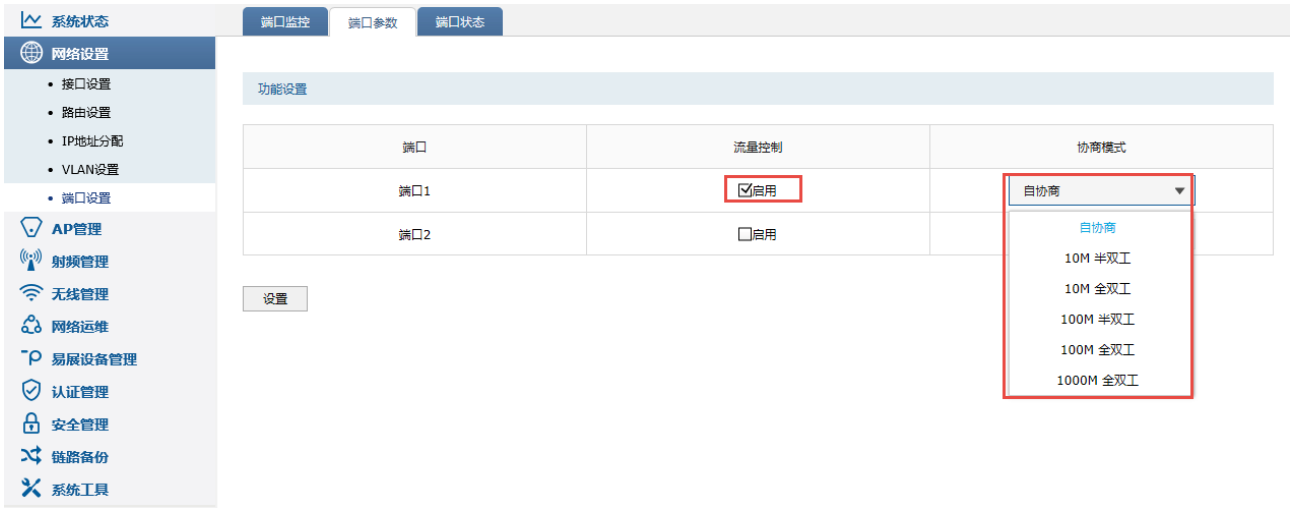


注意：

设置过多被监控端口可能造成网络不稳定，网络中流量较大时不建议一次性设置过多被监控端口。

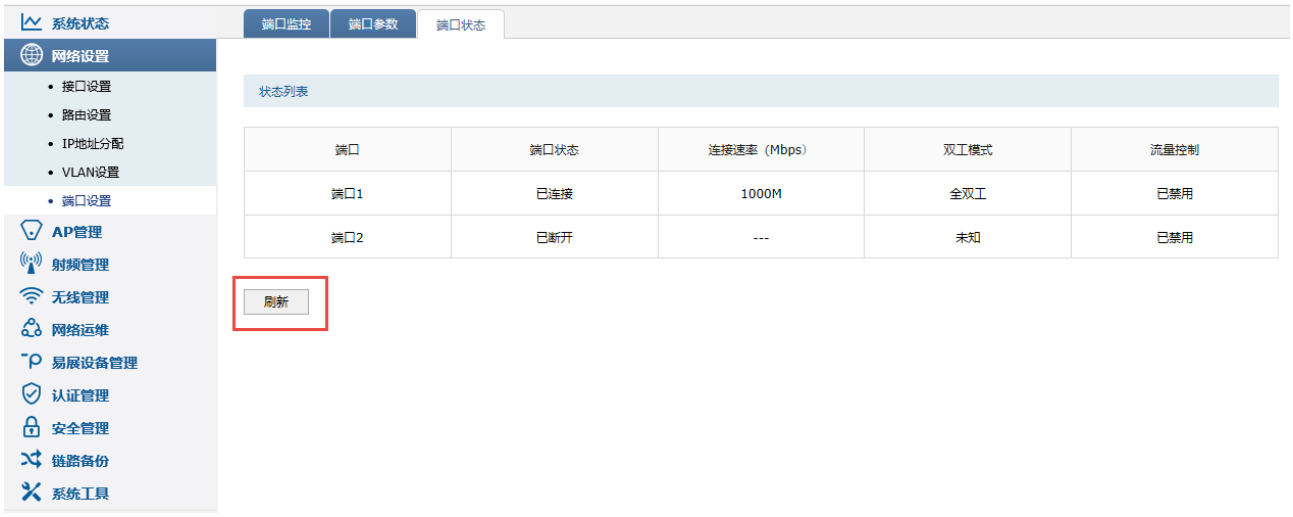
9.5.3 端口参数

进入页面：网络设置 >> 端口设置 >> 端口参数，可设置各个端口是否开启流量控制和协商模式，完成后点击<设置>，如下图。



9.5.4 端口状态

进入页面：网络设置 >> 端口设置 >> 端口状态，点击<刷新>，可查看当前各个端口的最新工作状态，如下图。

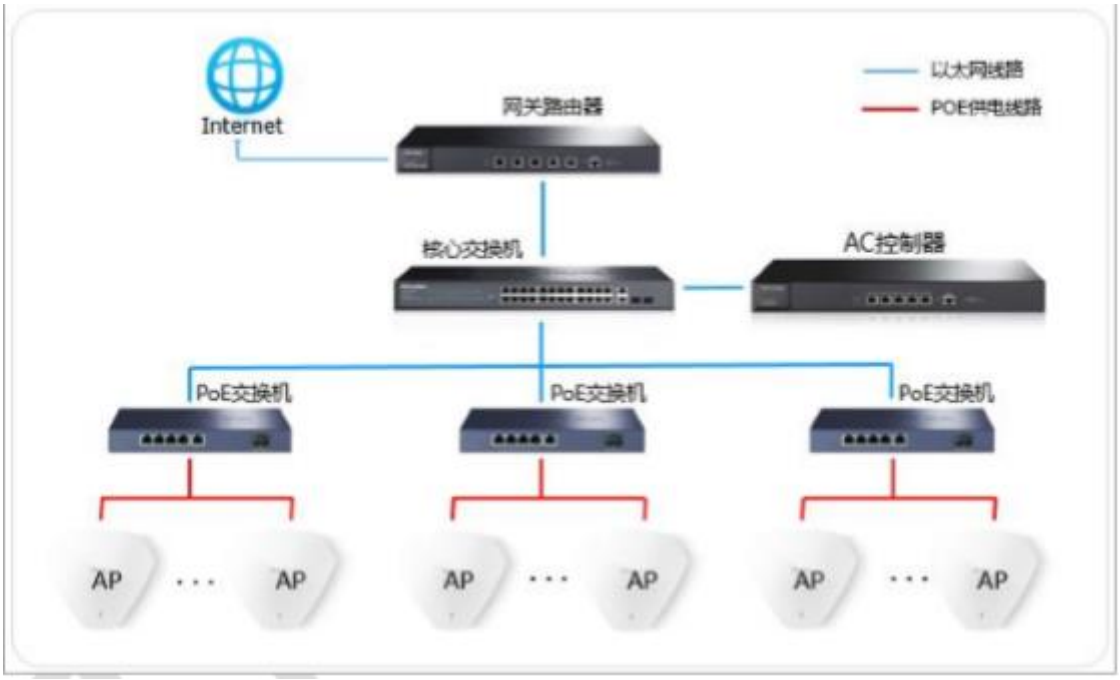


第10章 AP 管理

10.1 AP 管理

10.1.1 AP 设置

AC 控制器能自动发现所有工作在瘦 AP（FIT AP）模式下的 TP-LINK AP，并对 AP 进行统一配置和管理。



为了保证无线组网最基本的使用体验，就需要配置 AC 的 AP 管理功能，设置相应的 SSID 使用，并根据现场的环境条件设置 AP 的信道、功率等射频参数，防止互相干扰，保证无线网络的稳定性和流畅性。

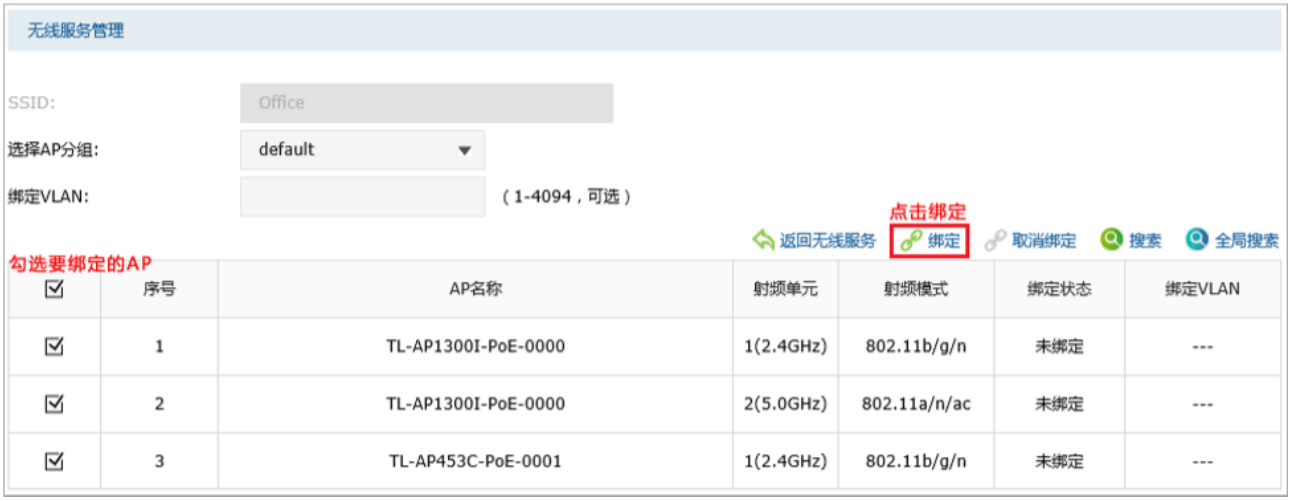
进入页面：AP 管理 >> AP 设置，可对 AP 进行全局设置和分组管理。

➢ AP 管理设置

1. 登录到 AC 界面，进入页面：无线管理 >> 无线服务，点击<新增>，设置无线网络，如下图：

2. 无线网络新增成功后，点击无线服务列表的射频绑定

选中要绑定该无线网络名称的 AP 射频，点击<绑定>，将该无线网络绑定到 AP。



若要为 AP 配置多个无线网络，也按照同样的方法进行步骤 1、2 的操作。

3. 射频设置包括频段带宽、信道等参数的设置。进入页面：射频管理 >> 射频设置，在射频列表中点击

对应的 AP 进行编辑。

4. 进入页面：射频管理 >> 频谱导航，启用频谱导航，如下图：

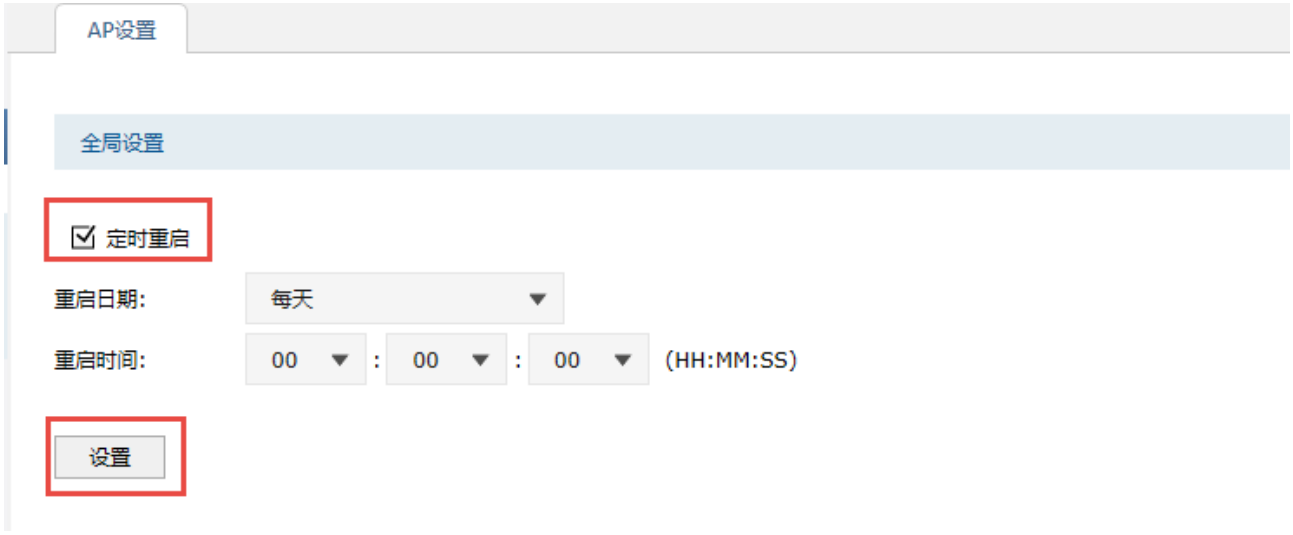
频谱导航的目的是为了将用户优先导向 5G 射频，并实现 5G 和 2.4G 射频负载均衡。

启用频谱导航时，请确认 2.4GHz 和 5GHz 的 SSID 设置相同。启用后，终端将优先连接 5G 信号。

5. 进入页面：射频管理 >> 射频管理 >> 射频调优，启用射频调优功能。

➢ 全局设置

选择<定时重启>功能，选择重启日期和重启时间，点击<设置>，即可在达到设定时间时重启所有接入的 AP，如下图。



➢ 分组管理

在分组列表一栏可以对 AP 进行分组管理，查看分组列表信息如下图。

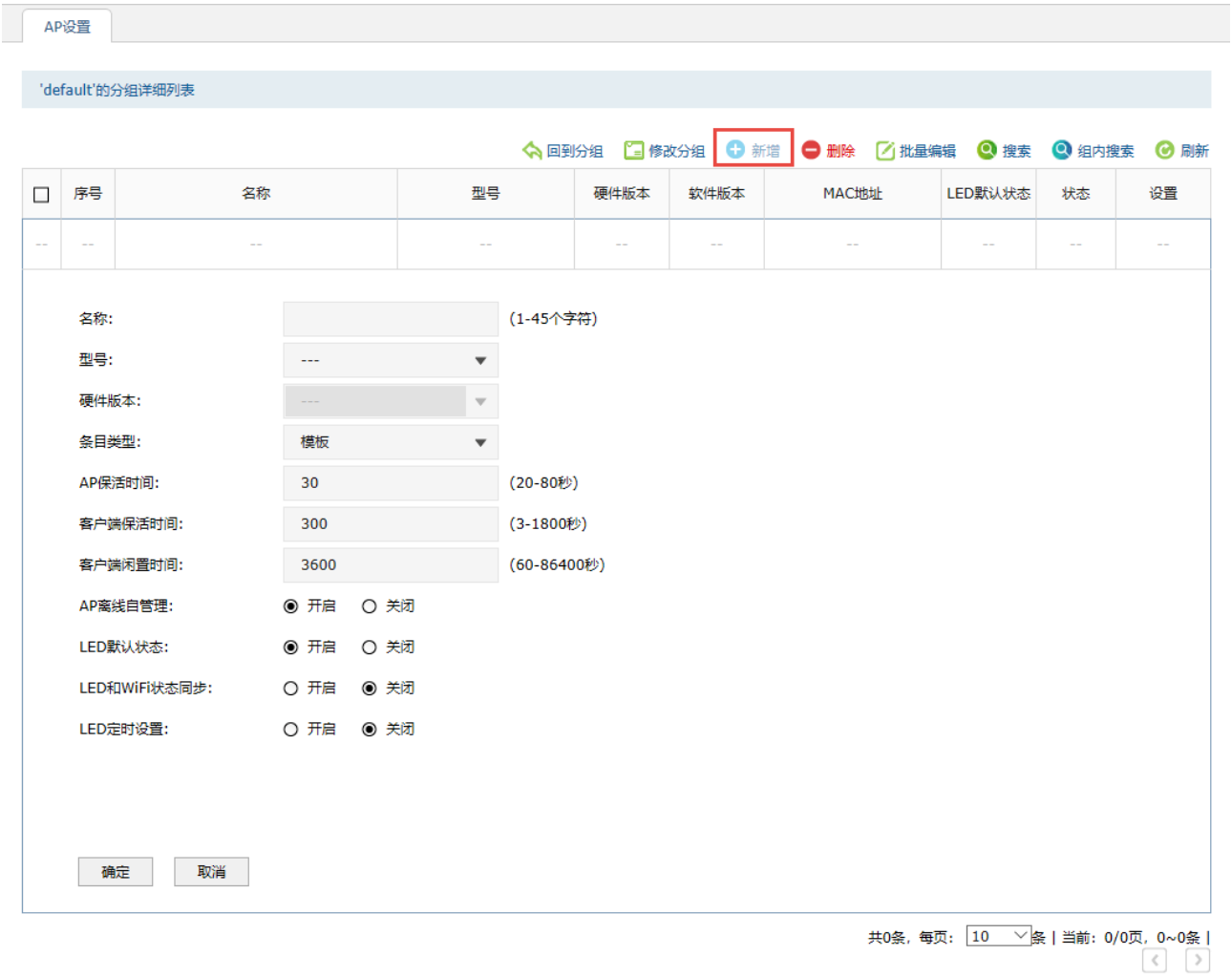
分组中的表项分为 AP 模板和 AP 条目两种类型，以下分别进行说明。

- AP 条目：用于对 AP 进行参数设置和管理。当一个 AP 接入之后，就会创建与其对应的 AP 条目，除非用户手动删除，否则一直存在，能够进行修改配置、修改分组、修改对应射频口配置和绑定无线服务等操作。
- AP 模板：用于设定某种硬件型号的 AP 的参数默认值，一种型号的 AP 只允许创建一个模板。当 AP 接入时，如果存在与其硬件型号匹配的 AP 模板，就会以其中的参数为默认值生成 AP 条目，且生成的 AP 条目位于模板所在的分组。AP 模板名称后会加注“(模板)”字样。

分组名称	默认分组的名称后会加注“（默认分组）”字样。不允许删除默认分组或非空分组。
分组统计信息	形如"X/Y, Z"，X 表示已经成功接入的 AP 数目，Y 表示分组中所有的 AP 数目，Z 表示分组中的模板数量。点击可以进入分组详细列表。

点击<导入>，以通过合法的 ANSI 编码格式的 CSV 文件来一次性修改多个 AP 条目；点击<备份>，可以备份所有的 AP 条目至 ANSI 编码格式的 CSV 文件中，如下图。

点击分组统计信息栏目下的信息，以查看并管理 AP 条目和 AP 模板，点击<新增>，可新增 AP 条目，如下图。



名称　　新 AP 接入时产生的 AP 条目的名称格式为'X-NNNN' (X 为型号名或匹配的模板名，N 为数字且四位数字唯一)。对于 HDAP1800C-PoE 1.0 类型的 AP，其内部的两台 AP 会自动在名称末尾添加后缀名以进行区分，且后缀名不可编辑。当修改 HDAP1800C-PoE 1.0 内部的某一台 AP 名称时，其修改也会同步到另一台 AP 上。

型号　　AP 的硬件型号。

MAC 地址　　AP 的 MAC 地址。不允许出现两条具有相同 MAC 地址的 AP 条目。

MAC 地址 2　　HDAP1800C-PoE 1.0 的特有属性。HDAP1800C-PoE 1.0 内部的右侧 AP 的 MAC 地址，其大小固定为"MAC 地址+2",仅在配置 HDAP1800C-PoE 1.0 类型的条目时显示。

LED 默认状态	设置 AP 接入时的 LED 指示灯的初始状态。修改该配置项，不会影响 AP 当前的 LED 状态。如果想操作 AP 当前的 LED 状态，请前往“AP 状态”页面进行设置。
AP 保活时间	AP 与 AC 之间采用保活机制来确认隧道是否正常工作。正常情况下，AP 周期性发送回声请求（Echo Request）报文给 AC，AC 收到后发送回声应答（Echo Response）报文给 AP。如果 AC 在本端的 6 倍保活时间内没有收到回声请求，或者 AP 在自己的 6 倍保活时间内没有收到 AC 的回声应答，则 AC/AP 会主动断开连接。
客户端保活时间	客户端保活机制用于检测客户端的异常下线。正常情况下，客户端下线时会向 AC 发送解关联报文,AC 收到之后就会删除客户端信息。如果客户端由于电源故障等原因异常下线就无法通知 AC,客户端的信息就会残留在 AC 的内存中，降低 AC 性能。因此，AP 会主动探测客户端是否存在，如果在保活时间内没有收到客户端的回复，就会通知 AC 删除客户端信息。
客户端闲置时间	AP 与客户端之间连接允许的最大闲置时间。如果 AP 在闲置时间内没有收到来自客户端的数据，那么该客户端将被删除。
有线 LAN 口 VLAN ID	设置 AP 额外有线 LAN 口的 VLAN ID，空表示不设置。只有具备额外有线 LAN 口的机型(如 TL-AP300I-PoE)才会显示该配置项。
AP 离线自管理	启用后，即使该 AP 与 AC 的连接中断也仍然可以接受新客户端的接入请求，但是该 AP 上配置的所有 Portal 认证条目将会失效。

AP 端口汇聚	将 AP 的多个物理端口绑定为一个逻辑端口来工作，以提高带宽。只有支持此功能的机型才会显示该选项。HDAP1800C-PoE 1.0 类型的机型在后缀名为"_01"的 AP 中显示。
LED 和 WiFi 状态同步	启用后，开启/关闭 LED 将会同时开启/关闭 AP 的 WiFi。
LED 定时设置	设置定时开启/关闭 LED 的功能。开启定时 LED 功能后，将以定时关闭/开启时间确定 AP 接入后的 LED 指示灯的初始状态，LED 默认状态配置将失效。

10.2 AP 升级

进入 AP 管理 >> AP 升级，可查看和配置各个 AP 的升级信息。

- AP 批量升级

一些大型项目的维护过程中，需要对无线 AP 进行升级维护，但是项目 AP 数量可能达到几十上百，一个一个升级费时费力，维护成本剧增，此时能够进行批量升级就尤为重要。不但可以提高效率，还可以避免升级出错。

在“AP 批量升级”栏目下，点击<新增>，选择 AP 分组及 AP 型号后，点击<确定>，即可对 AP 进行批量升级。若选择“定时升级”，则 AP 在指定时间进行升级，如下图。

➢ 单个 AP 升级

在“单个 AP 升级”栏目下，选择 AP 分组，可查看 AP 升级信息，如下图。

10.3 负载均衡

10.3.1 负载均衡

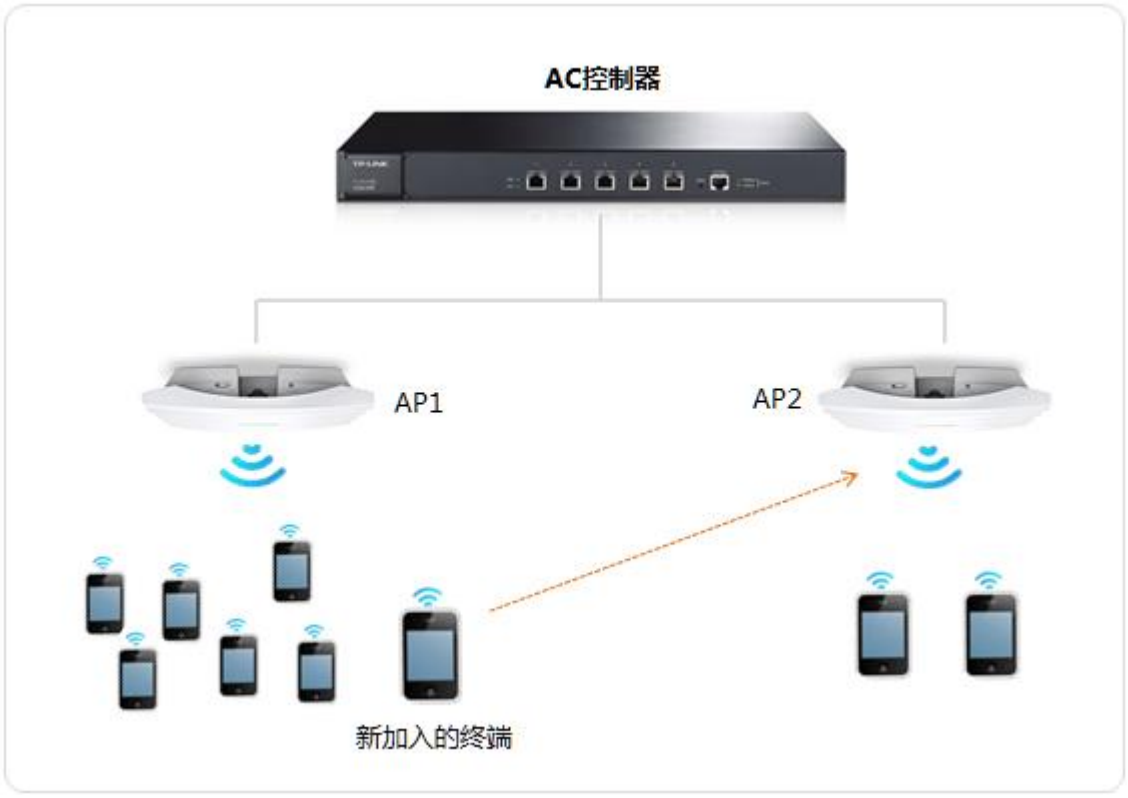
负载均衡功能可以准确的平衡 AP 的负载，确保终端有较好的无线网络的前提下尽可能合理的利用资源，实现该环境中无线终端的合理接入。

进入页面：AP 管理 >> 负载均衡，可开启/关闭负载均衡功能，如下图。

10.3.2 负载均衡配置实例

需求介绍：

在无线终端密集度较高的无线网络中，如酒吧、会议厅等环境，无线客户端物理位置分布可能不均匀，导致个别 AP 接入无线客户端数目过多，从而影响使用者的无线体验。



设置方法：

进入页面：AP 管理 >> 负载均衡，负载均衡开关选择“开启”，按照需求，门限可设置为 20（AP 接入终端的平均值），差值门限可设置为 4，最大失败测试设置为 3，即可实现 AP 客户端的负载均衡。

负载均衡模式　　默认为会话模式。

门限	当终端所要连接的 AP 挂载的终端数大于门限，负载均衡才有可能启动。当前连接的用户数量同时达到门限和差值门限，AP 才会启动负载均衡。
差值门限	当终端所要连接的 AP 挂载的终端数和至少一个终端覆盖到的其他 AP 挂载的终端数的差值大于差值门限，负载均衡才有可能启动。当前连接的用户数量同时达到门限和差值门限，AP 才会启动负载均衡。
最大失败次数	当用户想要连接到某个 AP，由于负载均衡，此 AP 拒绝这个用户的连接。当拒绝次数超过'最大失败次数'，则允许用户连接到此 AP。
RSSI 门限	忽略 RSSI 值低于 RSSI 门限的客户端。

10.4 智能漫游

10.4.1 智能漫游

智能漫游是无线控制器的一个功能模块，包括 802.11kvr、弱信号剔除、以及一些高级功能（漫游阈值检查周期、漫游差值、终端禁止接入时间、终端探测上报等等）。 通过配置智能漫游的相关参数可以保证终端漫游功能的使用体验。

