TP-LINK®

无线控制器

用户手册

1910041084 REV1.0.0

声明

目录

第1章　用户手册简介

本手册旨在帮助用户正确使用无线控制器，以 TL-AC1000 为例进行介绍。

本手册详细介绍登录无线控制器配置各项功能的方法，以及使用管理软件的方法。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 无线控制器。
- 全文如无特殊说明，Web 界面以 TL-AC1000 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

TP-LINK 无线控制器采用基于网络专用处理器的硬件平台，可对整个无线网络进行精细化的统一管理，实现 AP 零配置接入、即插即用，提供运行状态监控、AP 管理、射频管理、负载均衡、MAC 认证、Portal 认证等丰富的软件功能。

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。

回目录

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无线控制器。

2.1　本地 Web 管理

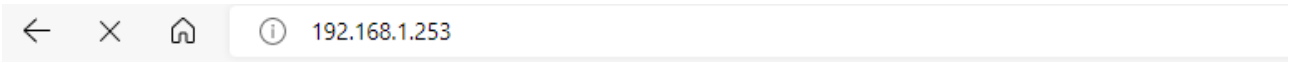
2.1.1 登录准备

可在机身底部的标贴上查找设备的 IP，TL-AC1000 的 IP 为 192.168.1.253，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 AC 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

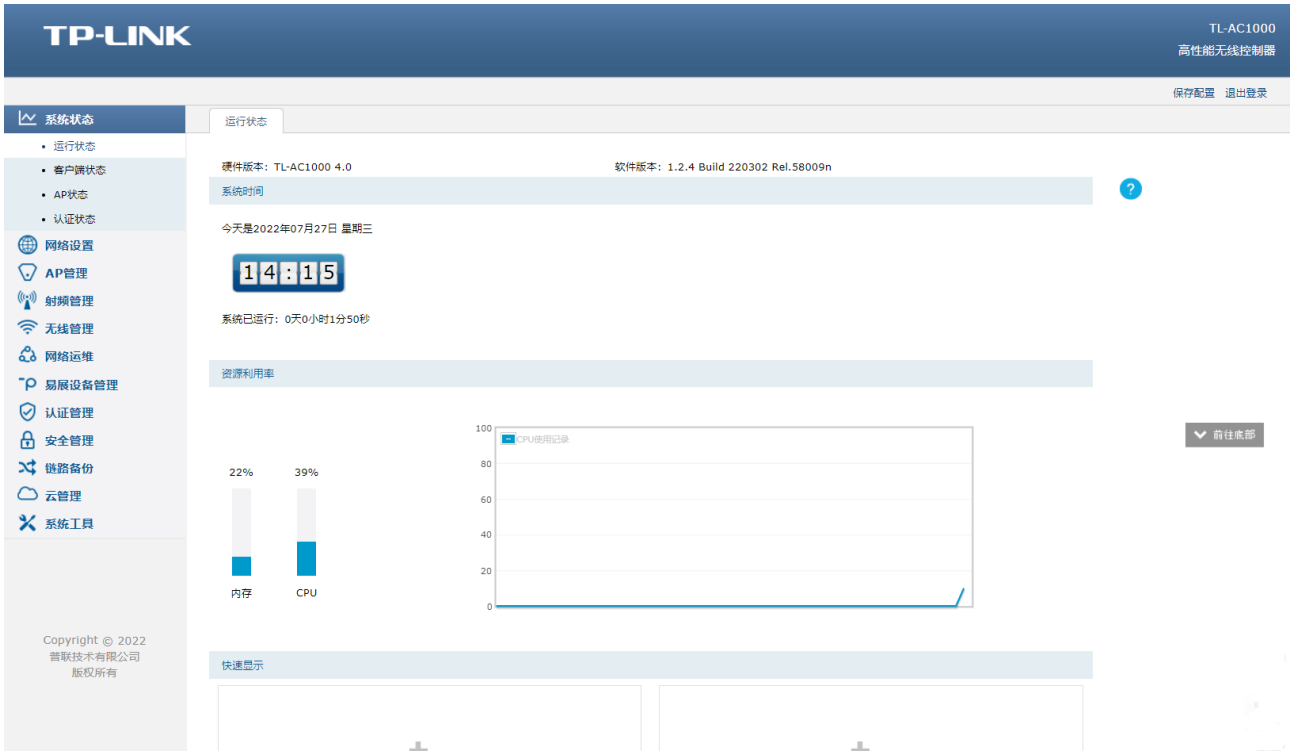
1. 打开浏览器，在地址栏中输入无线控制器默认管理地址 http://192.168.1.253 登录无线控制器的 Web 管理界面。



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. 登录后，进入无线控制器 Web 管理页面：系统状态 >> 运行状态，可查看系统软硬件版本、系统时间、系统运行时间、系统资源利用率等。



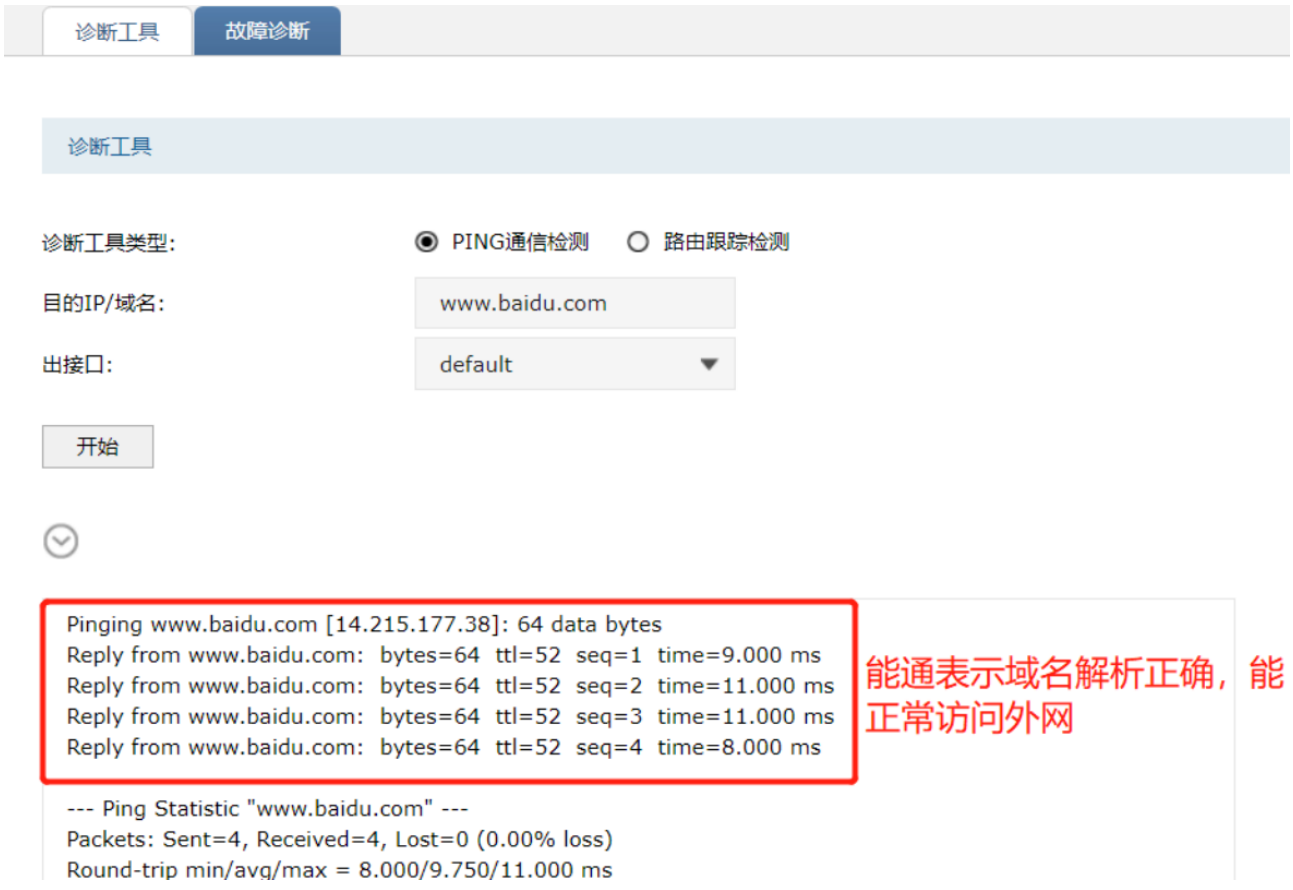
2.1.3 基础联网配置

无线控制器与终端 PC 和手机一样是可以联网的，AC 联网后就可以将设备添加上云或者进行远程管理等操作。可参考如下步骤对无线控制器进行联网配置。

1. 打开浏览器，在地址栏中输入无线控制器默认管理地址 http://192.168.1.253 登录无线控制器的 Web 管理界面。

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（www.baidu.com）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。



或者在页面：网络设置 >> 接口设置中，查看设备互联网连接状态。

2.2 TP-LINK 商用网络云平台管理

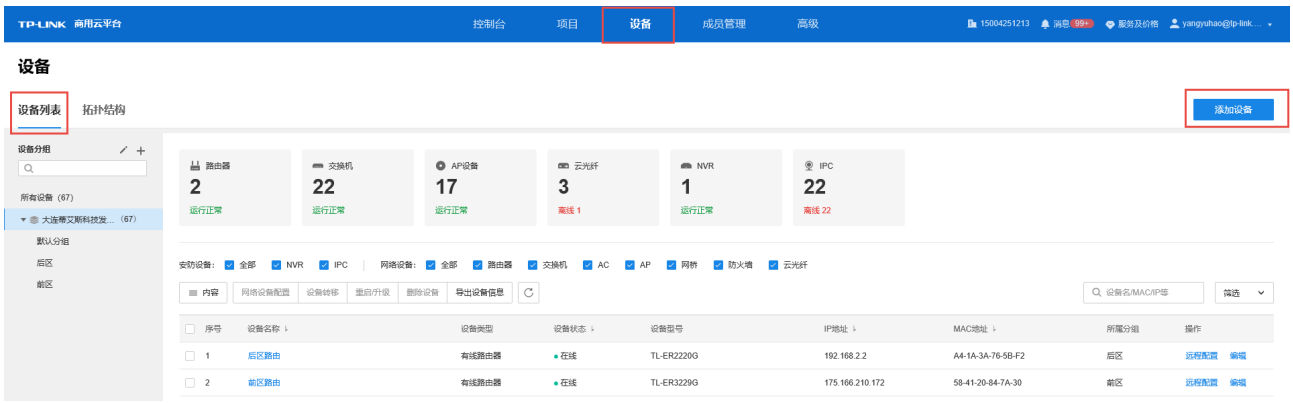
TP-LINK 商用网络云平台能将路由器、交换机、无线控制器、AP、网桥设备统一添加上云，提供多种将设备连云的方式供用户选择，实现有效的远程管理，本节将介绍如何配置 AC 控制器上云。

1. 将无线控制器配置联网，设置方法见 **2.1.3 基础联网配置**。

2. 进入页面：系统管理 >> 云管理，开启云管理功能，点击<设置>。

3. 电脑登录 TP-LINK 商用网络云平台 (https://smbcloud.tp-link.com.cn/)，并且登录已经在平台注册的 TP-LINK ID。

4. 进入页面：项目集中管理 >> 设备 >> 设备列表，点击<添加设备>。



5. 可选择“设备 ID 添加”：通过设备 ID 添加，输入底部标贴上的设备 ID 号，点击<添加>按钮即可添加上云：

或选择“通过设备 MAC 添加”：通过设备 MAC 添加，通过输入无线控制器本地 Web 管理界面的 MAC 地址和用户名密码。填完参数后点击<添加>即可。

说明：

- 如果设备在出厂状态下默认无用户名和密码，此处设置的用户名密码为以后登陆 web 所使用的用户

名和密码，如果设备已有用户名和密码，此时输入已有的用户名和密码即可。

或选择“导入文件”进行批量添加：

智能配置添加：可通过当前路由自动发现局域网中全部设备、统一添加、并进行集中管理。

说明：

- 部分机型有设备 ID。
- 标贴上有设备 ID 的机型，仅支持使用设备 ID 添加。

2.3 TP-LINK 商云 APP 管理

扫描二维码可获取 iOS 版 APP、Android 版 TP-LINK 商云 APP 最新版下载链接。将无线控制器配置连网后可使用商云 APP 添加设备上云进行管理。

➢ 扫码添加设备上云

1. 将无线控制器配置联网后，打开 TP-LINK 商云 APP，在项目中选择“添加设备 >> 网络设备 >> 扫码添加”，扫描设备机身标贴上的二维码。

2. 设置账号密码，点击<添加>将设备添加上云：

3. 添加完成后，在设备列表中点击无线控制器进入管理界面，可查看并配置设备信息。

在基本信息页面，点击<远程管理>，可进入设备 Web 远程管理页面。

➢ 通过设备 ID/MAC 添加设备上云

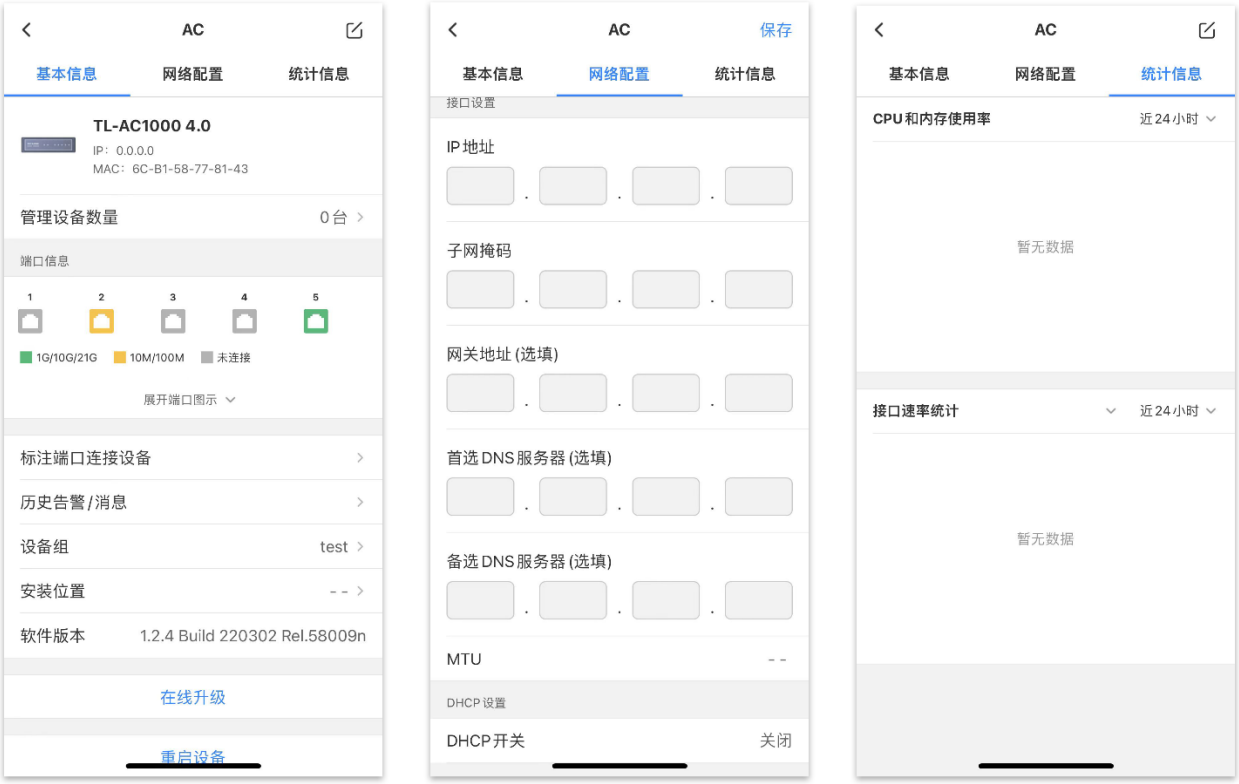
1. 将无线控制器配置连网后，打开 TP-LINK 商云 APP，在项目中选择“添加设备>>网络设备>>扫码添加>>手动输入”，通过设备机身标贴上的设备 ID 添加上云：

说明：

- 仅部分机型有设备 ID。
- 标贴上有设备 ID 的机型，仅支持使用设备 ID 添加。

2. 设置账号密码，点击<添加>将设备添加上云：

3. 添加完成后，在设备列表中点击无线控制器进入管理界面，可查看并配置设备信息。



在基本信息页面，点击<远程管理>，可进入设备 Web 远程管理页面。

说明：

- 如果设备在出厂状态下默认无用户名和密码，此处设置的用户名密码为以后登陆 web 所使用的用户名和密码，如果设备已有用户名和密码，此时输入已有的用户名和密码即可。

2.4 Web 远程管理

远程管理功能可以在网络任何地方远程实时、安全地监控和配置网络。本节介绍如何在外网远程管理无线控制器。

2.4.1 设置方法

1. 配置 AC 的 IP 地址及网关

   登录到无线控制器的 Web 管理界面，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：

2. 查看 AC 的 HTTP 服务端口

进入页面：系统工具 >> 管理账号 >> 系统管理设置，开启 Http 服务，并查看 HTTP 服务端口。

3. 在前端路由器上映射 AC 的 HTTP 端口

登录到前端路由器的管理界面，在虚拟服务器的设置中映射 AC 的 HTTP 端口。

2.4.2 访问方法

在前端路由器运行状态查看 WAN 口 IP 地址，在外网电脑的浏览器地址栏输入 http://WAN 口 IP:外部端口 来远程访问无线控制器，其中，WAN 口 IP 必须为公网 IP 地址。

121.201.33.100 仅为举例，实际访问时请以实际查看到的 IP 地址为准。

至此，在外网电脑上远程访问 AC 设置完成。

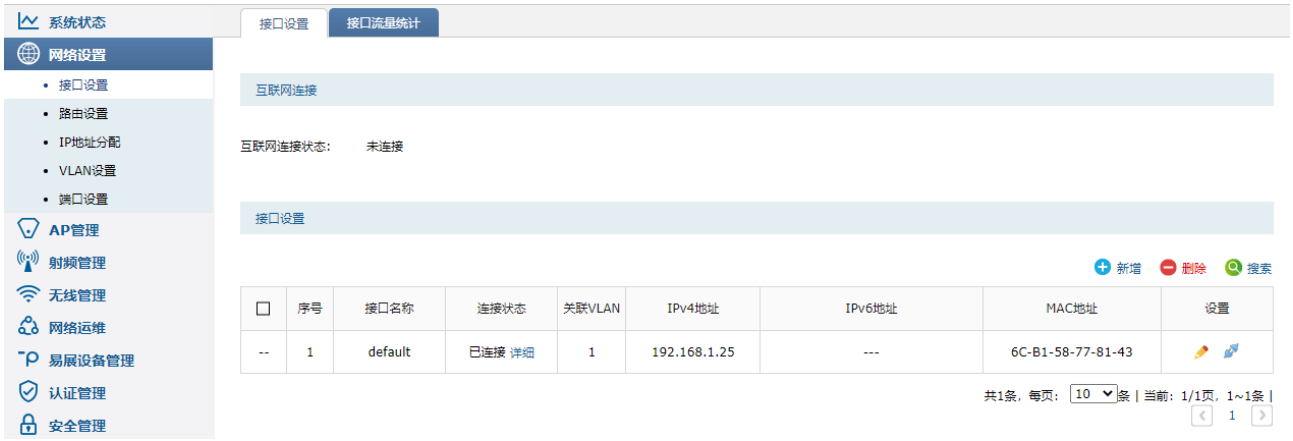
回目录

第3章　网络设置

3.1　接口设置

3.1.1 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。点击<>，将断开接口连接。

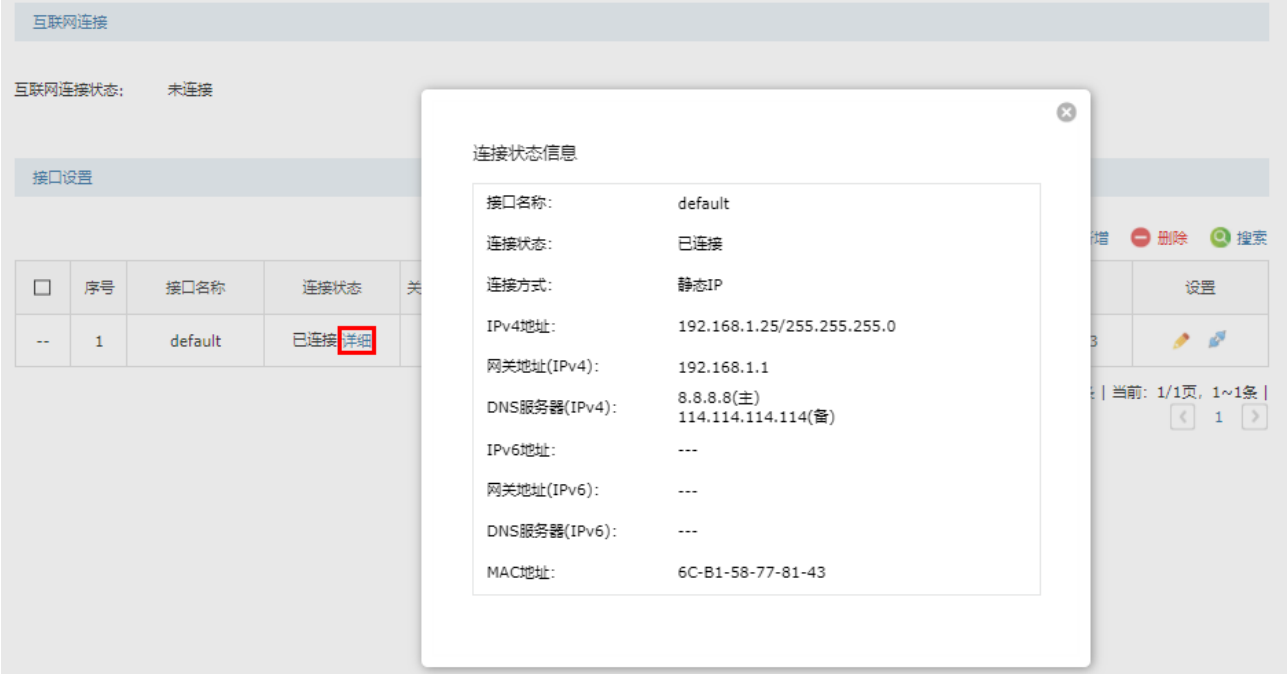


在此界面，可以对已有条目进行操作。点击<>，可设置接口信息。

序号为 1 的条目是系统预定义接口，不可删除。

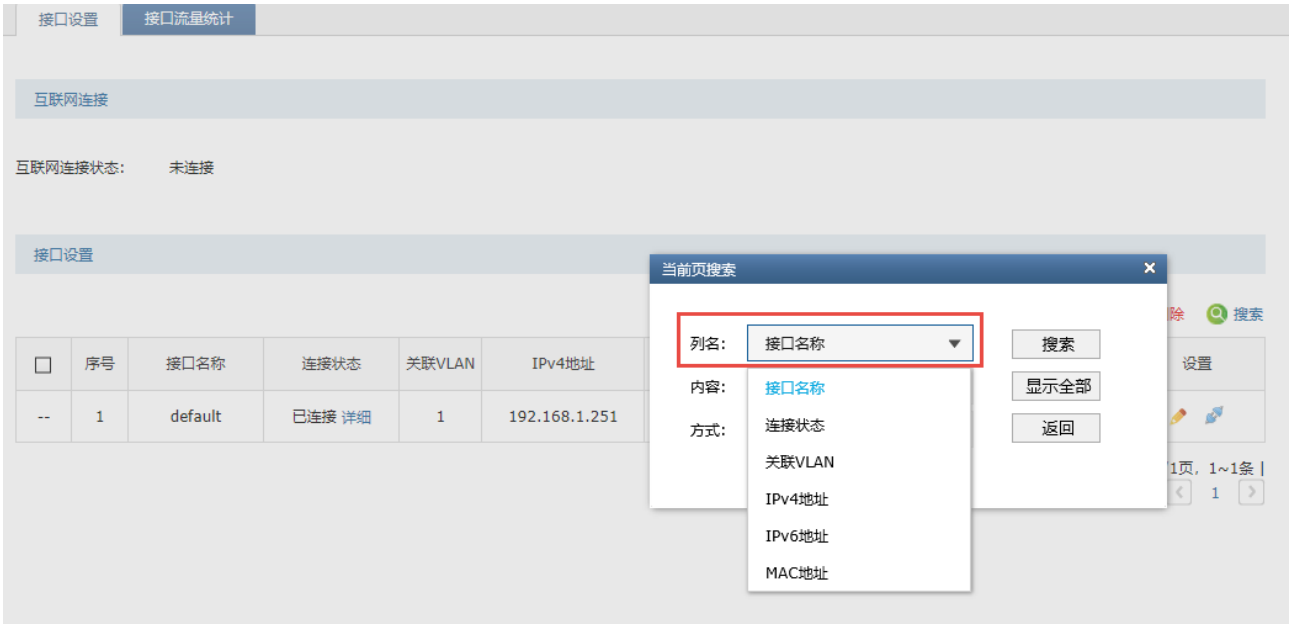
- **查看接口详细信息**

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。



3.1.2 配置接口

进入页面：网络设置 >> 接口设置，可在此界面创建接口。创建接口必须保证有 VLAN 可供选择，如需设

置 VLAN，请参考 VLAN 设置。

点击<新增>，选择关联 VLAN，填写接口名称、IP 地址等信息，点击<确定>。

接口名称	接口的名称，以方便识别和查找。
连接方式	接口的连接方式，目前只支持静态 IP 方式。
MTU	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1500 之间的整数，默认值为 1500。若 ISP 未提供 MTU 值，请保持默认值不变。
首选/备用 DNS 服务器	输入 DNS 服务器的 IP 地址，允许留空。

也可为接口配置 IPv6 地址。“IP 协议类型”选择“IPv6”，选择“启用”，填写相应参数即可：

地址配置方式	EUI-64 表示自动获取 64 位 IPv6 的前缀地址。
子网前缀长度	前缀长度是一个十进制数，表示 IPv6 地址最左边多少位为地址前缀。一般为 64。

3.1.3 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。

点击<清空>，可以清空设备各接口的流量统计信息。

➢ **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。

3.2 路由设置

3.2.1 路由功能介绍

路由是指根据数据包的目的 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。设备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，设备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。

设备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。

1. 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。
2. 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。
3. 动态路由：通过相互连接的设备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。

TP-LINK 无线控制器支持静态路由配置。

3.2.2 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。

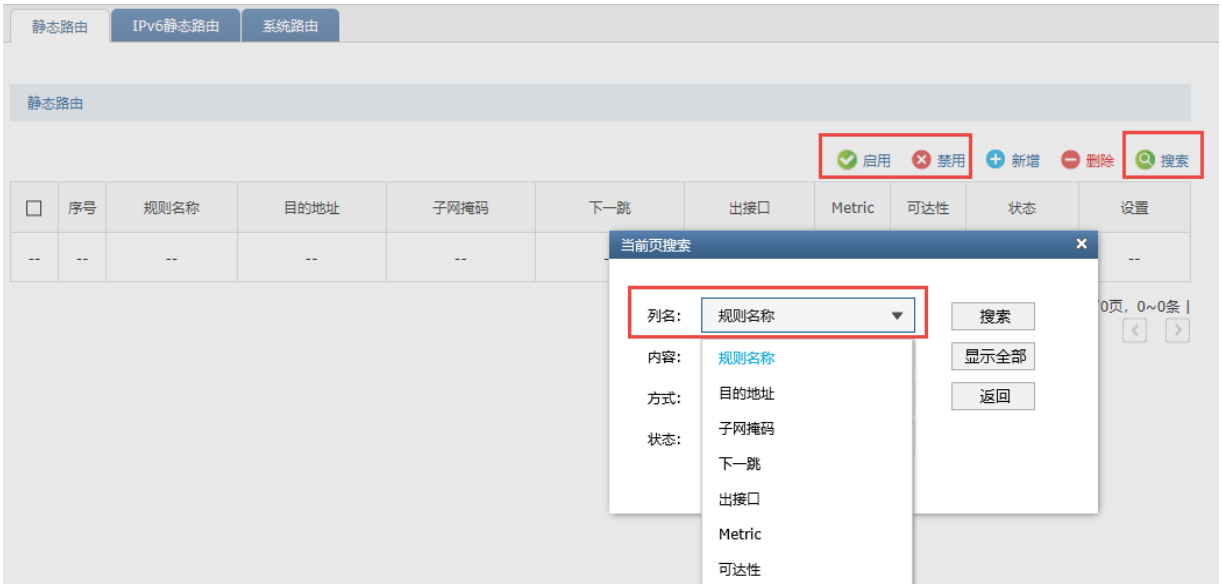
目的地址/子网掩码	设置目的地址和子网掩码，确定路由生效的网段。
下一跳	数据包将发往的下一个路由点。
出接口	设置数据包出接口。
Metric	静态路由规则的度量值，数值越小优先级越高，默认为 0。

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。

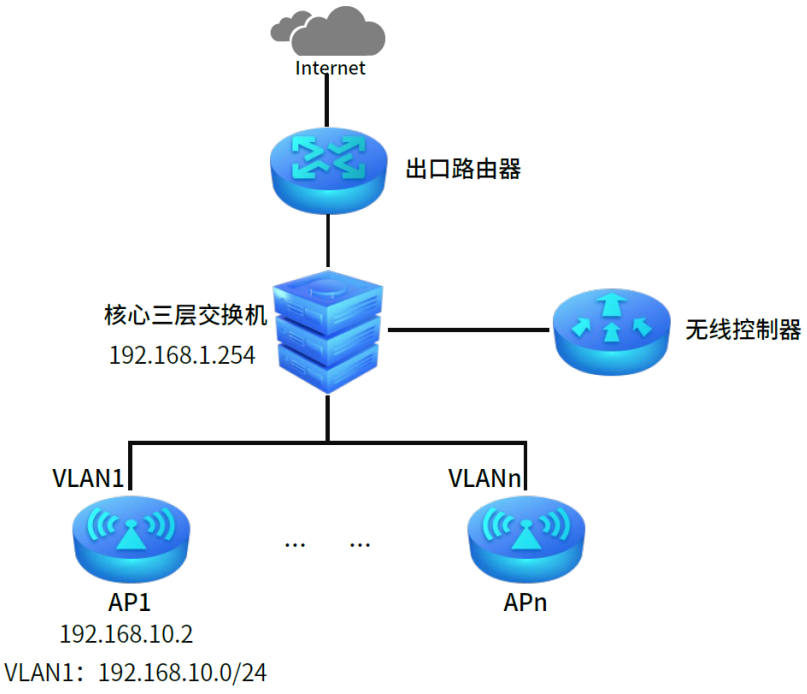
选中路由条目，点击<启用/禁用>，即可设置路由条目生效或不生效，如下图。



3.2.3 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。

3.2.4 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。

3.2.5 查看系统路由

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。

3.3 DHCP 服务

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）协议应用于 TCP/IP 网络中，基于该协议标准，DHCP 服务器给网络中的 DHCP 客户端动态分配 IP 地址等网络参数，以便于网络管理员对网络中计算机的 TCP/IP 参数进行统一管理。

当网络规模扩大，计算机数量日益增多时，DHCP 功能能够高效的完成 TCP/IP 参数配置，并将 IP 地址循

环运用，提高使用效率。而随着无线网络的广泛使用，计算机的位置也经常变化，其所连接的子网也处于动态变化的过程，由此产生的 TCP/IP 参数变更问题基于 DHCP 也能够高效解决。

3.3.1 设置 DHCP 服务

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。

仅为 AP 分配	DHCP 服务器只能为 TP-LINK 系列 AP 分配 IP 地址。
为 AP 和用户终端分配	DHCP 服务器可以为所有客户端分配 IP 地址。

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 AC 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，AC 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。
地址租期	DHCP 服务器所分配 IP 地址的有效使用时间，超时将重新分配。
网关地址	输入此地址给客户端分配的默认网关，建议填入当前 DHCP 服务生效接口的 IP 地址。
缺省域名	输入此地址池给客户指定的域，与 IP 地址一样共同表示相同子网的计算机集合，同一接口网络中的计算机通常配置为相同的域名。

注意：

DHCP 服务的服务接口 IP 和开始/结束地址池必须在同一网段，否则 DHCP 服务不生效。

3.3.2 设置 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。

仅为 AP 分配	DHCP 服务器只能为 TP-LINK 系列 AP 分配 IP 地址。
为 AP 和用户终端分配	DHCP 服务器可以为所有客户端分配 IP 地址。

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。

服务接口	选择需要提供 DHCPv6 服务的 Ethernet 接口。
开始/结束地址	设置 IP 地址池，DHCP 服务器开启状态下，AC 自动从地址池中给局域网中的设备分配 IPv6 地址。
地址租期	DHCP 服务器所分配 IP 地址的有效使用时间，超时将重新分配。
首选 DNS 服务器	输入此地址池给客户端分配的首选 DNS 服务器，也可以将接口 IPv6 地址配置为 DNS 服务器地址，并由接口为客户端转发域名解析请求。
备用 DNS 服务器	输入此地址池给客户端分配的备用 DNS 服务器，当首选 DNS 服务器失效时，客户端可以向备用 DNS 服务器申请域名解析。

3.4 客户端列表

3.4.1 客户端列表

客户端列表显示已由 DHCP 服务器分配 IP 参数的设备信息。

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

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。

3.4.2 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。

3.5 静态地址分配

3.5.1 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>。

点击<导入>按钮，可导入多个静态地址条目。可通过<备份>功能获取符合规则的.csv 文件，以查看文件的正确格式。

文件格式示例(必须包含首行提示栏)：

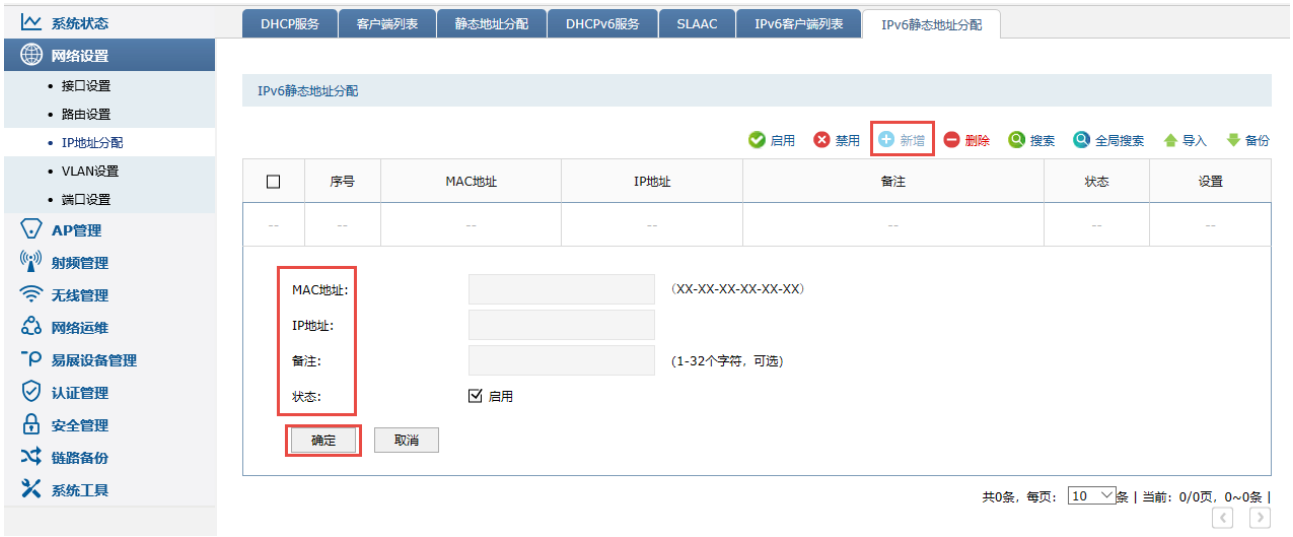
状态	MAC 地址	IP 地址	备注
1	XX-XX-XX-XX-XX-XX	192.168.1.100	TP-LINK

点击<备份>按钮备份所有静态地址条目。备份文件可直接通过<导入>功能重新添加到静态地址列表中。

3.5.2 IPv6 静态地址分配

可根据接入设备的 MAC 地址手动分配 IPv6 地址。当对应的客户端设备请求 DHCPv6 服务器分配 IPv6 地址时， DHCPv6 服务器将自动为其分配指定的 IPv6 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 IPv6 地址，点击<确定>，如下图。



点击<导入>按钮，可导入多个静态地址条目。可通过<备份>功能获取符合规则的.csv 文件，以查看文件的正确格式。

文件格式示例(必须包含首行提示栏)：

状态	MAC 地址	IP 地址	备注
1	XX-XX-XX-XX-XX-XX	2000:1:2:3:4:5:6:7	TP-LINK

点击<备份>按钮备份所有静态地址条目。备份文件可直接通过<导入>功能重新添加到静态地址列表中。

3.6 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。

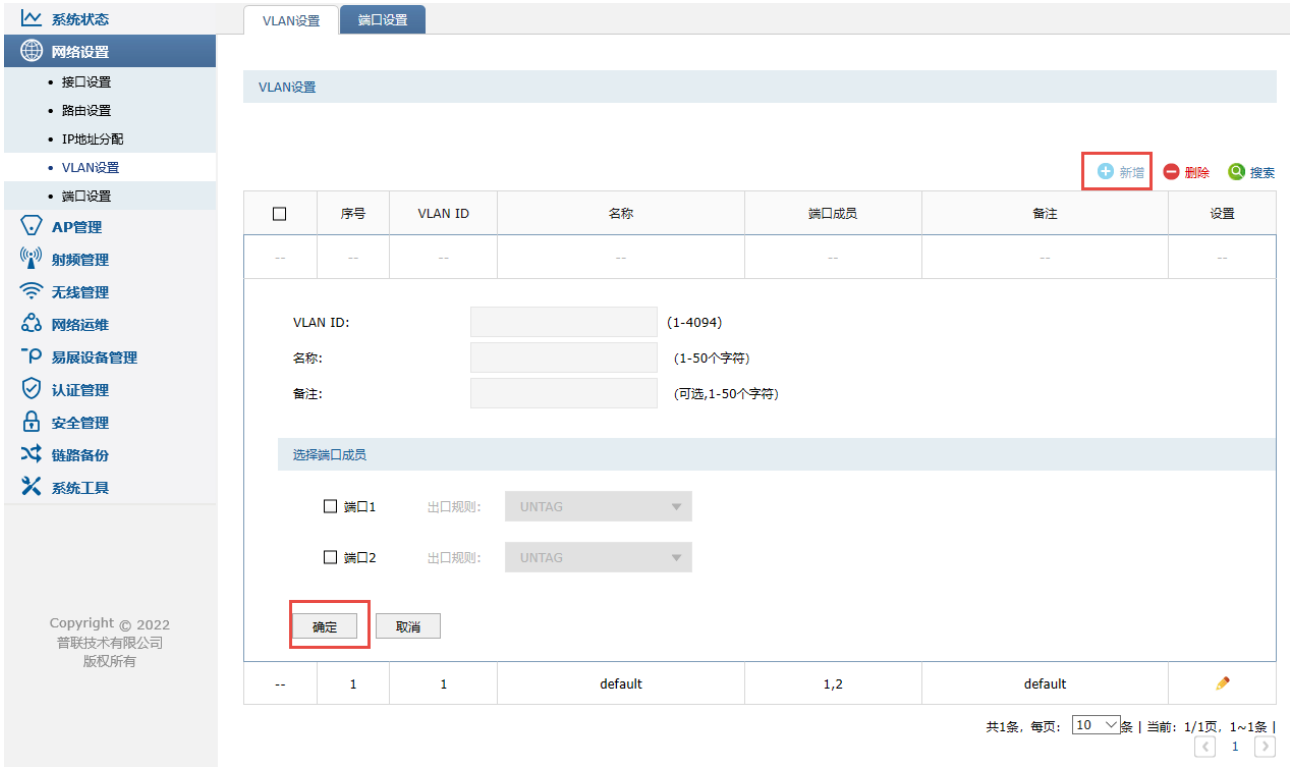
进入页面：网络设置 >> IP 地址分配 >> SLAAC。点击<新增>，选择 DNS 配置方式。配置完成后，点击<确定>，如下图。

3.7 VLAN 设置

3.7.1 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。

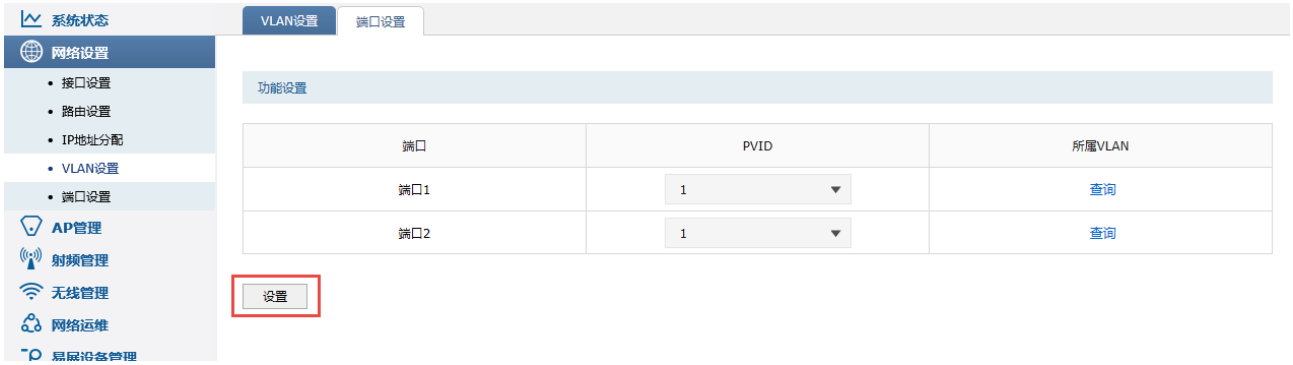


端口成员	显示 VLAN 的端口成员，带't'标识表示该端口的出口规则为 TAG。
出口规则	选择 VLAN 端口成员的出口规则：TAG 表示输出的数据帧带有 tag 信息；UNTAG 表示输出的数据帧不带 tag 信息。

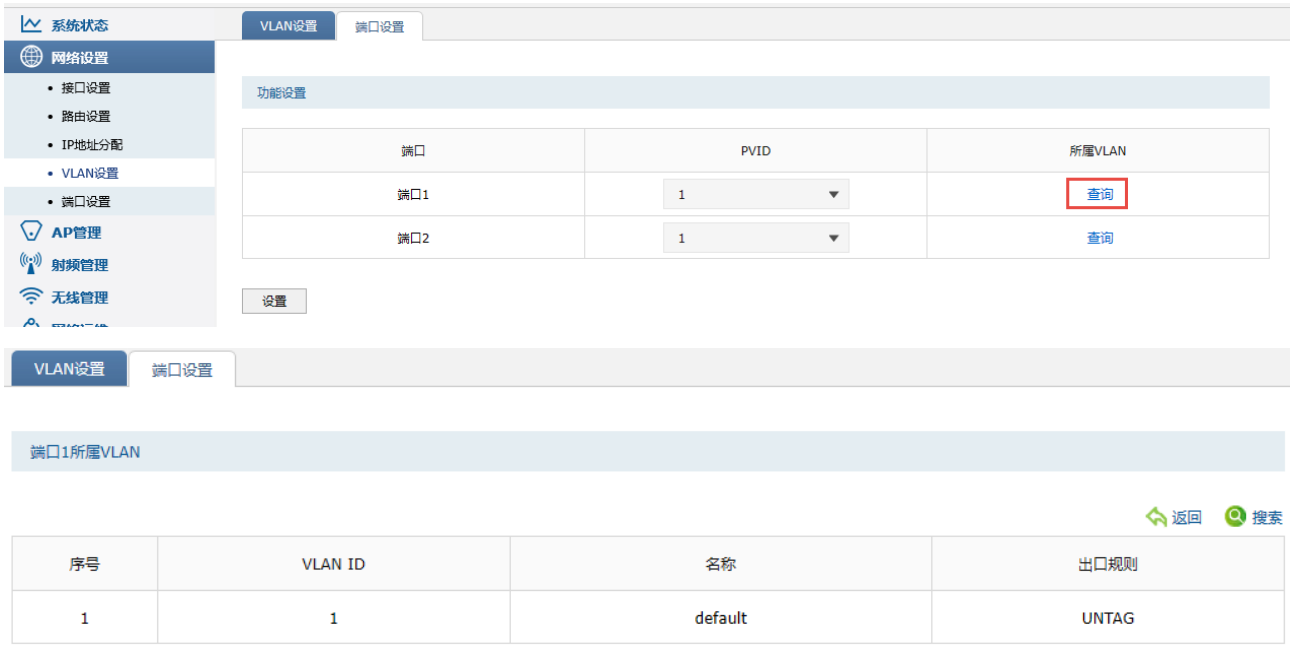
3.7.2 端口设置

PVID（Port VLAN ID），就是端口的缺省 ID。当端口接收到的报文不带 VLAN Tag 时，会根据接收端口的 PVID 值为该报文插入 VLAN Tag，并进行转发。

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。



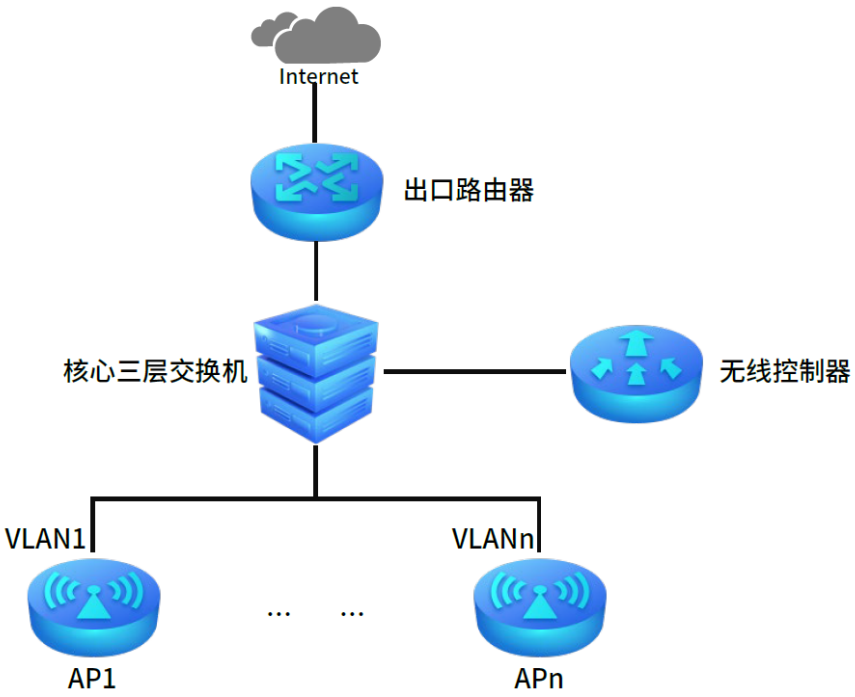
点击端口所属 VLAN 下的<查询>按键，即可查询端口的具体 VLAN 信息，如下图。