智能漫游的条件：

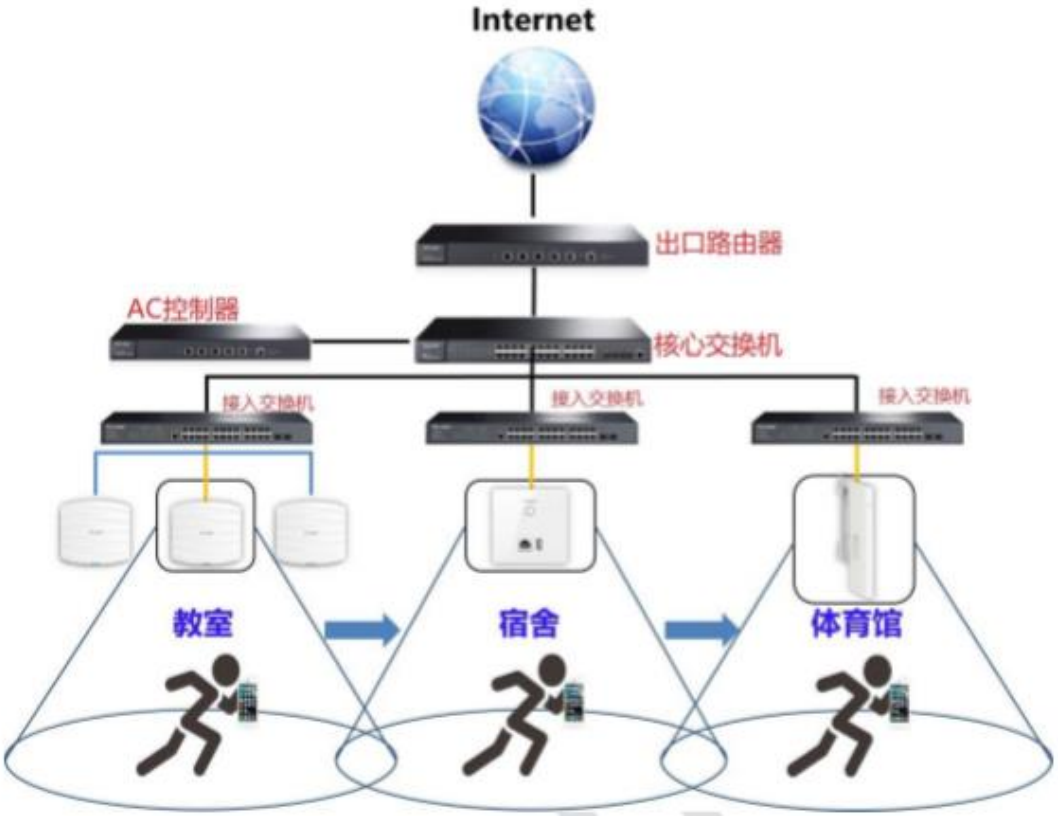
- 无线网络覆盖时多个 AP 都配置了相同的 SSID 和密码；
- 不同 AP 之间信号覆盖范围有一定的重叠；
- 无线终端在无线网络覆盖区域内移动。

进入页面：AP 管理 >> 智能漫游，可开启/关闭智能漫游功能，可选择 802.11k/802.11v/802.11r 快速漫游功能，如下图。

10.4.2 智能漫游配置实例

需求介绍：

随着手机、平板和电脑等终端的使用率日益增长，人们对无线的需求愈来愈大，对无线使用体验需求也愈来愈高，而无线漫游则是无线使用体验的重要组成部分。TP-LINK 为了让用户在使用无线网络时能够获取到更好的使用体验，特别推出无线控制器的智能漫游功能。



设置方法：

进入页面：AP 管理 >> 智能漫游，可开启/关闭智能漫游功能，可选择 802.11k/802.11v/802.11r 快速漫游功能，如下图。

检测漫游阈值类型	配置主动触发用户漫游的检测策略。基于信号强度：在信号强度低于阈值时触发终端漫游；基于速率：在终端速率低于阈值时触发终端漫游。同时启用时，只要满足其中一个条件，就会触发终端漫游。
触发漫游 RSSI 阈值	当终端的信号强度低于所设阈值时，将主动触发终端漫游。触发漫游 RSSI 阈值不能小于弱信号用户下线阈值。
弱信号用户下线	启用/禁用弱信号用户踢除功能，启用并设置踢除阈值，将在终端有更合适的目标 AP 可漫游，且信号强度低于设置的踢除阈值时，踢除终端，以迫使终端连接到体验更好的 AP 上。弱信号用户下线阈值不能大于触发漫游 RSSI 阈值。

触发漫游速率阈值	当终端速率低于所设阈值时，将主动触发终端漫游。终端速率是指终端和 AP 关联时，根据协议、信号强度等协商的速率能力，并非实际速率。假设 AP 能力集和终端能力集的交集对应的最大速率为 54Mbps，此时触发漫游速率阈值为 20%，则表示当终端的速率低于 54Mbps×20%=10.8Mbps 后，将触发终端漫游。触发漫游速率阈值不能小于低速率用户下线阈值。
低速率用户下线	启用/禁用低速率用户踢除功能，启用并设置踢除阈值，将在终端有更合适的目标 AP 可漫游，且速率低于设置的踢除阈值时，踢除终端，以迫使终端连接到体验更好的 AP 上。低速率用户下线阈值不能大于触发漫游速率阈值。
漫游阈值检查周期	检测终端 RSSI 或速率的时间间隔。
漫游差值	触发终端主动漫游的信号强度差值，只有当邻居 AP 的信号强度减去当前连接 AP 的信号强度大于漫游差值时，才建议终端进行主动漫游。
终端禁止接入时间	当触发终端进行主动漫游时，将在非漫游目标的 AP 上设置黑名单，在终端禁止接入时间范围内不让终端接入。
终端探测上报	开启时 AP 会探测周围终端信息并上报给 AC，AC 根据这些信息构建在线终端的 AP 邻居表，对不支持 802.11k 的终端漫游有辅助作用。

第11章 射频管理

11.1 射频设置

11.1.1 射频设置

本页面可以查看 AP 射频的主要参数，并通过按钮对相关射频参数进行编辑。

进入页面：射频管理 >> 射频设置。选择对应的 AP 进行编辑。

射频单元	显示/设置当前 AP 射频的射频单元。
射频模式	设置 AP 射频单元的工作模式。
频段带宽	当射频模式支持 11n、11ac 或者 11ax 时，设置频段带宽。
信道	设置 AP 射频单元工作的信道，如果设置为"自动"，AP 会自动选择一个合适的信道。若选择了 DFS 信道或 160M 带宽，AP 会进行大概一分钟的雷达探测，在此期间对应 AP 的 5G 无线功能无法使用。
动态信道切换（DCS）	当信道设置为"自动"时方可配置。可选项有自动、手动和关闭。自动模式会在当前信道环境较差时自动切换到最优信道（默认需处于无客户端连接状态才会切换）；手动模式点击"重选信道"按钮可立即切换到最优信道（无论是否有客户端连接）；关闭时不会自动切换信道。
客户端在线切换	当"动态信道切换"选择为"自动"时，勾选此项后，AP 在有客户端连接时也会立即执行动态信道切换，这将导致无线客户端断线重连，影响用户使用，请谨慎勾选！
检查周期	检查无线信道环境的周期。若发现当前信道环境较差，则在检查周期到达时会触发信道切换。
信道占用率门限	信道占用率门限值。超过该值即认为当前信道环境较差。
容限系数	信道质量提升的门限值。高于该门限才会真正切换到新信道。
发射功率	设置 AP 射频单元的最大发射功率。
客户端限制	设置 AP 射频单元关联客户端的最大数目。

无线客户端正向接入	无线客户端正向接入功能，用于引导客户端接入其正对方向的射频。比如四频 AP 中：1(2.4G)、2(5G)与 3(2.4G)、4(5G)互为正对方向的射频。
信号强度门限	AP 其中一个方向射频获取到客户端的信号强度弱于信号强度门限，无线客户端正向接入才有可能启用。当 AP 某一方向射频获取到客户端的信号强度满足信号强度门限和差值门限，该方向射频才会启动无线客户端正向接入。
差值门限	当 AP 其中一个方向射频获取到客户端的信号强度比其反方向射频获取到客户端的信号强度弱于差值门限时，无线客户端正向接入才有可能启用。当某一方向射频获取到客户端的信号强度满足信号强度门限和差值门限，该方向射频才会启动无线客户端正向接入。
天线	设置 AP 射频单元的天线模式。
分片门限	设置无线帧的分片门限。
beacon 间隔	设置发送信标帧的实际间隔，单位：TU(Time Unit)，1TU=1024 微秒。
管理帧速率	设置管理帧发送速率，以调整 Beacon 帧对无线资源的占用比例，单位为 Mbps。修改 Beacon 帧发送速率可能会影响 STA 的关联体验，建议谨慎使用。

Airtime 调度	启用或禁用 Airtime 调度算法。由于不同速率的用户传输相同的数据包占用信道的时间不一样，高速率的用户占用的时间少，而低速率的用户却占用了更多的时间，降低了 AP 的传输效率。启用 Airtime 调度功能，使不同传输速率的用户公平的占用信道时间，提高用户的上网体验。
RTS 门限	启用 RTS(Request To Send，要求发送)机制所要求的无线帧的长度门限值。当无线帧长度超过该门限值时，启用 RTS 机制。设置为 2347 表示关闭 RTS 功能。
DTIM 周期	设置信标的 DTIM 周期(Delivery Traffic Indication Message，数据待传指示信息)。
WMM	启用或禁用 WMM 功能。
响应广播探测	启用或禁用 AP 对客户端的广播探测请求。
Short GI	启用或禁用 Short GI 功能。
弱信号限制	启用或禁用弱信号禁止接入功能。

11.1.2 射频调优

TP-LINK AC/AP 的射频调优功能可以实现一键自动规划 AP 的信道和功率，调优过程 5 分钟内即可完成，智能减少 AP 之间的信号干扰。射频调优是通过动态信道分配（Dynamic Channel Assignment，DCA）和发射功率调整（Transmit Power Control，TPC）实现统一对 AP 的信道和功率进行规划，尽可能的提高覆盖率，减少整个系统的信道干扰，从而提高整个无线网络的上网体验。

射频调优的工作过程主要分为三个步骤，分别为收集邻居关系、动态信道调整、发射功率调整。

- 收集邻居关系

AC 下发收集邻居关系的命令后，所有 AP 工作在同一信道并周期性发送特定的报文，所有 AP 将监听到的邻居信息上报给 AC 进行后续处理。

➢ 动态信道调整

AC 根据收集到的邻居关系，通过 DCA 算法得到一个最优的 AP 信道划分结果，并将结果下发给所有的 AP。

➢ 发射功率调整

AC 根据邻居关系、动态信道调整的结果，通过 TPC 算法得到一个最优的 AP 功率划分结果，尽可能的提高覆盖率，同时减少整个系统的同信道干扰，并将结果下发给所有的 AP。

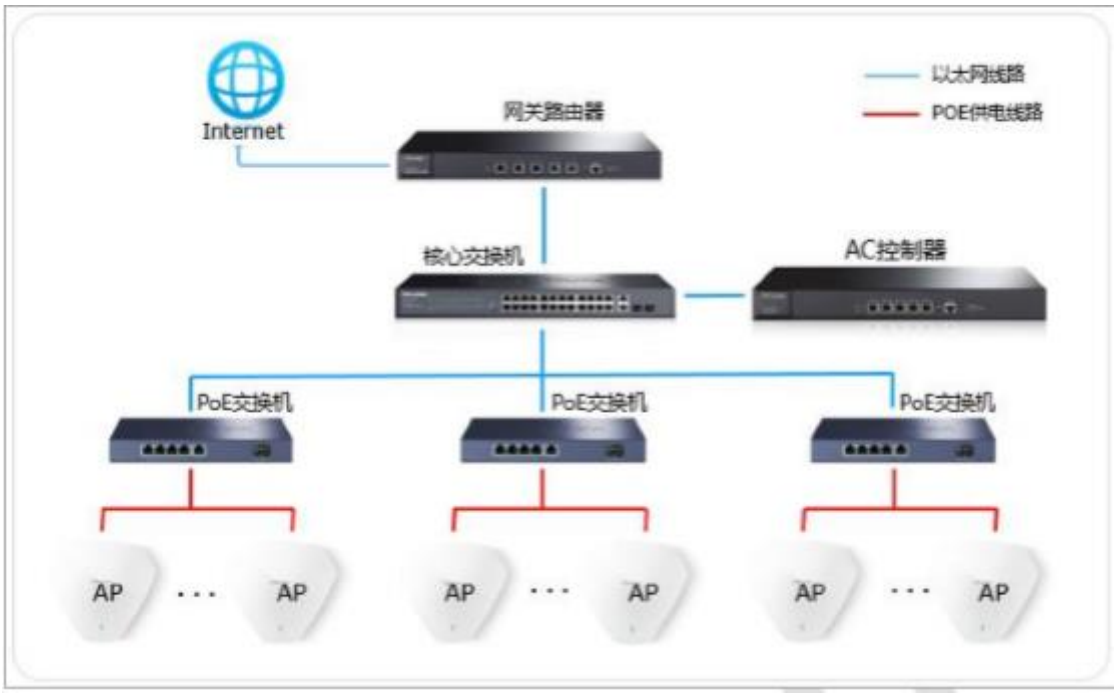
11.1.3 射频调优配置实例

- **需求介绍**

在一些酒吧、餐厅、宿舍等密集接入环境下，每个 AP 下都可能存在较大的无线流量，AP 与 AP 之间可能就存在较大的无线干扰，从而影响到整体网络的使用体验，典型的现象就是人少的时候网络很快，使用的人一多网络就慢了。使用 TP-LINK 的 AC 中的射频调优功能对网络的信道进行自动规划，功率进行自动调整，将网络中的干扰降到最小，保障无线使用的体验。

- **设置方法**

拓扑图：



➢ 信道调优

进入页面：射频管理 >> 射频调优。开启信道调优功能，2.4G 的频段带宽会统一设置为 20MHz，信道集合可以设置为 1/6/11 和 1/5/9/13；5G 的频段带宽可选设置为 20MHz 或 40MHz，信道集合可选设置为 36/44/149/157、40/48/153/161、36/48/149/161，如下图。

➢ 频率调优

可以设置覆盖的阈值、AP 的最大功率和最小功率，一般保持默认即可。

注意：

覆盖阈值：当开启功率调优时，对于 AP 的布放场景不同，AP 布放距离不同或 AP 布放高度不同，TPC 的覆盖阈值不同，实际使用时需要根据 AP 的实际布放调整 AP 的 TPC，以使 TPC 的结果能达到最优的覆盖效果。阈值越大，TPC 调整的功率值会整体提高。

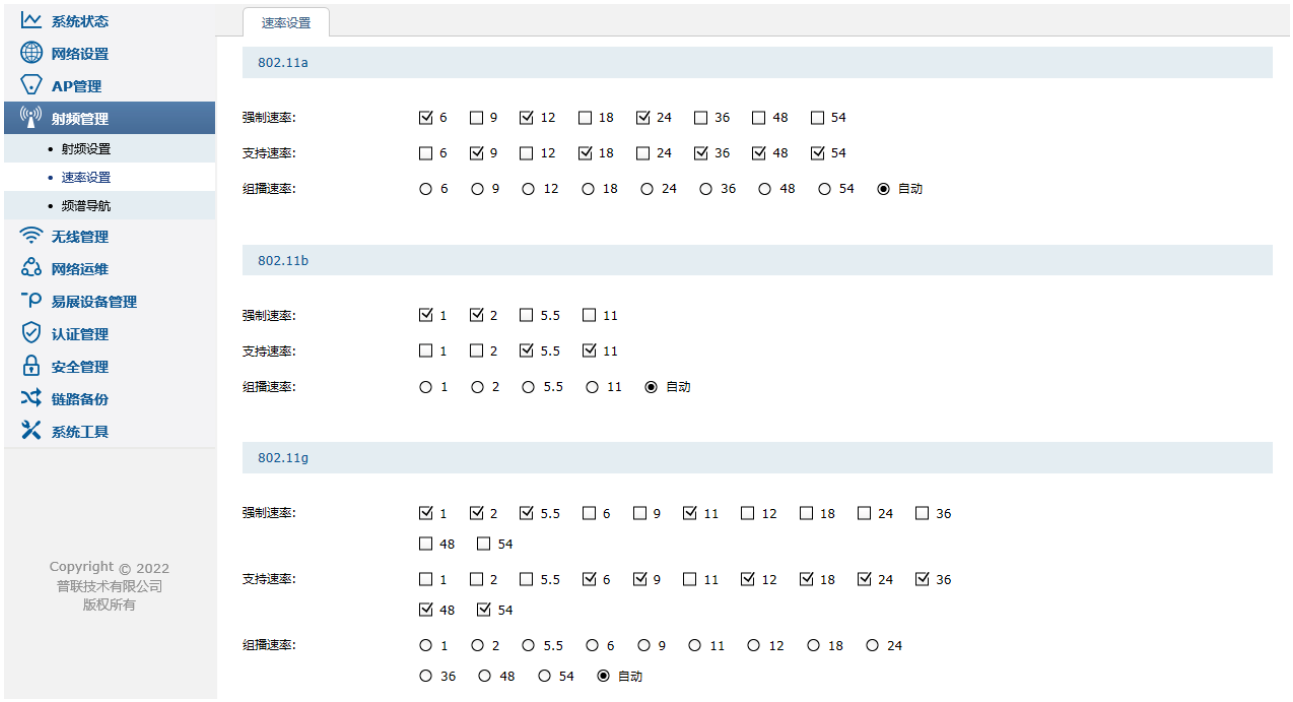
最大/最小功率：设置功率调优时，AP 允许调节的最大/最小功率。配置最大调优功率值和最小调优功率值后，AP 在进行功率调优后，最终生效的功率会在这两个值之间。

➢ 定时调优

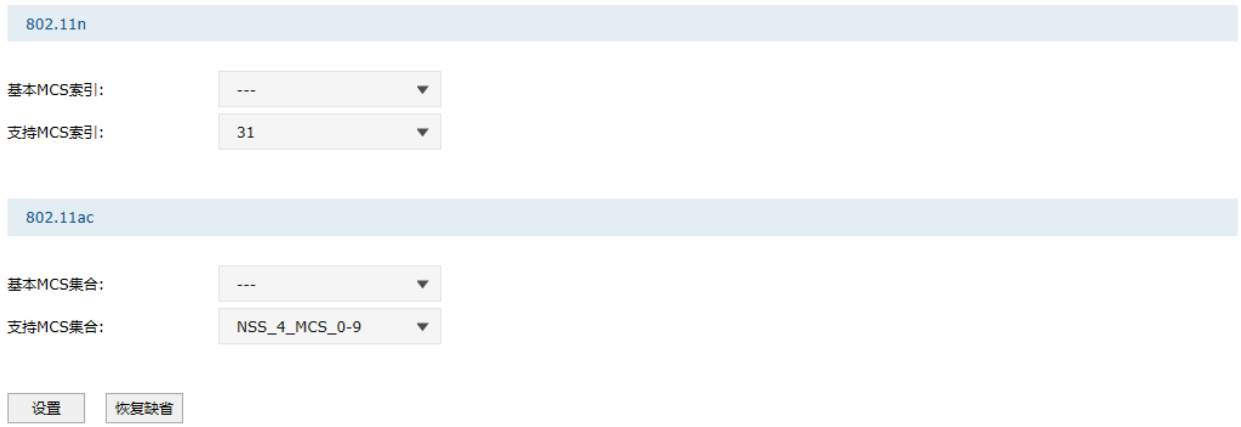
考虑到调优过程中 AP 会有最长 5min 无法正常使用，射频调优支持设置一个特定的时间进行定时调优，避免因为射频调优带来的断网影响。

11.2 速率设置

进入页面：射频管理 >> 速率设置，可以进行各个速率的设置，如下图。



强制速率	客户端允许接入无线网络的基本速率集合，集合中至少设置一种速率。
支持速率	扩展速率集合，该集合不能与强制速率集合有交集。
组播速率	用于发送多播报文的速率，该速率必须从强制速率集合中选取，设置为"自动"时，系统将自动从强制速率集合中选取。



基本 MCS 集合	客户端必须支持"基本 MCS 集合"对应的天线数和 MCS 索引范围，才能接入无线网络，缺省值为空。如果该值不为空，则非 11n/ac 客户端不能接入 AP。
支持 MCS 集合	扩展 MCS 集合，该集合对应的天线数和 MCS 索引范围不能小于"基本 MCS 集合"对应的天线数和 MCS 索引范围。

注意：

- 对于已接入无线控制器的 AP，如果开启了射频，需要重启 AP 或关闭再开启射频，设置的速率参数才会生效。
- 如果 11n 的 MCS 索引值大于 AP 支持的最大值，则该 AP 的 MCS 索引生效值即为该 AP 支持的最大 MCS 索引值。

11.3 频谱导航

进入页面：射频管理 >> 频谱导航，可以启用/禁用频谱导航功能。频谱导航功能可以将支持双频工作的客户端优先接入 5GHz 射频，使得两个频段上的客户端数量相对均衡，从而提高网络整体性能，如下图。

5G 频段连接门限	设定 AP 设备下允许连接到 5G 频段的最大客户端数目。 当 5G 频段连接门限条件和差值门限条件均满足时，将会拒绝客户端接入 5G 频段。
差值门限	设定 AP 设备下允许连接到 5G 频段和 2.4G 频段客户端数目的最大差值。 当 5G 频段连接门限条件和差值门限条件均满足时，将会拒绝客户端接入 5G 频段。
最大失败次数	设定客户端尝试连接的最大失败次数。 当被拒绝接入的客户端尝试连接 5G 频段的次数超过最大失败次数时，AP 将会允许客户端接入 5GHz 频段。

第12章 无线管理

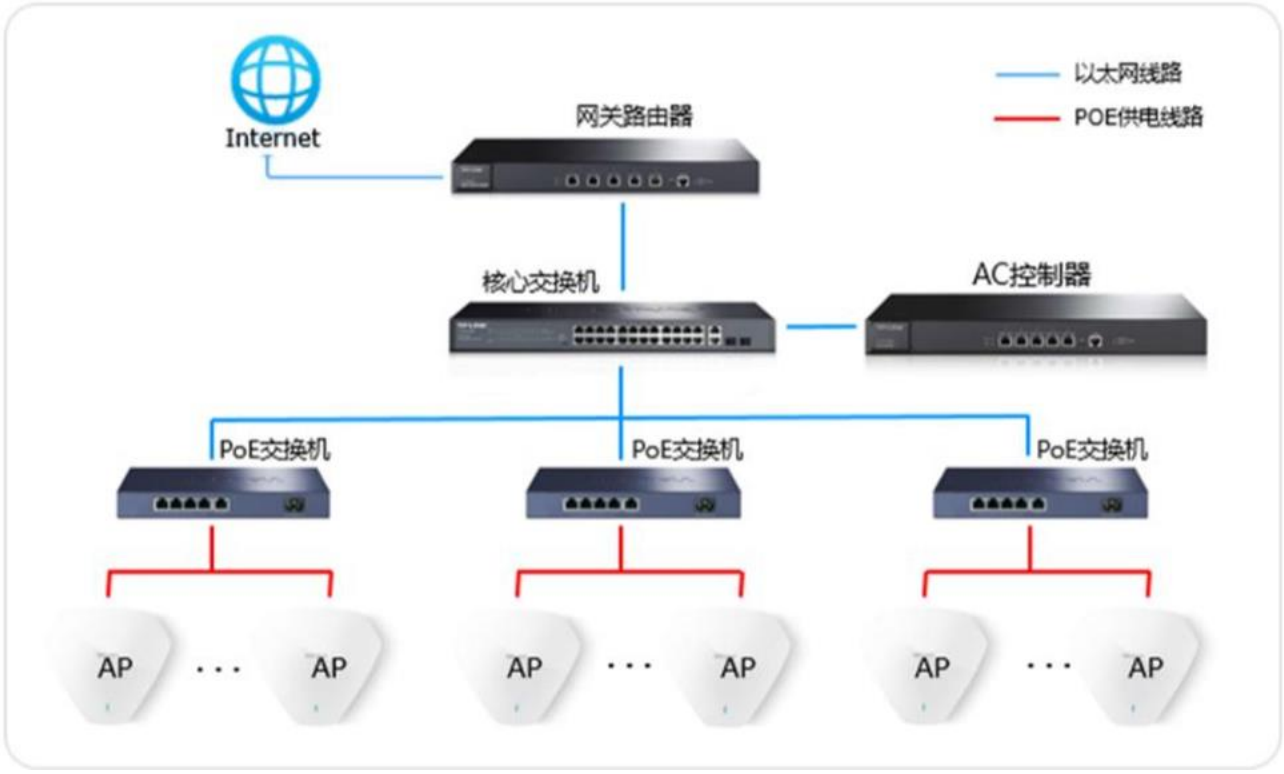
12.1 无线服务

本页面可以查看并设置连接到无线控制器上网络设备的无线参数。

12.2 无线服务配置实例

需求介绍：

某公司办公需要，要为无线控制器新增无线服务并设置自动绑定所有 AP，网络拓扑如下图所示。



设置方法：

➢ 新增无线设备

进入页面：无线管理 >> 无线服务，点击<新增>，可添加无线设备，如下图。

SSID	设置 SSID（Service Set Identifier，服务集识别码），SSID 的名称应该尽量具有唯一性。
无线网络内部隔离	启用无线网络内部隔离，选择此项可以使连接到同一个无线服务的主机之间不能互相通信。该功能不能跨 AP 生效。
组密钥更新周期	定时更新用于广播和组播的密钥的周期，不更新则为 0。
Radius 服务器 IP	进行身份认证的 Radius 服务器的 IP 地址。

控制模式	设置客户端带宽控制模式。共享模式：所有客户端均分共享带宽控制值；独占模式：所有客户端独占带宽控制值。

➢ 查看射频绑定参数

点击<>，可查看并修改无线设备的射频绑定参数，如下图

自动绑定	设置无线服务是否自动绑定 AP，包含之前已经接入的 AP 和之后新接入的 AP（开启此功能后手动绑定功能禁用）。
射频选择	自动绑定功能开启时，绑定的射频。
绑定 VLAN	自动绑定功能开启时，绑定的 VLAN。