3.7.3 VLAN 配置实例

➢ **需求介绍**

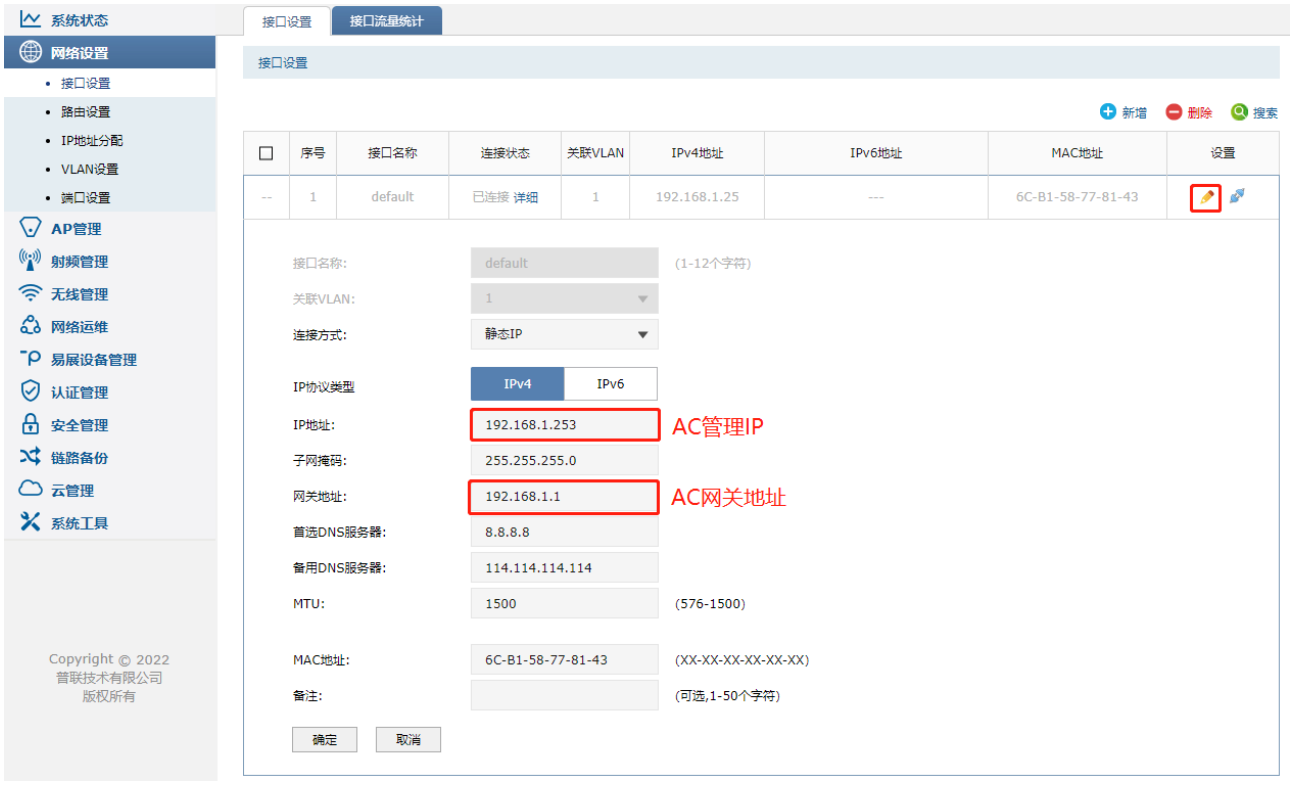
大型网络环境中，使用三层交换机将网络分为多个不同的网段。这种情况下，AC 控制器与 AP 如果处于不同网段，则需要跨三层交换机进行管理。



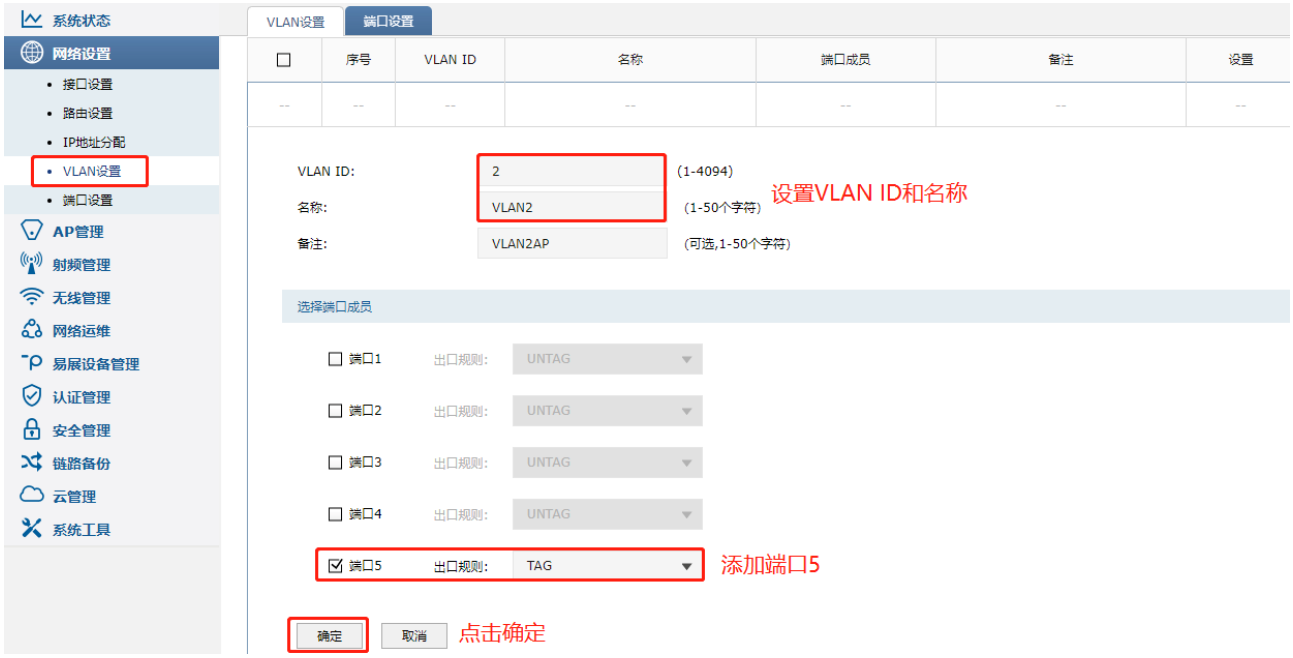
➢ **配置步骤**

将 AC 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 192.168.1.253（本例中在 VLAN2、3、4、5 中有需要管理的 AP）：

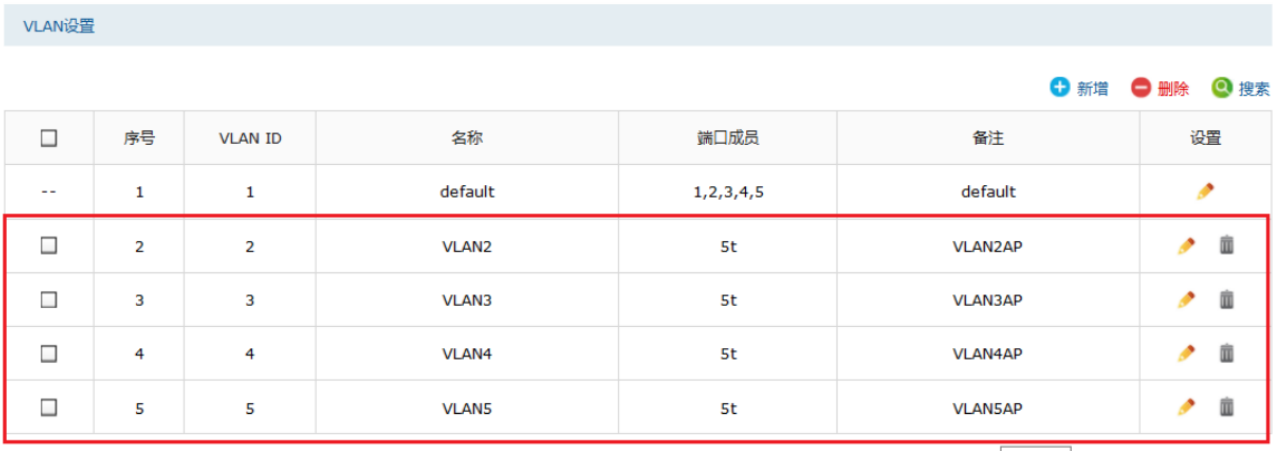
1. 进入页面：网络设置 >> 接口设置，配置 AC 的管理 IP：



2. 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 5）加入到 AP 所在 VLAN。



3. 重复以上设置将 AC 的端口 5 加入到 VLAN2、3、4、5 中。



4. 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。 以上配置完成后， AC 即可实现跨三层交换机发现不同 VLAN 中的 AP。

3.8 端口设置

3.8.1 端口统计

进入页面：网络设置 >> 端口设置 >> 端口统计，可查看各端口接收和发送参数。

点击<刷新>按钮获取最新的统计结果。点击<清空>，清空统计结果。

单播帧	接收/发送目的 MAC 地址为单播 MAC 地址的正常数据帧数目。
广播帧	接收/发送目的 MAC 地址为广播 MAC 地址的正常数据帧数目。
流控帧	接收/发送的流控帧（起流量控制作用的数据帧）数目。
多播帧	接收/发送目的 MAC 地址为多播 MAC 地址的正常数据帧数目。
过小帧	接收的长度小于 64 字节的数据帧数目（包含错误帧）。
正常帧	接收的长度在 64 字节到最大帧长的数据帧数目（包含错误帧）。
过大帧	接收的长度大于最大帧长的数据帧数目（包含错误帧）。

说明：

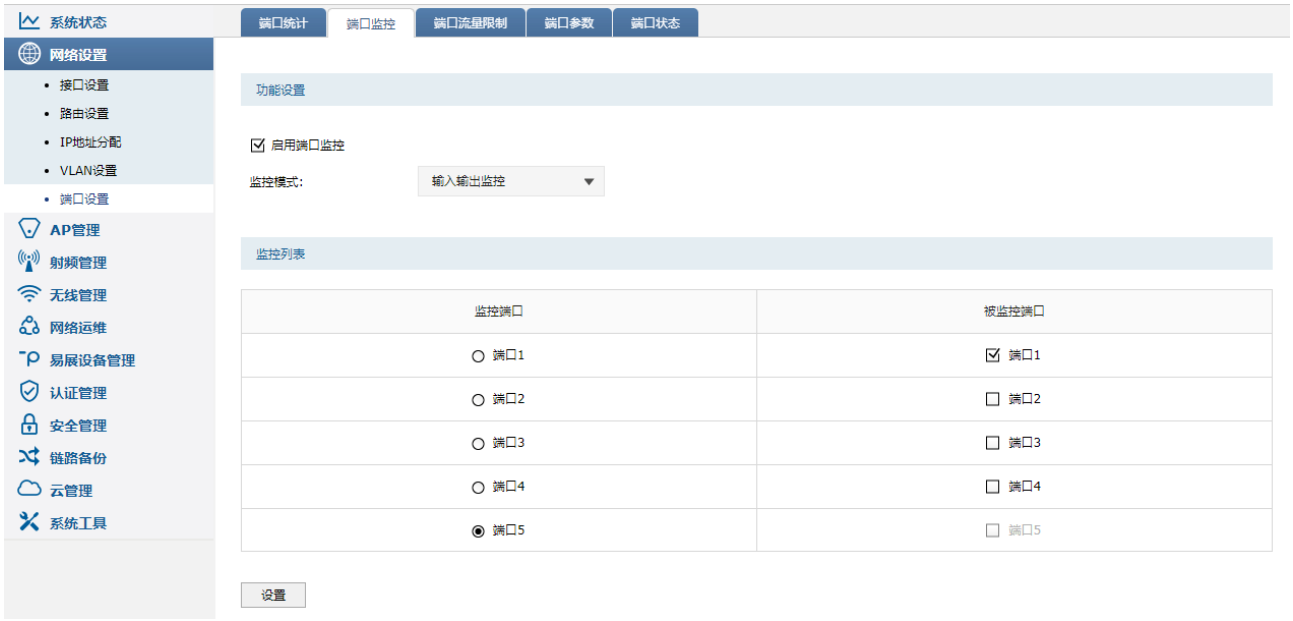
- 错误帧：指校验和错误的帧。
- 最大帧长：设备支持的最大帧的大小，对于不带 Tag 标签的帧该值为 1518 字节，对于带 Tag 标签的帧该值为 1522 字节。

3.8.2 端口监控

无线控制器端口监控功能支持以下三种监控模式：

- 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。

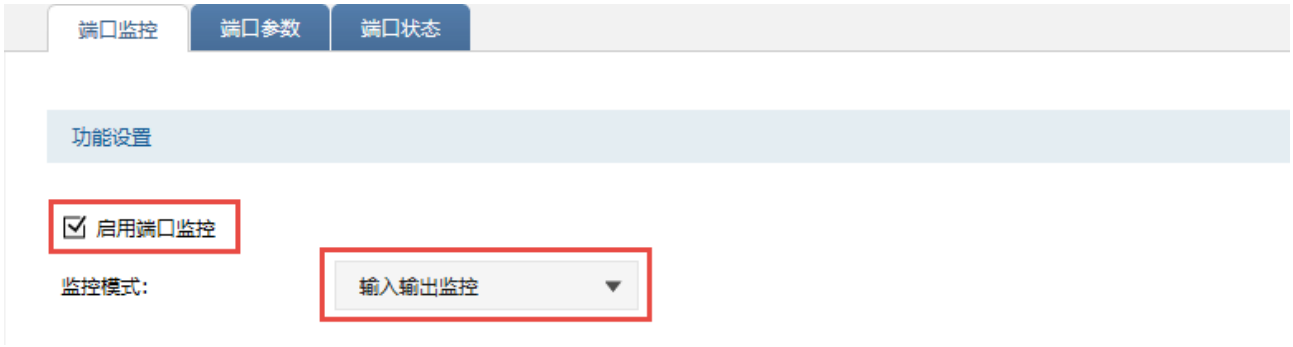
3.8.3 端口监控配置实例

需求介绍：

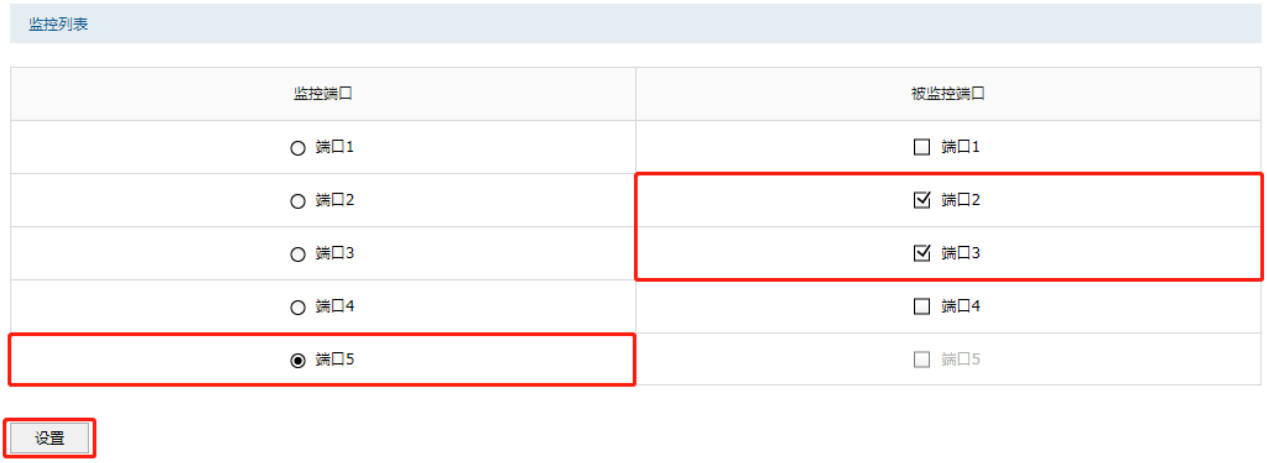
现需要对无线控制器的端口 2、3 中输入输出数据进行监控，将其复制到监控端口 5。

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 5 为监控端口，端口 2、3 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。

3.8.4 端口流量限制

进入页面：网络设置 >> 端口设置 >> 端口流量限制，可对流经端口的特定类型数据帧的速率进行控制。

3.8.5 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。

3.8.6 端口状态

进入页面：网络设置 >> 端口设置 >> 端口状态，点击<刷新>，获取各个端口的最新工作状态。


系统状态
网络设置
接口设置
路由设置
IP地址分配
VLAN设置
端口设置
AP管理
射频管理
无线管理
网络运维
易展设备管理
认证管理
安全管理
链路备份
云管理
系统工具
端口统计
端口监控
端口流量限制
端口参数
端口状态
状态列表
端口
端口状态
连接速率（Mbps）
双工模式
流量控制
端口1
已断开

未知
已禁用
端口2
已断开

未知
已禁用
端口3
已连接
100M
全双工
已禁用
端口4
已连接
100M
全双工
已禁用
端口5
已断开

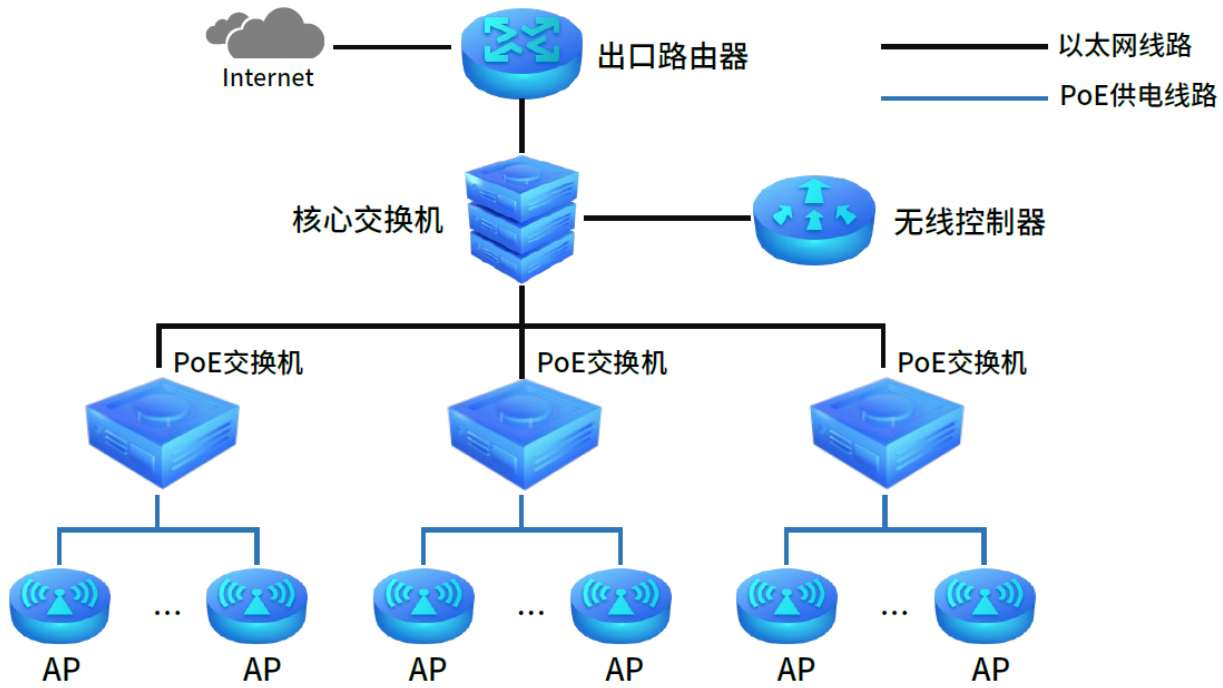
未知
已禁用
刷新

回目录

第4章　AP 管理

TP-LINK 无线控制器可以自动发现所有工作在瘦 AP（FIT AP）模式下的 AP，并对 AP 进行统一配置和管理，实现 AP 零配置接入，即插即用；支持信道自动调整，AP 启动时会根据周围无线环境自动选择干扰最小的无线信道，支持手动调整 AP 发射功率，降低 AP 之间的相互干扰，提高无线网络质量；支持弱信号剔除，可设信号强度阈值，智能识别并禁止、踢除低于指定信号强度的设备，避免弱信号设备拖累整个无线网络效率，提升无线漫游质量和整个无线网络的性能；支持频谱导航，智能分配客户端连接的频段，引导双频无线客户端优先关联到 5GHz 射频上，避免无线终端扎堆 2.4GHz 信道造成网络拥塞；支持基于接入用户数的负载均衡，当 AP 间的用户数量超过设定的阀值时，AC 能够动态调整用户在不同 AP 间的均匀分布，防止个别 AP 过载。

4.1　AP 设置



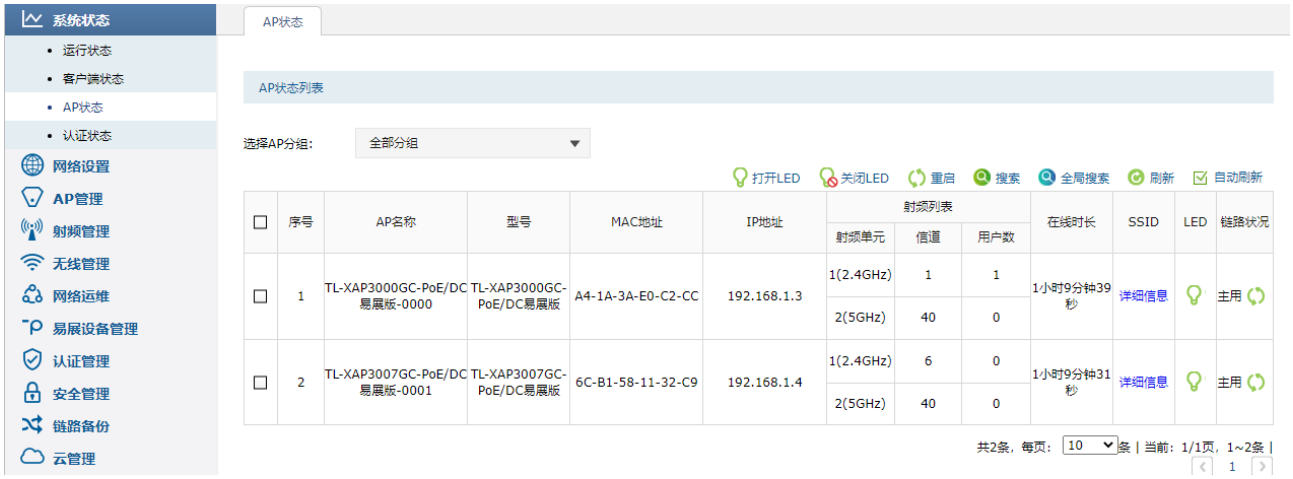
为了保证无线组网最基本的使用体验，就需要配置 AC 的 AP 管理功能，设置相应的 SSID 使用，并根据现场的环境条件设置 AP 的信道、功率等射频参数，防止互相干扰，保证无线网络的稳定性和流畅性。

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

4.1.1 添加 AP

将需要管理的 AP 与 AC 连接后，登录无线控制器的管理页面，可在页面：系统状态 >> AP 状态，AP 状态列表中查看 AP 信息。

点击<>或<打开 LED>，可开启或关闭 AP 指示灯。点击<重启>，可重启选中的 AP。



打开 LED/关闭 LED	打开或关闭选中的 AP 的 LED 指示灯。在 AP 未开启 LED 定时功能时，本页面中 LED 灯的打开或关闭操作结果，将同步设置为 AP 接入 AC 时的 LED 默认状态。
AP 名称	AP 的名称，可以在 AP 管理页面中修改。
型号	AP 的硬件型号。
射频列表	AP 的射频信息列表。 • 射频单元：AP 下的射频单元名称。 • 信道：射频单元实际工作的信道数。 • 用户数：射频单元下接入的用户数量。

链路状态	显示 AP 的双链路角色，"主用"表示此 AP 正在接受本 AC 的管理，"备用"表示此 AP 与本 AC 建立了连接，但只是作为备份链路，并不接受本 AC 的管理。对于"备用"状态下的 AP，<重启>按钮只能切断连接而不能将 AP 重启。

点击<详细信息>，可查看 AP 绑定的无线服务列表。

'TL-XAP3000GC-PoE/DC易展版-0000'绑定的无线服务列表

返回AP列表

序号	射频单元	SSID	描述	VLAN ID	安全选项	状态
1	1(2.4GHz)	TP-LINK_8143	---	---	WPA-PSK/WPA2-PSK	启用
2	2(5GHz)	TP-LINK_5G_8143	---	---	WPA-PSK/WPA2-PSK	启用

- **搜索**

点击<全局搜索>，可基于列名和内容对列表进行搜索。

点击<搜索>，可基于列名、内容对当前页进行搜索，可选“在结果中搜索”及“在所有条目中搜索”两种方式。

4.1.2 AP 管理

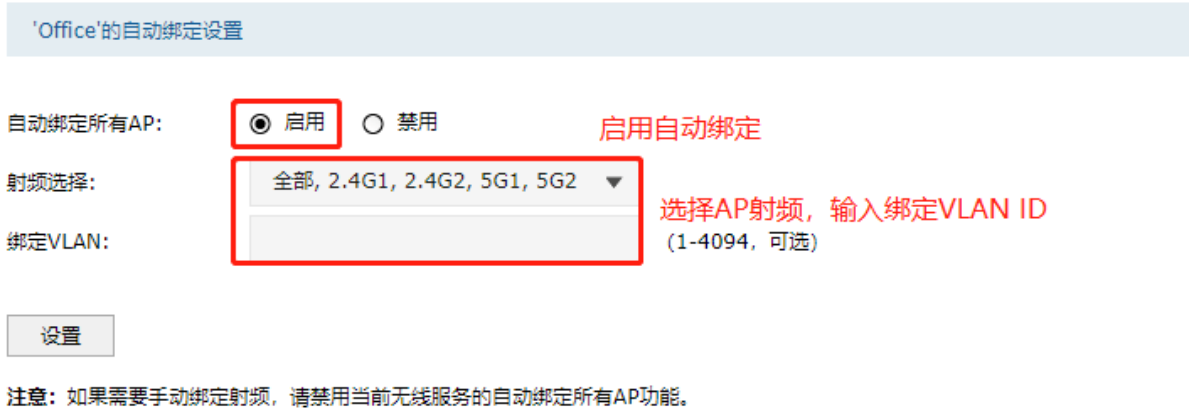
1. 设置无线网络

登录到 AC 管理界面，进入页面：无线管理 >> 无线服务，点击<新增>，设置无线网络，具体请参考**第 6 章 无线管理**。

2. 射频绑定

无线网络新增成功后，点击无线服务列表的射频绑定 按钮。

自动绑定：



手动绑定：

若要为 AP 配置多个无线网络，也按照同样的方法进行以上操作。

3. 射频设置

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。详情请参考 **5.1 射频设置**。

4. 启用频谱导航

进入页面：射频管理 >> 频谱导航，启用频谱导航。详情请参考 **5.3 频谱导航**。

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. 启用射频调优

进入页面：射频管理 >> 射频管理 >> 射频调优，启用射频调优功能。详情请参考 **5.1.2 射频调优**。

4.1.3 AP 定时重启

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。

4.1.4 AP 分组管理

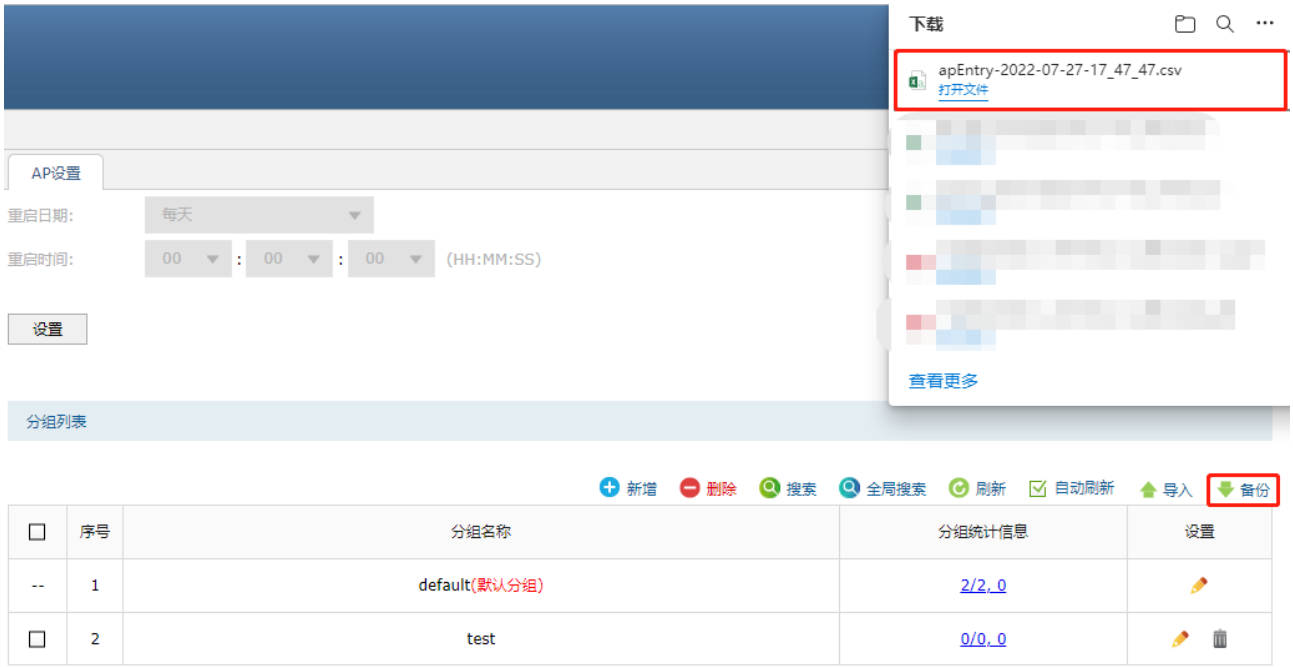
➢ **分组列表**

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<新增>，可新增 AP 分组。点击<删除>可删除 AP 分组。“default（默认分组）”不可被删除。

- 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。



备份.csv 文件示例：

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	AP分组	AP名称	条目类型	型号ID（只	型号（只读	硬件版本号	MAC地址（只	AP保活时间	客户端保活	客户端空闲	离线自管理	有线LAN 1	有线LAN 2	有线LAN 3	有线LAN 4	AP端口汇聚	LED默认状态
2	default	TL-XAP30(	AP条目	6784032	TL-XAP30(	v1.0	A4-1A-3A-	30	300	3600	开启	---	---	---	---	---	开启
3	default	TL-XAP30(	AP条目	1.49E+09	TL-XAP30(	v1.0	6C-B1-58-	30	300	3600	开启	---	---	---	---	---	开启

➢ 分组详细列表

点击分组统计信息栏目下的信息，进入分组以查看并管理分组内 AP：

序号	名称	型号	硬件版本	软件版本	MAC地址	LED默认状态	状态	设置
1	TL-XAP3000GC-PoE/DC易展版-0000	TL-XAP3000GC-PoE/DC易展版	1.0	1.0.2	A4-1A-3A-E0-C2-CC	开启	运行	
2	TL-XAP3007GC-PoE/DC易展版-0001	TL-XAP3007GC-PoE/DC易展版	1.0	1.0.9	6C-B1-58-11-32-C9	开启	运行	

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。

选择 AP，点击<修改分组>，可将 AP 移动到指定分组。

点击<新增>，可新增 AP 条目。点击< >，可对在线 AP 进行配置。

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。

4.2 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。

4.2.1 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。升级开始时间可选择“立即升级”或选择“定时升级”手动选择升级开始时间；升级方式可选择“在线升级”或“手动上传升级软件”从本地上传升级软件。

升级软件版本号　　显示当前 AP 待升级的软件版本号。

升级开始时间	设置升级开始时间，可以设置为立即升级和定时升级两种模式。 • 立即升级：点击确定之后，该型号的 AP 设备将立即升级。 • 定时升级：到达指定时间，该型号的 AP 设备将进行升级。
升级进度	显示当前升级的进度，X/Y/Z 表示当前检测到有 Z 台该型号的 AP，其中有 Y 台需要升级，X 台已经升级成功。点击可以查看各个 AP 当前的升级状态。
升级失败	显示当前升级失败的 AP 数目。点击可以查看详细日志信息。
升级状态	显示当前 AP 型号的升级状态。点击可查看该型号下的 AP 的具体升级状态信息。 • 等待升级：当前 AP 型号下的 AP 在等待升级 • 正在升级：当前 AP 型号下的 AP 正在升级 • 升级完成：当前 AP 型号下的所有 AP 都升级完成 • 无需升级：当前 AP 型号下没有 AP 需要升级
升级方式	显示当前 AP 型号的升级方式，包括在线升级和手动导入软件两种方式。

说明：

- 您可以到 TP-LINK 官网 www.tp-link.com.cn 下载最新的升级软件。

4.2.2 单个 AP 升级

在“单个 AP 升级”栏目下，选择 AP 分组，点击<手动升级>或<在线升级>按钮，对单个 AP 进行升级。

升级软件版本	显示该 AP 即将升级的软件版本
升级状态	显示该 AP 的升级状态。 ● 在线：该 AP 在线但未进行升级 ● 等待升级：该 AP 在等待升级 ● 检查更新：正在检测该 AP 是否有软件可以更新 ● 等待下载软件：检测到有新软件后等待下载软件 ● 下载软件：正在下载软件 ● 正在升级：该 AP 正在升级 ● 正在确认升级结果：正在等待 AP 接入，以确认升级是否成功 ● 升级完成：该 AP 升级完成 ● 确认升级结果失败：AP 接入版本非升级软件版本 ● 传输升级文件失败：在传输升级软件的过程中发生错误 ● 确认升级结果超时：AP 在升级后未在规定时间内接入 ● 获取软件失败：未获取到最新软件 ● 下载软件失败：下载最新软件失败 ● 无需升级：该 AP 不需要升级 ● 软件不匹配：导入的 AP 软件与当前 AP 的软件版本不兼容
软件管理	可以选择在线升级或手动升级。如果对应的 AP 不支持在线升级功能，则只提供手动升级方式。

4.3 负载均衡

4.3.1 负载均衡

在无线终端密集度较高的无线网络中，无线客户端的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。

TP-LINK 无线控制器支持基于接入用户数的负载均衡功能，当 AP 间的用户数量超过设定的阈值时，AC 能够动态调整用户在不同 AP 间的均匀分布，防止个别 AP 过载，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。

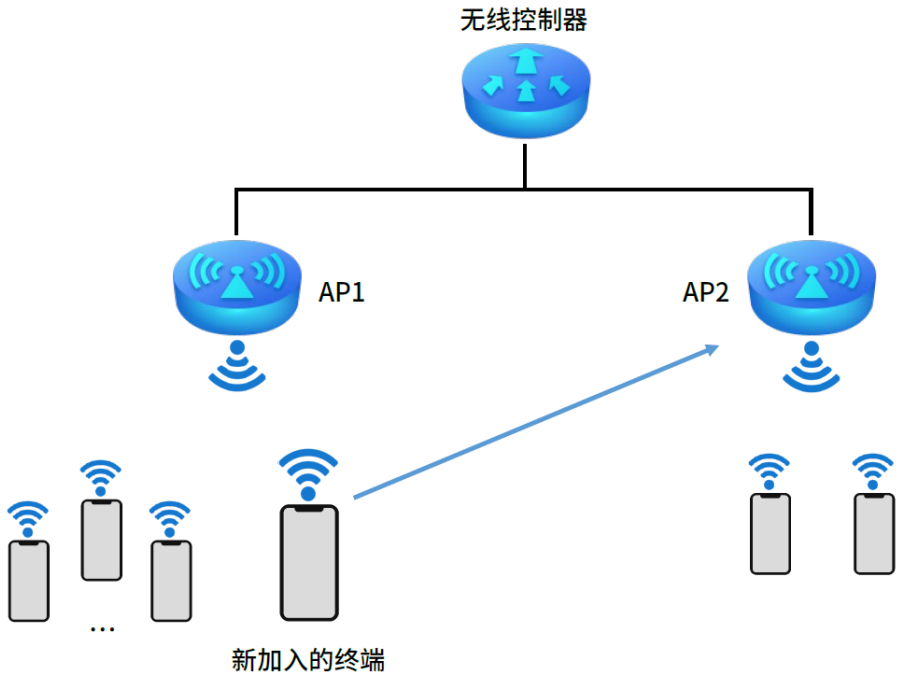
负载均衡模式	默认为会话模式。
门限	当终端所要连接的 AP 挂载的终端数大于门限，负载均衡才有可能启动。当前连接的用户数量同时达到门限和差值门限，AP 才会启动负载均衡。

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。

4.3.2 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。

4.4 智能漫游

4.4.1 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）。智能漫游的作用在于，对于无线体验较差的终端，AC 主动选取更优的候选 AP，并建议或迫使终端切换到所选择的候选 AP 上，以改善无线上网体验。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。

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。

4.4.2 弱信号剔除配置指南

无线网络中往往会存在部分弱信号设备，占用无线信道，缓慢地收发数据，从而影响到其他无线终端的上网效果，拖垮整体无线网络的使用。TP-LINK 无线控制器支持弱信号剔除，可设信号强度阈值，智能识别并禁止、剔除低于指定信号强度的设备，避免弱信号设备拖垮整个无线网络的效率，提升无线漫游质量和无线网络的性能。

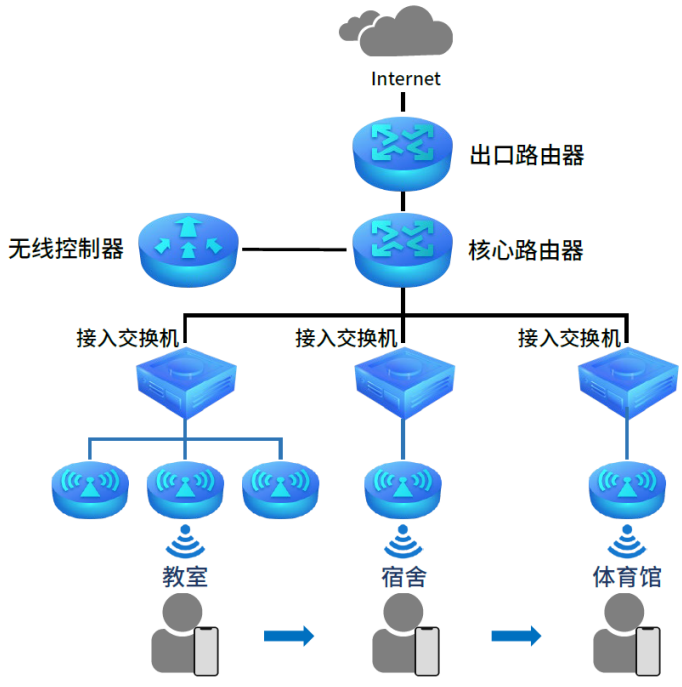
进入页面：AP 管理 >> 智能漫游，在基本设置启用“弱信号用户下线”功能。

至此，就完成了弱信号剔除和弱信号限制功能的配置。

4.4.3 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。

回目录

第5章　射频管理

5.1　射频设置

5.1.1 射频设置

进入页面：射频管理 >> 射频设置 >> 射频设置，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。

点击<导入>可以通过合法的 ANSI 编码格式的 CSV 文件来一次性修改多个射频条目。可以通过“备份”功能获取符合规则的 CSV 文件，以查看文件的正确格式。

点击<备份>可以备份所有射频条目至 ANSI 编码格式的 CSV 文件中。

选择 AP，点击< >。

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。

5.1.2 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。

TP-LINK 无线控制器支持信道调优、功率调优和定时调优功能。

进入页面：射频管理 >> 射频调优，可进行射频调优参数的设置，还可以通过点击<立即调优>按钮立即进行射频调优。

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。

注意：

- 只有信道调优功能开启时，才能开启功率调优功能。

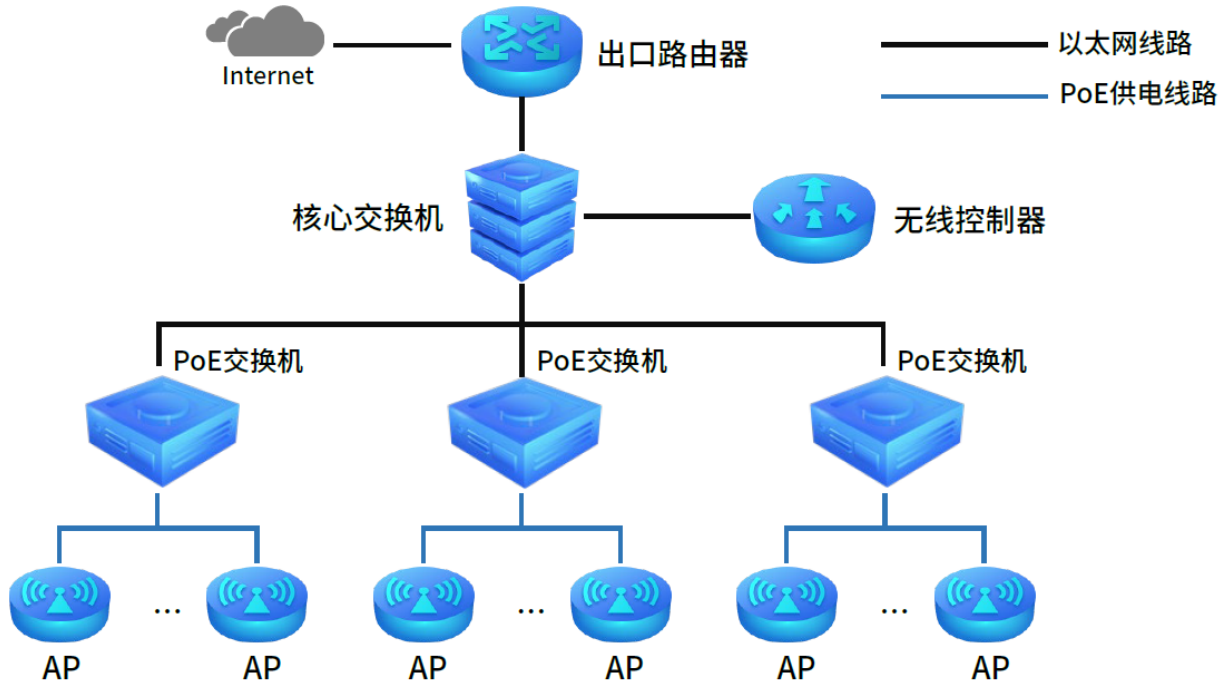
5.1.3 射频调优配置实例

➢ **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。

➢ 功率调优

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：

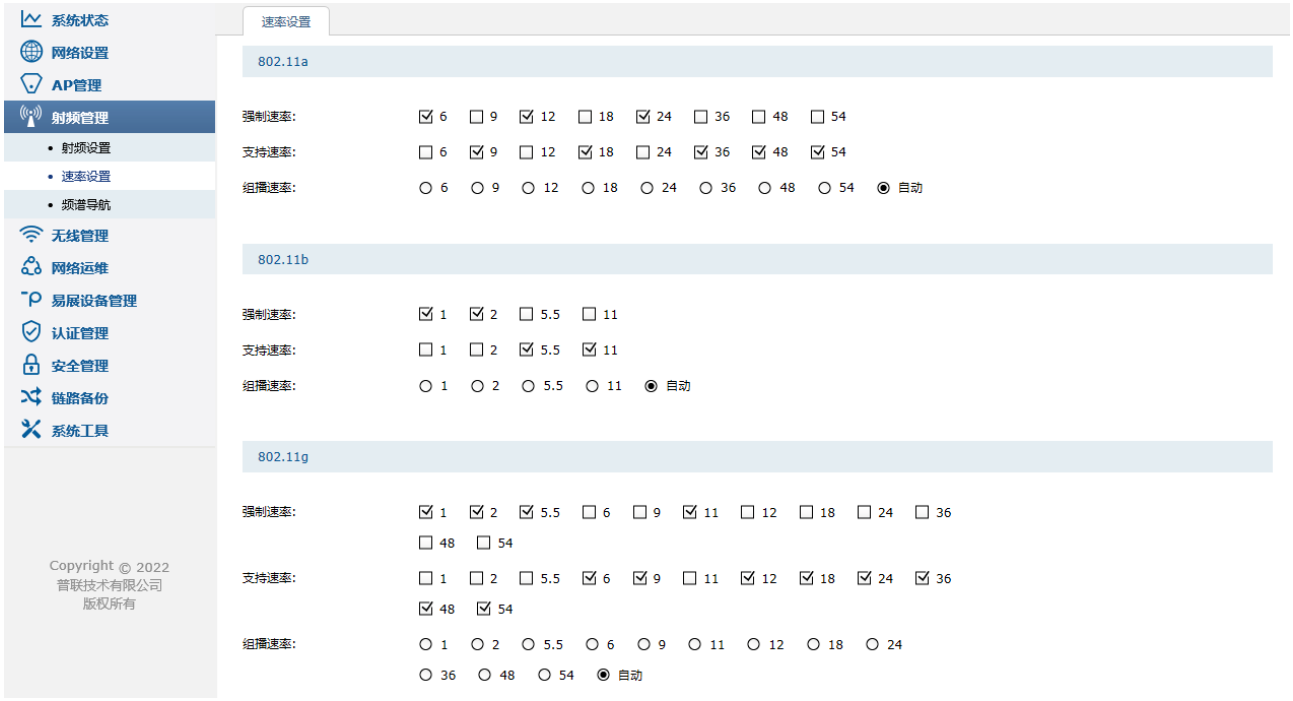
- 只有信道调优功能开启时，才能开启功率调优功能。

➢ 定时调优

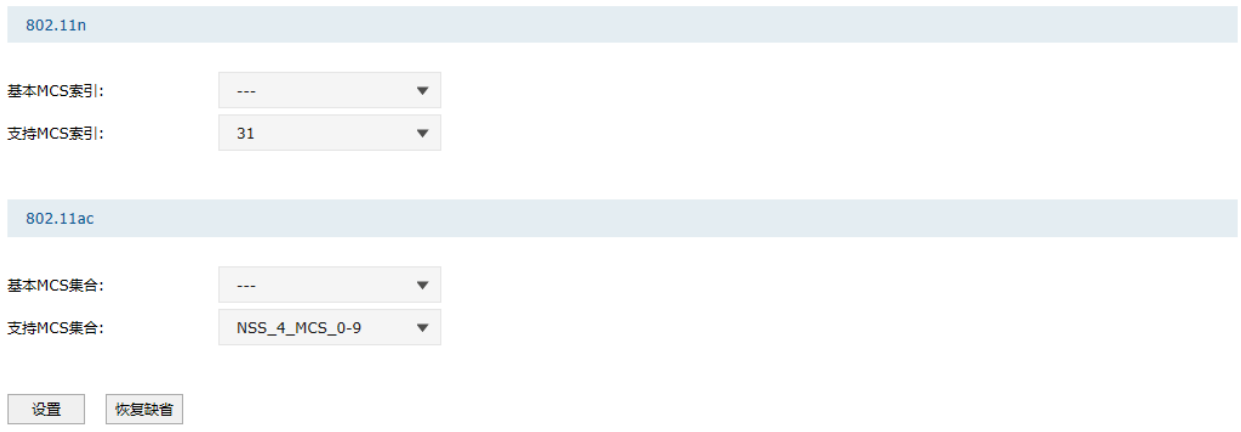
考虑到调优过程中 AP 会有最长 5min 无法正常使用，射频调优支持设置一个特定的时间进行定时调优，避免因为射频调优带来的断网影响。