第13章 网络运维

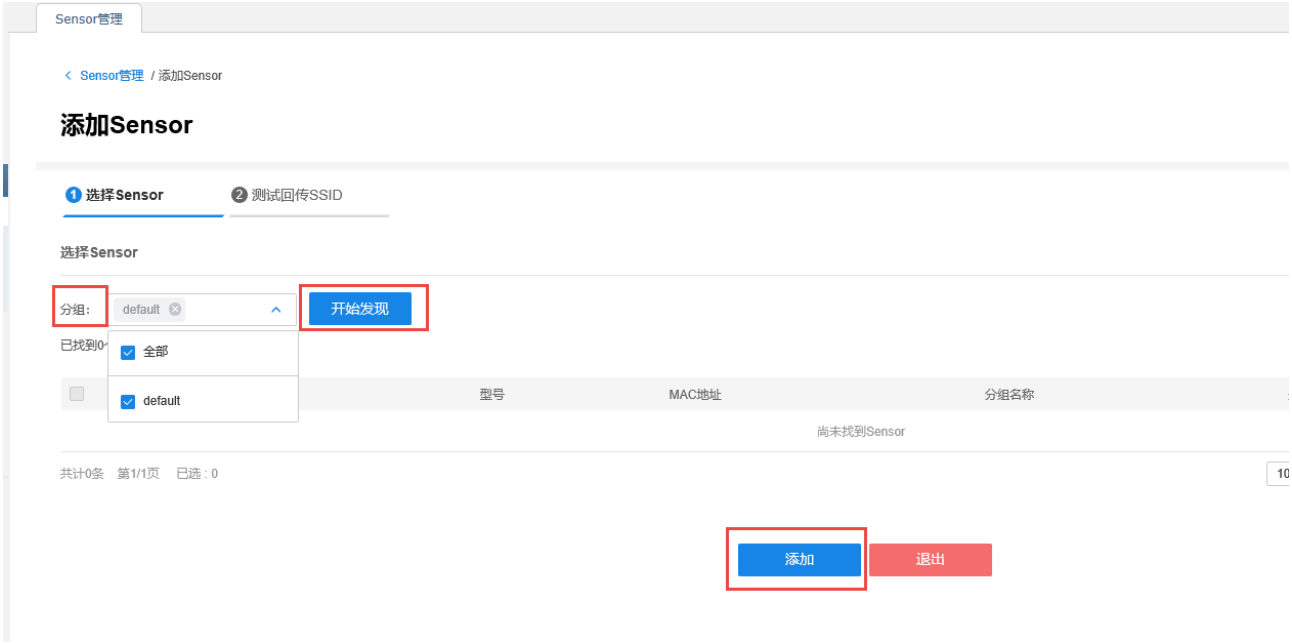
13.1 Sensor 管理

13.1.1 Sensor 管理

进入页面：网络运维 >> Sensor 管理，按以下步骤和对应操作提示进行 Sensor 添加和配置。

1. 设置回传无线服务（SSID），用于 Sensor 与 AP 之间的无线通信，使 Sensor 测试结果回传至 AC 统计显示。

2. 点击<添加 Sensor>，进入添加界面后，选择分组，点击<开始发现>，等待扫描并发现可添加的 Sensor，勾选需添加的 Sensor，点击<添加>。



3. 点击<测试回传 SSID>，此时将测试待添加的 Sensor 是否可正常通过所设置的回传无线服务（SSID）接入网络。

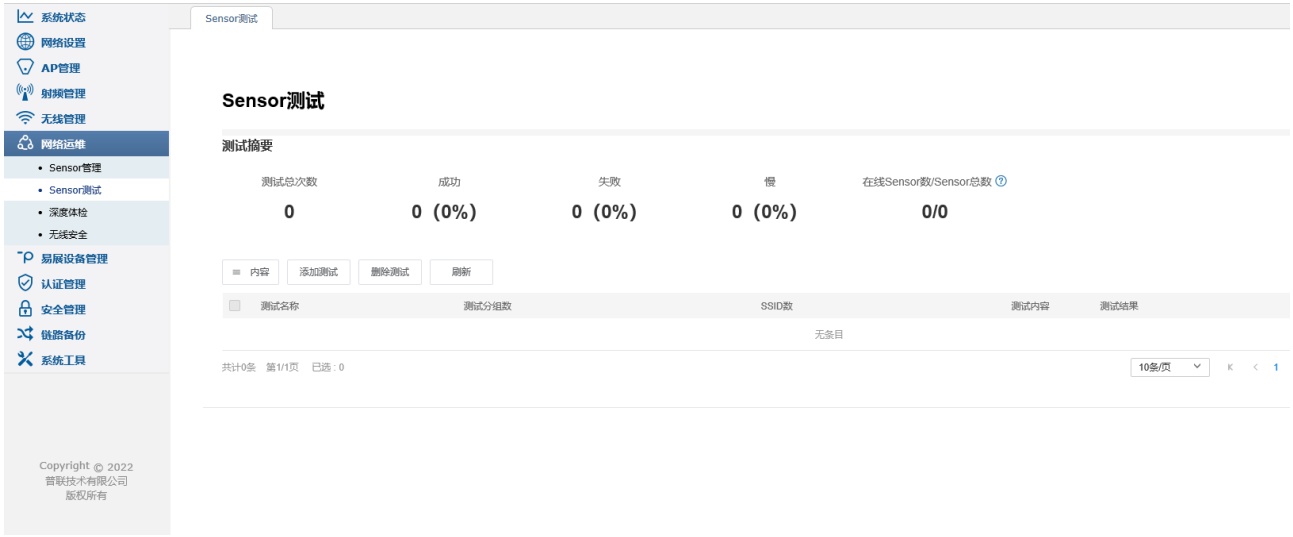
4. Sensor 成功接入网络后，设备指示灯由红色变为绿色，即可正常使用 Sensor 的各项应用功能。

回传无线服务设置	为当前 AC 管理下的所有无线接入点（AP）统一下发无线回传服务，用于 Sensor 设备与网络设备之间无线通信和测试数据回传。该配置会占用 AP 设备的一个无线服务条目。添加 Sensor 前请先配置回传无线服务。

13.2 Sensor 测试

13.2.1 Sensor 测试

进入页面：网络运维 >> Sensor 测试，本页面可以通过模拟终端上网行为，进行无线覆盖区域和网络设备上网行为及体验检测，包含终端上线测试、网络性能测试（延迟、网速）、网站访问、FTP 文件下载速率等测试。

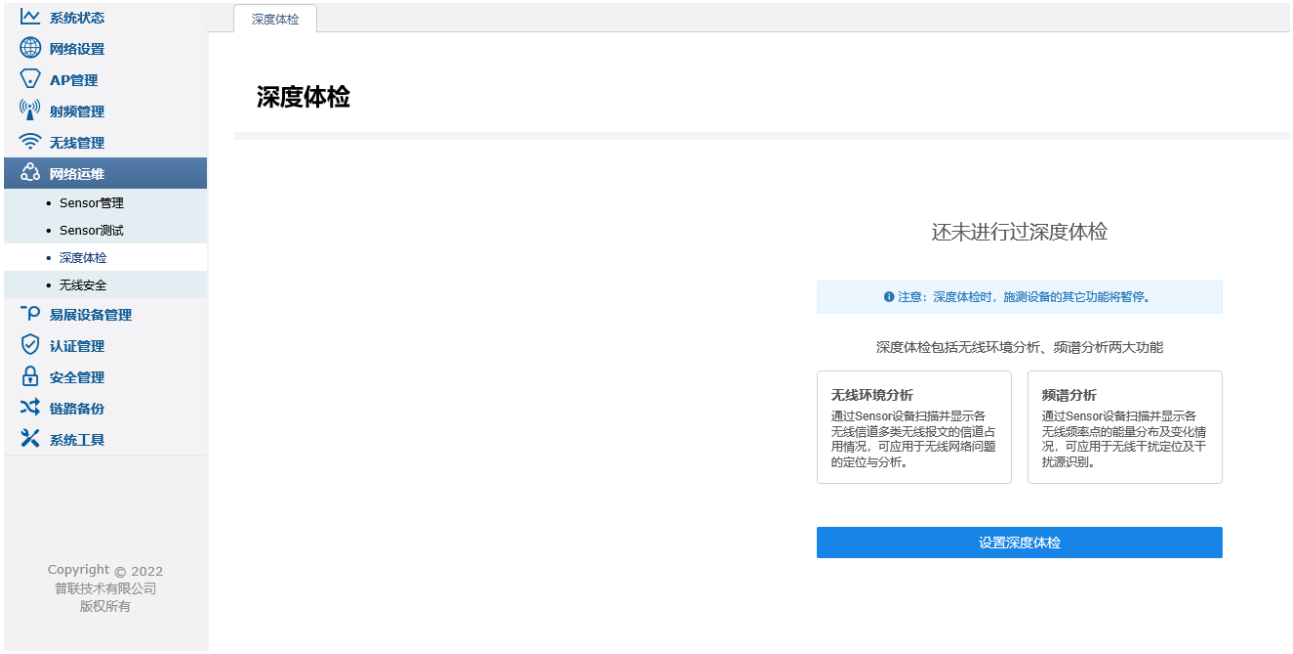


测试摘要	显示测试总次数、测试结果为成功/失败/慢的总次数以及参与测试的在线/所有 Sensor 总数。
内容	勾选显示 Sensor 测试列表页面显示项。
测试分组数	Sensor 测试对应的 AP 设备所在分组数量，点击数字可查看详细 AP 分组列表。
SSID 数	Sensor 测试的 SSID 数量，点击数字可查看测试的 SSID 列表。
测试内容	查看测试内容，如终端上线测试、DNS 测试、主机访问测试、radius 测试、网速测试、邮件测试、web 测试、FTP 测试等。
测试结果	点击对应测试点测试结果，可进入结果详情页。通过结果详情页，可查看测试结果概要以及测试详细结果。注意：测试过程中，当测试项涉及内容在其他页面被修改，如 AP 分组、所绑定的 SSID、AP 射频配置等，可能会导致测试异常或测试失败。

13.3 深度体检

13.3.1 深度体检

进入页面：网络运维 >> 深度体检，本界面可以对监测区域进行无线环境分析和频谱分析，如下图。



无线环境分析	通过 Sensor 设备扫描并显示各无线信道多类无线报文的信道占用情况，可应用于无线网络问题的定位与分析。
频谱分析	通过 Sensor 设备扫描并显示各无线频率点的能量分布及变化情况，可应用于无线干扰定位及干扰源识别。

13.4 无线安全

13.4.1 无线安全

进入页面：网络运维 >> 无线安全，本界面可以扫描环境中的非法设备，定位区域，以便用户排查网络安全问题；检测报文洪流攻击，防止恶意网络攻击行为造成上网体验异常，如下图。

威胁事件数	统计时间段（24 小时）内出现的威胁事件数量。
威胁事件多的 Sensor 分组	依据 Sensor 分组情况，统计威胁事件数量，进行排名。
威胁事件多的 Sensor 设备	依据所检测的威胁事件数量，对各 Sensor 设备进行统计排名。
威胁设备数	包含网络中检测到的无加密设备，以及可触发洪流攻击的终端威胁设备。
非法设备数	即钓鱼 AP 设备数量，未知设备提供无线服务名称与当前网络已有的无线服务名称相同，客户端关联存在安全性风险。
干扰设备数	Sensor 可探测到，但当前网络中未存在的无线服务，客户端关联存在安全性风险。
Dos 攻击事件	包括常见的设备威胁 Dos 和环境威胁 Dos，例如 Beacon 洪流、Auth 洪流攻击。
批量反制	对于可进行无线反制的威胁设备，功能开启后可阻止 Sensor 附近的无线终端关联非法设备，支持批量开启反制功能。
批量关闭反制	批量关闭当前正在进行的无线反制任务。

搜索/筛选	支持基于 Sensor 名称进行威胁事件搜索，支持基于威胁等级、威胁事件类型进行威胁事件筛选。
白名单	设置可信任的 SSID 或设备（MAC 地址），当 Sensor 设备检测到对应 SSID 或 MAC 地址后，将不会判断为威胁事件或威胁设备。可手动进行添加白名单信息。部分旧设备不支持 BSSID 上报，需手动加入 Mac 白名单，避免威胁事件误报。
威胁等级	无线安全事件严重等级，根据所检测的事件对网络可能造成的影响，区分为严重、一般和轻微。
威胁事件类型	包含未加密无线服务、设备威胁 Dos、环境威胁 Dos、终端威胁 Dos、干扰设备、钓鱼 AP。
威胁设备/受威胁设备	威胁设备：威胁事件的产生源，对于部分威胁事件，可检测出对应的设备 MAC 地址或无线服务（SSID）名称；对于部分安全事件，如环境 Dos 攻击，无固定威胁源标识，因此无法检测和显示相关信息。 受威胁设备：对于事件类型为设备威胁 Dos 的安全事件，无固定威胁源标识，但是往往是针对固定目标设备的攻击，此处显示受威胁的设备 MAC。
最近 24 小时威胁设备在线时间	最近 24 小时内，所检测到的威胁事件发生的时间点，可看出各威胁事件的发生频次和影响程度（时间长度）。
事件状态	当前事件状态，包含待处理、已加入白名单两种状态，对于部分事件，可加入信任白名单。
反制状态	当前事件是否处于反制状态，对于部分支持无线反制的安全事件，进行无线反制后，对应状态变更为反制中，请尽快确认并清除威胁源。

详情	查看威胁事件详情，对于部分威胁设备，可手动添加信任白名单或进行无线反制。

第14章 易展设备管理

随着互联网技术的快速发展，需求无线网络覆盖的地方越来越多，此时出现了一些传统网络无法解决的复杂区域和快速完成组网的需要，也有个人用户不想破坏原有的装修环境来进行网络覆盖。对于一些区域来说传统网络的组网方案不仅复杂且成本较高。为了解决这些问题，TP-LINK 新推出了带有“易展”功能的AP，能够实现快速组网，无需布线，简单实现组网，且可以替换某些传统组网，优化整个网络。

某多层写字楼想要在已有的 AP 组网中增加部分区域的无线覆盖范围，但是想要覆盖的区域不方便布线，区域的终端接入数和流量不大。

组网特点：

(1) 不方便布线；

(2) 不想破坏办公环境；

(3) 有临时增加网络位点的需求；

(4) 需要对设备统一管理，方便维护。

14.1 设备列表

14.1.1 设备列表

➢ 易展主设备列表

在 FIT 模式下，易展 AP 的功能和普通 AP 基本是一样的，例如 LED 开关、射频编辑、设备升级、AP 列表查看等等；易展 AP 特有的功能主要有“易展主子 AP 列表分开展示”和“子设备更换主 AP”，如下图。

➢ 易展子设备列表

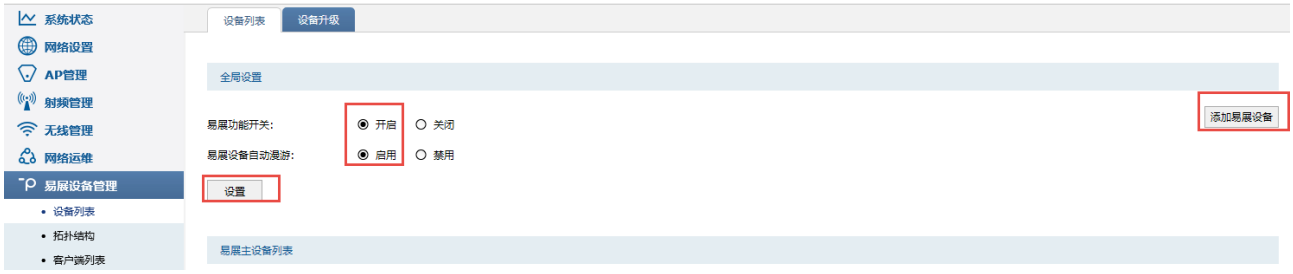
子设备更换主设备，灵活调整组网，可以通过手动设置将子 AP 关联到信号更好的主 AP 上。

14.1.2 添加易展设备

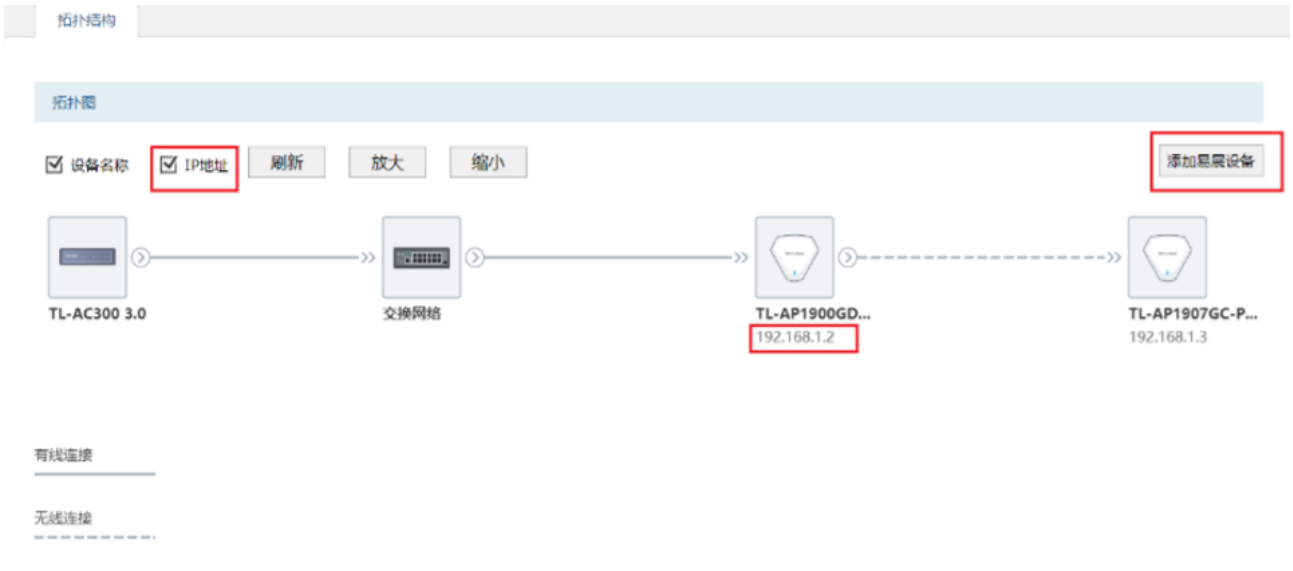
需要使用 FIT 模式下进行多个 MESH 单元组网，出厂状态下，将设备接入局域网中，若局域网中存在开启 AP 管理功能的 AC 控制器，易展 AP 将自动识别并工作在 FIT 模式；同时 AC 控制器需要开启易展管理功能，即可发现并管理易展 AP。

➢ 全局设置

进入页面：易展设备管理 >> 设备列表，在全局设置中开启“易展功能”和“易展设备自动漫游”，点击<设置>。



添加易展 AP 子设备，点击设备列表或拓扑结构页面右上角的<添加易展设备>按钮，此时主 AP 会自动搜索周围待配对的子 AP，发现设备后点击全部添加，等待一会儿即可完成配对。



14.1.3 设备升级

进入页面：易展设备管理 >> 设备列表 >> 设备升级，可查看和配置各个 AP 的升级信息。

➢ AP 批量升级

一些大型项目的维护过程中，需要对无线 AP 进行升级维护，但是项目 AP 数量可能达到几十上百，一个一个升级费时费力，维护成本剧增，此时能够进行批量升级就尤为重要。不但可以提高效率，还可以避免升级出错。

在“AP 批量升级”栏目下，点击<新增>，选择 AP 分组及 AP 型号后，点击<确定>，即可对 AP 进行批量升级。若选择“定时升级”，则 AP 在指定时间进行升级，如下图。

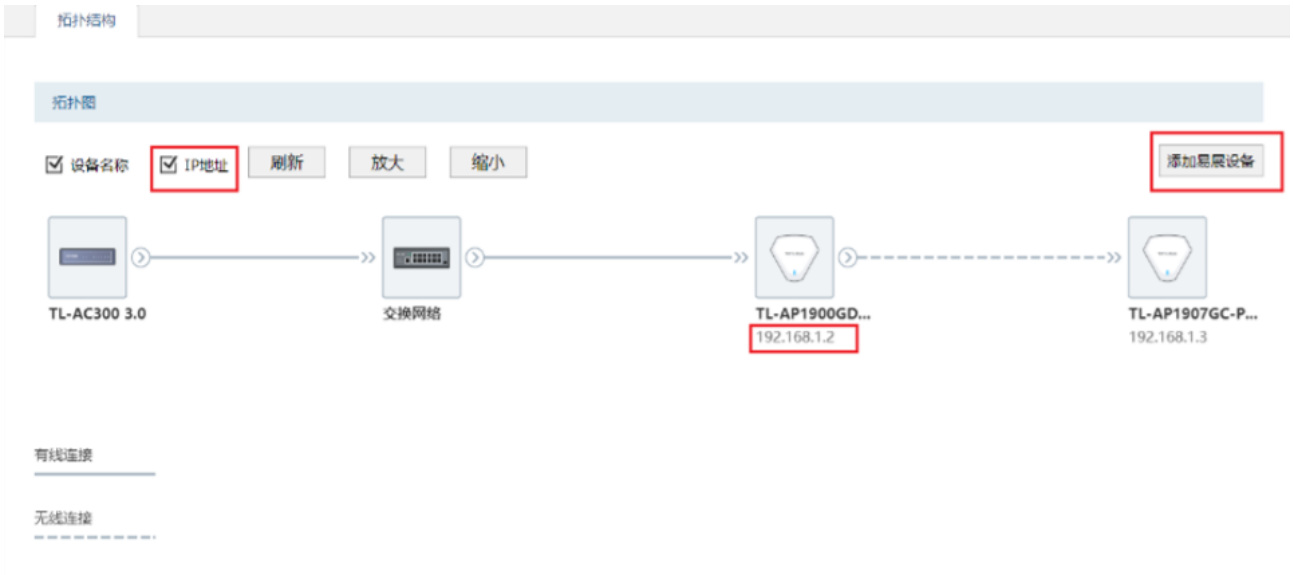
➢ 单个 AP 升级

在“单个 AP 升级”栏目下，选择 AP 分组，可查看 AP 升级信息，如下图。

14.2 拓扑结构

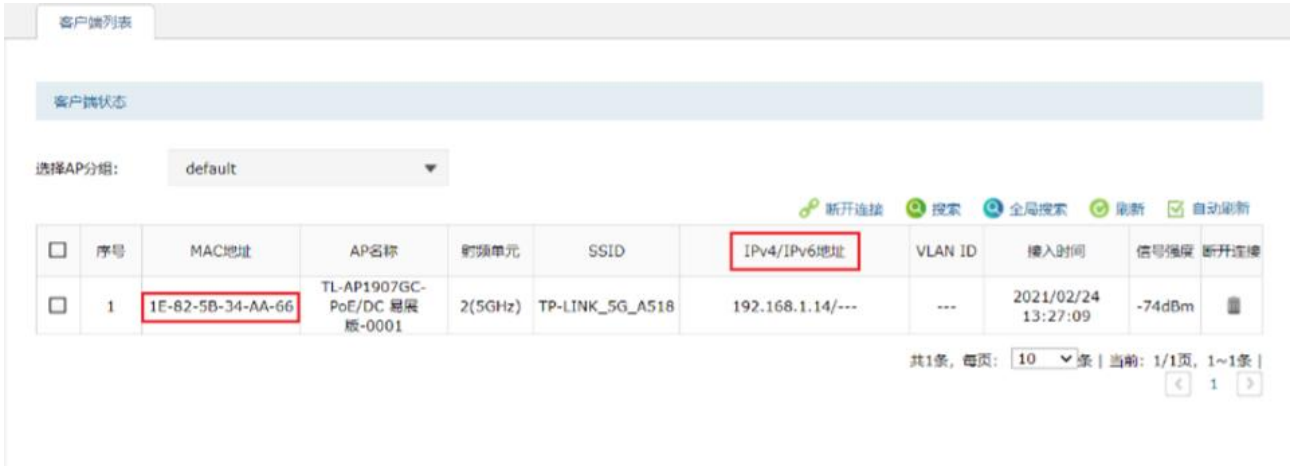
进入页面：易展设备管理 >> 拓扑结构，可查看设备的网络拓扑，型号（名称）、IP 地址等参数，如下图。

点击右上角的<添加易展设备>按钮，此时主 AP 会自动搜索周围待配对的子 AP，发现设备后点击全部添加，等待一会儿即可完成配对。



14.3 客户端列表

进入页面：易展设备管理 >> 客户端列表，可查看接入易展设备的终端情况，包括接入时间，设备 MAC，接入射频，信号强度、IP 地址等信息，如下图。



第15章 认证管理

无线控制器提供 Portal 认证服务，包括 Web 认证、一键上网和远程 Portal 认证方式，以及跳转页面、免认证策略和认证参数相关功能。

说明：

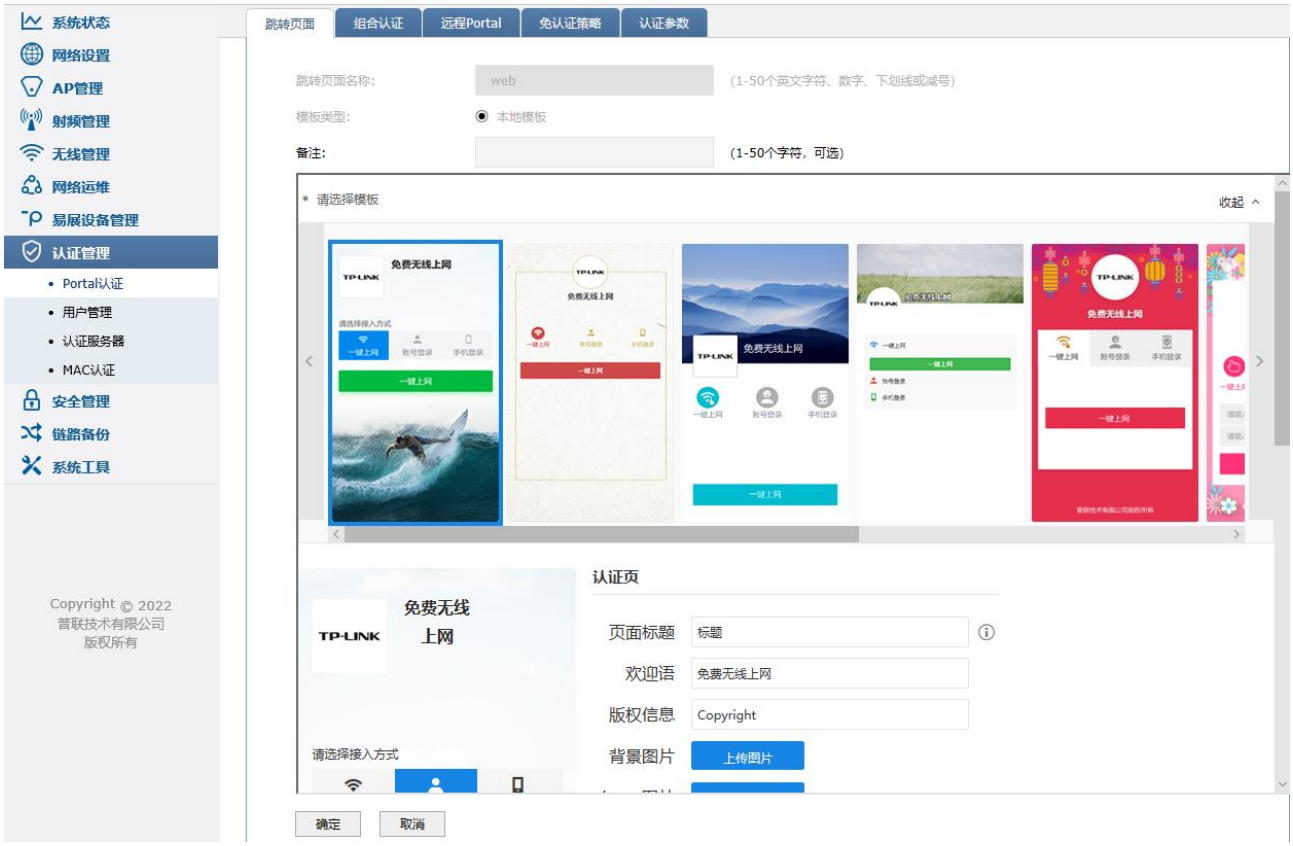
- 在进行 Portal 认证的相关设置之前，请先确保无线控制器管理 AP 的接口 IP 地址与待认证客户端的 IP 地址之间路由可达。

15.1 认证设置

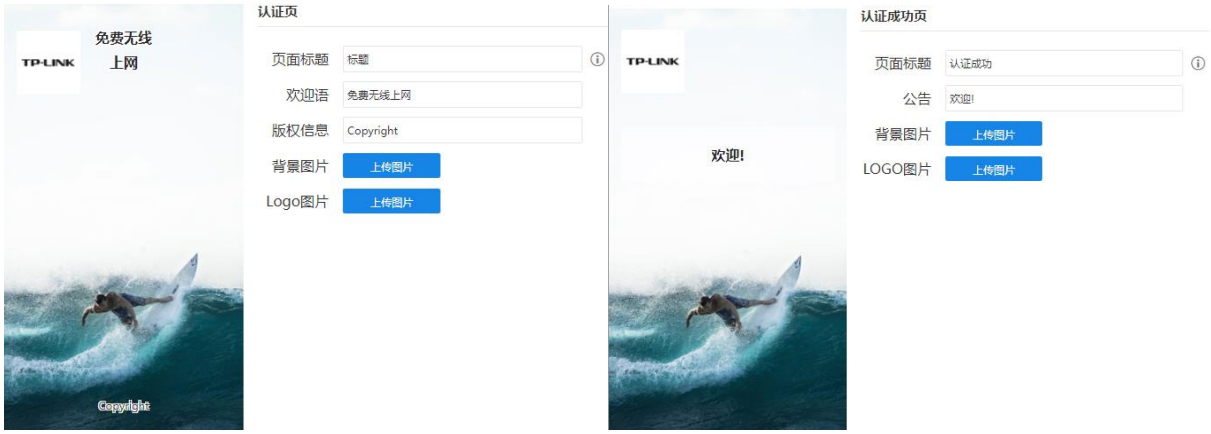
15.1.1 跳转页面

在此设置用户认证过程中所看到的认证页面和认证成功页面，可通过图片上传、外部链接或使用默认模板，满足推送广告，推广微信公众号等需求。

进入页面：认证管理 >> Portal 认证 >> 跳转页面，点击<新增>，添加认证跳转页面。设置跳转页面名称，选择模板。



点击模板，设置认证页面和认证成功页面的标题、内容和背景图片。设置完成后，点击<确定>。



15.1.2 组合认证

多功能无线控制器提供一键上网、Web 认证、短信认证三种认证方式。

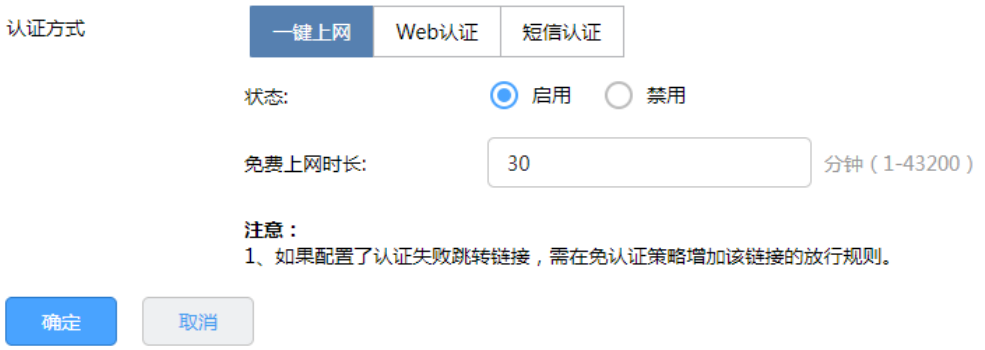
进入页面：认证管理 >> Portal 认证 >> 组合认证，点击<新增>设置认证规则。

跳转页面名称	选择所设置的跳转页面模板，模板设置可参考 12.1.1 跳转页面。
生效 SSID	选择该认证规则生效的无线网络。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。
认证失败跳转连接	设置认证失败后跳转的 URL 地址。

下面介绍一键上网、Web 认证、短信认证三种认证方式的设置方法。

- **一键上网**

认证方式选择一键上网，启用该认证方式，设置认证用户可以免费上网的时长。若 radius 服务器设置了免费上网时长，生效的时间为 radius 服务器设置的时间。点击<确定>。



注意：

- 如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。

➢ Web 认证

认证方式选择 Web 认证，启用该认证方式，选择认证服务器类型。点击<确定>。

认证服务器类型	选择本地服务器或远程服务器进行认证。
认证服务器组	选择进行远程 Portal 认证的服务器组。
免费上网时长	选择远程服务器进行认证时，若服务器未配置用户上网时长，则使用该时长作为用户的免费上网时长。

点击页面 ，查看更多页面设置参数信息。

注意：

- 如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。
- 认证服务器类型为远程服务器时，若服务器配置了用户上网时间，则免费上网时长为服务器返回的时

间，否则为本页面配置的免费上网时长。

➢ **短信认证**

认证方式选择短信认证，启用该认证方式，设置各项参数，点击<确定>。

状态	启用短信认证方式
免费上网时长	设置认证用户可以免费上网的时长。若 radius 服务器设置了免费上网时长，生效的时间为 radius 服务器设置的时间。
验证码有效期	用户在该时间内输入验证码进行验证有效，否则需重新获取验证码。
通道类型	选择发送短信的平台，本产品支持阿里云、网易云信、腾讯云、百度云和 HTTP 协议五种平台。

点击页面 ，查看更多页面设置参数信息。

注意：

- 如果配置了认证失败跳转链接，需在免认证策略增加该链接的放行规则。

- 配置了短信认证条目，为了无线 PC 能够顺利完成认证，需要保证设备可以联网。
- 使用短信认证功能前，必须要先在“系统工具->时间设置”中正确地配置本机系统时间。。

15.1.3 远程认证

可以通过本页面设置和查看远程 Portal 认证条目。

进入页面：认证管理 >> Portal 认证 >> 远程 Portal，点击<新增>设置远程认证规则。

生效 SSID	选择该认证规则生效的无线网络。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。

认证失败跳转连接	设置认证失败后跳转的 URL 地址。
远程 Portal 地址	每个用户允许接入的最大客户端数量。注意：用户类型为自动的用户，意味着 L2TP 和 PPTP 的最大接入客户端数量均为最大会话数。
认证服务器类型	选择本地服务器或远程服务器进行认证。
认证服务器组	选择进行远程 Portal 认证的服务器组。
免费上网时长	选择远程服务器进行认证时，若服务器未配置用户上网时长，则使用该时长作为用户的免费上网时长。

点击页面  ，查看更多页面设置参数信息。

15.1.4 免认证策略

免认证策略可配置用户在 Portal 认证成功前能够免费访问的资源。

进入页面：认证管理 >> Portal 认证>> 免认证策略，点击<新增>设置远程认证规则。

免认证策略提供两种认证方式：五元组方式和 URL 方式。

- **五元组方式**

主要依据 IP 地址范围、MAC 地址、VLAN ID、端口和服务协议设置策略，当需要限制的免认证参数种类较多时，推荐使用五元组方式。

策略名称	填写免认证策略条目的名称。
免认证方式	免认证策略的匹配方式：五元组方式
源/目的 IP 地址范围	设置免认证策略的源/目的 IP 地址和网络掩码。。
源 MAC 地址	设置免认证策略的源 MAC 地址。
源/目的端口范围	设置免认证策略的源/目的端口范围。
服务协议	设置免认证策略的服务协议。

点击页面 ，查看更多页面设置参数信息。

- URL 方式

主要依据 URL 设置策略，当已知 URL 时，推荐使用 URL 方式。

策略名称	填写免认证策略条目的名称。
免认证方式	免认证策略的匹配方式： URL 方式
URL 地址	输入 URL 地址
源 IP 地址范围	设置免认证策略的源 IP 地址和网络掩码。。
源 MAC 地址	设置免认证策略的源 MAC 地址。

点击页面 ，查看更多页面设置参数信息。

15.1.5 认证参数

通过本页面可设置认证老化时间和 Portal 认证端口。

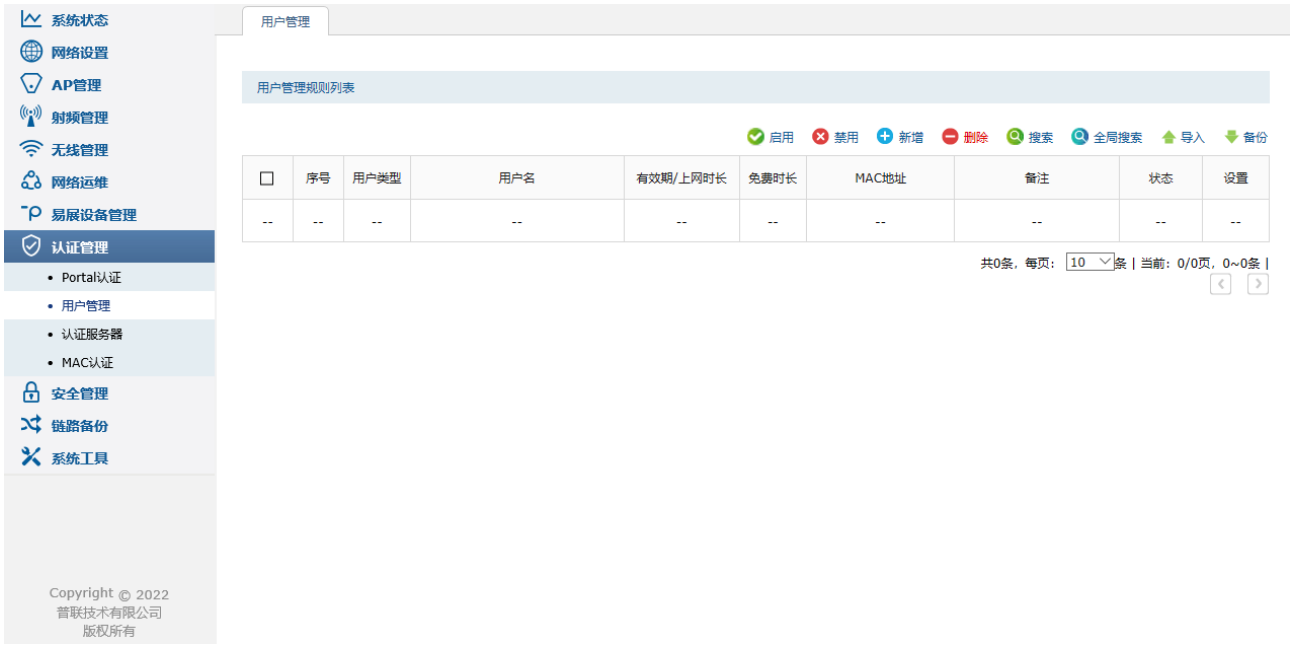
进入页面：认证管理 >> Portal 认证>> 认证参数，设置认证老化时间和 Portal 认证端口，点击<设置>。

认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。
认证模式	支持基于 SSID 和基于接口两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于接口表示与这个接口的终端都需要认证才能上网。默认基于 SSID。

15.2 用户管理

15.2.1 认证用户管理

进入页面：认证管理 >> 用户管理，可查看已添加的认证用户列表。点击<新增>，添加用户账号。



用户类型	选择用户类型。 正式用户：存留在系统中的正式用户，具有一定的有效期，且可以绑定相应的设备 MAC 地址。可以记录更多用户的资料信息。 免费用户：免费用户具有一定的上网时长限制。
用户名	用于认证登录的用户名。
密码	用户登录所使用的密码。
有效期至	正式用户的有效期。
允许认证时间段	允许用户进行认证的时间。
MAC 地址绑定方式	选择是否绑定 MAC 地址，以及绑定的方式。 不绑定：不绑定用户的 MAC 地址。 静态绑定：绑定一个静态的 MAC 地址。 动态绑定：进行动态绑定。
同时登录用户数	最多允许同时使用该账号登录的用户数量。

上/下行带宽	当前用户允许的上/下行带宽，以 Kbps 为单位，0 表示不限制。当开启此功能时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。
姓名	可选记录当前用户姓名。
电话	可选记录当前用户电话。

点击页面，查看更多页面设置参数信息。

15.2.2 用户配置备份

进入页面：认证管理 >> 用户管理。

点击<备份>，可将当前信息保存至本地。

点击<导入>，可批量导入用户信息。

15.3 认证服务器

网关提供指定外部 Radius 服务器进行认证的功能。

外部 Radius 服务器认证，即当用户接入时，无线控制器将用户的身份认证信息提交给外部服务器，由外部服务器认证身份信息。

➢ **配置 Radius 认证服务器步骤**

3. 设置 Radius 服务器。必须操作。配置界面：认证管理 >> 认证服务器 >> Radius 服务器。

4. 设置服务器组。必须操作。配置界面：认证管理 >> 认证服务器 >> 认证服务器。

15.3.1 Radius 服务器

可以通过本界面添加、修改或删除一个外部 Radius 服务器。Radius 支持认证服务和计费服务功能。

进入页面：认证管理 >> 认证服务器 >> Radius 服务器，点击<新增>，设置 Radius 服务器。

服务器名称	您可以配置 Radius 服务器的名称。
服务器地址	设置服务器的地址，IPv4 地址或者 DNS 域名。
认证端口	服务器监听认证报文的端口。

计费端口	服务器监听计费报文的端口，0 表示不启用计费功能。
共享密钥	Radius 服务器配置的共享密钥。
重复发送次数	当客户端发送请求后，如果没有收到回复，重复发送请求的次数。
超时时间	当客户端发送请求后，数据包超时时间。
NAS 标识	进行 Radius 认证或计费时，用于标识 NAS 设备。
NAS IP 地址	进行 Radius 认证或计费时，NAS-IP-Address 字段的 IP 地址值（一般填写 AC 与 Radius 服务器交互的实际 IP 地址，也可以为空）。
认证方式	使用的认证方式，有 PAP、CHAP、MSCHAP 和 MSCHAPv2。

点击页面 ，查看更多页面设置参数信息。

15.3.2 认证服务器

可以通过本界面设置和查看认证服务器组。

进入页面：认证管理 >> 认证服务器，点击<新增>，设置认证服务器组。

组名称	自定义的认证服务器组名称，注意不能与已有服务器组名称重复。。

协议类型	该组中认证服务器的类型，目前只支持 Radius。
主服务器	选择特定类型的认证服务器为该组的主服务器，主服务器在认证过程中将优先被使用。
备用服务器	备用服务器在主服务器发生故障时启用，备份服务器为可选项。
恢复时间	当主服务器发生故障后，重新尝试使用主服务器的时间间隔。

点击页面 ，查看更多页面设置参数信息。

15.4 MAC 认证

15.4.1 MAC 认证

可以通过本界面设置和查看 MAC 认证。只有连接了该 SSID 或该 VLAN 的终端才需认证。

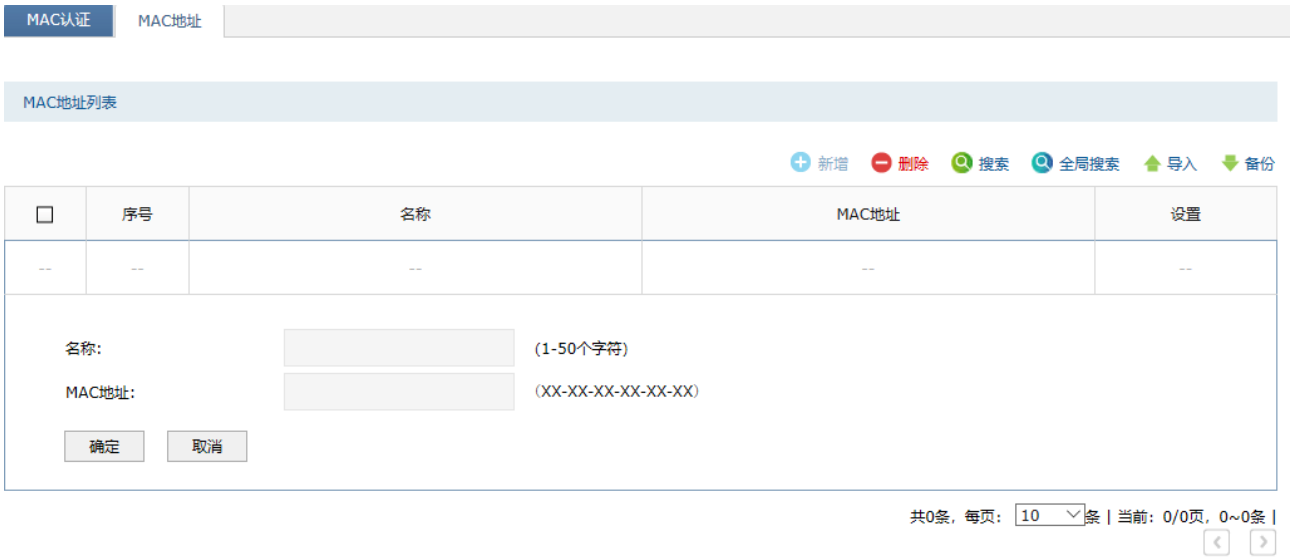
进入页面：认证管理 >> MAC 认证，设置 MAC 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式。

进入页面：认证管理 >> MAC 认证，点击<新增>，设置 MAC 认证条目。

15.4.2 MAC 地址

可以通过本界面设置和查看 MAC 地址条目。

进入页面：认证管理 >> MAC 认证 >> MAC 地址，点击<新增>，添加 MAC 地址条目。



15.5 MAC 认证配置实例

15.5.1 应用介绍

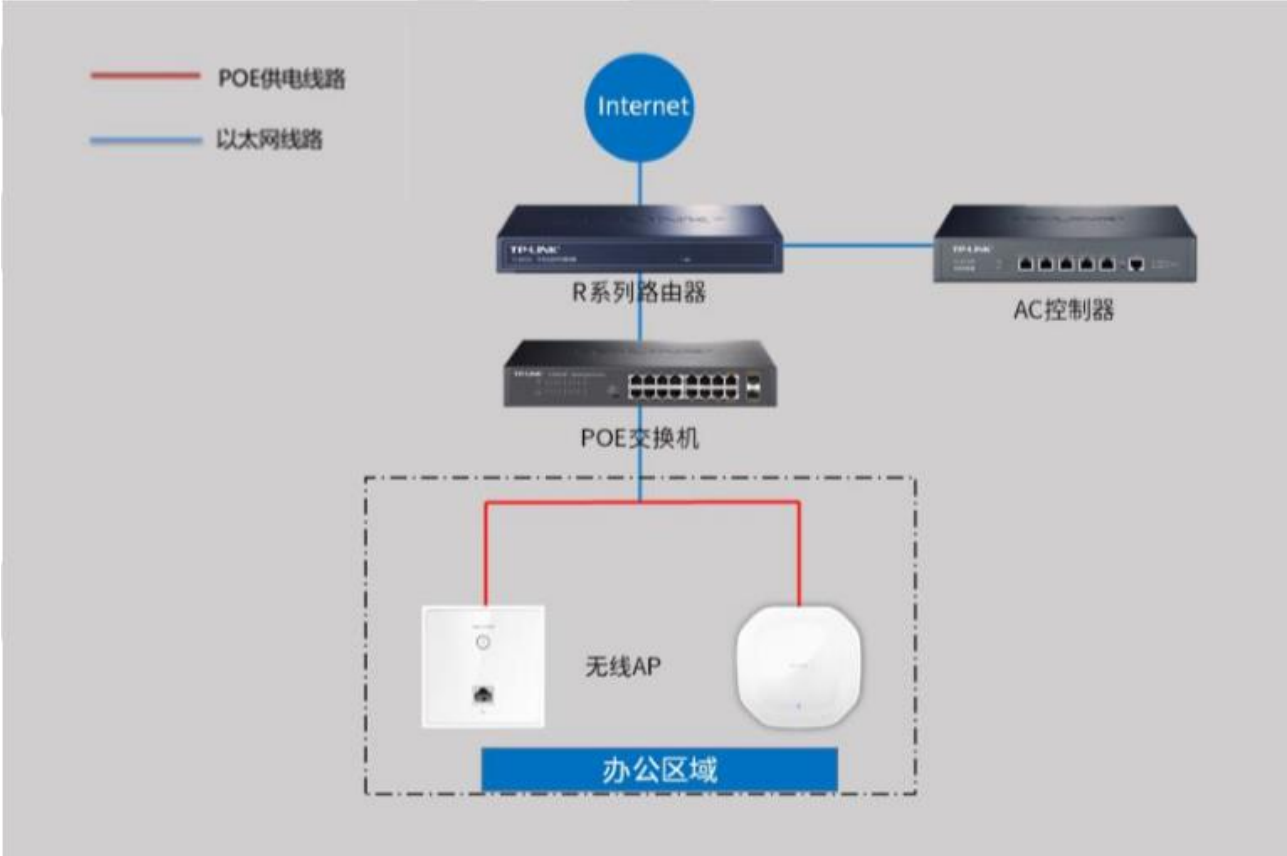
无线控制器提供 MAC 认证功能，禁止非法用户或者仅允许特定用户连接使用无线网络。设置时只需要知

道终端的 MAC 地址，无需安装任何客户端软件，认证过程中也不需要进行任何操作，直接在设备上完成对用户 MAC 地址的认证。本章节以某公司要求实现只有允许的 MAC 地址能连接到 AP 且使用网络为例，详细讲解 AC 控制器中 MAC 认证的设置方法。

15.5.2 需求介绍

某办公室需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

只有指定的员工设备才能上网，其它设备不能上网。



15.5.3 设置方法

1. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

2. 进入页面：认证管理 >> MAC 认证 >> MAC 地址，点击<新增>，添加如下条目：

其它 MAC 地址按照上述方法依次添加，如果需要添加的 MAC 地址较多时，可以通过导入 MAC 地址表来添加。

3. 进入页面：认证管理 >> MAC 认证 >> MAC 认证，点击<新增>，添加如下条目：

其中我们要选择生效的 MAC 地址，如下图：

认证可以设置多个黑白名单条目，在设置 MAC 认证条目时，MAC 认证名称不能与已有 MAC 认证名称重复；生效 VLAN 范围不能和其他条目重复，必须是唯一的。以上内容配置完毕，AC 控制器的 MAC 认证设置指南设置完成。如果是白名单就只有在 MAC 地址列表的无线终端才能连接 AP 的信号并使用网络，如果为黑名单在列表中的 MAC 地址对应的终端无法连接 AP 的无线信号。

说明：

- 认证模式：设置认证模式，支持基于 SSID 和基于 VLAN 两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于 VLAN 表示连接到这个 VLAN 中的终端都需要认证才能上网。

- 认证类型：设置认证类型，支持基于黑/白名单两种模式，黑名单表示 MAC 地址表中的设备都不能上网，白名单表示只有 MAC 地址表中的设备才能上网 。

15.6 Portal 认证

15.6.1 需求介绍

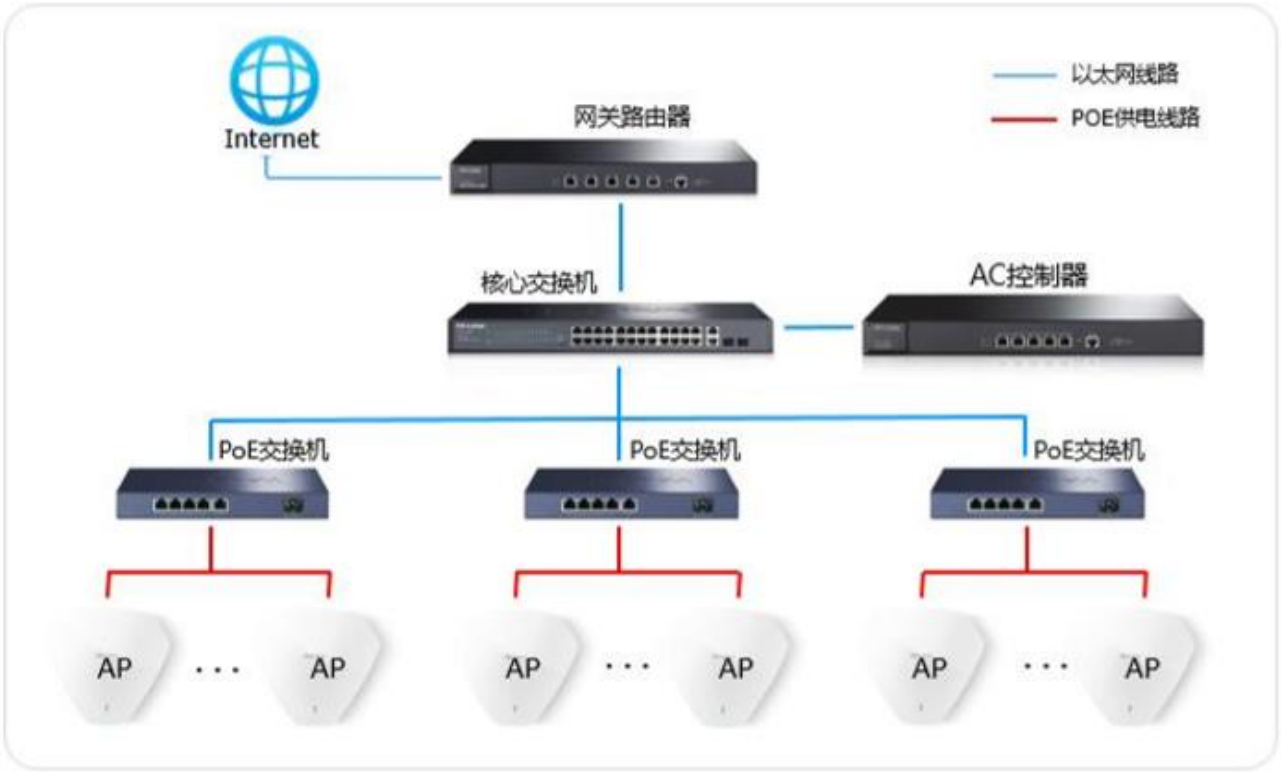
随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。AC 控制器支持 Portal 功能，认证方式灵活，支持广告推送。本节通过典型应用实例介绍多功能无线控制器 Portal 认证功能的应用与配置。