5.2 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。

5.3 频谱导航

TP-LINK 无线控制器支持频谱导航，智能分配客户端连接的频段，引导支持双频工作的客户端优先接入 5GHz 射频，避免无线终端扎堆 2.4GHz 信道造成网络拥塞，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。

进入页面：射频管理 >> 频谱导航，可以启用/禁用频谱导航功能。

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。

回目录

第6章　无线管理

6.1　无线服务

进入页面：无线管理 >> 无线服务，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。

点击<新增>可添加无线网络设置，点击 可编辑现有的无线网络。

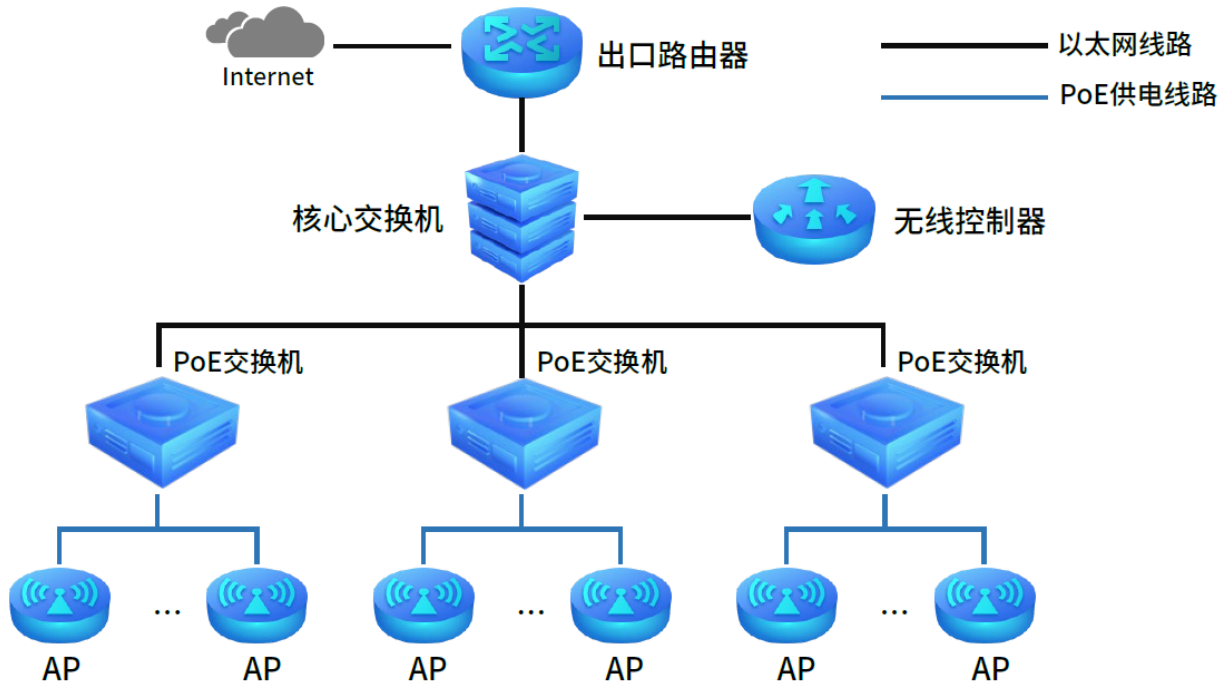
SSID　　设置无线网络名称 SSID（Service Set Identifier，服务集识别码），SSID 的名称应该尽量具有唯一性。

编码方式	设置 SSID 的编码方式（GBK 或 UTF-8）。包含中文字符时，可以选择 GBK 和 UTF-8 两种编码方式；若无中文字符，则默认使用 UTF-8 编码，提交后无线服务表格中“编码方式”栏不显示。
AP 设备	点击<绑定 AP>，设置使用该无线名称的 AP。
无线网络内部隔离	启用内部隔离，可以使连接到同一个无线服务的无线终端之间不能互相通信，此功能不能跨 AP 生效。
隐藏无线网络	启用隐藏无线网络，局域网中无线终端将搜不到该无线名称。
安全选项	设置关联无线服务时是否需要认证。
加密方式	用于无线网络连接时的加密方式，有三种加密方式可选。 不设密码：无线终端无需密码即可连接到 AP 上。 WPA-PSK/WPA2-PSK(推荐)：使用 WPA2-PSK/WPA-PSK 加密方式，该加密方式无需自设认证服务器，设置无线密码即可。 WPA/WPA2:使用 WPA/WPA2 加密方式，该加密方式需要自行配置 Radius 服务器进行相关认证。 WPA2-PSK/WPA3-SAE：基于共享密钥的 WPA2 或 WPA3 模式。
无线密码	选择 WPA-PSK/WPA2-PSK 加密时连接无线网络的密码，由 8-63 个 ASCII 码字符或 8-64 个十六进制字符组成。
控制方式	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。
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）。

6.2 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。

6.3 带宽控制配置实例

无线控制器的带宽控制，是基于 SSID 进行限速，不同于路由器的 IP 带宽控制。可以满足对不同的 SSID 进行区别管理的需求。

➢ **需求分析**

某企业使用 AC+AP 设置了两个无线网络，分别供内部人员和来访客人使用。为了防止访客进行下载、视频等占用大部分的带宽，需要对访客的无线终端进行带宽控制。而员工则不受带宽限制。

网络类别	无线网络名称（SSID）	最大带宽
员工网络	Office	不限制
访客网络	Guest	100KBps

➢ **设置方法**

1. 设置员工网络和访客网络

登录到 AC 管理界面，进入页面：无线管理 >> 无线服务，点击<新增>，分别添加员工网络和访客网络，并设置相应的带宽控制。

2. 将无线网络绑定到对应的 AP

添加完毕后，无线网络列表如下，点击员工网络对应<>按钮：

选择 AP 分组，勾选要绑定到的 AP，并点击<绑定>：

同样的方法，对访客网络也进行射频绑定。绑定完成后，员工和来访客人都可以连接对应的无线网络上网。

至此，无线控制器的带宽控制配置完成。

回目录

第7章　网络运维

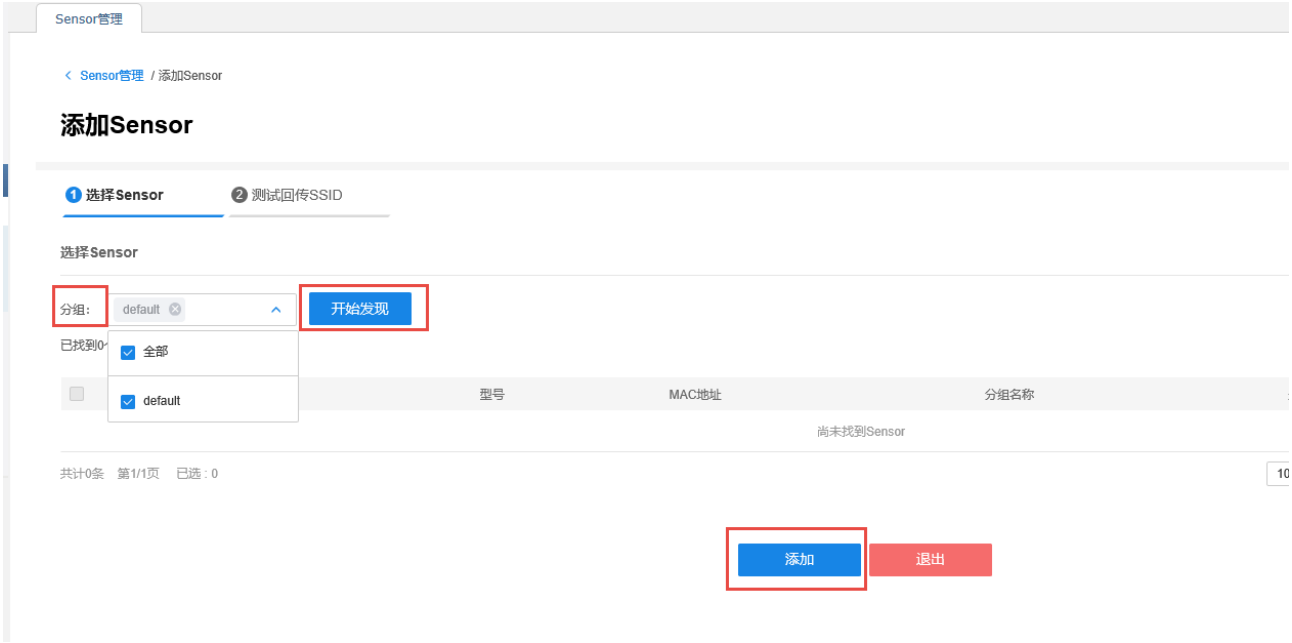
7.1　Sensor 管理

7.1.1 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。

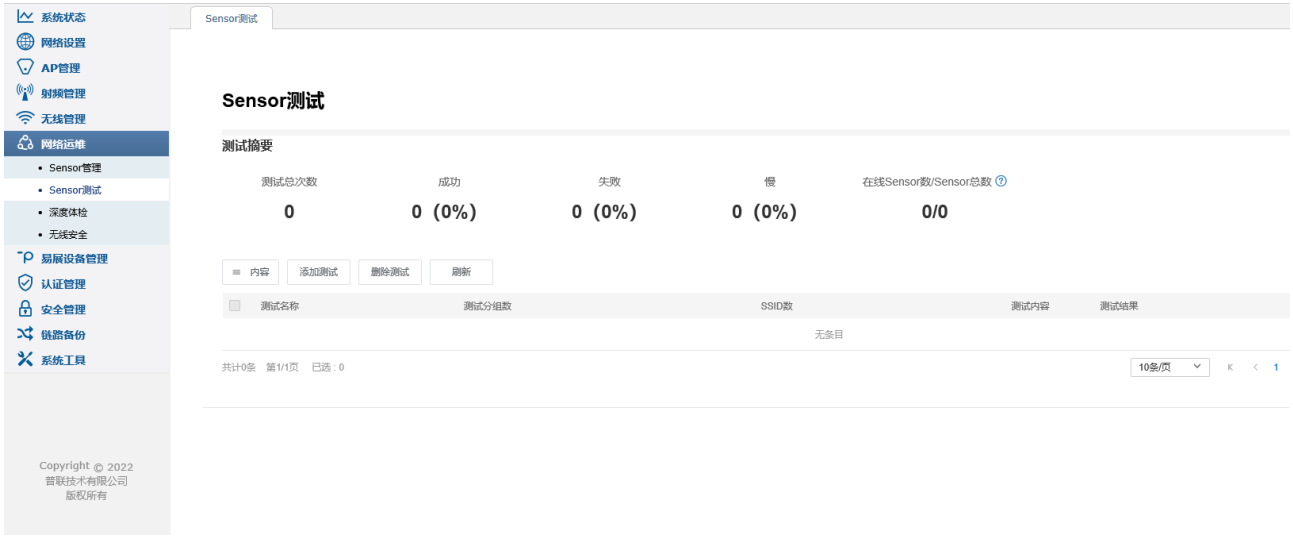
4. Sensor 成功接入网络后，设备指示灯由红色变为绿色，即可正常使用 Sensor 的各项应用功能。

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。

7.2 Sensor 测试

7.2.1 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。

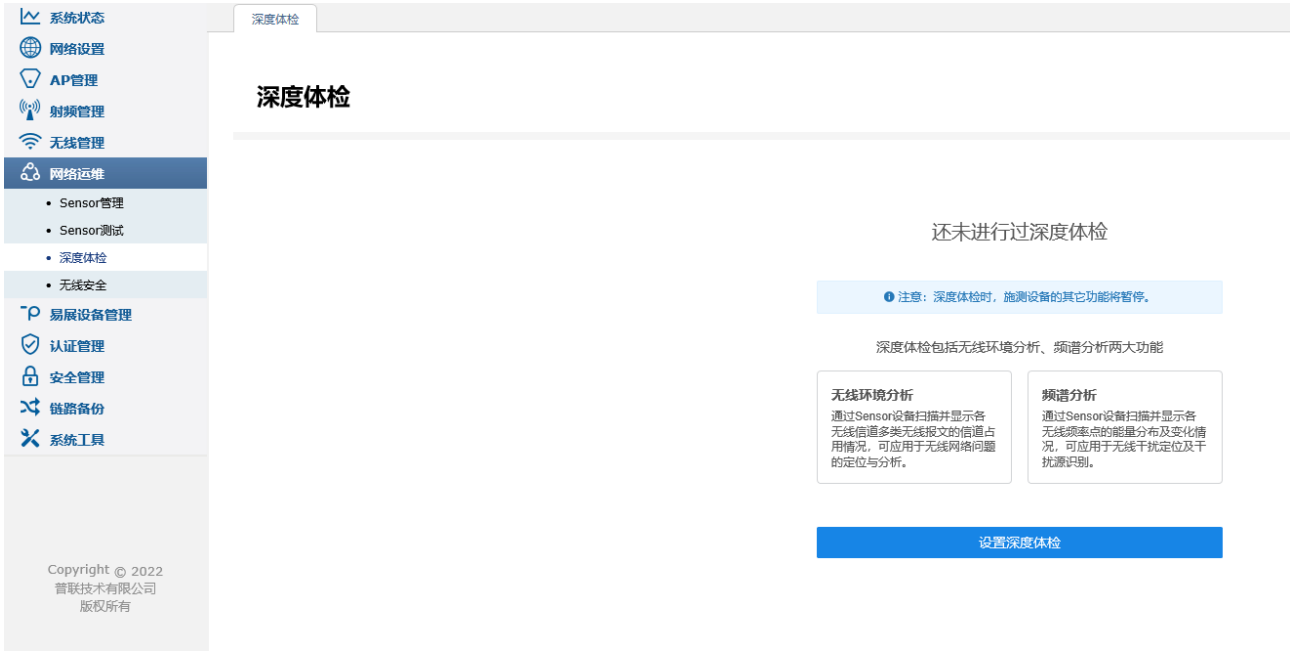


测试摘要	显示测试总次数、测试结果为成功/失败/慢的总次数以及参与测试的在线/所有 Sensor 总数。
内容	勾选显示 Sensor 测试列表页面显示项。
测试分组数	Sensor 测试对应的 AP 设备所在分组数量，点击数字可查看详细 AP 分组列表。
SSID 数	Sensor 测试的 SSID 数量，点击数字可查看测试的 SSID 列表。
测试内容	查看测试内容，如终端上线测试、DNS 测试、主机访问测试、radius 测试、网速测试、邮件测试、web 测试、FTP 测试等。
测试结果	点击对应测试点测试结果，可进入结果详情页。通过结果详情页，可查看测试结果概要以及测试详细结果。注意：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。

7.3 深度体检

7.3.1 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。

7.4 无线安全

7.4.1 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。

回目录

第8章　易展设备管理

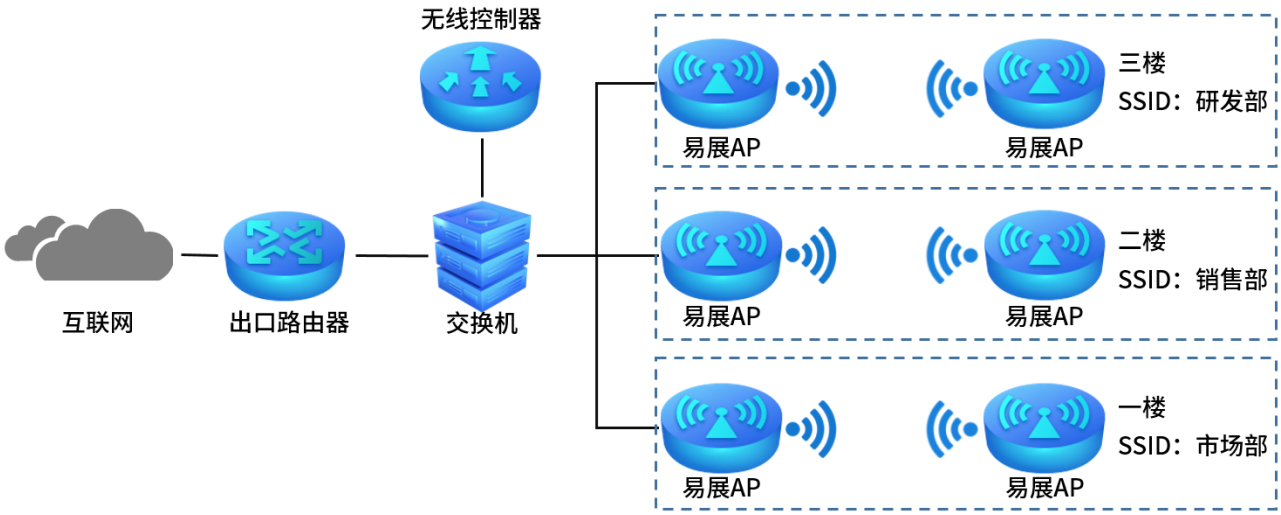
随着互联网技术的快速发展，需求无线网络覆盖的地方越来越多，此时出现了一些传统网络无法解决的复杂区域和快速完成组网的需要，也有个人用户不想破坏原有的装修环境来进行网络覆盖。对于一些区域来说传统网络的组网方案不仅复杂且成本较高。为了解决这些问题，TP-LINK 新推出了带有“易展”功能的AP，能够实现快速组网，无需布线，简单实现组网，且可以替换某些传统组网，优化整个网络。

- **易展 AP**

传统的无线 AP 组网，设备众多，且需要专业人员施工，费时、费力、费钱。TP-LINK“易展”系列 AP 产品颠覆传统 AP 复杂的布线方式，通过 TP-LINK Mesh 技术，无需布线，可实现最多 8 台“易展”AP 一键无线互联，仅需简单设备单台 AP 网络配置，即可自动同步到所有 AP，让 AP 组网、管理更加省时、省力、省钱。

易展 AP 的无线 Mesh 组网模式，作为传统有线组网的扩展和补充，推荐用于终端密度不高的场所，优势在于免布线，便捷且成本低，对于带机量要求较高的高密度场景，建议采用传统有线组网方式。

- **易展 AP 组网**



- **如何辨别易展 AP**

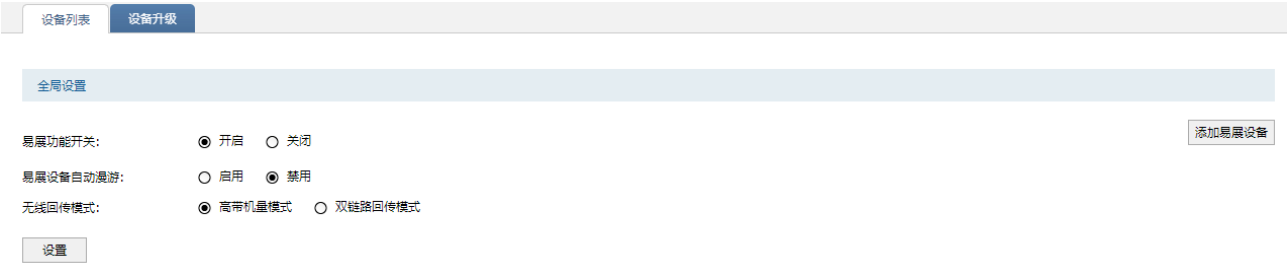
产品型号中有“易展”二字，或设备上有“易展”按键的 AP 产品就是易展 AP。

下面介绍如何使用 TL-LINK 无线控制器产品添加和管理易展 AP。

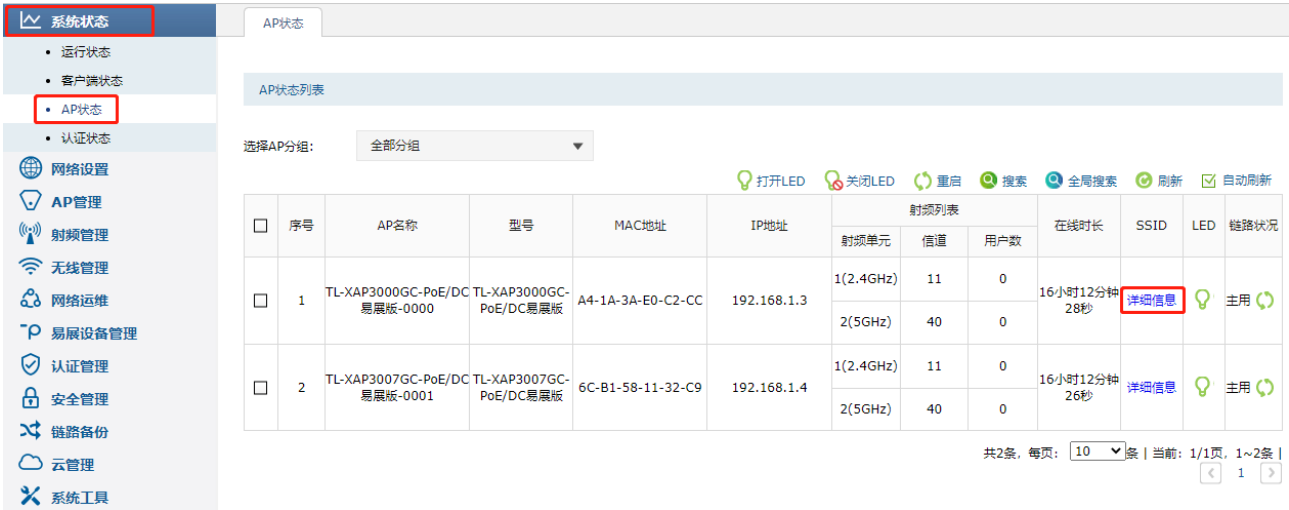
8.1 添加易展设备

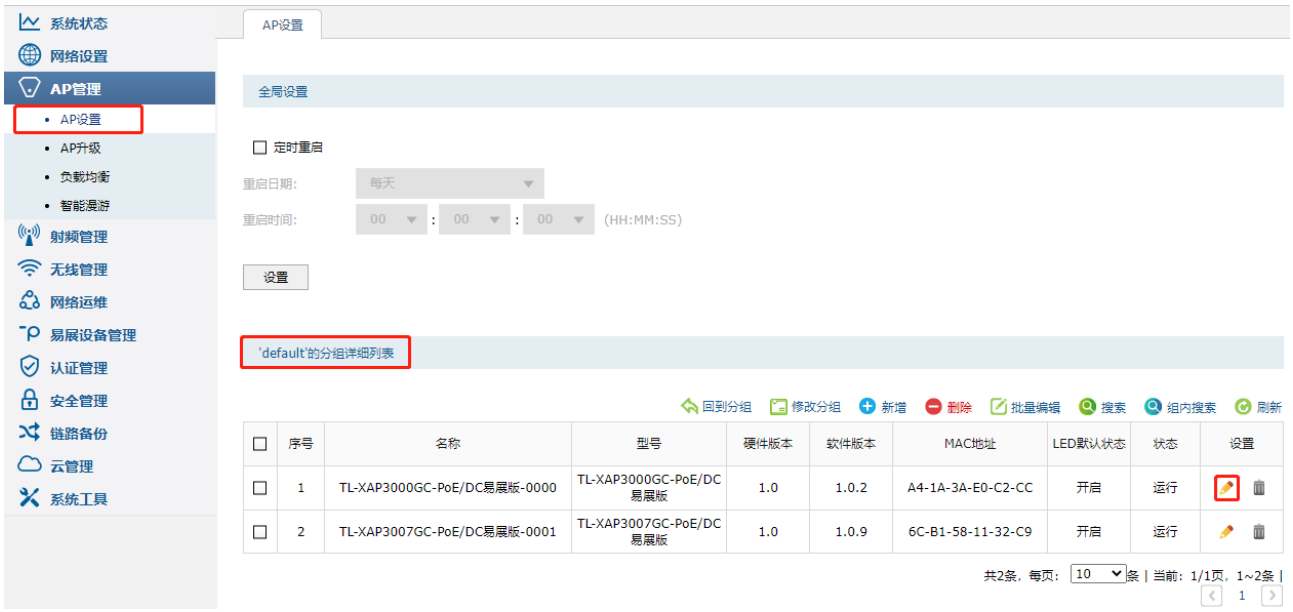
无线控制器需要开启易展管理功能，即可发现并管理易展 AP。无线控制器可以自动发现所有工作在瘦 AP（FIT AP）模式下的 AP，并对 AP 进行统一配置和管理，实现 AP 零配置接入，即插即用。