15.6.2 Portal 认证配置实例——使用内置 WEB 服务器和内置认证服务器

某商场需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

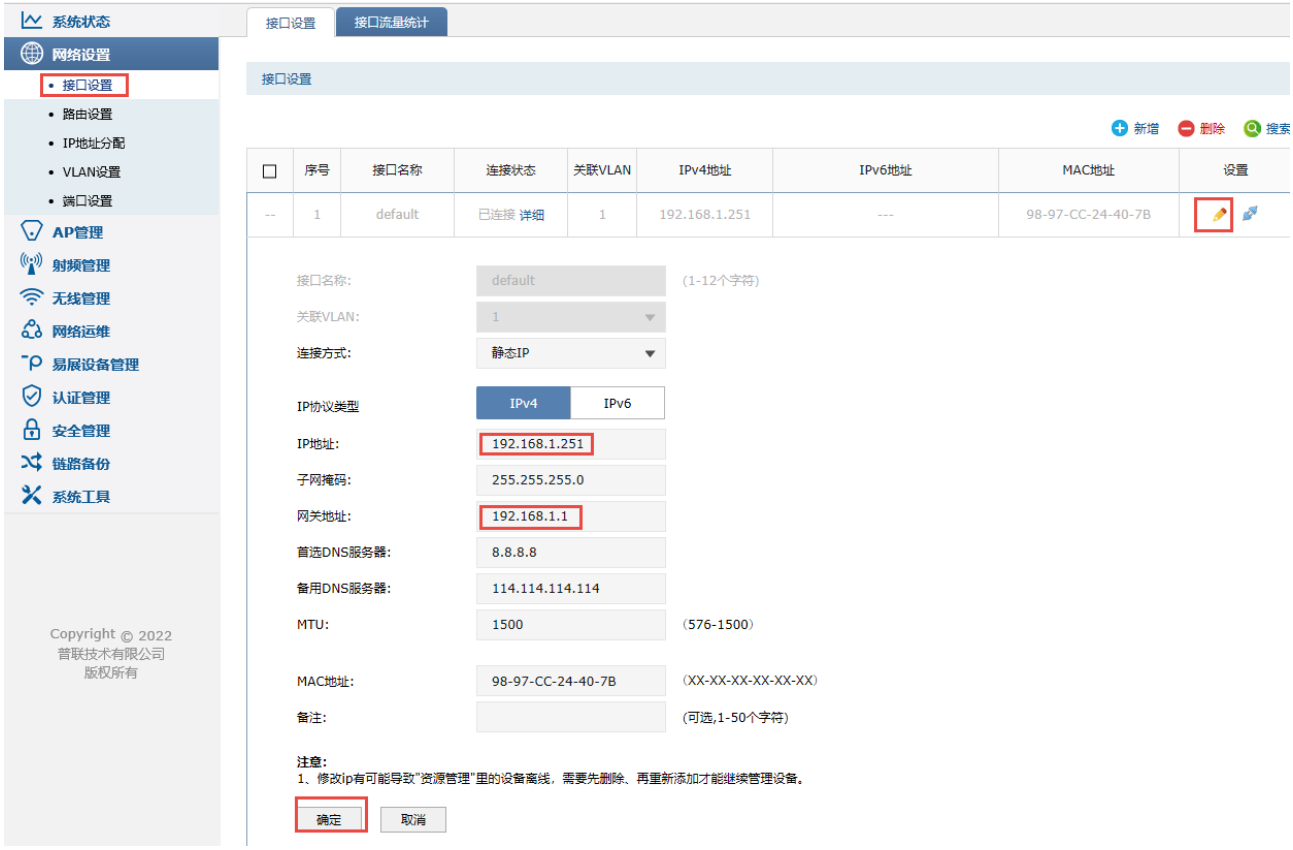
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

根据用户需求，AC、AP 以及路由器连接参考拓扑如下：



配置步骤：

1. 进入页面：网络设置 >> 接口设置， 在系统默认条目的后面点击编辑 ，填写配置 AC 的管理 IP 和网络中正确的网关（一般是路由器的 IP 地址），如下图。

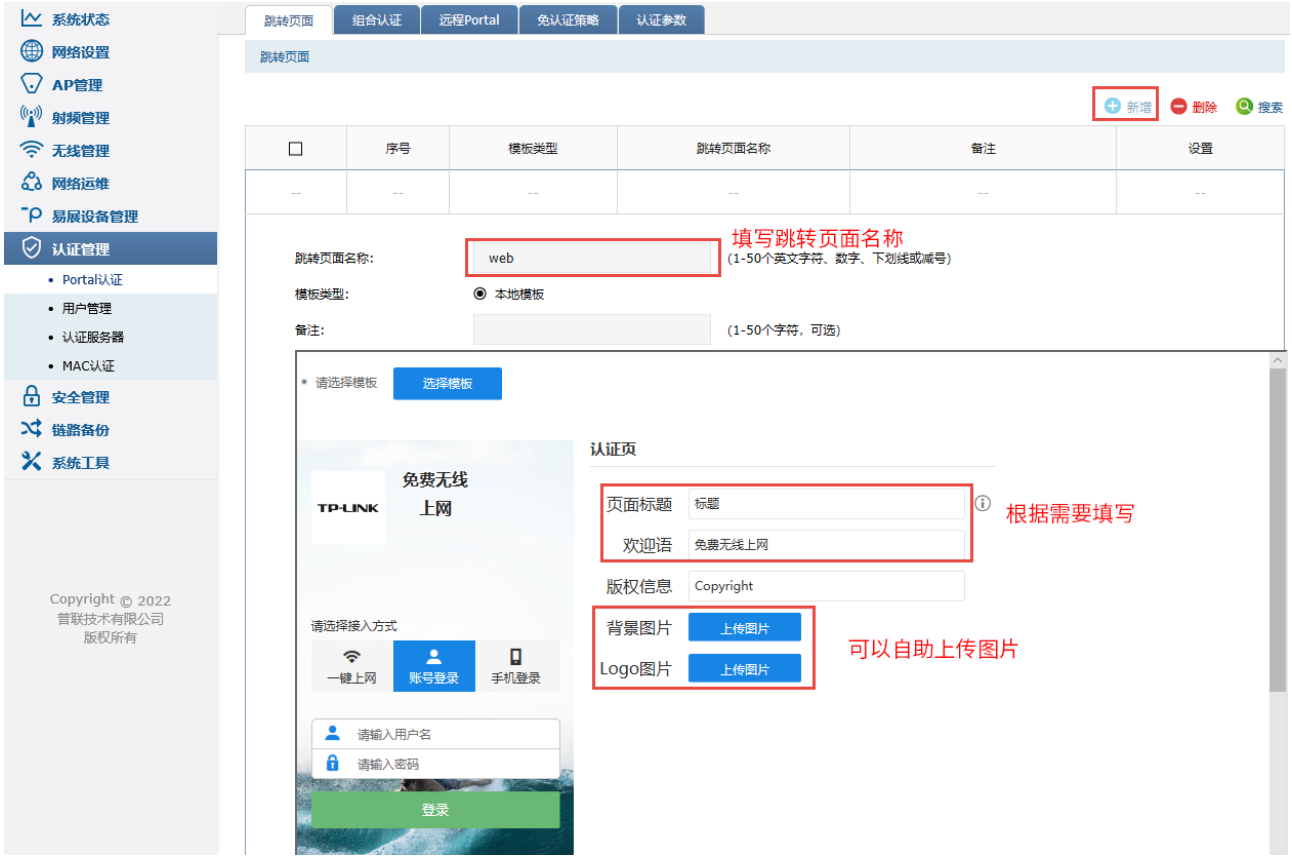


2. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服务端口重复。
认证模式	设置 Portal 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于 VLAN 表示连接到这个 VLAN 中的终端都需要认证才能上网。

4. 进入页面：认证管理 >> Portal 认证 >> 跳转页面， 点击<新增>，根据实际需求设置跳转页面标题、欢迎信息等，如下图。



5. 进入页面：认证管理 >> Portal 认证 >> 组合认证， 点击<新增>，选择模板和生效 SSID，设置成功和失败跳转链接，选择 Web 认证并启用，点击<确定>，如下图。

注意：

- 若启用无感知认证，无感知认证用户免费上网时长用尽或再次接入无线服务时会自动进行认证。

6. 进入页面：认证管理 >> 用户管理， 点击<新增>,，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，点击<确定>，如下图。

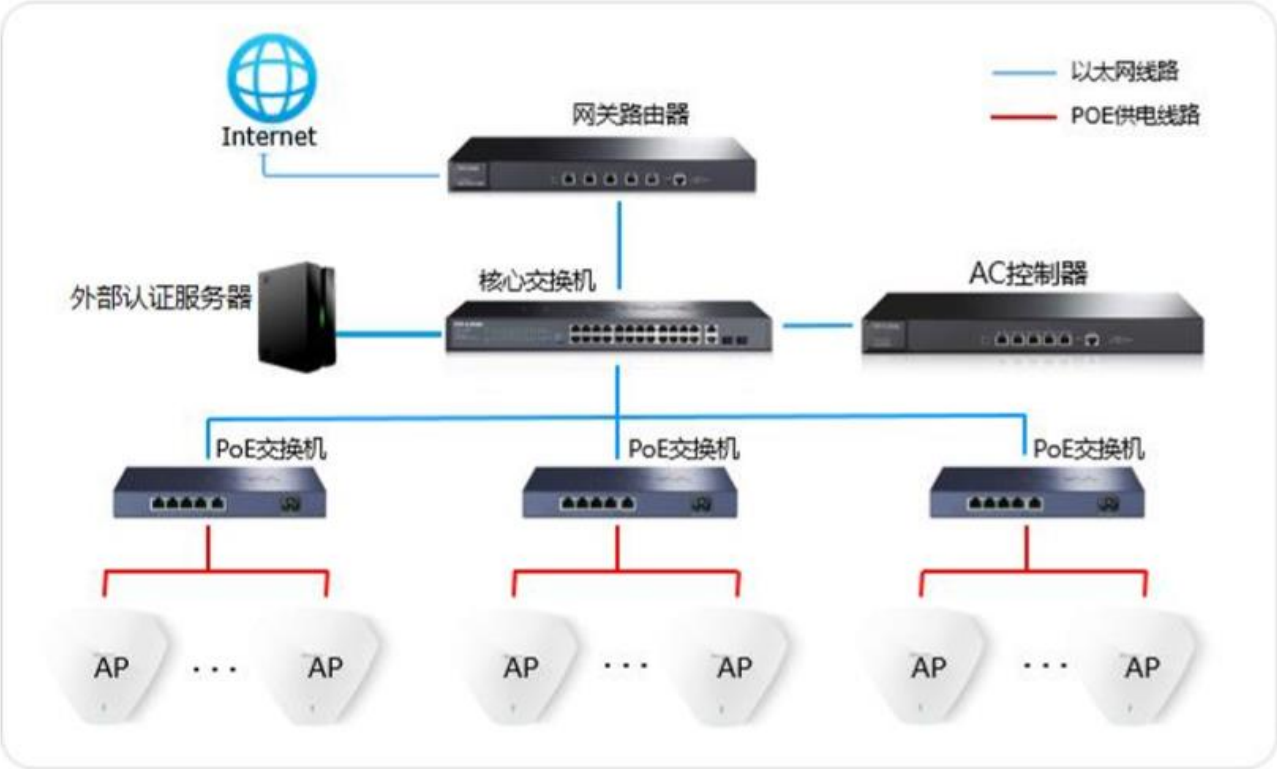
以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

15.6.3 Portal 认证配置实例——使用内置 WEB 服务器和外部认证服务器

某商场需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

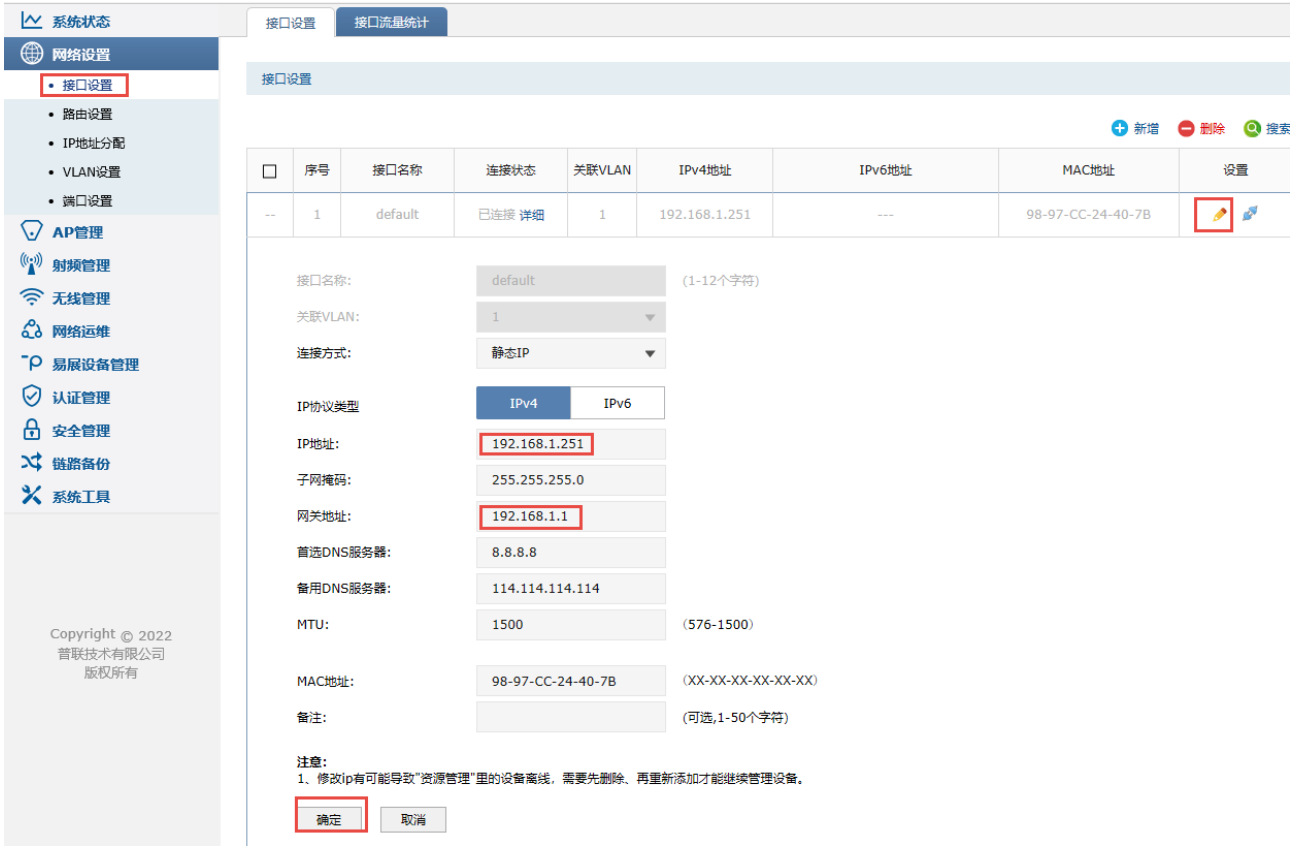
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

根据用户需求，AC、AP 以及路由器连接参考拓扑如下：



配置步骤：

1. 进入页面：网络设置 >> 接口设置， 在系统默认条目的后面点击编辑 ，填写配置 AC 的管理 IP 和网络中正确的网关（一般是路由器的 IP 地址），如下图。



2. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

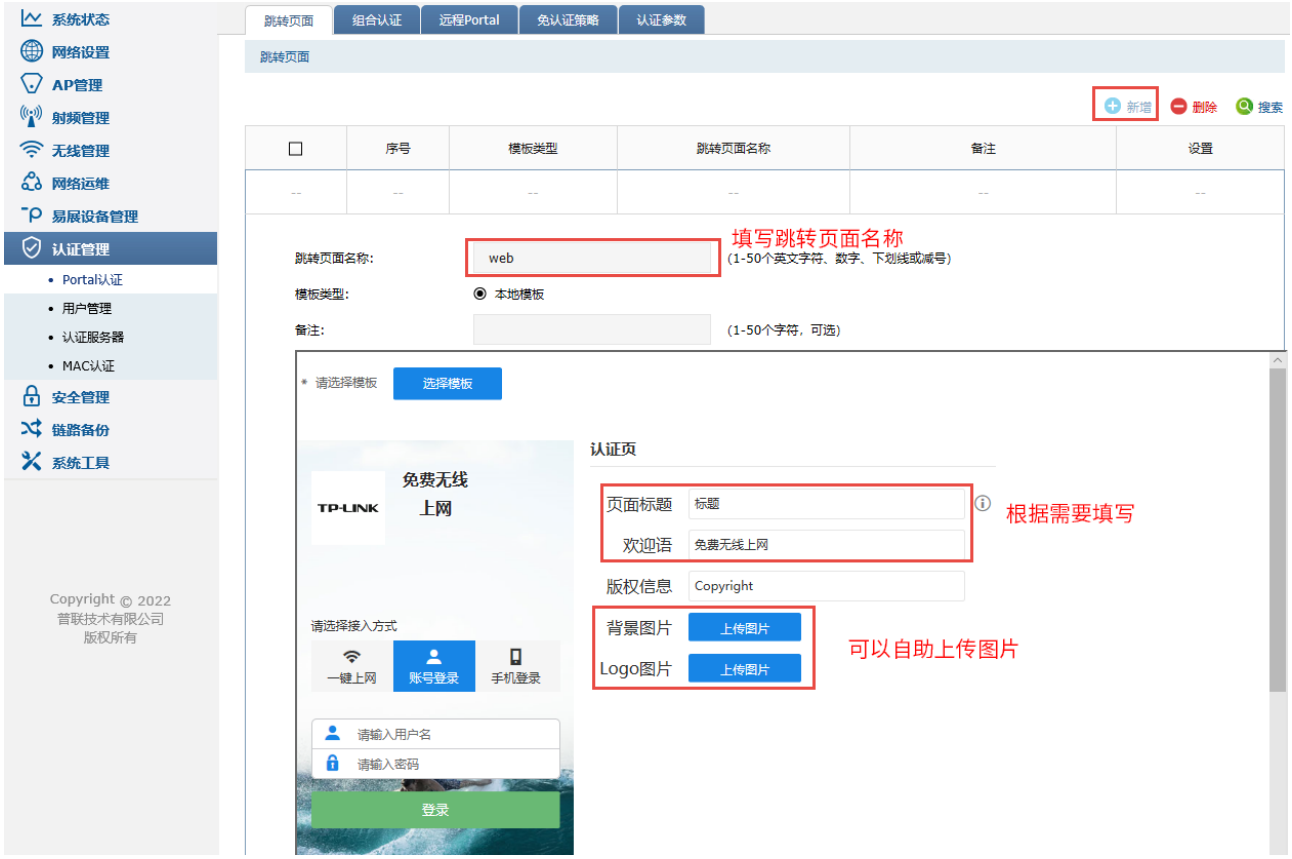
3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服务端口重复。
认证模式	设置 Portal 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于 VLAN 表示连接到这个 VLAN 中的终端都需要认证才能上网。

4. 进入页面：认证管理 >> 认证服务器 >> Radius 服务器， 点击<新增>，服务器地址填写搭建的专用认证服务器（如 Radius 服务器）的 IP 地址，填写 Radius 服务器的共享密钥，如下图。

5. 进入页面：认证管理 >> 认证服务器 >> 认证服务器， 点击<新增>，主服务器选择上一步设置的 Radius 服务器名称，如下图。

6. 进入页面：认证管理 >> Portal 认证 >> 跳转页面， 点击<新增>，根据实际需求设置跳转页面标题、欢迎信息等，如下图。



7. 进入页面：认证管理 >> Portal 认证 >> 组合认证， 点击<新增>，认证服务器类型选择远程服务器，点击<确定>，如下图。

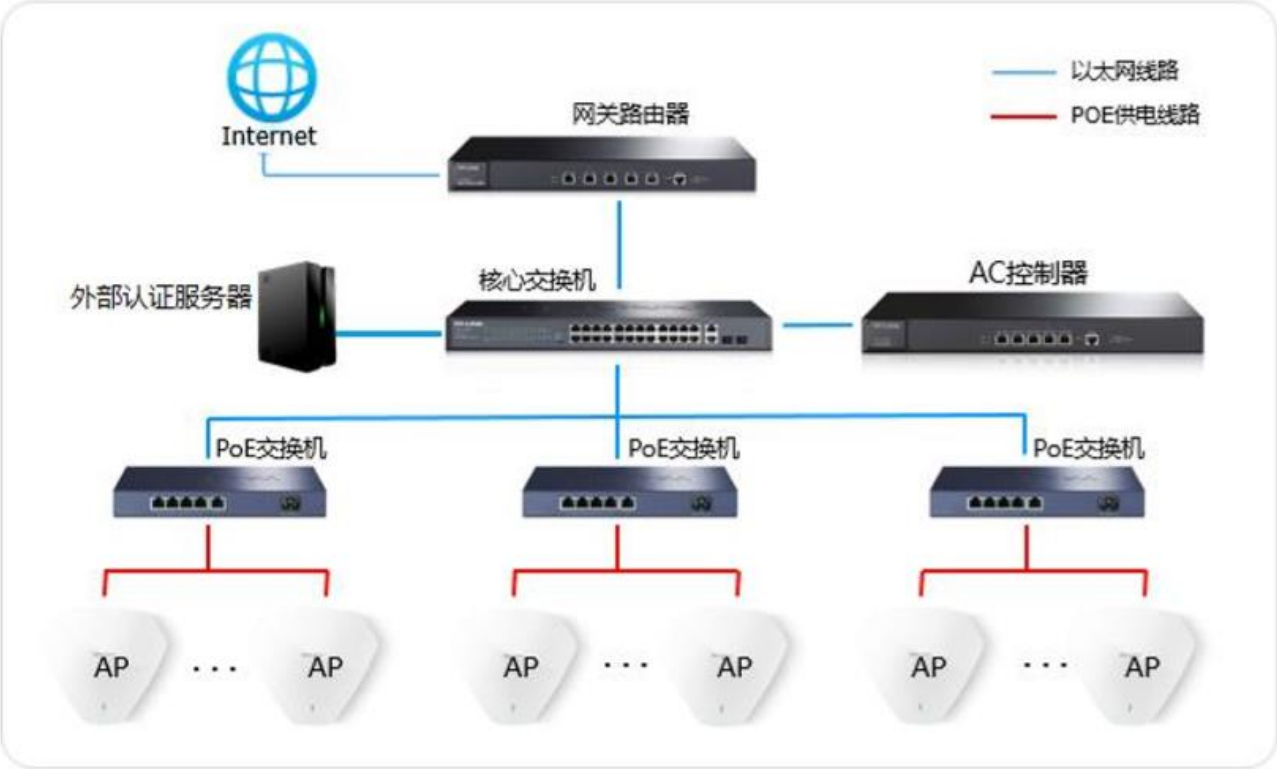
以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

15.6.4 Portal 认证配置实例——使用外置 WEB 服务器和内部认证服务器

某商场需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

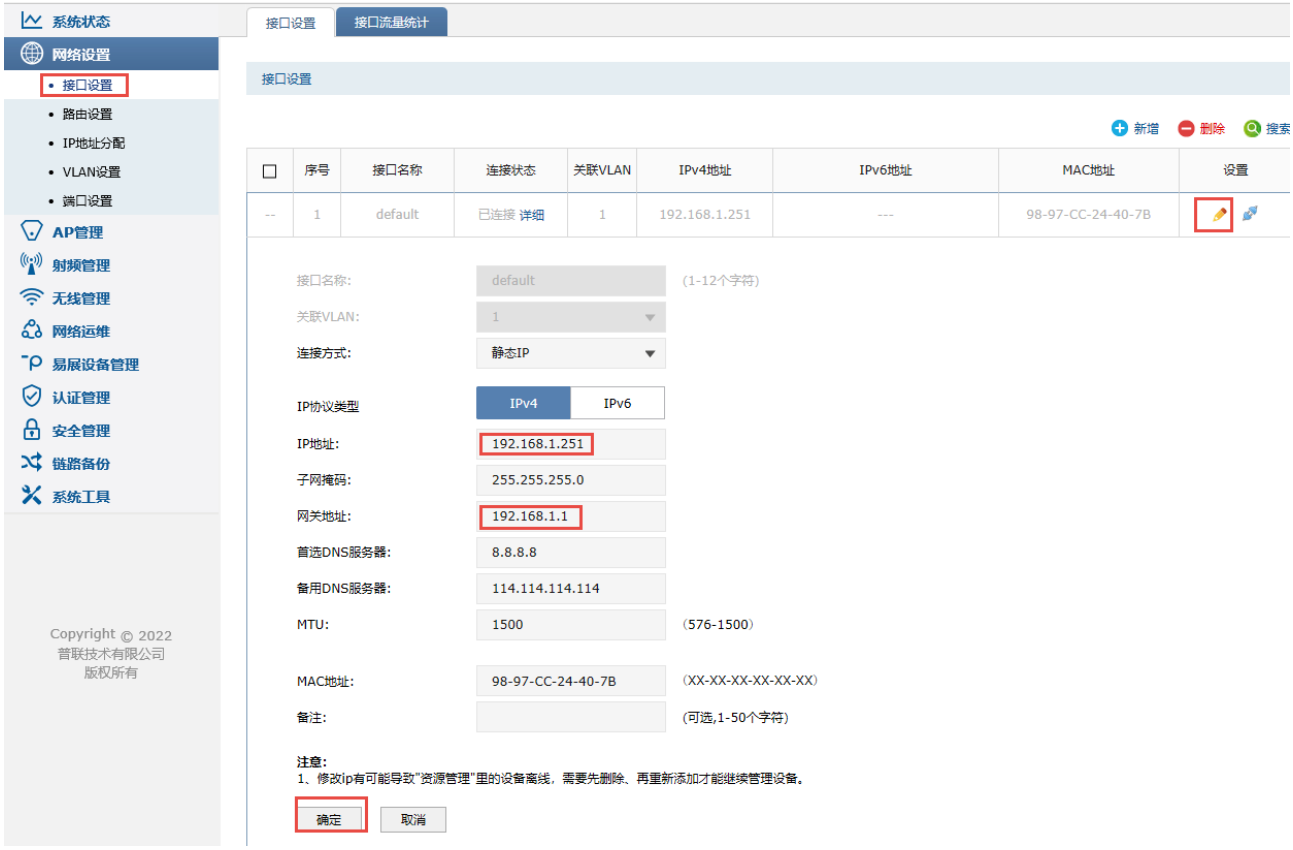
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

根据用户需求，AC、AP 以及路由器连接参考拓扑如下：



配置步骤：

1. 进入页面：网络设置 >> 接口设置， 在系统默认条目的后面点击编辑 ，填写配置 AC 的管理 IP 和网络中正确的网关（一般是路由器的 IP 地址），如下图。



2. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服务端口重复。
认证模式	设置 Portal 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于 VLAN 表示连接到这个 VLAN 中的终端都需要认证才能上网。

4. 进入页面：认证管理 >>Portal 认证>> 远程 Portal， 点击<新增>，填写已搭建好的外部 WEB 服务器地址，认证服务器类型选择本地服务器，如下图。

5. 进入页面：认证管理 >> 用户管理， 点击<新增>，设置认证用户名和密码，根据实际需求可以设置免费用户和正式用户，并设置其他参数，如下图。

以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码

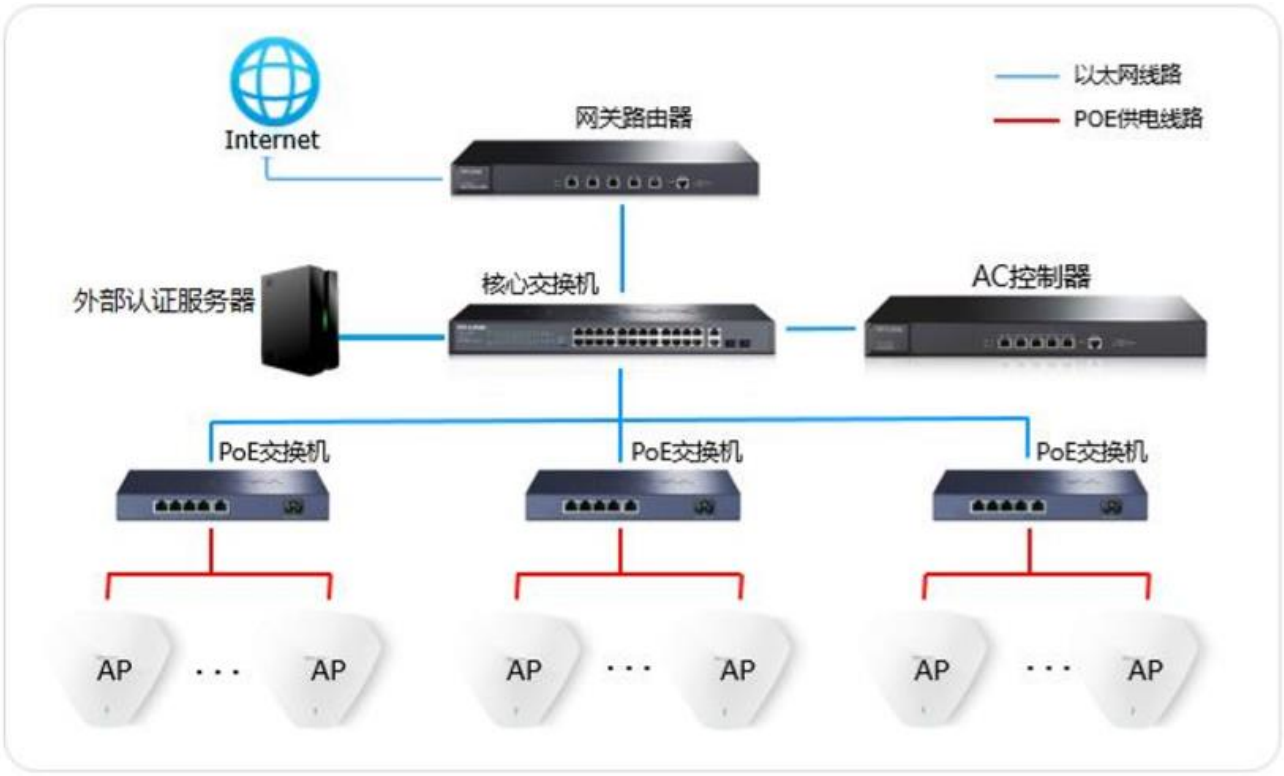
认证通过后即可上网。

15.6.5 Portal 认证配置实例——使用外置 WEB 服务器和外部认证服务器

某商场需要实现无线覆盖，为员工提供无线网络接入，有以下需求：

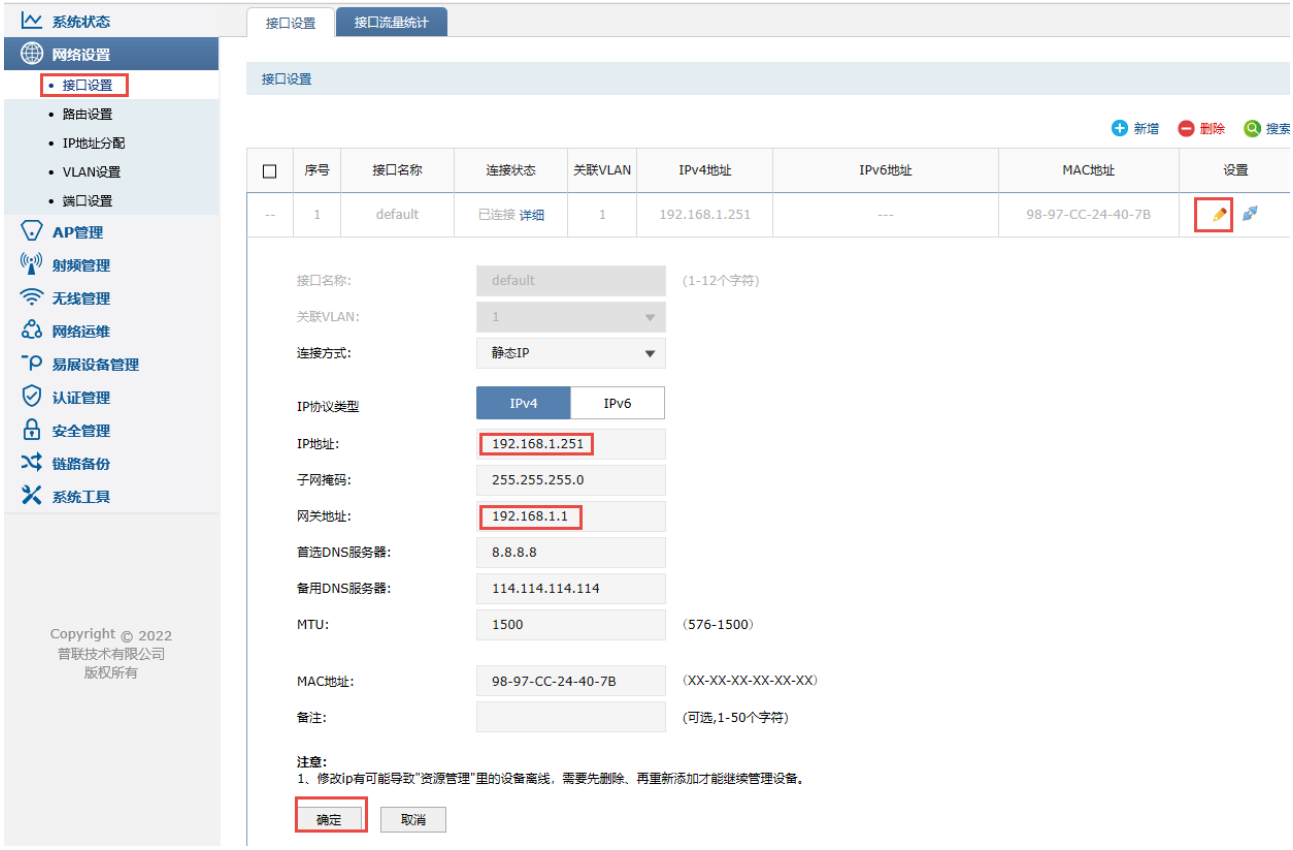
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

根据用户需求，AC、AP 以及路由器连接参考拓扑如下：



配置步骤：

1. 进入页面：网络设置 >> 接口设置， 在系统默认条目的后面点击编辑 ，填写配置 AC 的管理 IP 和网络中正确的网关（一般是路由器的 IP 地址），如下图。



2. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服务端口重复。
认证模式	设置 Portal 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于 VLAN 表示连接到这个 VLAN 中的终端都需要认证才能上网。

4. 进入页面：认证管理 >> 认证服务器 >> Radius 服务器， 点击<新增>，服务器地址填写搭建的专用认证服务器（如 Radius 服务器）的 IP 地址，填写 Radius 服务器的共享密钥，如下图。

5. 进入页面：认证管理 >> 认证服务器 >> 认证服务器:， 点击<新增>，主服务器选择上一步设置的 Radius 服务器名称，如下图。

6. 进入页面：认证管理 >> Portal 认证 >> 远程 Portal， 点击<新增>，填写已搭建好的外部 WEB 服务器的 IP 地址，认证服务器类型选择远程服务器，点击<确定>，如下图。

以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

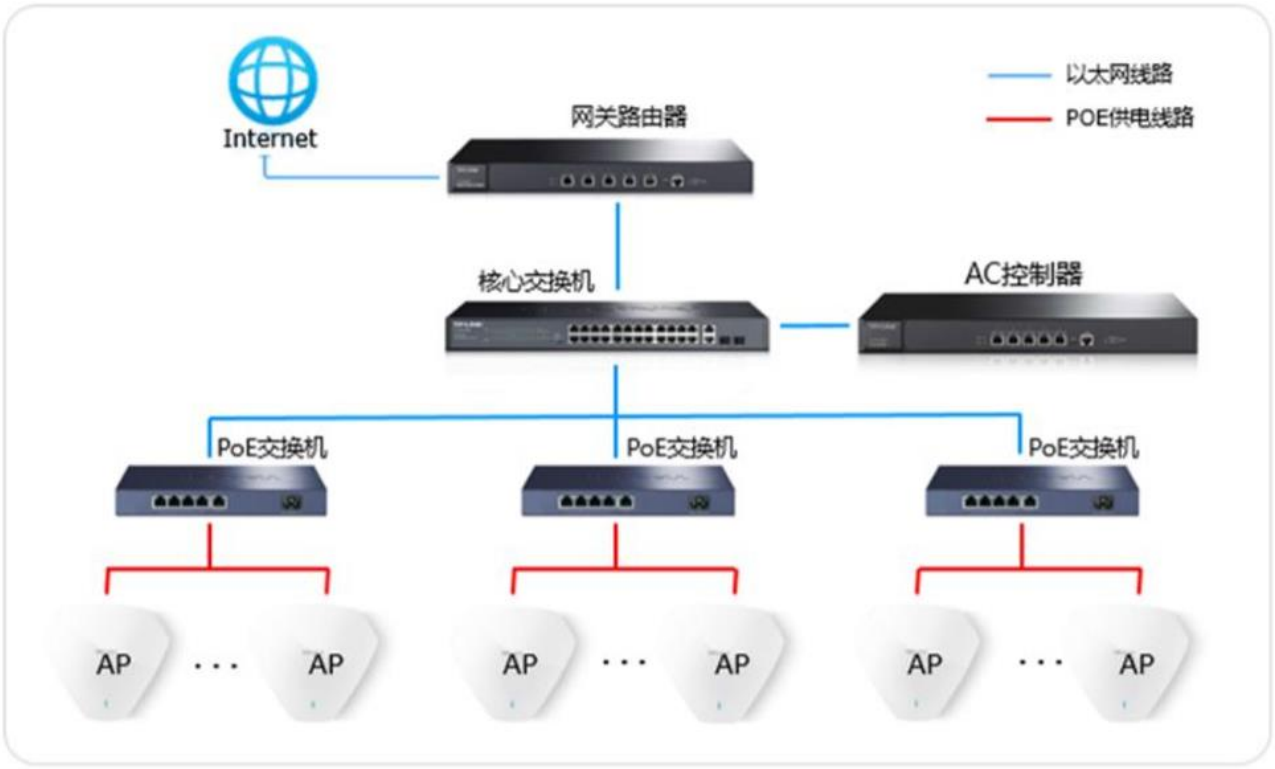
15.6.6 短信认证配置实例

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。AC 控制器支持短信认证功能，本节通过典型应用实例介绍 AC 控制器的短信认证功能的应用与配置。

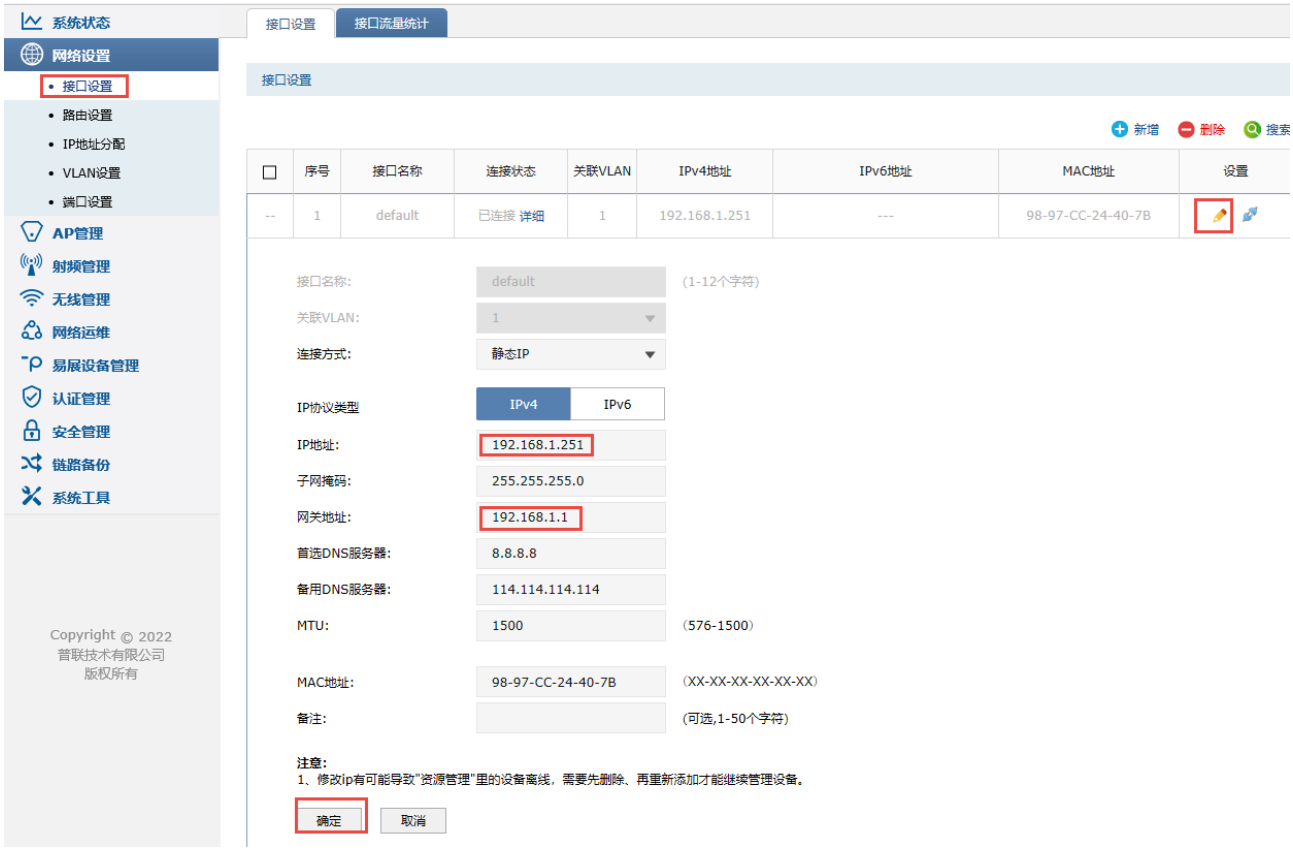
某商场需要实现无线覆盖，为顾客提供无线网络接入，有以下需求：

商场无线网络需要顾客通过短信认证的方式认证通过之后才能上网。

根据用户需求，AC、AP 以及路由器连接参考拓扑如下：



1. 进入页面：网络设置 >> 接口设置， 在系统默认条目的后面点击编辑 ，填写配置 AC 的管理 IP 和网络中正确的网关（一般是路由器的 IP 地址），如下图。



2. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服务端口重复。
认证模式	设置 Portal 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于 VLAN 表示连接到这个 VLAN 中的终端都需要认证才能上网。

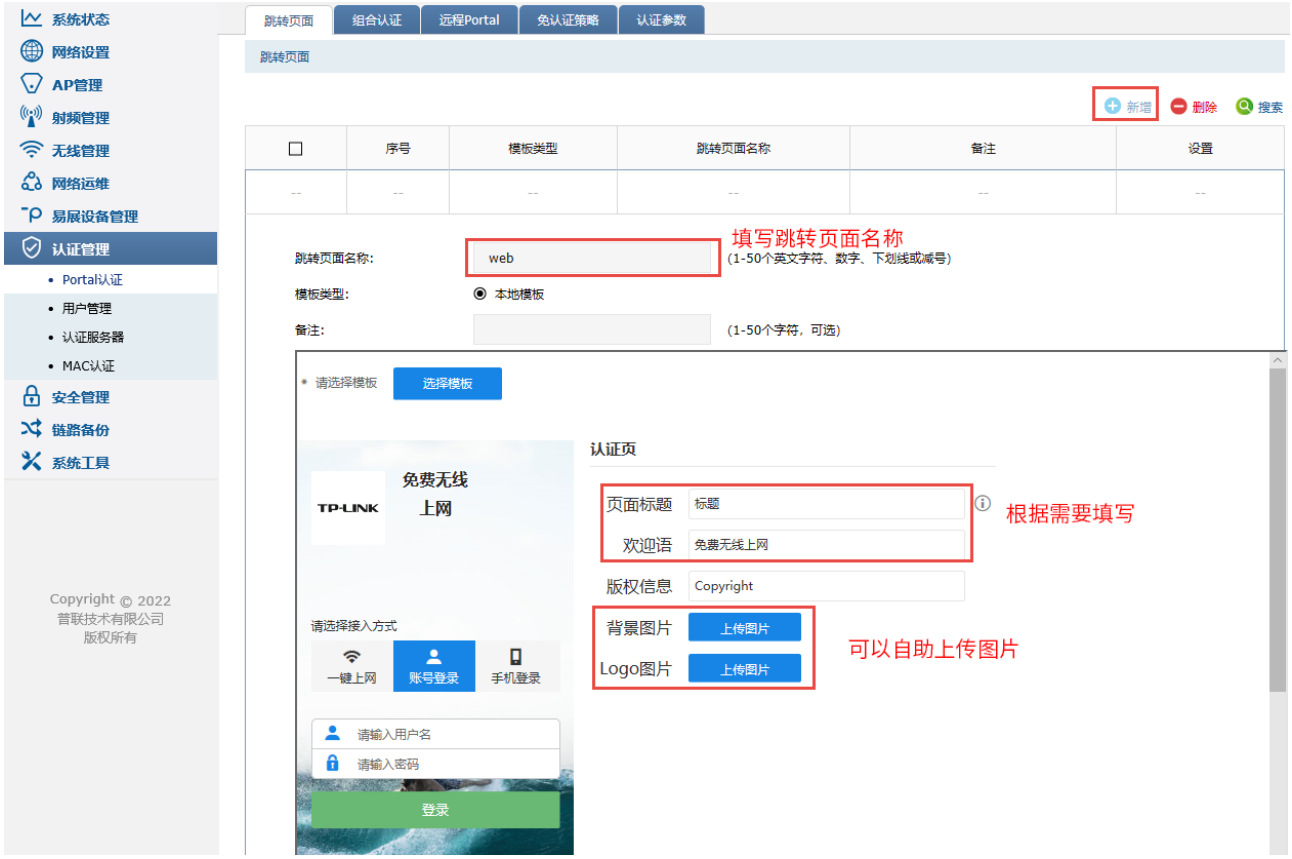
4. 短信设置

（1） 短信服务设置

详细设置方法可参考官网设置文档： 不同平台短信服务的设置方法

（2） 跳转页面设置

进入页面：认证管理 >> Portal 认证 >> 跳转页面， 点击<新增>，根据实际需求设置跳转页面标题、欢迎信息等，如下图。



（3） 认证参数配置

进入：认证管理 >> Portal 认证 >> 组合认证，点击<新增>，选择短信认证设置短信认证参数：

认证参数设置中，请根据第一步所选择的短信服务平台（阿里云、腾讯云、百度云、网易云信、HTTP 协议的服务器），相应填写平台中所获取到的参数信息（不同平台短信服务的设置方法）：

- 阿里云


一键上网
Web认证
短信认证
状态:
启用
禁用
免费上网时长:
30
分钟（1-43200）
验证码有效期:
1
分钟（1-3）
通道类型:
阿里云
阿里云提供相关参数
Access Key ID:
填写Access Key ID
(1-50个字符)
Access Key Secret:
填写Access Key Secret
(1-50个字符)
模板CODE:
填写模板CODE
(1-50个字符)
签名名称:
填写签名名称
(1-50个字符)

- 网易云信


一键上网
Web认证
短信认证
状态:
启用
禁用
免费上网时长:
30
分钟（1-43200）
验证码有效期:
1
分钟（1-3）
通道类型:
网易云信
网易云信提供相关参数
AppKey:
填写APP ID
(1-50个字符)
App Secret:
填写App Secret
(1-50个字符)
模板ID:
填写模板ID
(1-50个字符)
短信签名:
填写短信签名
(1-50个字符)

- 腾讯云


一键上网
Web认证
短信认证
状态:
启用
禁用
免费上网时长:
30
分钟（1-43200）
验证码有效期:
1
分钟（1-3）
通道类型:
腾讯云
腾讯云提供相关参数
SMK_App_ID:
填写SMK_App_ID
(1-50个字符)
App Secret:
填写App Secret
(1-50个字符)
模板ID:
填写模板ID
(1-50个字符)
签名:
填写短信签名
(1-50个字符)

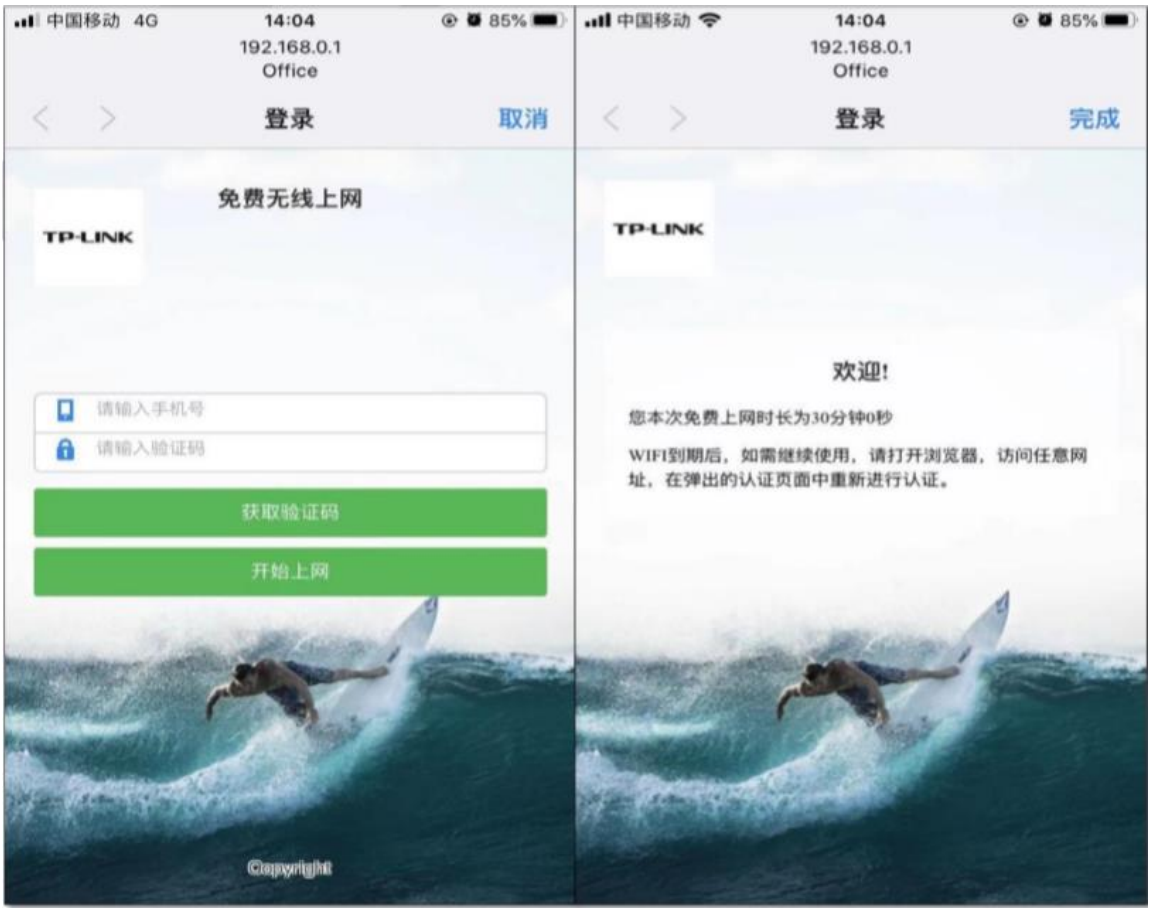
- 百度云


一键上网
Web认证
短信认证
状态:
启用
禁用
免费上网时长:
30
分钟（1-43200）
验证码有效期:
1
分钟（1-3）
通道类型:
百度云
百度云提供相关参数
Access Key ID:
填写Access Key ID
(1-50个字符)
Secret Access Key:
填写Secret Access Key
(1-50个字符)
模板ID:
填写模板ID
(1-50个字符)
短信签名:
填写短信签名
(1-50个字符)
签名ID:
填写签名ID
(1-100个字符，可选)

- HTTP 协议

填写完毕点击<确定>，至此短信认证设置完成，顾客连接商场的无线网络 SSID 通过短信认证后即可上网。

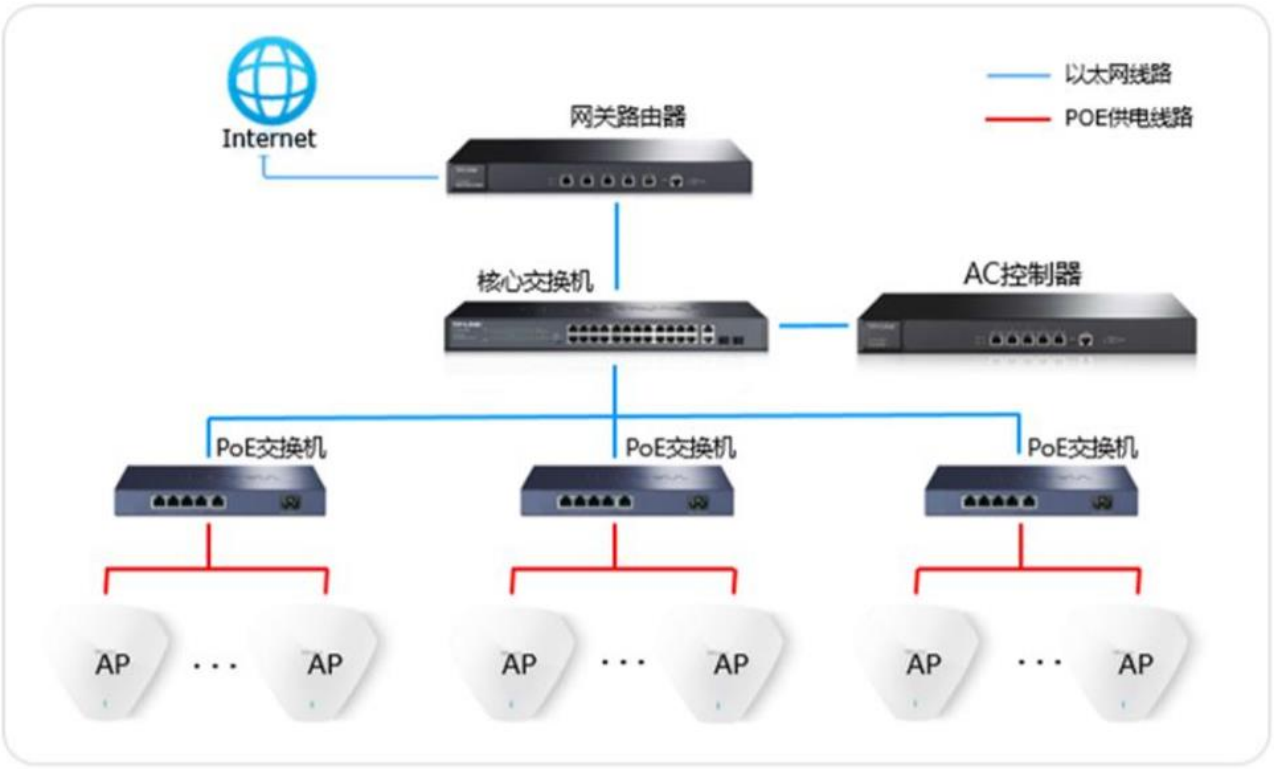
效果图如下：



15.7 一键上网使用方法

15.7.1 应用介绍

随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。AC 控制器支持 Portal 功能，认证方式灵活，支持广告推送。本文通过典型应用实例介绍 AC 控制器 Portal 认证功能的应用与配置。根据用户需求，AC、AP 以及路由器连接参考拓扑如下：