进入页面：易展设备管理 >> 设备列表 >> 设备列表，在“全局设置”模块开启易展管理功能，点击<设置>。



将有“易展”功能的AP与无线控制器有线连接，作为易展主AP。可进入页面“系统状态 >> AP状态”、“AP 管理 >>AP 设置 >>AP 设置：分组统计信息”或“易展设备管理 >> 设备列表：易展主设备列表”查看或配置主 AP 信息。

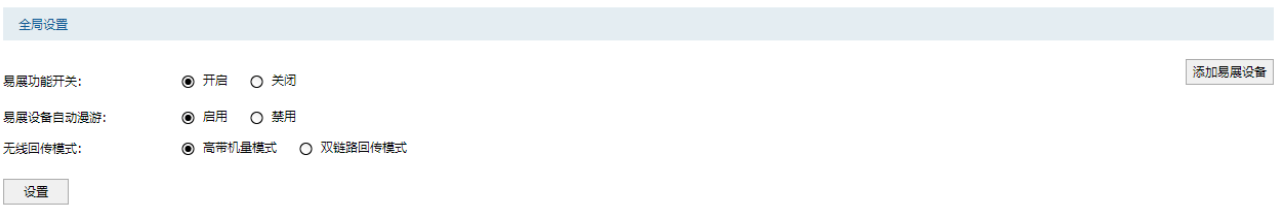




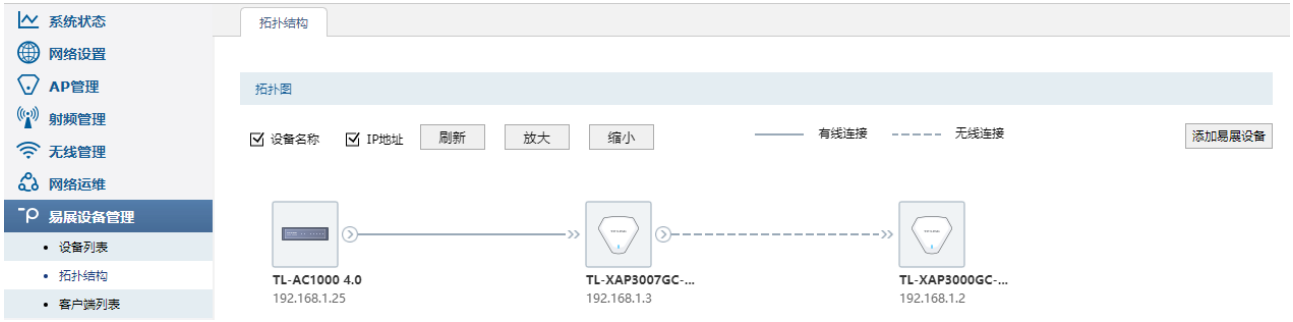
易展主 AP 连接并配置完成后，可通过以下两种方式添加易展子 AP：

8.1.1 通过 Web 管理页面添加易展子设备

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，同时按下易展子 AP 上的“易展”按键。



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。

添加完成后，可在易展子设备列表中查看并配置易展子 AP 的信息。

8.1.2 使用“易展”按键一键互联

“易展”设备带有易展按键，可与其他带有易展按键的 TP-LINK 设备实现“一键互联”，与易展主设备互联的其他设备将会获取到易展主设备的所有配置参数。

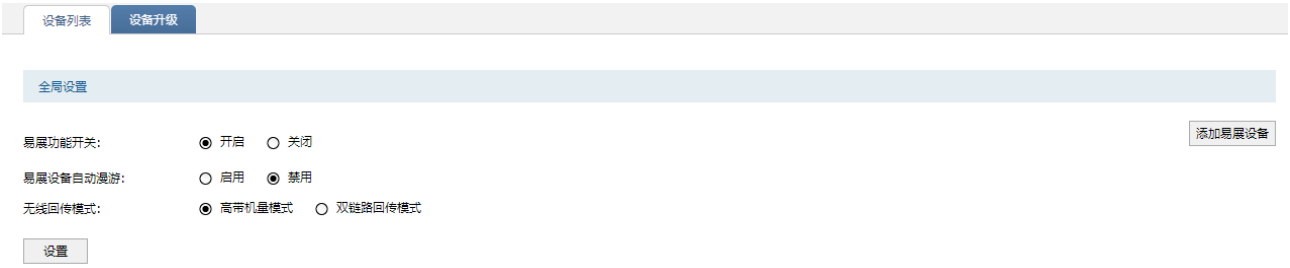
选择邻近插座，将一台出厂状态的“易展”子 AP 接通电源，系统指示灯绿色常亮，等待一段时间，指示灯闪烁 2s，表明子 AP 启动成功；此时按下子 AP 的“易展”按键触发设备配对状态；当系统指示灯变为红色闪烁，表明子 AP 进入待配对状态；此时再按已有线连接到无线控制器的易展主 AP 的“易展”按键，系统指示灯变为红色闪烁，表明正在搜索；搜索到子 AP 后，系统将自动连接。

当主 AP 与子 AP 的系统指示灯均变为绿色常亮，表明配对完成，可在易展子 AP 列表中查看并配置该 AP 信息，实现“一键互联”。

8.2 易展设备管理

8.2.1 设备列表

进入页面：易展设备管理 >> 设备列表 >> 设备列表，在“全局设置”模块开启易展管理功能，点击<设置>。



易展功能开关	功能开启后，将允许易展设备通过无线或者有线方式进行易展组网，可在 AC 端添加和管理易展设备并下发对应易展配置。如采用传统有线 FIT AP 组网方案，可不开启此功能。
易展设备自动漫游	功能开启后，易展设备将根据与前端设备连接链路是否连通以及链路质量，自动尝试切换连接质量更好的主设备。切换后，设备将自动从新的主设备同步无线服务及射频配置。

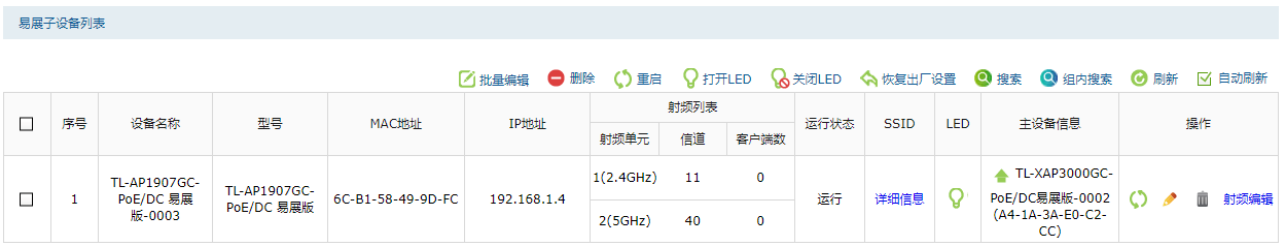
无线回传模式　　配置易展设备的无线回传链路信息，可以根据不同的网络需求使用不同的回传模式，可以提高使用体验。(模式切换可能会对易展子设备的 2.4G 信道进行调整，造成 2.4G 频段已关联终端短暂离线。)

- 高带机量模式：单 5G 频段链路回传，2.4G 频段全部用于用户链接，带机量更大。允许对各个易展子设备的 2.4G 信道进行单独配置，增加信道容量
- 双链路回传模式：易展 AP 之间 2.4G/5G 双链路同时回传，吞吐量更大，组网稳定性更强。网络中易展子设备 2.4G/5G 频段将自动同步易展主 AP 信道设置。

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”、“主 AP 冗余”和“子设备更换主 AP”：

➢ 易展主设备列表

➢ 易展子设备列表



点击页面  ，查看更多页面设置参数信息。

点击 ，可断开与易展 AP 的连接。

点击 ，可对易展 AP 重新启动。

点击 ，可开启或关闭易展 AP 指示灯。

点击<恢复出厂设置>，可重置易展子 AP。

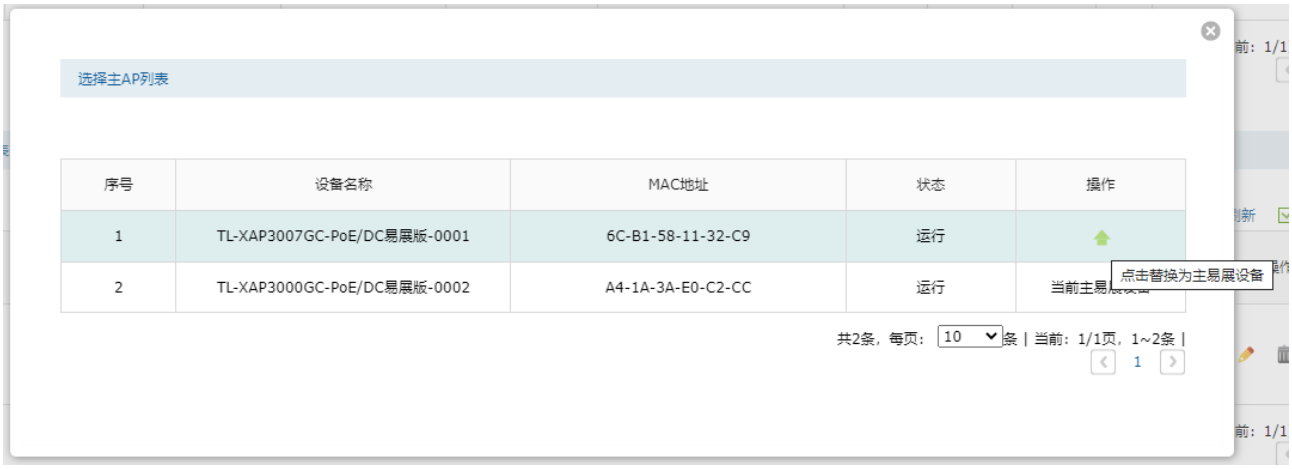
点击 ，可编辑主子设备信息。

➢ **主 AP 冗余**

在易展主 AP 列表，点击 ，主设备冗备功能，可以通过此功能，将某个主 AP 的设备备份到新加入的主 AP，主要是用于主 AP 故障/替换的场景。

➢ **子 AP 更换主 AP**

在易展子 AP 列表，点击，使子设备更换主设备功能，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。



➢ **待授权设备列表**

点击<易展>授权选中的易展设备，授权后设备会加入易展网络。

点击<拒绝授权>拒绝选中的易展设备，被拒绝的易展设备会被删除。被拒绝授权的设备如要重新进行授权，需要重新点击设备上的易展按钮。

8.2.2 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。详情可参考 **4.2AP 升级**。

➢ 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。

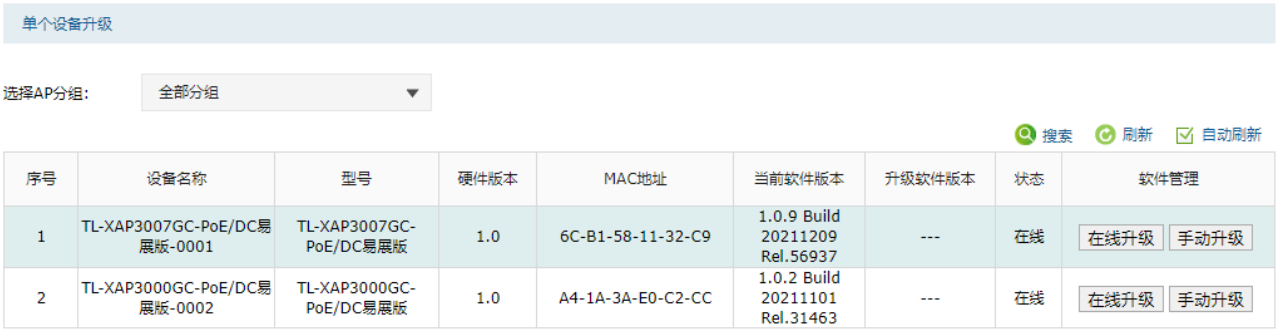
在“AP 批量升级”栏目下，点击<新增>，选择 AP 分组及 AP 型号后，点击<确定>，即可对 AP 进行批量升级。若选择“定时升级”，则 AP 在指定时间进行升级，如下图。

说明:

- 对于相同型号的设备，“批量升级”任务和“单个设备升级”任务，不能同时使能。
- 使用“单个设备升级”操作对多个设备进行升级时，建议先给易展子设备升级，再给易展主 AP 升级。

➢ 单个 AP 升级

在“单个 AP 升级”栏目下，选择 AP 分组，可对单个设备进行<在线升级>或<手动升级>。



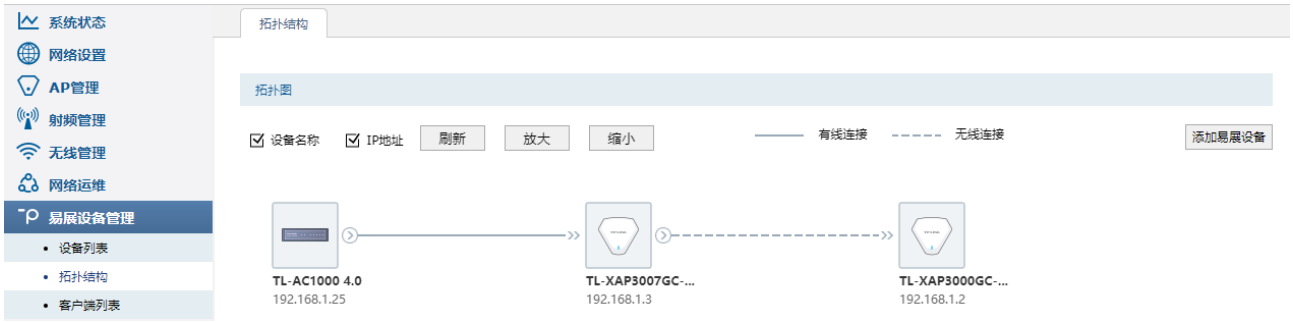
说明:

- 您可以到 TP-LINK 官网 www.tp-link.com.cn 下载最新的升级软件。

8.3 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。



8.4 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。点击<刷新>获取最新客户端列表，点击<断开连接>断开客户端的连接。


系统状态
网络设置
AP管理
射频管理
无线管理
网络运维
易展设备管理
设备列表
拓扑结构
客户端列表
认证管理
安全管理
客户端列表
客户端状态
选择AP分组:
全部分组
断开连接
搜索
全局搜索
刷新
自动刷新
备份
序号
客户端名称
MAC地址
AP名称
射频单元
SSID
IPv4/IPv6地址
VLAN ID
接入时间
信号强度
设置
1 --- E2-24-45-8F-05-B2 TL-XAP3007GC-PoE/DC易展版-0001 2(5GHz) TP-LINK_5G_8143 ---/--- --- 2022/07/18 16:39:17 -86dBm
2 --- F2-EA-30-9B-FE-5E TL-XAP3000GC-PoE/DC易展版-0002 2(5GHz) TP-LINK_5G_8143 ---/--- --- 2022/07/18 16:39:08 -90dBm
3 --- 62-F2-71-54-6B-D4 TL-XAP3000GC-PoE/DC易展版-0002 2(5GHz) TP-LINK_5G_8143 ---/--- --- 2022/07/18 16:42:28 -84dBm

回目录

第9章　认证管理

TP-LINK 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：

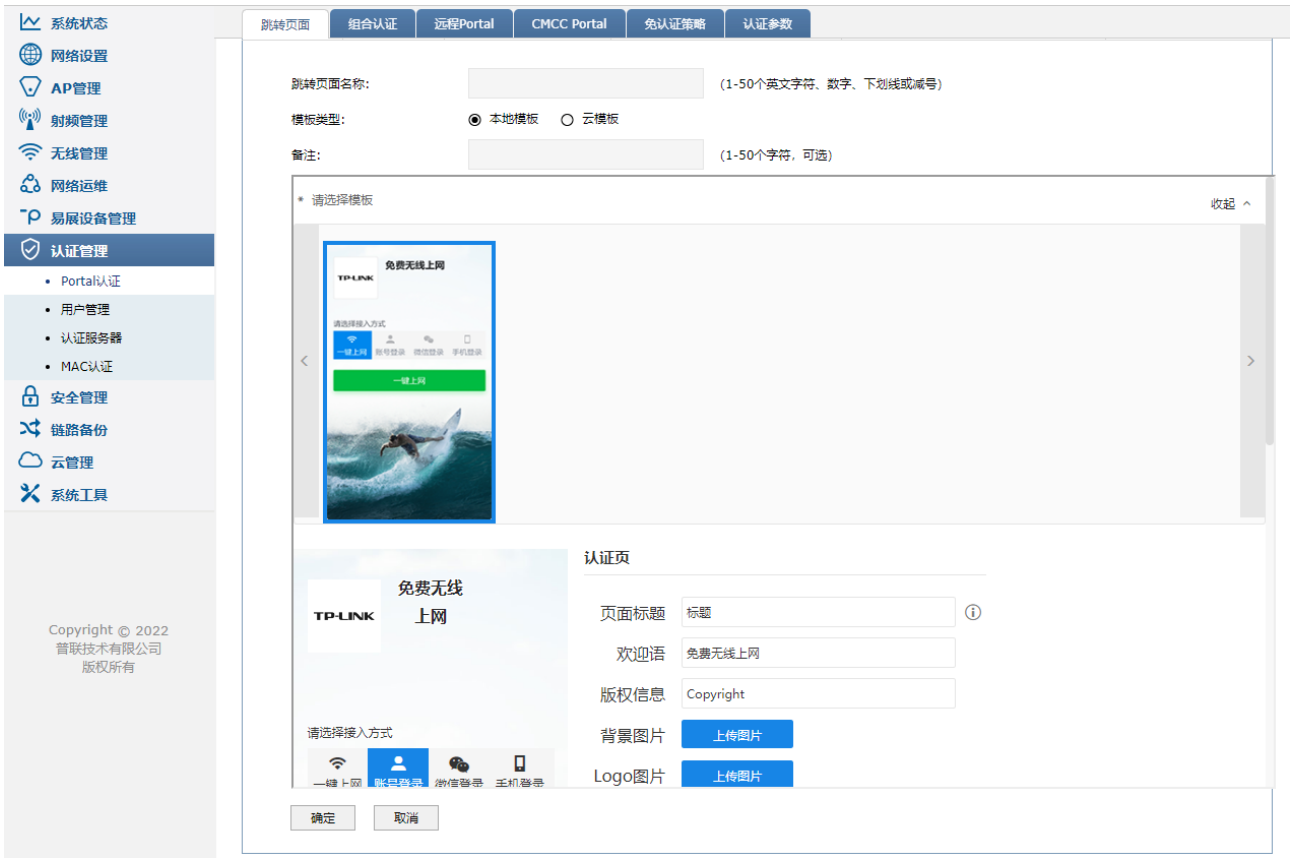
- 在进行 Portal 认证的相关设置之前，请先确保无线控制器管理 AP 的接口 IP 地址与待认证客户端的 IP 地址之间路由可达。

9.1　Portal 认证

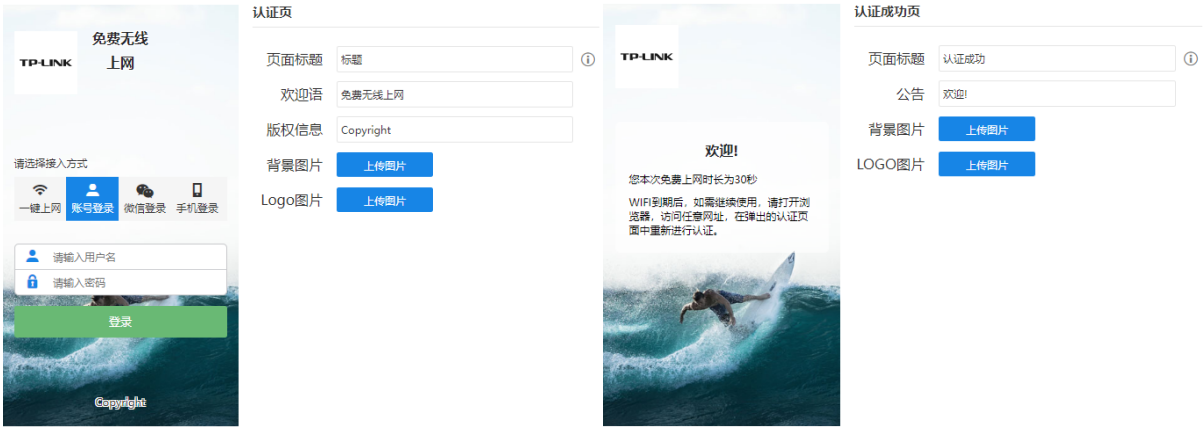
9.1.1 跳转页面

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>。



模板类型	选择跳转页面的模板类型，有本地模板和云模板可供选择。 • 本地模板：终端将使用设备自带的页面版式。 • 云模板：设备将向云端服务器获取页面样式，需联网才能使用。
背景图片	用于页面的背景展示图，图片大小限制在 200KB 以内。
Logo 图片	设置页面的 Logo 图片，图片大小限制在 100KB 以内。