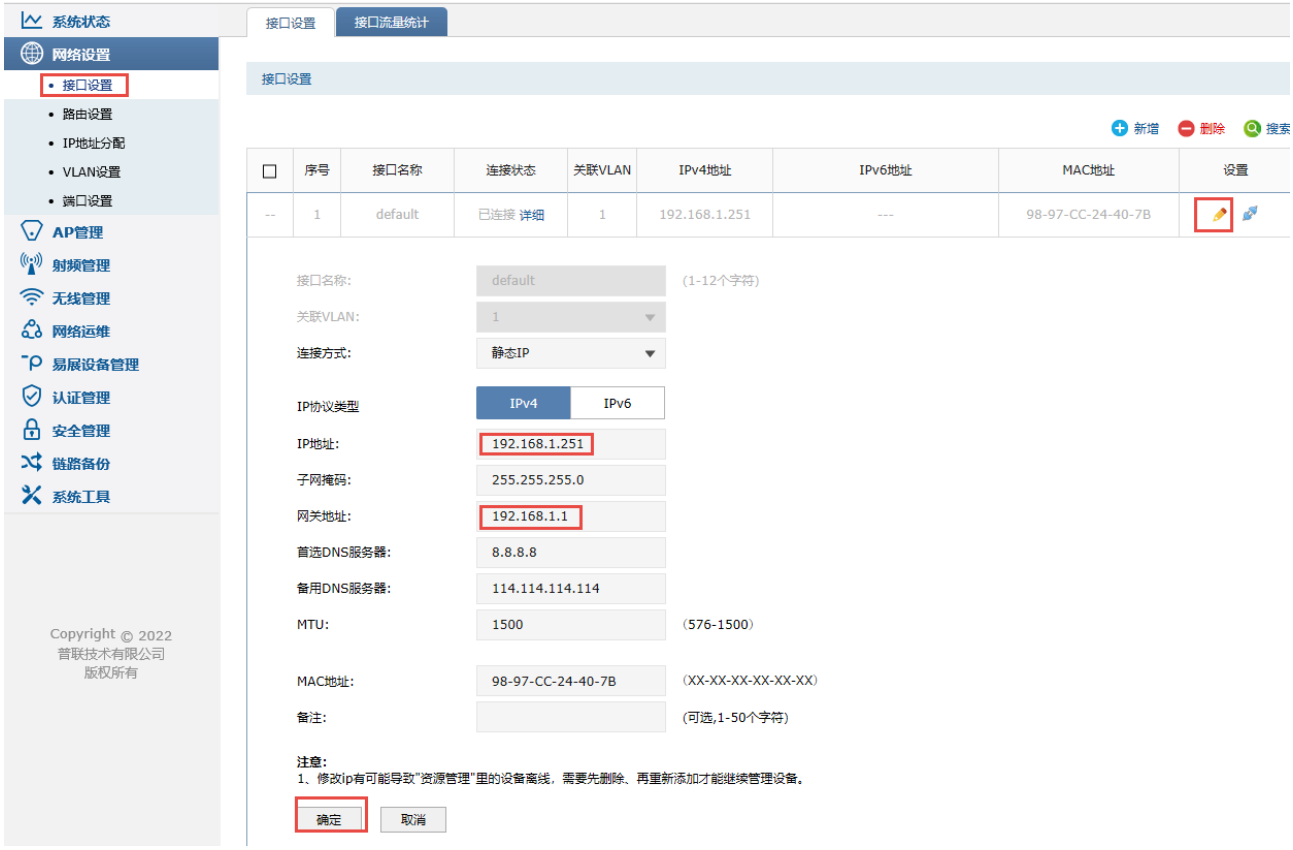
15.7.2 需求介绍

某商场需要实现无线覆盖，为顾客提供无线网络接入，有以下需求：

顾客在商场内都能连接 WIFI，且无需认证即可上网。

15.7.3 设置方法

1. 进入页面：网络设置 >> 接口设置， 在系统默认条目的后面点击编辑 ，填写配置 AC 的管理 IP 和网络中正确的网关（一般是路由器的 IP 地址），如下图。



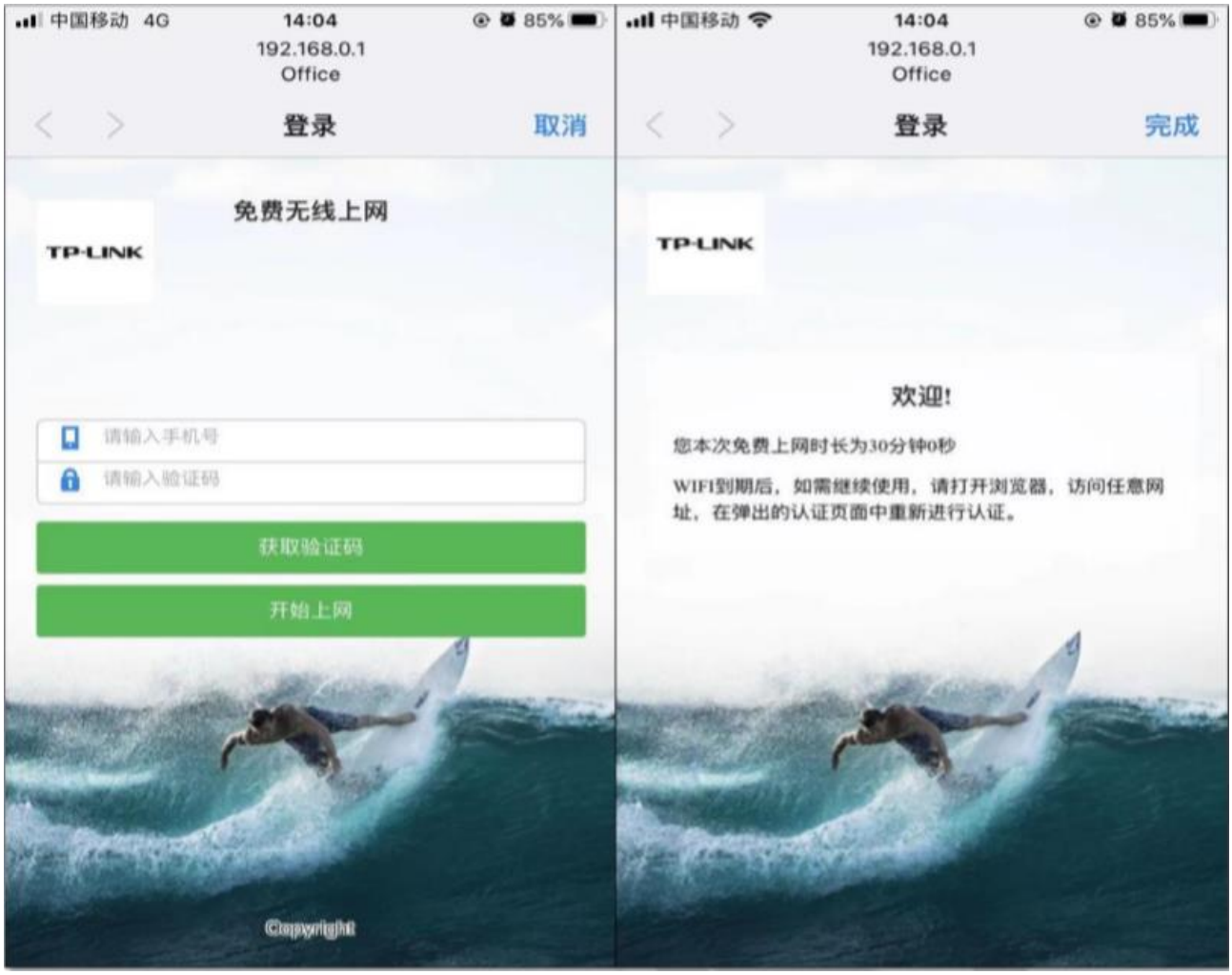
2. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服务端口重复。
认证模式	设置 Portal 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式，基于 SSID 表示连接这个 SSID 的终端都需要认证才能上网，基于 VLAN 表示连接到这个 VLAN 中的终端都需要认证才能上网。

4. 进入页面：认证管理 >> Portal 认证 >> 组合认证， 点击<新增>，启用一键上网功能，如下图。

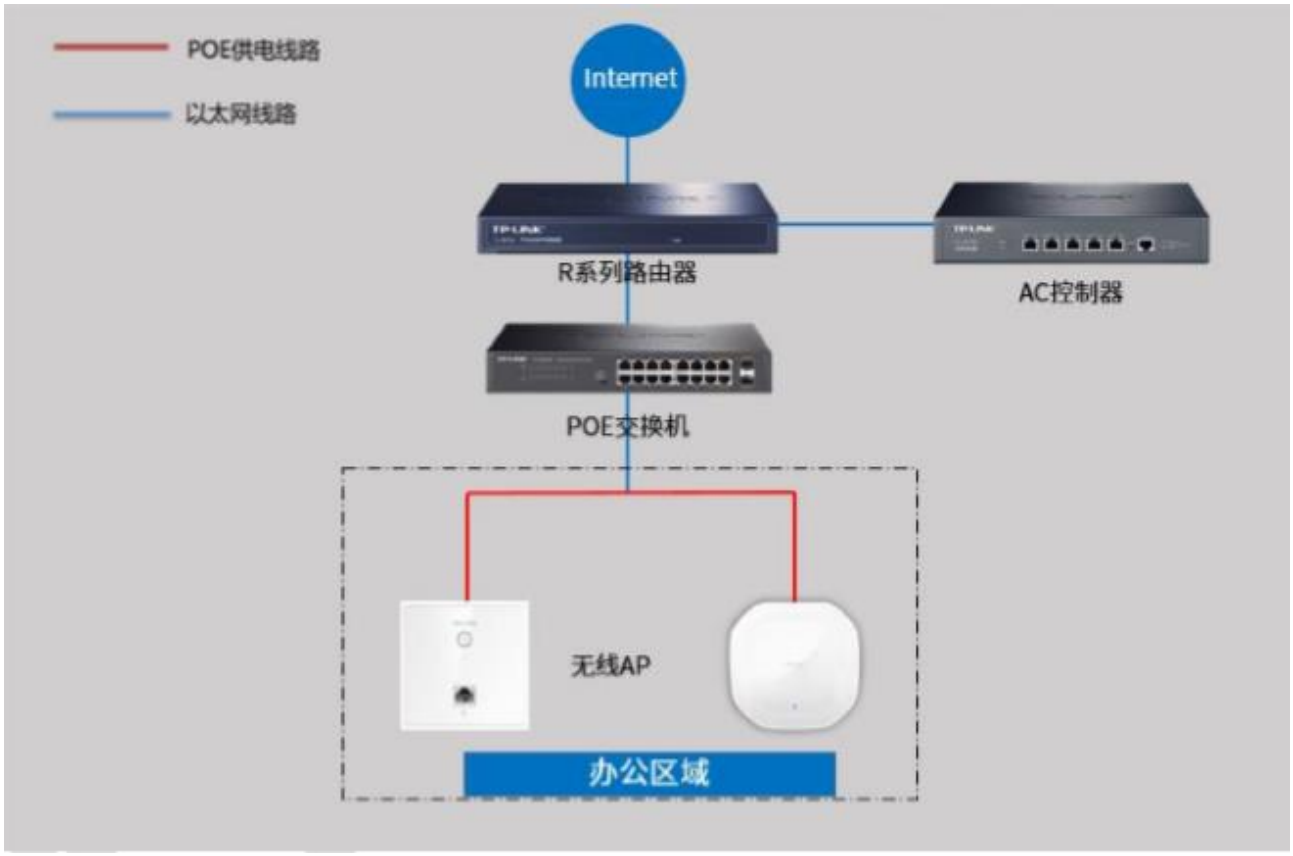
以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接商场的无线可以一键上网。效果图如下：



15.8 免认证策略的使用方法

15.8.1 应用介绍

目前越来越多的公共场所（如商场、酒店、景区等）需要提供免费网络供访客使用，访客连接网络后需要通过认证才可以免费使用网络。免认证策略可以实现客户端不需要认证就能访问指定的网站或者服务器。本文通过典型应用实例介绍 AC 控制器免认证策略的应用与配置。根据用户需求，路由器和 AC、AP 连接参考拓扑如下：



15.8.2 需求介绍

某办公室需要实现无线覆盖，员工需要通过认证后才能上网，有以下需求：

1、 特定终端如打印机不需要认证即可上网；

2、 员工无需认证也可以访问公司外网服务器；

3、 员工无需认证也可以访问公司网站；

15.8.3 设置方法

1. 进入页面：认证管理 >> Portal 认证 >> 免认证策略， 添加免认证策略，如下图。

以上设置可以实现固定设备无需认证就可以上网。

2. 进入页面：认证管理 >> Portal 认证 >> 免认证策略，添加免认证策略，如下图。

以上设置可以实现局域网的所有电脑，无需认证即可访问 121.202.33.100 的外网服务器。

3. 进入页面：认证管理 >> Portal 认证 >> 免认证策略， 点击<新增>，添加免认证策略，如下图。

以上设置可以实现局域网的所有电脑，无需认证即可访问公司网站。

由于终端上网可能即需要使用 UDP 协议又需要使用 TCP 协议，所以一个终端设备需要建立两条免认证策略服务协议，分别选择 UDP 和 TCP。

第16章 安全管理

16.1 广播风暴抑制

广播风暴，是指网络上的广播帧由于网络拓扑的缺陷等原因导致被大量复制转发而影响正常网络通信的现象。广播风暴抑制，是指 AP 在收到的广播帧速率到预定门限值时，将自动丢弃收到的广播帧，防止广播风暴。

本页面开启 AP 的广播风暴抑制功能和设置广播风暴抑制的门限速率。

进入页面：安全管理 >> 广播风暴抑制，点击<开启>，启用广播风暴抑制功能，并选取预定义速率或自定义抑制速率，点击<设置>，如下图。

16.2 广播风暴抑制配置实例

16.2.1 需求介绍

广播风暴抑制功能可以抑制从有线到无线的广播数据，一定程度降低广播风暴对无线网络的影响，需要用

户根据实际应用场景配置合适的抑制速率。如果在无线环境中有大量的广播数据传输，由于广播包需要发送给每个 STA 采用所以采取低速率传输的方式，大量广播包将会长时间的占用无线信道，大幅度降低无线性能，严重影响无线体验。大量广播包可能导致无线延迟高、丢包甚至无线连接不上等问题。

16.2.2 广播风暴抑制设置

进入页面：安全管理 >> 广播风暴抑制，点击<开启>，启用广播风暴抑制功能，并选取预定义速率或自定义抑制速率，点击<设置>，如下图。

16.3 DHCP 防护

DHCP 防护，是指 AP 在接收到 DHCP 报文时检查其 IP 或 MAC，只允许绑定到该 AP 的 DHCP 服务器报文通过。该功能可以防止无线客户端从非法 DHCP 服务器获取 IP。

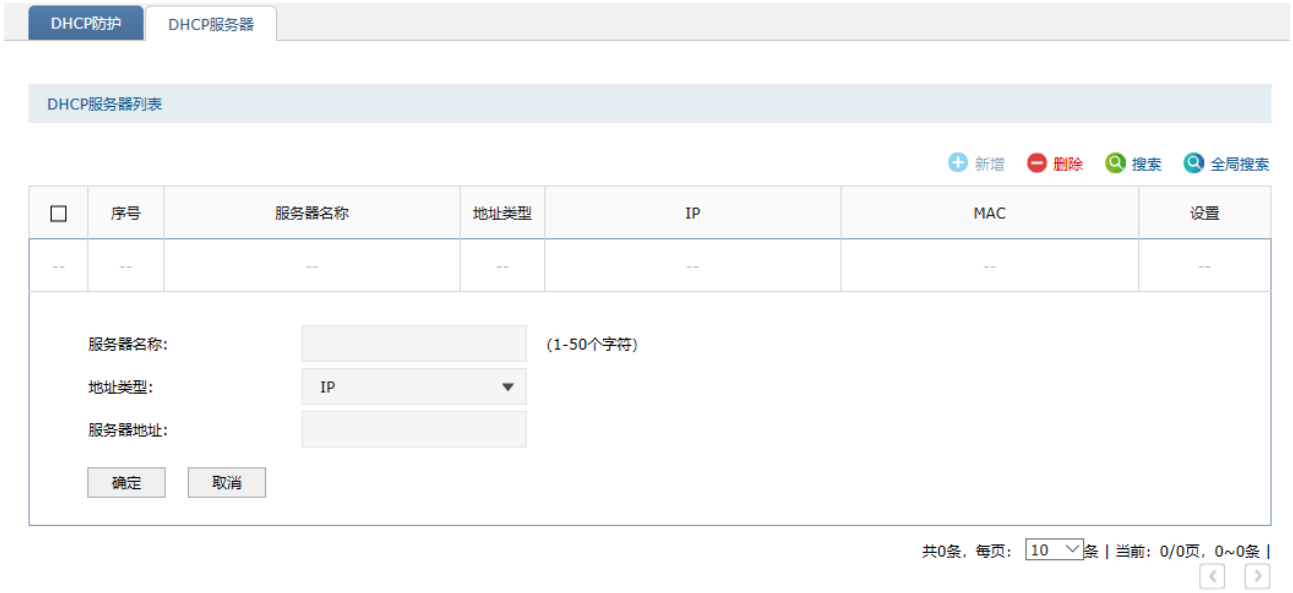
本页面可以查看已关联 AP 的 DHCP 防护设置，单独或批量修改每个 AP 绑定的 DHCP 防护条目。

进入页面：安全管理 >> DHCP 防护，查看已关联 AP 的 DHCP 防护设置，单独或批量修改每个 AP 绑定的 DHCP 防护条目，如下图。

批量绑定	勾选多个 AP 条目，再点击<批量绑定>按钮，可以进入多个 AP 的 DHCP 防护设置页面。在其中勾选服务器条目，执行<绑定>或<取消绑定>操作。
批量清空	勾选多个 AP 条目，再点击<批量清空>按钮，可以清空多个 AP 绑定的所有 DHCP 服务器条目。

16.4 DHCP 服务器

进入页面：安全管理 >> DHCP 防护 >> DHCP 服务器，查看、新增、修改和删除 DHCP 服务器，以供 AP 绑定，点击<新增>，可添加 DHCP 服务器。

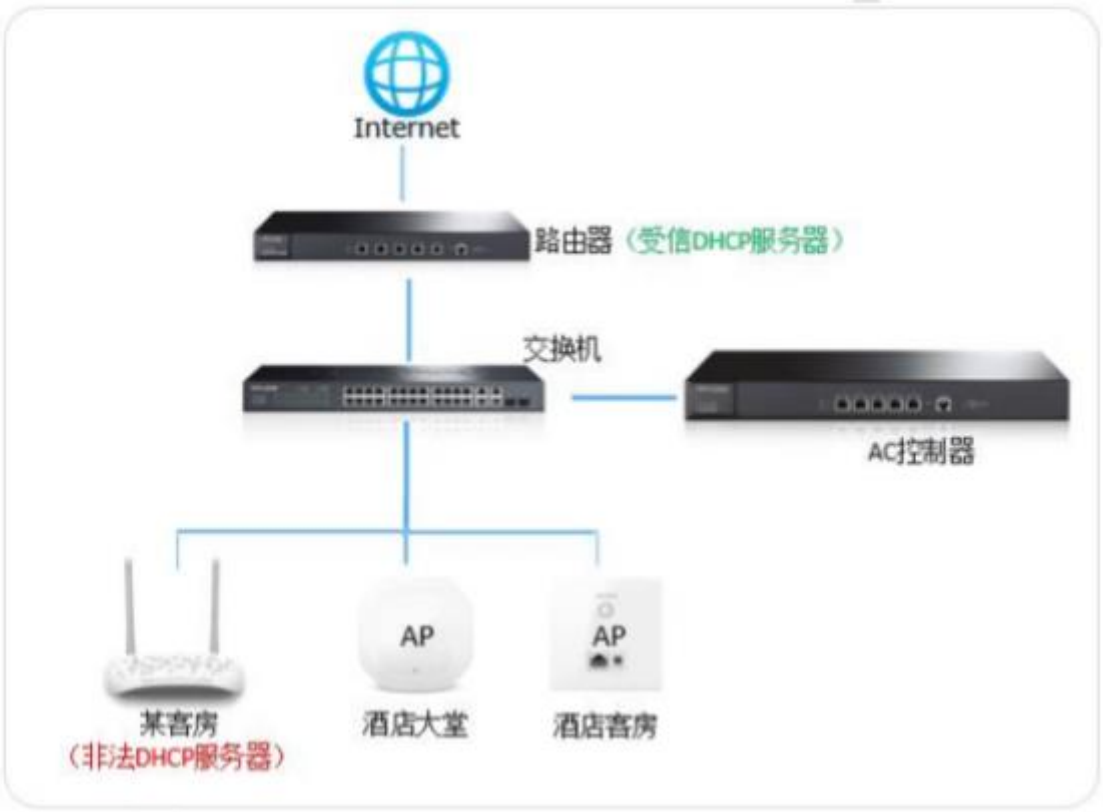


16.5 DHCP 防护配置实例

16.5.1 需求介绍

AC 控制器的 DHCP 防护功能，可以防止连接在 AP 上面的无线终端和有线终端，从非法 DHCP 服务器获取 IP 地址，避免因为终端获取到错误的网关而影响到上网。

公共场所如酒店、宿舍、企业，其 Wi-Fi 信号较为开放，为了避免私接路由器、接入其他 DHCP 服务器，导致破坏网络结构、终端出现获取不到正确 IP、IP 地址混乱等情况，就需要用到 AC 的 DHCP 防护功能。



16.5.2 DHCP 防护设置

- 添加 DHCP 服务器

进入页面：安全管理 >> DHCP 防护 >> DHCP 服务器，点击<新增>，添加 DHCP 服务器，地址类型可以选择 IP 或者 MAC，并填写对应的地址，如下图。

➢ 将 DHCP 服务器绑定到 AP

选择 AP 分组，勾选要绑定的 AP，并点击 <批量绑定>，如下图。

如果不需要批量绑定，也可以点击要绑定 AP 条目的<DHCP 绑定>进行绑定。勾选要绑定的 DHCP 服务器，并点击<绑定> ，如下图。

➢ 启用 DHCP 防护

点击<返回 DHCP 防护>，此时 DHCP 防护仍是已禁用的状态，需要启用。勾选所有已绑定 DHCP 服务器的 AP，并点击<启用>，如下图。

设置完毕，DHCP 防护列表如下：

16.6 ARP/ND 防护

ARP/ND 防护，是指 AP 在接收到 ARP 或 IPv6 的 ND 协议报文时检查其 IP 和 MAC，只有源 IP 和源 MAC 地址均匹配的数据报文才进行转发。该功能可以对 AP 有线口收到的 ARP/ND 报文进行检测，防止 ARP/ND 攻击，确保无线网络的稳定性。

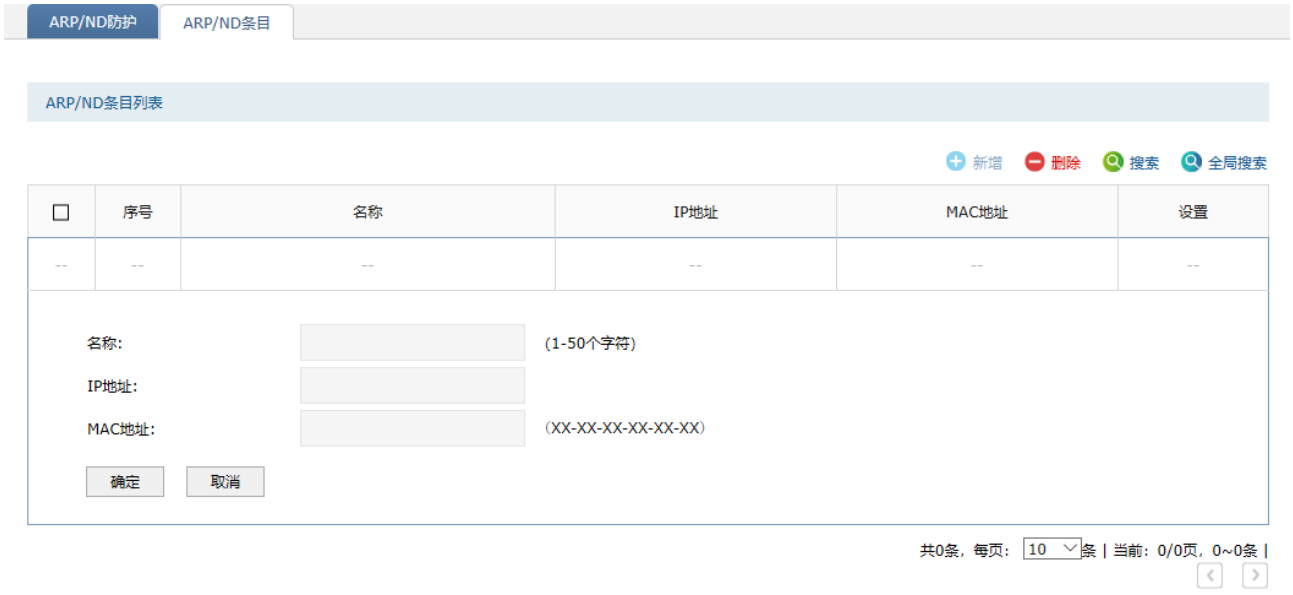
本页面可以查看已关联 AP 的 ARP/ND 防护设置，单独或批量修改每个 AP 绑定的 ARP/ND 防护条目。本页面可以查看已关联 AP 的 DHCP 防护设置，单独或批量修改每个 AP 绑定的 DHCP 防护条目。

进入页面：安全管理 >>ARP/ND 防护，查看已关联 AP 的 ARP/ND 防护设置，单独或批量修改每个 AP 绑定的 ARP/ND 防护条目，如下图。

批量绑定	勾选多个 AP 条目，再点击<批量绑定>按钮，可以进入多个 AP 的 ARP/ND 防护设置页面。在其中勾选服务器条目，执行<绑定>或<取消绑定>操作。
批量清空	勾选多个 AP 条目，再点击<批量清空>按钮，可以清空多个 AP 绑定的所有 ARP/ND 服务器条目。

16.7 ARP/ND 条目

进入页面：安全管理 >> ARP/ND 防护 >> ARP/ND 条目，查看、新增、修改和删除需要绑定设备的 IP 地址和 MAC 地址，点击<新增>，添加需要绑定的设备。