9.1.2 组合认证

多功能无线控制器提供一键上网、Web 认证、微信认证和短信认证四种认证方式。

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，点击<启用>或<禁用>选择是否开启当前认证方式。

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 **9.1.1 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、微信认证和短信认证四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。

➢ **微信认证**

认证方式选择微信认证，启用该认证方式，设置免费上网时长及认证 Token，上传二维码图片，点击<确定>。

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。
认证 Token	启用微信认证后，请在微信后台增加该消息跳转链接，用户点击后即可上网。
二维码图片	公众号的二维码图片。

➢ **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>。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。

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。

使用阿里云平台进行短信发送：

Access Key ID	访问阿里云平台短信接口所对应的用户名。
Access Key Secret	访问阿里云平台短信接口所对应的密码。
模板 CODE	阿里云平台所提供的模板 ID 号。
签名名称	阿里云平台发送的短信模板对应的签名名称。

使用腾讯云平台进行短信发送：

SMK_App_ID	访问腾讯云平台短信接口所对应的用户名。
App Secret	访问腾讯云平台短信接口所对应的密码。
模板 ID	腾讯云平台所提供的模板 ID 号。
签名	腾讯云平台发送的短信模板对应的签名名称。

使用百度云平台进行短信发送：

Access Key ID	访问百度云平台短信接口所对应的用户名。
Secert Access Key	访问百度云平台短信接口所对应的密码。
模板 ID	百度云平台所提供的模板 ID 号。
短信签名	百度云平台发送的短信模板对应的签名名称。
调用 ID	百度云平台调用短信发送应用的调用 ID。

使用网易云信平台进行短信发送：

AppKey	访问网易云信平台短信接口所对应的用户名。
App Secret	访问网易云信平台短信接口所对应的密码。
模板 ID	网易云信平台所提供的模板 ID 号。
短信签名	网易云信平台发送的短信模板对应的签名名称。

使用 HTTP 协议方式发送短信：

URL 地址	所选择平台的 URL 地址。
请求方式	向服务器发送请求的 HTTP 报文类型。
编码类型	所选择平台要求的编码格式。
短信模板	当为 http 类型时，短信模板为 url 参数。其中手机号与验证码分别采用'{PHONE}'与'{CODE}'关键字替换，例如： user=zhangsan&password=12345678&phone={PHONE}&msg=您的验证码为{CODE}，请不要告诉他人!。 参数中可增加其它固定的参数信息，如：action=send。不可添加不固定项，主要包括时间戳、MD5 项、校验和项等。

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，必须要先在页面“系统工具->时间设置”中正确地配置本机系统时间。

9.1.3 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。

9.1.4 CMCC Portal

进入页面：认证管理 >> Portal 认证 >> CMCC Portal，可以设置和查看 CMCC Portal 认证条目。

生效 SSID	选择需要进行 CMCC Portal 认证的无线网络。

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 CMCC 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。
无感知认证	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进入无线服务时会自动进行认证。
ACNAME 属性	CMCC Portal 跳转地址的 acname 属性，用于识别不同的 AC 设备。
备注	设置 CMCC Portal 认证条目的备注信息，以方便管理和查找。


注意：

- CMCC Portal 地址会自动加入免认证策略，无需用户配置。
- 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。
- ACNAME 属性会添加到跳转链接的 wlanacname 属性中。

9.1.5 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，可设置和查看免认证策略信息，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。

9.1.6 认证参数

进入页面：认证管理 >> Portal 认证>> 认证参数，可设置认证的全局参数，点击<设置>。

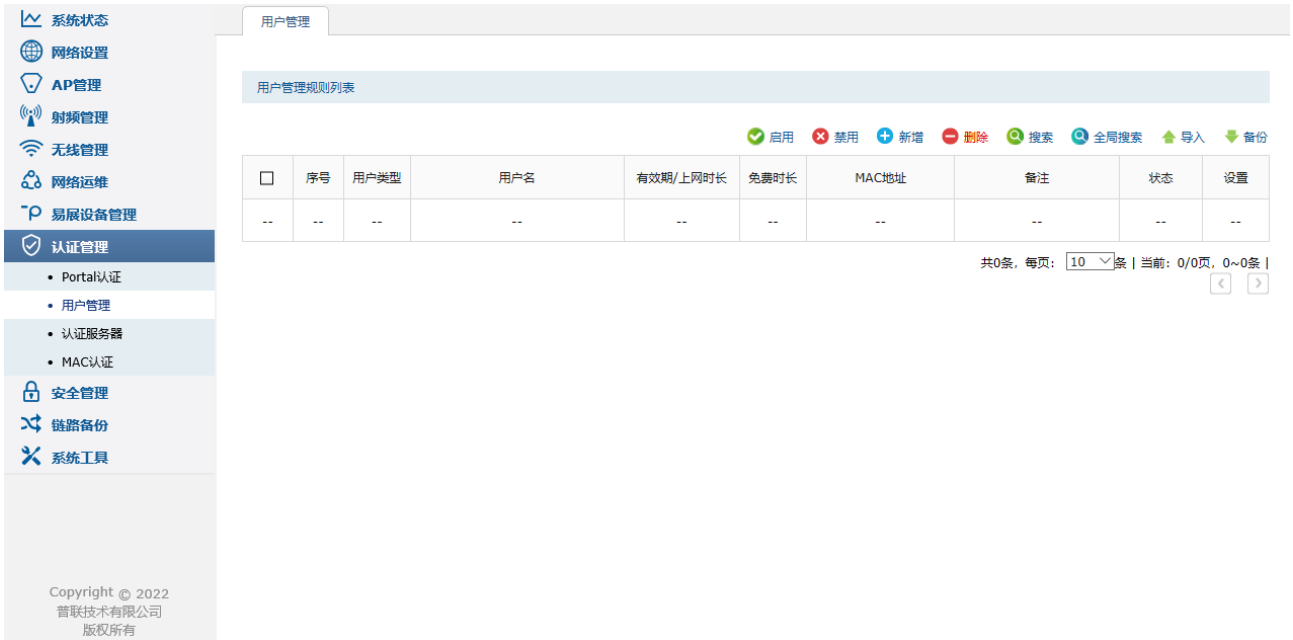
认证老化时间	当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口，不能与其它的服务端口重复。

认证模式	设置 Portal 认证的认证模式，现支持基于 SSID 和基于 VLAN 两种模式。
CMCC Portal 认证端口	设置 AC 的 CMCC Portal 认证端口，用于接收 Portal 服务器发送的认证报文。
CMCC Portal 服务器端口	设置 CMCC Portal 服务器的端口号，用于 CMCC Portal 认证时 AC 发送 NTF_LOGOUT 报文的目的端口号。
单点认证	勾选后会将认证终端的用户名和 IP 上报给防火墙等指定设备。
对接厂商	单点认证对接厂商的类型。
服务器 IP 地址	单点认证对接设备的 IP 地址。
服务器端口	单点认证对接设备的端口。

9.2 用户管理

9.2.1 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。

9.2.2 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。

9.3 认证服务器

TP-LINK 无线控制器提供指定外部 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**

1. 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。
2. 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。

9.3.1 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	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。

9.3.2 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。

9.4 MAC 认证

因为无线的开放性，在没有设置 WIFI 密码或者密码安全性不够高的情况下，无线覆盖范围内的终端均可能通过搜索信号连接上 WIFI，给无线网络带来了一定的安全隐患。当我们只需要让指定的设备使用无线网络时，可以通过设置 MAC 认证来实现。

与 Portal 认证不同的是，MAC 认证功能等同于无线 MAC 过滤白名单，不需要在服务器上进行认证，而是在连接无线过程中，不合法 MAC 地址的设备将无法连接上无线。

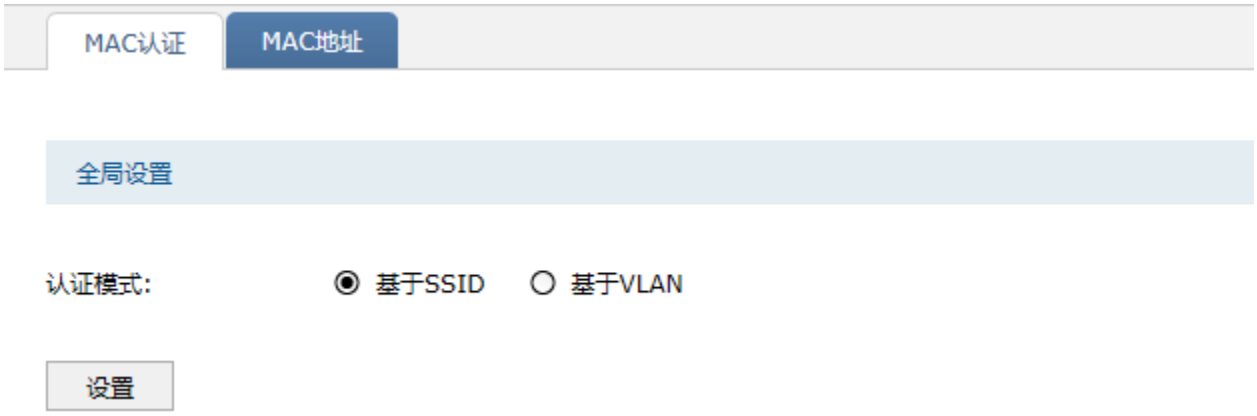
9.4.1 MAC 地址

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。

9.4.2 MAC 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，选择生效的 SSID 或 VLAN 范围。

点击<选择/查看生效 MAC>，可查看并选择生效 MAC 地址，点击<绑定>或<取消绑定>对选择的 MAC 地址

进行操作。

注意：

- 生效 VLAN 范围中用 0 标识空 VLAN，若生效 VLAN 范围输入为空或者只输入 0，则标识 MAC 认证条目只在空 VLAN 中生效。

9.5 MAC 认证配置实例

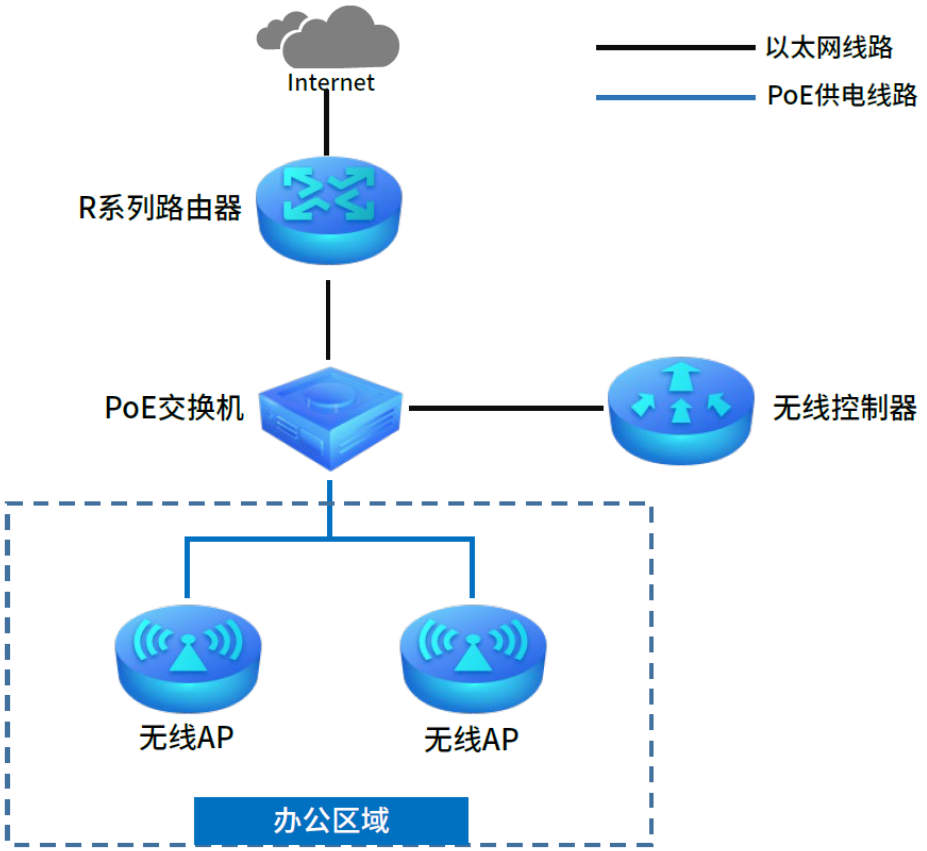
9.5.1 应用介绍

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。

9.5.2 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。



9.5.3 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 。

9.6 Portal 认证配置实例

9.6.1 需求介绍

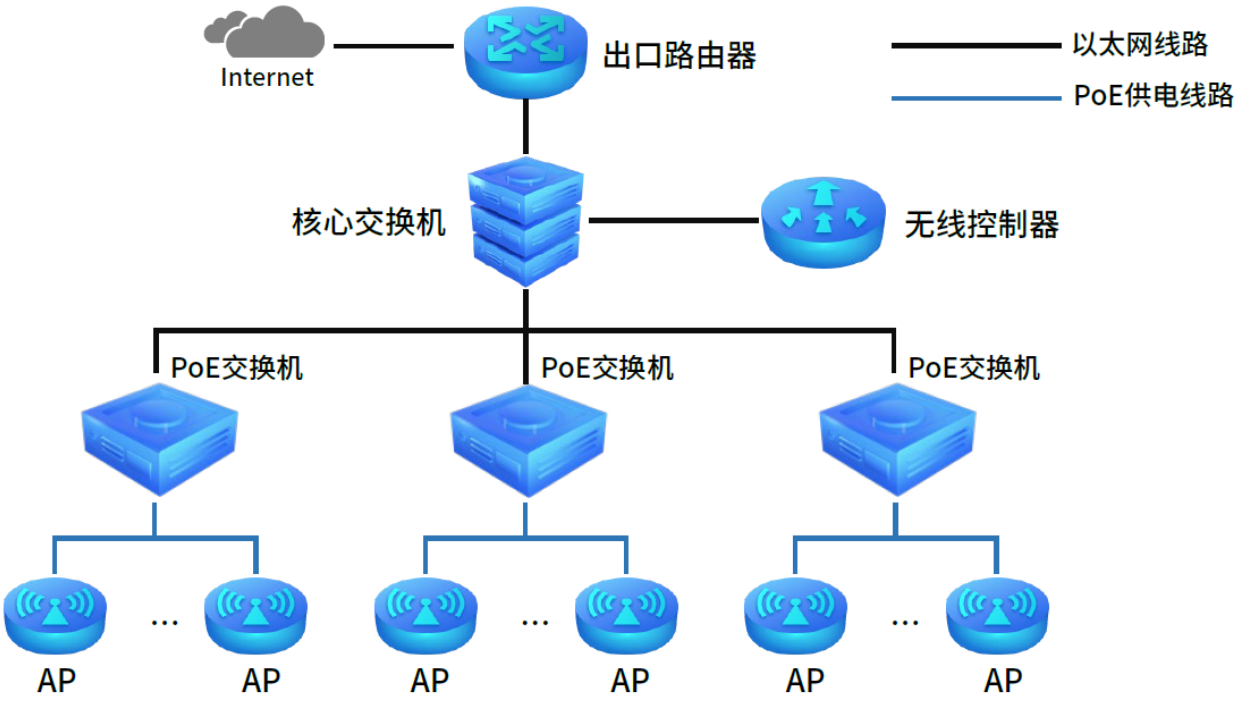
随着智能手机、平板电脑等移动互联网终端的普及，酒店、商场、餐厅等越来越多的服务场所需要给客户提供免费 Wi-Fi。对无线接入用户的认证和推送广告信息成为该类公共无线网络的基础要求。TP-LINK 无线控制器支持 Portal 功能，认证方式灵活，支持广告推送。本节通过典型应用实例介绍多功能无线控制器 Portal 认证功能的应用与配置。

9.6.2 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：

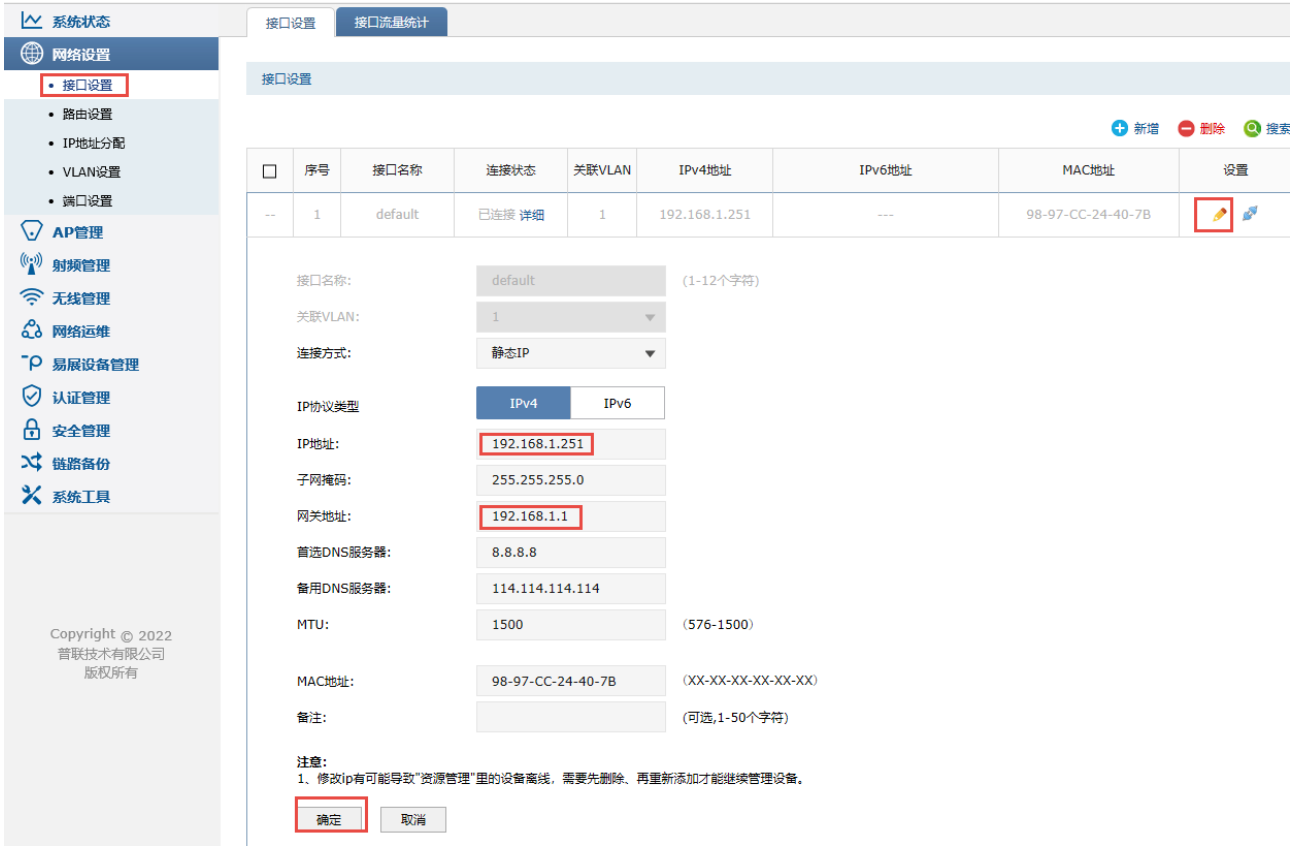
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

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。

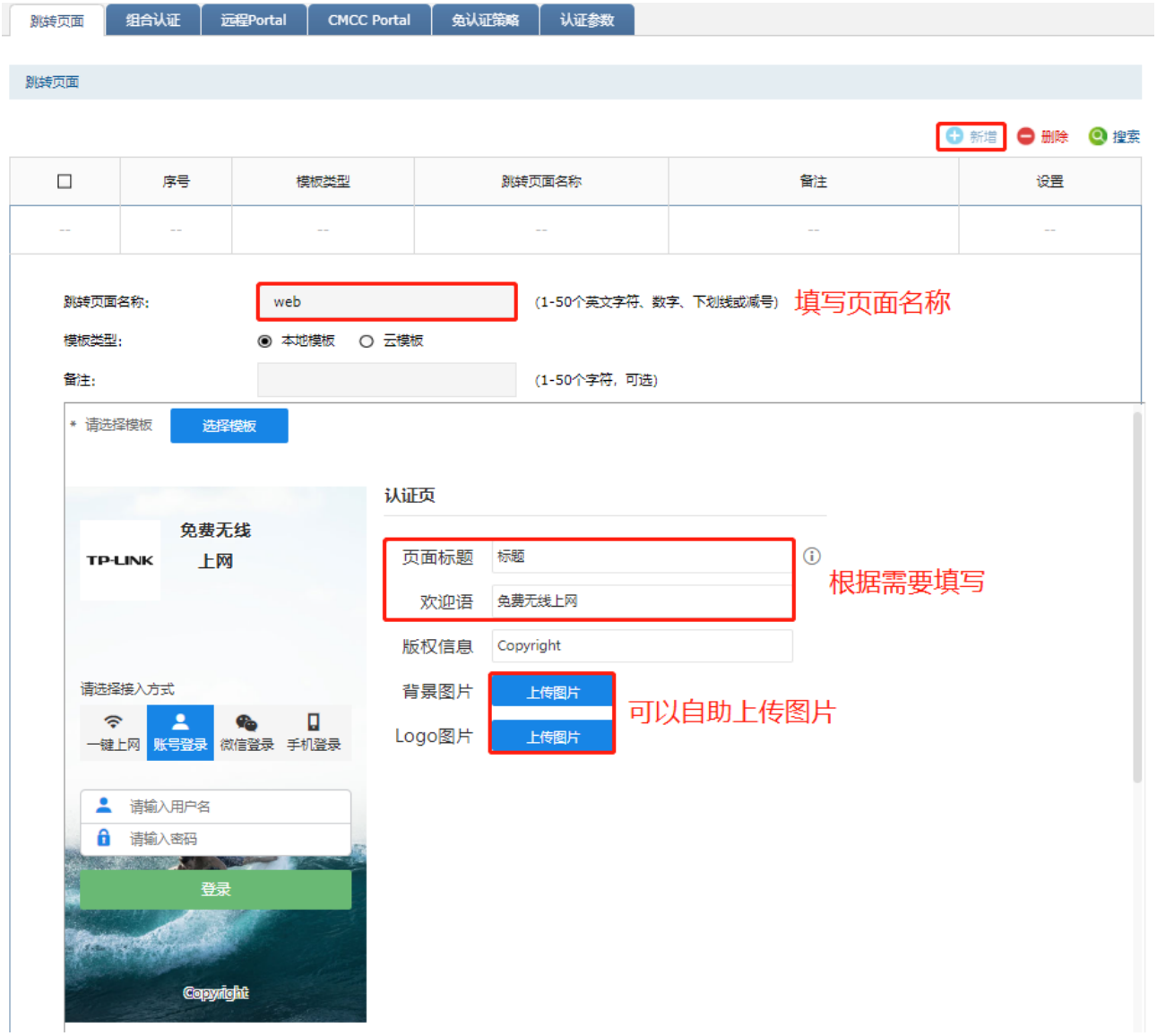


2. 进入页面：无线管理 >> 无线服务， 设置办公 SSID，如下图。

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。

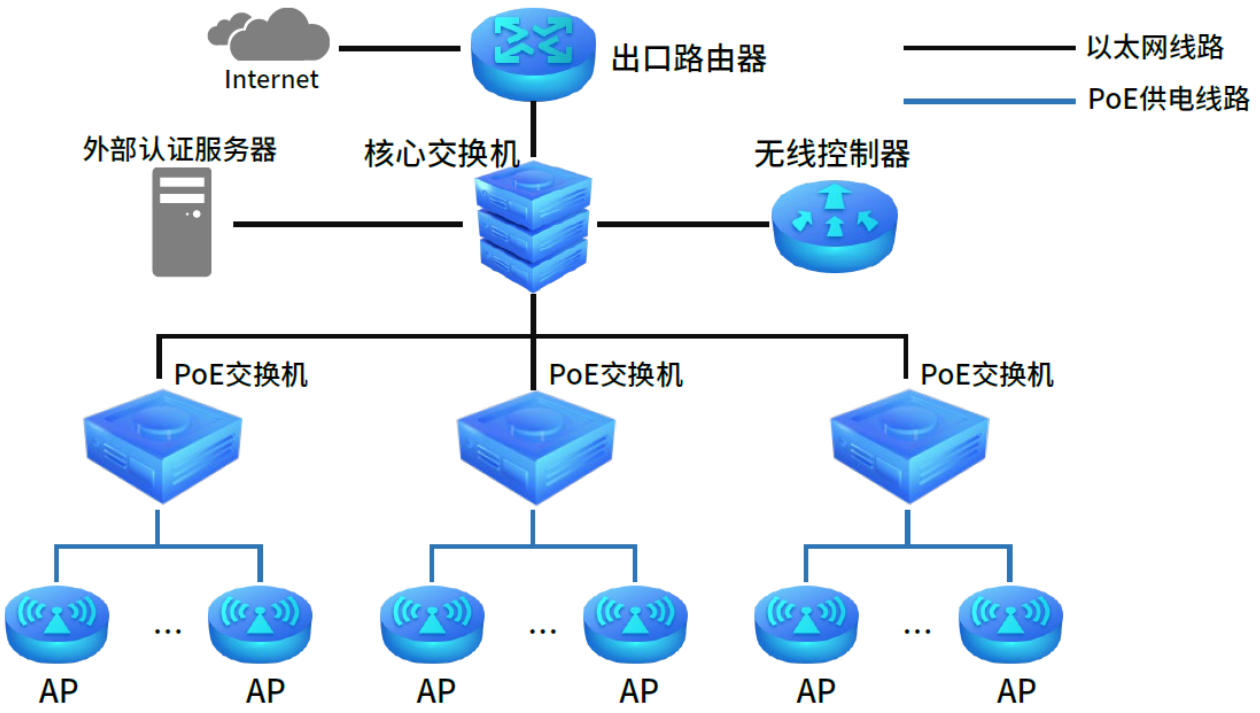
以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