16.8 ARP/ND 防护配置实例

16.8.1 需求介绍

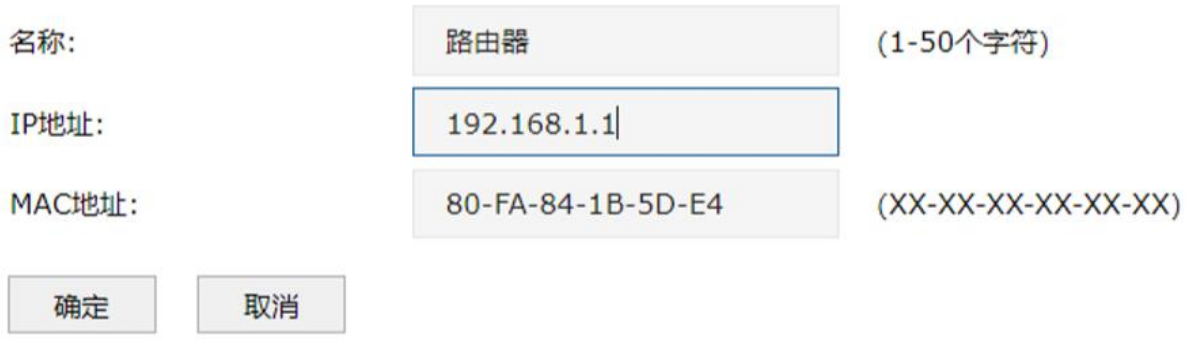
AC 控制器的 ARP 防护功能，可以对 AP 有线口收到的 ARP 报文进行检测，防止 ARP 攻击，确保无线网络的稳定性。

ARP 是 IP 与 MAC 地址的解析协议，对网络通信至关重要。但是，由于 ARP 没有保护机制，所以伪造的 ARP 数据包会欺骗通信终端或设备，导致出现通信异常。一般情况下，上网数据直接在主机和网关之间进行交互，ARP 欺骗主要针对网关和主机的 ARP 列表进行欺骗，导致通信异常。那么 ARP 防护就需要从两个方面着手，在网关上绑定主机的 ARP 信息，在主机上绑定网关的 ARP 信息，从而实现双向绑定，确保网络安全。

16.8.2 ARP/ND 防护设置

- 添加 ARP 防护条目

进入页面：安全管理 >>ARP/ND 防护 >>ARP/ND 防护条目，点击<新增>，添加要绑定设备的 IP 及 MAC 地址，如下图。



- 将 ARP 防护条目绑定到 AP

选择 AP 分组，勾选要绑定的 AP，并点击<批量绑定> ，如下图。

勾选要绑定的 ARP 条目，并点击<绑定> ，如下图。

➢ 启用 ARP 防护

点击<返回 ARP 防护>，确定每个 AP 绑定 ARP 的防护状态，如下图。

第17章 链路备份

17.1 双链路备份

本页面用于配置双链路功能。

双链路功能允许 AP 与两台 AC 分别建立主/备链路，主用链路上的 AC 负责为 AP 提供服务，备用链路为 AP 提供冗余备份。当主用链路发生故障时，备用链路升级为主用链路，继续为 AP 提供服务。

进入页面：链路备份 >> 双链路备份，点击<启用双链路>，设置链路优先级和对端 IP 地址，如下图。

17.2 双链路备份配置实例

17.2.1 需求介绍

在大中型网络中，如果只使用一台 AC，同时又在 AC 上配置了认证等业务。当 AC 发生故障或 AC 与核心交换机线路故障时，会导致整个无线网络无法使用认证，对用户影响较大。

- AC 链路备份

双链路功能允许 AP 与两台 AC 分别建立主/备链路，主用链路上的 AC 负责为 AP 提供服务，备用链路为 AP 提供冗余备份。

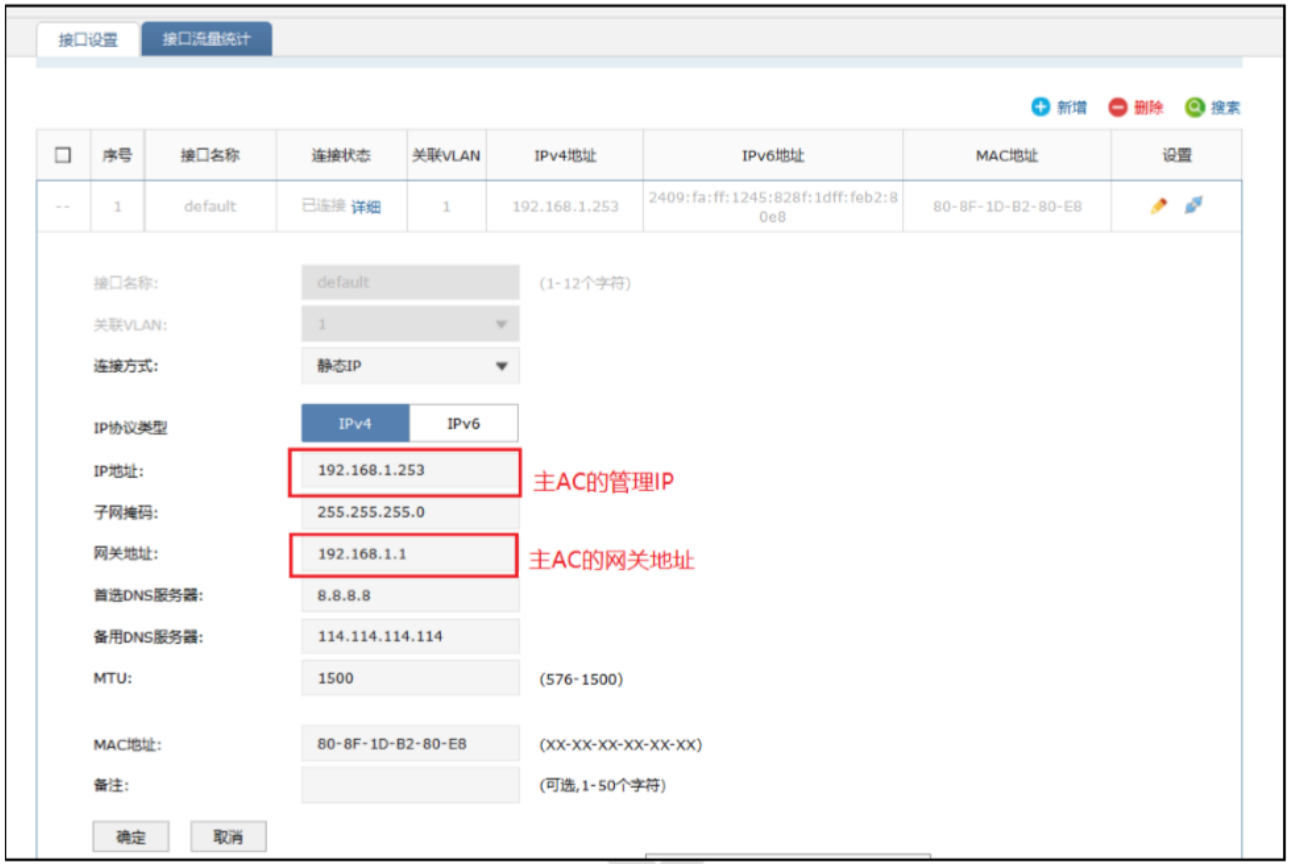
➢ 主链路异常，备链路升级主链路

当主用链路发生故障时，备用链路会自动升级为主用链路，继续为 AP 提供服务，保障无线网络正常运行。

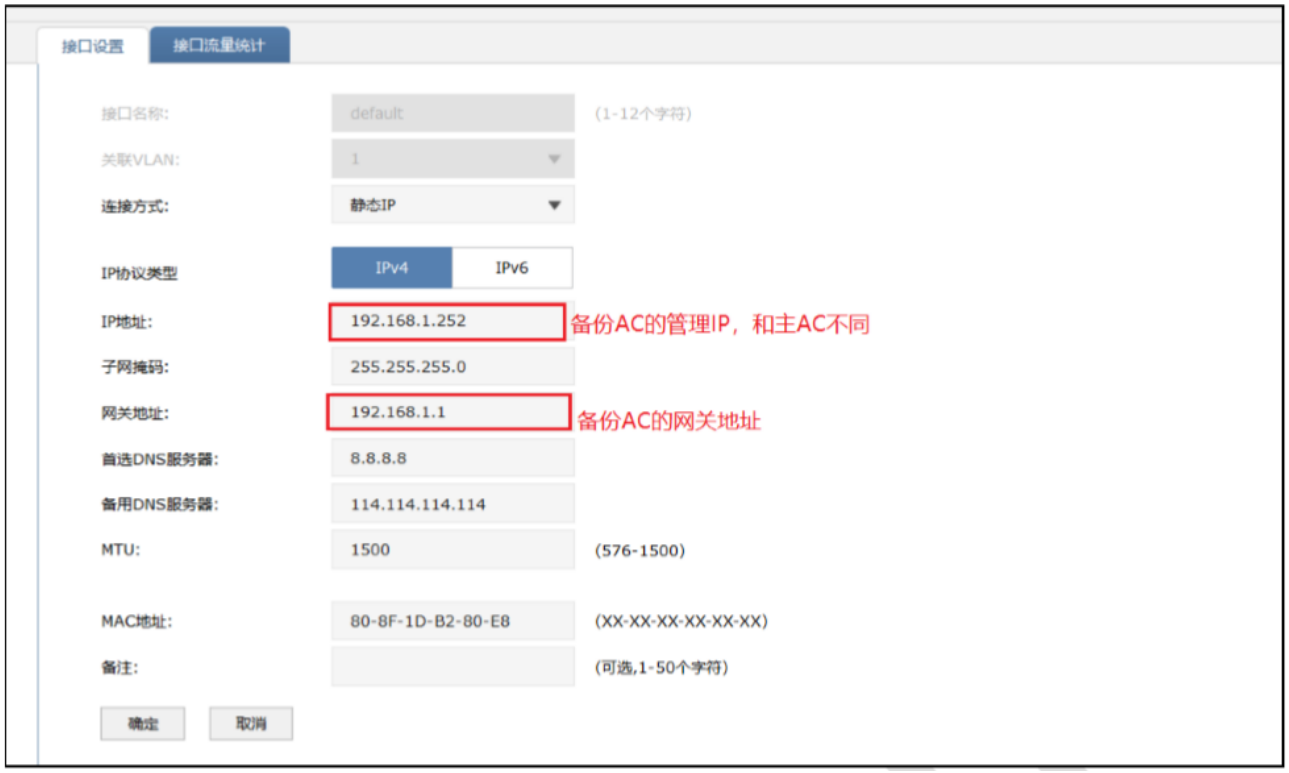
17.2.2 链路备份设置

➢ 配置主备 AC 的管理 IP

登录到主 AC 界面，进入页面：网络设置 >> 接口设置，配置主 AC 的管理 IP，如下图。

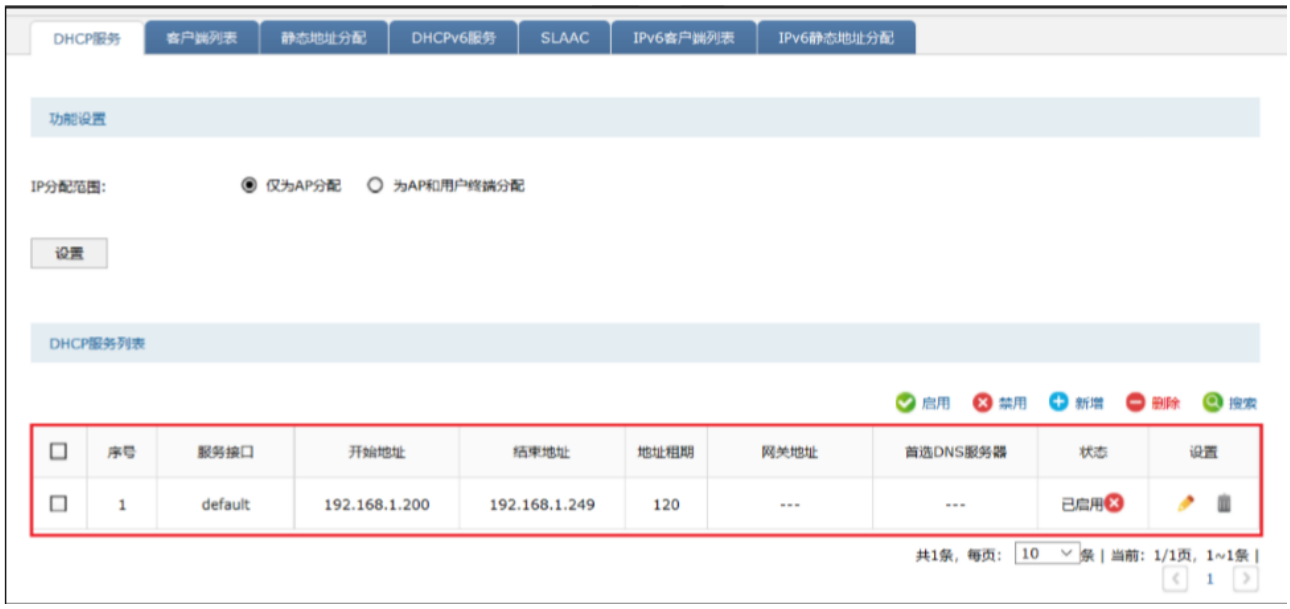


登录到备 AC 界面，进入页面：网络设置 >> 接口设置，配置备 AC 的管理 IP，如下图。



➢ 配置主备 AC 的 DHCP 服务

在 AC 界面，进入页面：网络设置 >>IP 地址分配 >>DHCP 服务，配置主备 AC 的 DHCP 服务器，如下图。



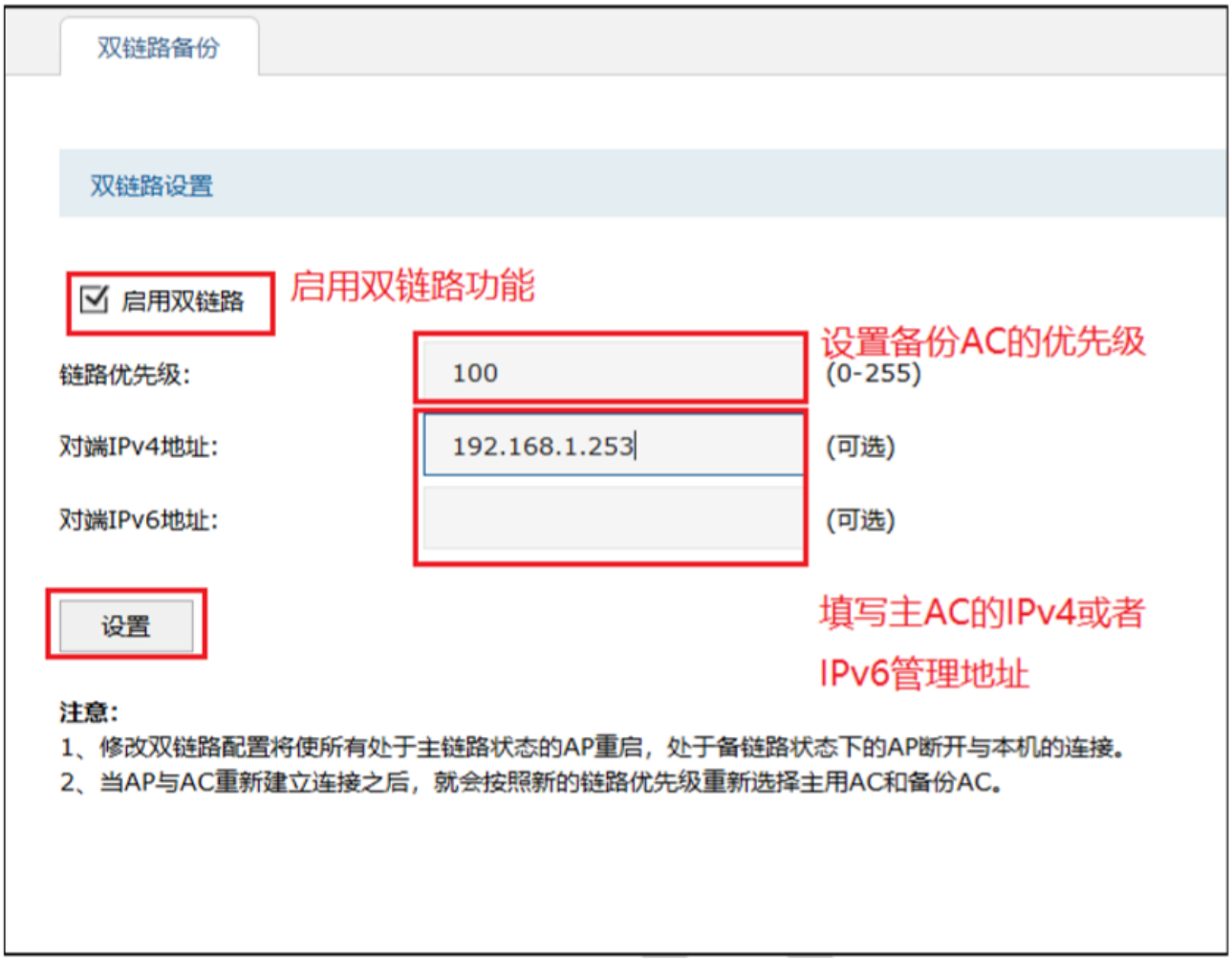
➢ 主备 AC 的其他配置

主 AC 中关于 AP 的配置项如 AP 管理，射频管理，无线管理，认证管理，安全管理等，在备用 AC 中也做同样的配置，确保 AP 切换到备用 AC 后网络功能不改变。

➢ 配置主备 AC 的双链路备份功能

进入主 AC 页面：链路备份 >> 双链路备份，点击<启用双链路>，设置链路优先级和对端 IP 地址，如下图。

进入备 AC 页面：链路备份 >> 双链路备份，点击<启用双链路>，设置链路优先级和对端 IP 地址，如下图。



链路优先级	AP 选择本 AC 作为主用 AC 的优先级,数字越大优先级越高。
对端 IPv4 地址	对端 AC 的地址，通过本机配置的 DHCPv4 服务器的报文下发，让 AP 在通过本机提供的 DHCPv4 服务获取 IP 时获得对端 AC 的地址。需要开启本机的 DHCPv4 服务才能生效。
对端 IPv6 地址	对端 AC 的地址，通过本机配置的 DHCPv6 服务器的报文下发，让 AP 在通过本机提供的 DHCPv6 服务获取 IP 时获得对端 AC 的地址。需要开启本机的 DHCPv6 服务才能生效。

说明:

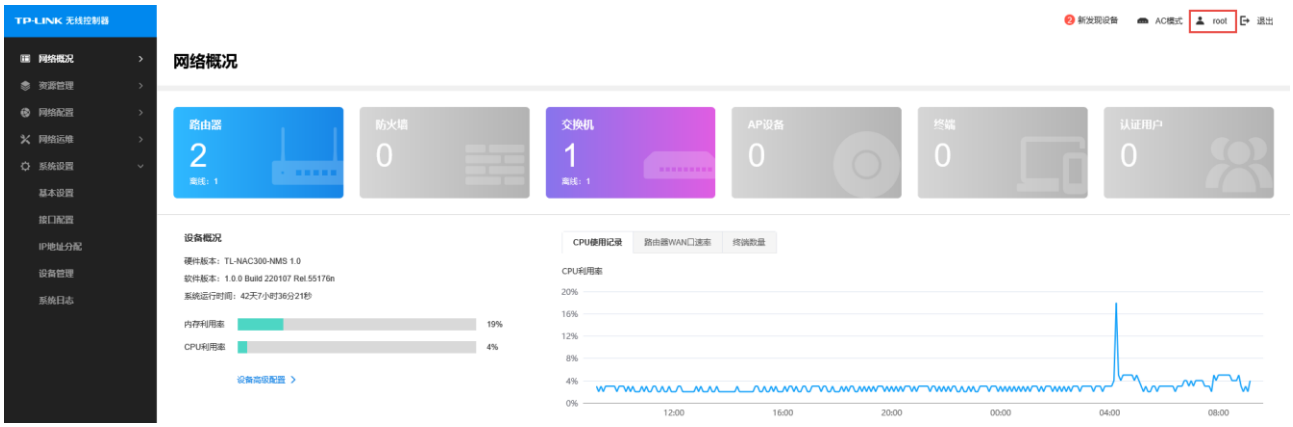
- 修改双链路配置将使所有处于主链路状态的 AP 重启，处于备链路状态下的 AP 断开与本机的连接。
- 当 AP 与 AC 重新建立连接之后，就会按照新的链路优先级重新选择主用 AC 和备份 AC。

- 当 AP 从主 AC 切换至备份 AC 时，已认证的无线客户端需要重新认证。
- 使用双链路备份时，用户需自行确保主、备 AC 之间配置的一致性

第18章 系统工具

18.1 修改用户名和密码

登录无线控制器主页面后，点击右上角 图标，可重新设置用户名和密码，如下图。



18.2 设备管理

18.2.1 恢复出厂设置

进入页面：系统工具 >> 设备管理 >> 恢复出厂设置，点击<恢复出厂设置>，即可将设备的所有配置恢复到出场时的默认状态，如下图。

18.2.2 备份与导入配置

进入页面：系统工具 >> 设备管理 >> 备份与导入配置，可查看设备当前配置版本。点击<备份>，即可保存当前的配置信息。点击<导入>，即可导入配置文件来恢复所备份的配置，如下图。

18.2.3 重启设备

进入页面：系统工具 >> 设备管理 >>重启设备，点击<重启设备>，可对设备进行重启，如下图。

说明：

- 在重启设备过程中，请不要将设备断电！

18.2.4 软件升级

进入页面：系统工具 >> 设备管理 >>软件升级，可查看软硬件版本，并进行云端软件升级和本地硬件升级，如下图。

说明：

- 在设备升级过程中，请不要将设备断电，不要对页面进行刷新！
- 使用在线升级的时候请确保设备正常联网。
- 进行软件升级后，当前的配置信息可能会丢失。请您在升级前备份产品配置信息。
- 请到网址 www.tp-link.com.cn 下载最新的升级软件。

18.2.5 设备管理

进入页面：系统工具 >> 设备管理 >>设备管理，可查看并修改设备名称，如下图。

18.3 诊断工具

18.3.1 诊断工具

进入页面：系统工具 >> 诊断工具，可使用 ping 通信检测或路由跟踪检测，查看当前网络状况，如下图。

18.3.2 故障诊断

进入页面：系统工具 >> 诊断工具 >> 故障诊断，可开启/关闭故障诊断模式，如下图。

可选择发送调试日志信息，导出诊断信息和一键清理功能，如下图，请在技术支持人员指导下使用相关功能！

说明:

- 请在技术支持人员指导下使用故障诊断功能!

18.4 时间设置

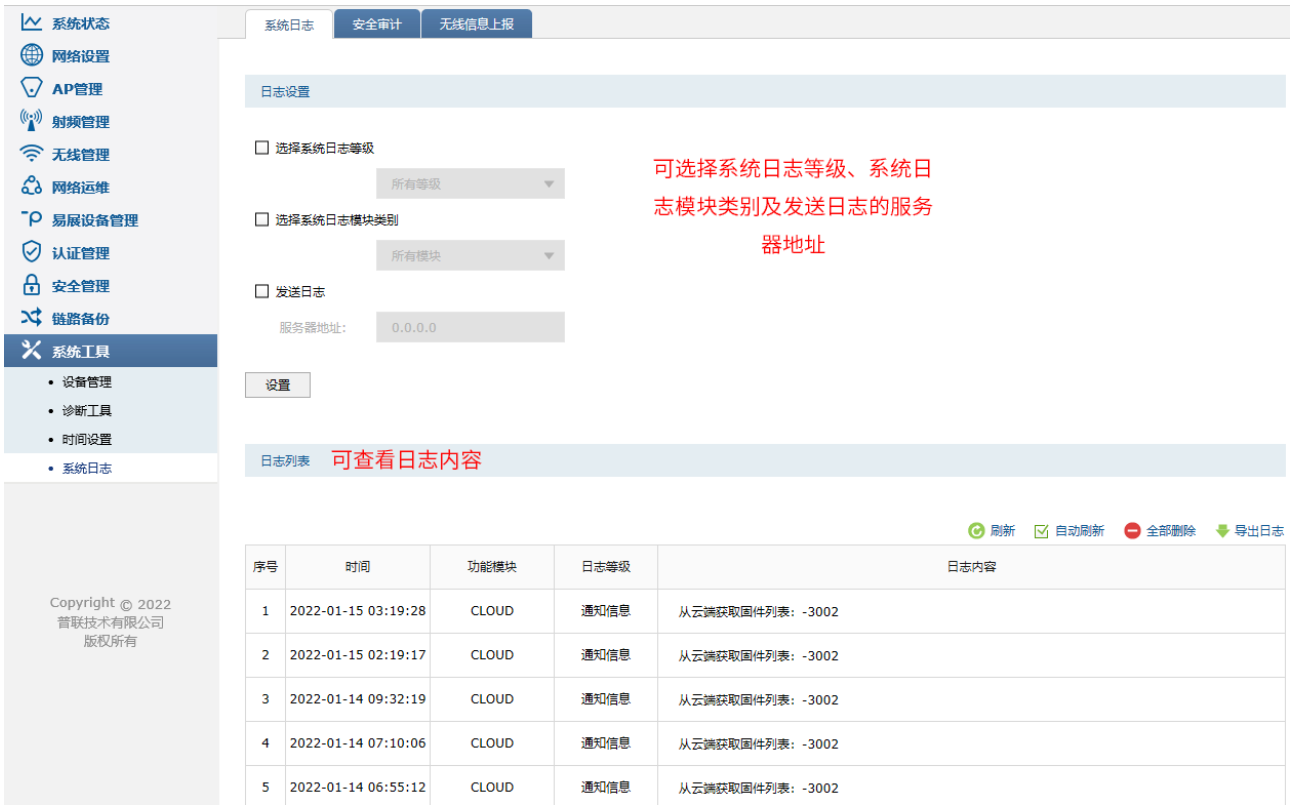
18.4.1 时间设置

进入页面:系统工具 >> 时间设置,可查看和设置系统时间,如下图。

18.5 系统日志

18.5.1 系统日志

进入页面：系统工具 >> 系统日志，可查看系统的运行状况，如下图。



18.5.2 安全审计

进入页面：系统工具 >> 系统日志 >> 安全审计，可开启支持安全审计功能路由器的相关功能，输入路由器的 IP 地址，点击<设置>，如下图。

18.5.3 无线信息上报

进入页面：系统工具 >> 系统日志 >> 无线信息上报，可开启无线信息上报功能，并设置无线信息上报的参数，点击<设置>，如下图。

上报协议　　提供 TCP、UDP、HTTP 三种协议进行无线信息上报。

服务器地址	使用 TCP、UDP 协议进行无线信息上报时，服务器地址填写 IP（Ipv4 或 Ipv6）或域名，而在使用 HTTP 协议时服务器地址填写 URL。
服务器端口号	在使用 TCP、UDP 协议进行无线信息上报时，需要设置服务器的端口号才可以完成上报。
单包最大负载	限制每个数据包最多携带多少个设备信息。

点击页面  ，查看更多页面设置参数信息。