9.6.3 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：

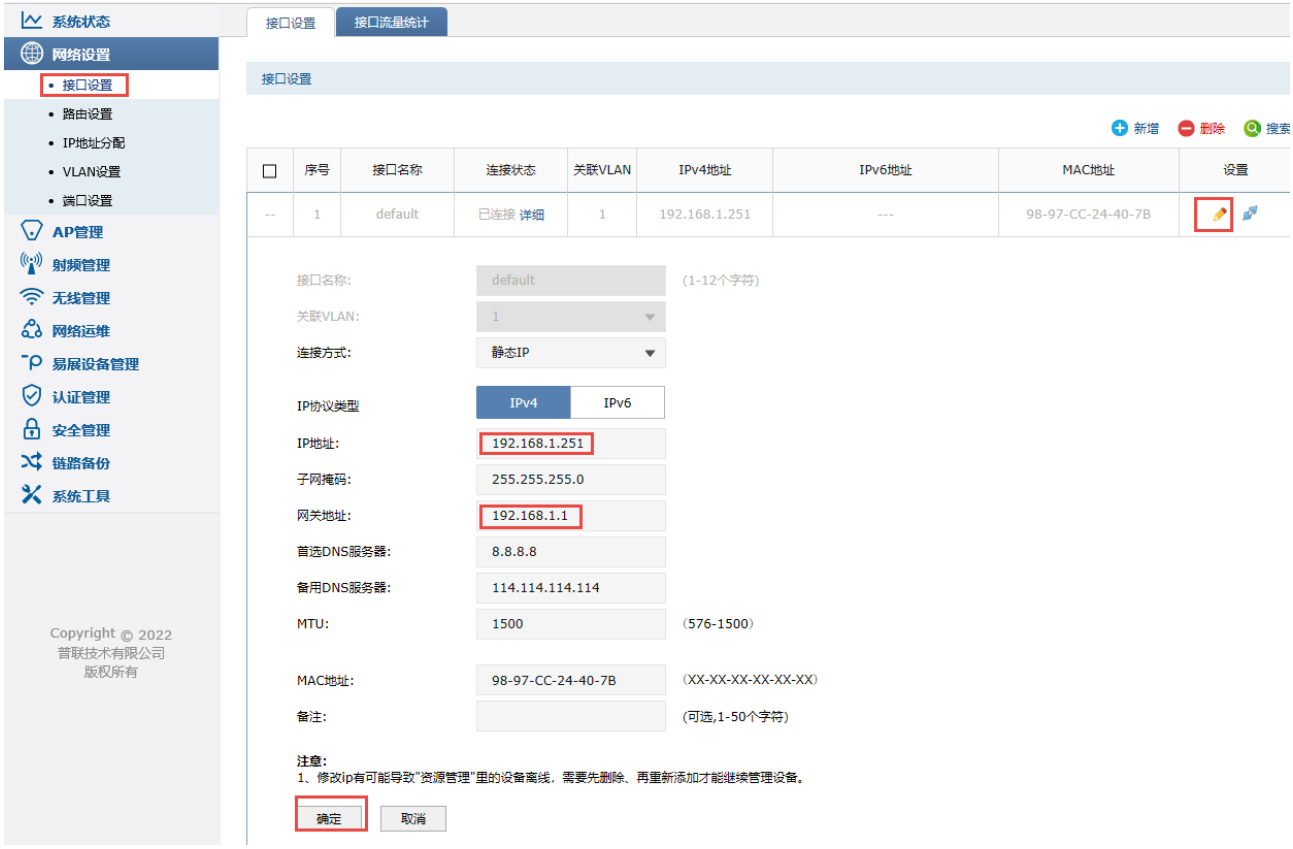
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

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。

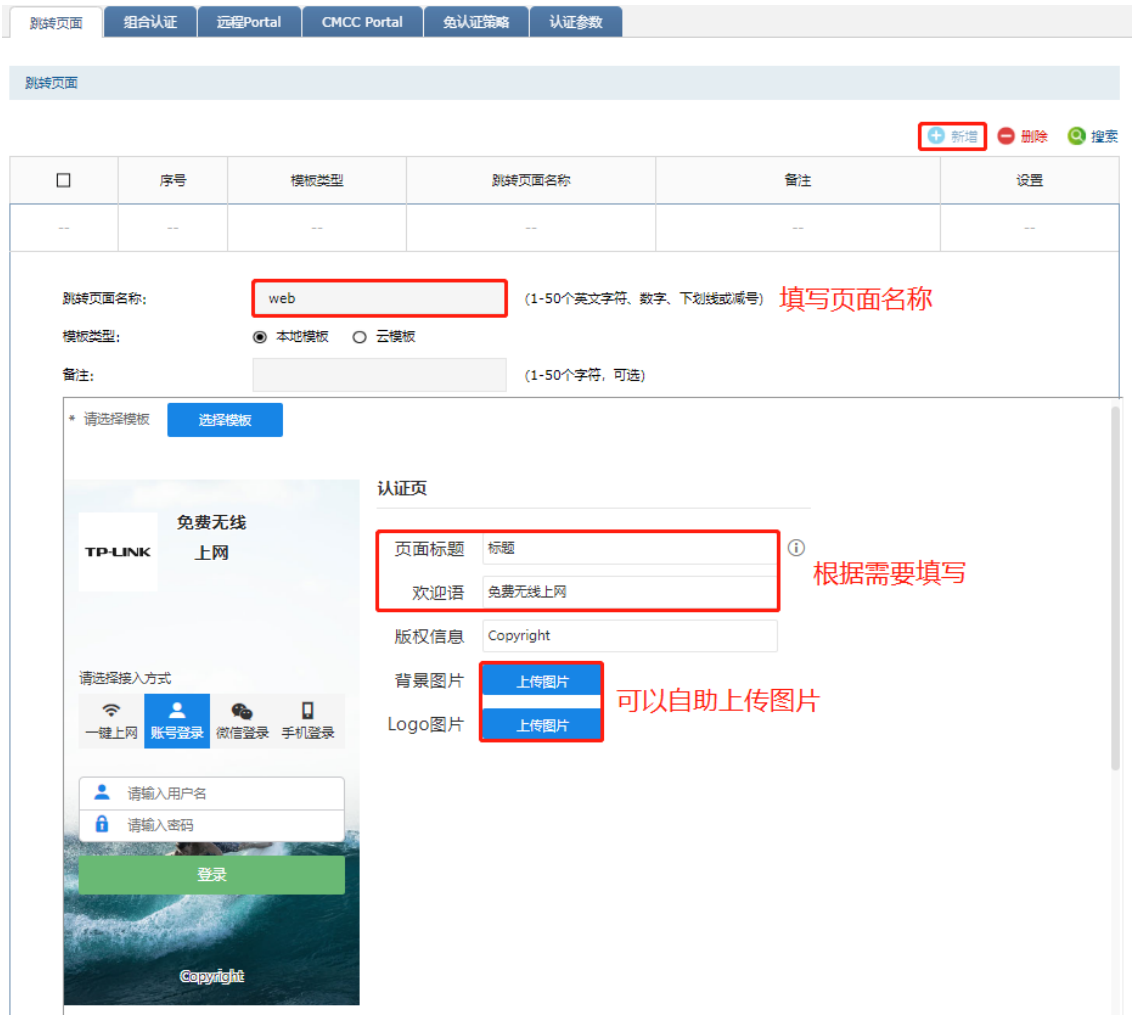
3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

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。

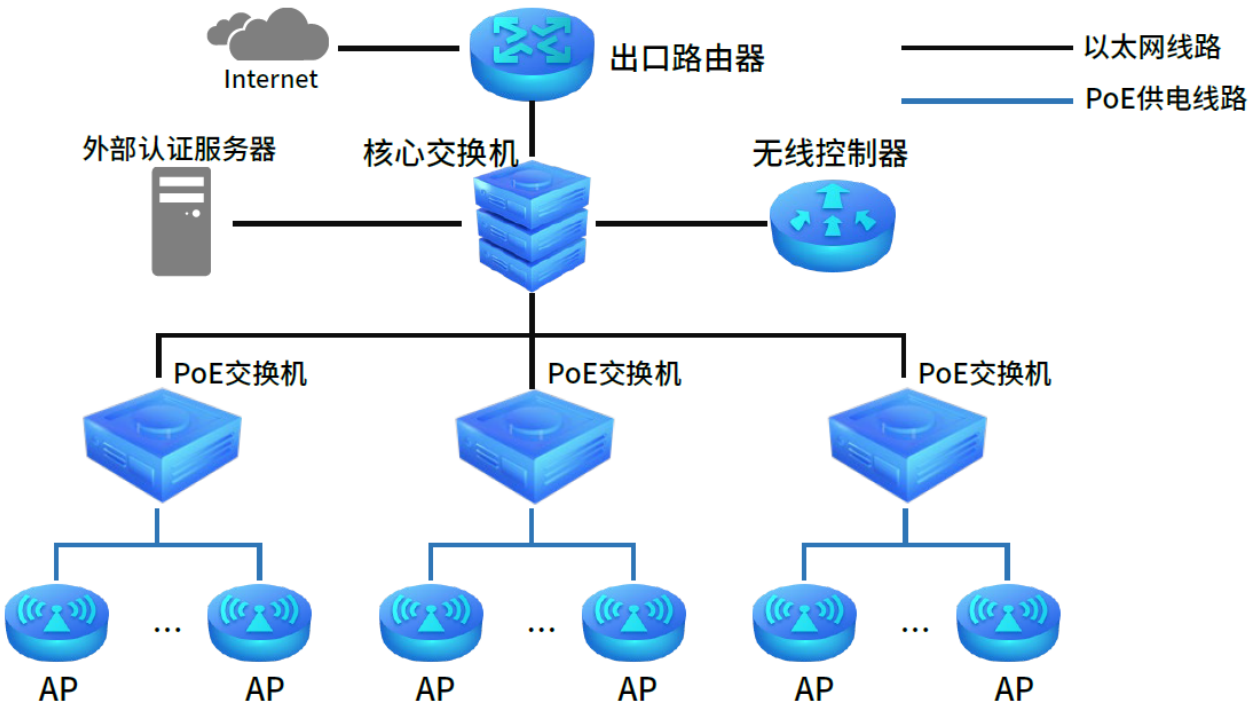
以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

9.6.4 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：

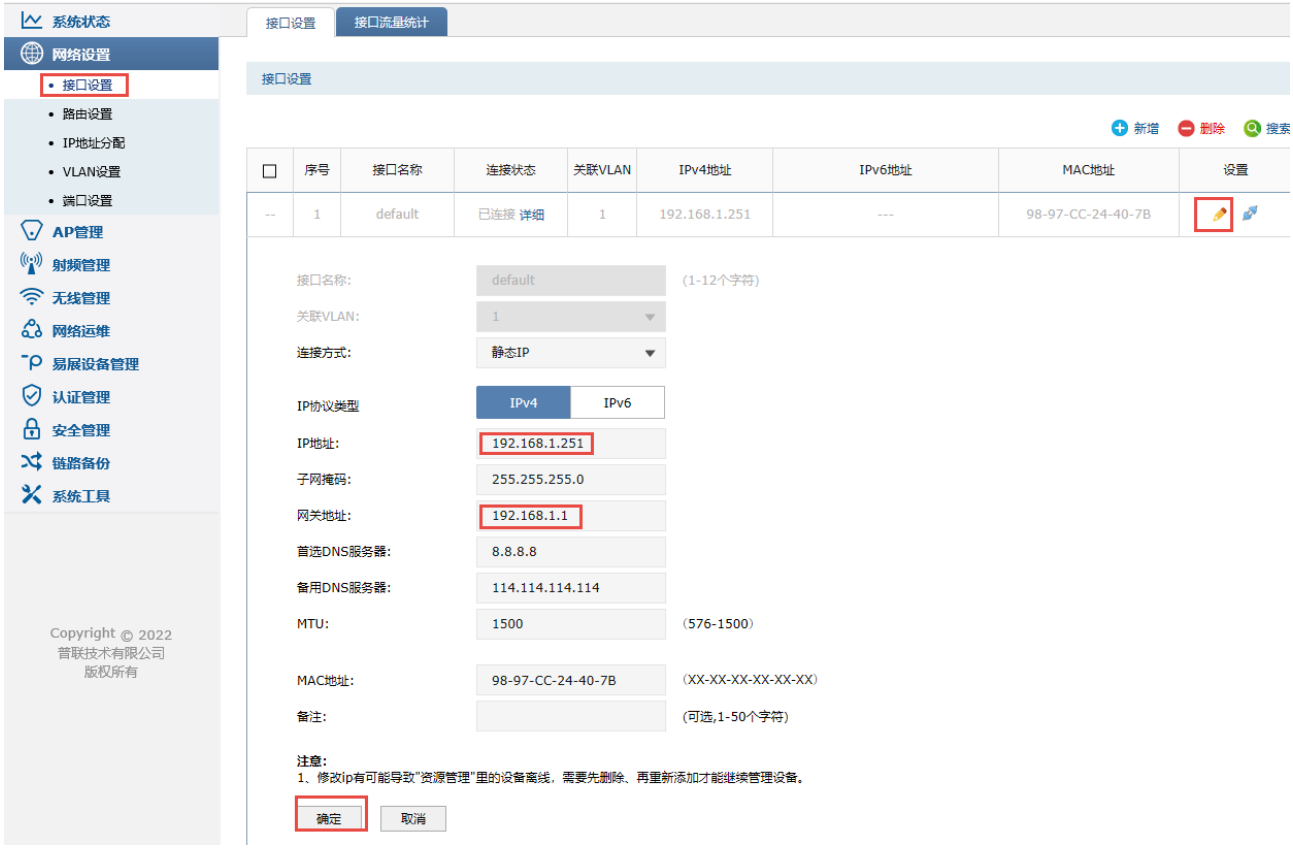
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

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。

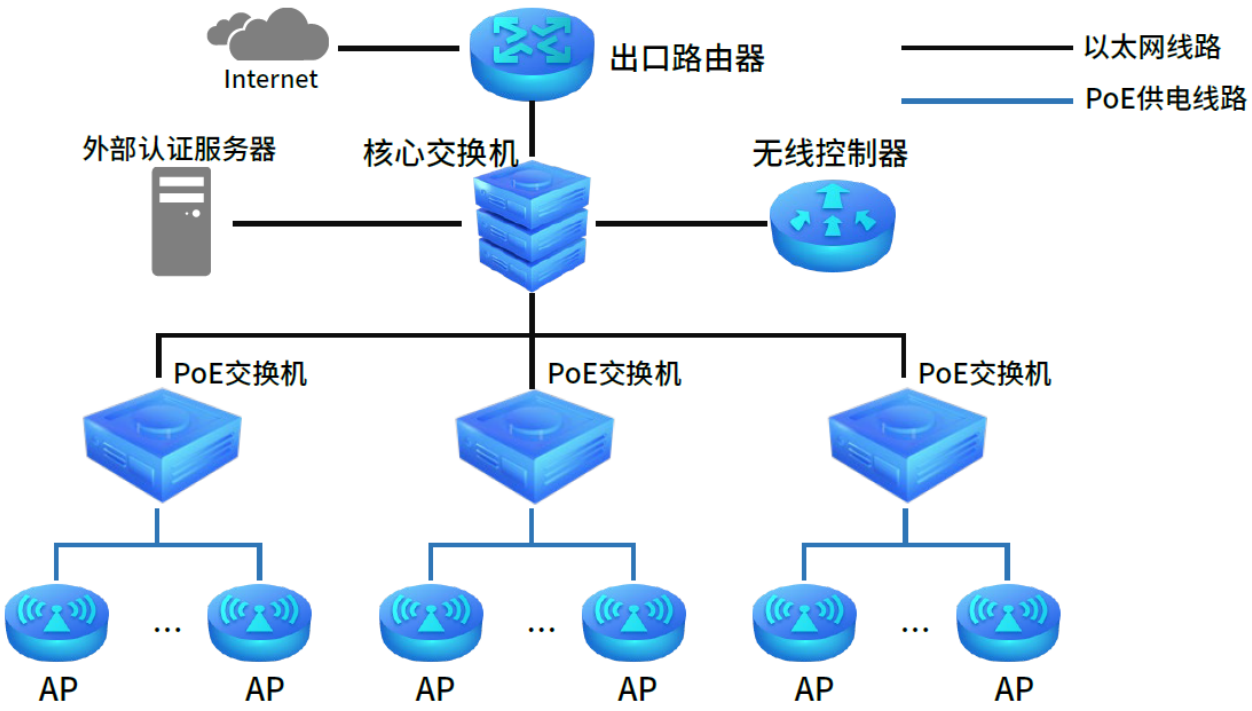
以上内容配置完毕，AC 控制器的 Portal 认证服务设置成功，连接办公区的无线 SSID 输入用户名和密码认证通过后即可上网。

9.6.5 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：

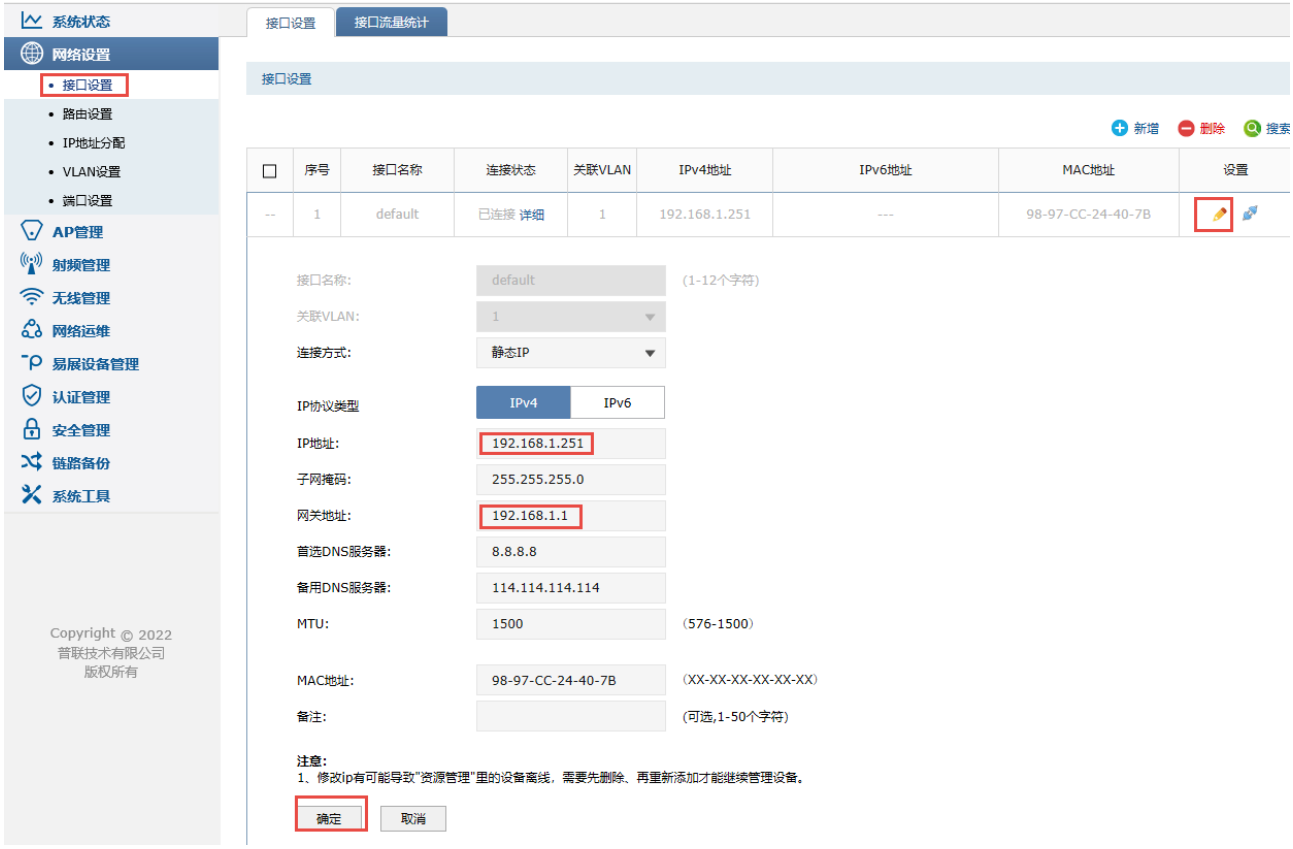
办公区无线需要在 WEB 页面中输入正确的用户名和密码，认证通过之后才能上网。

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。

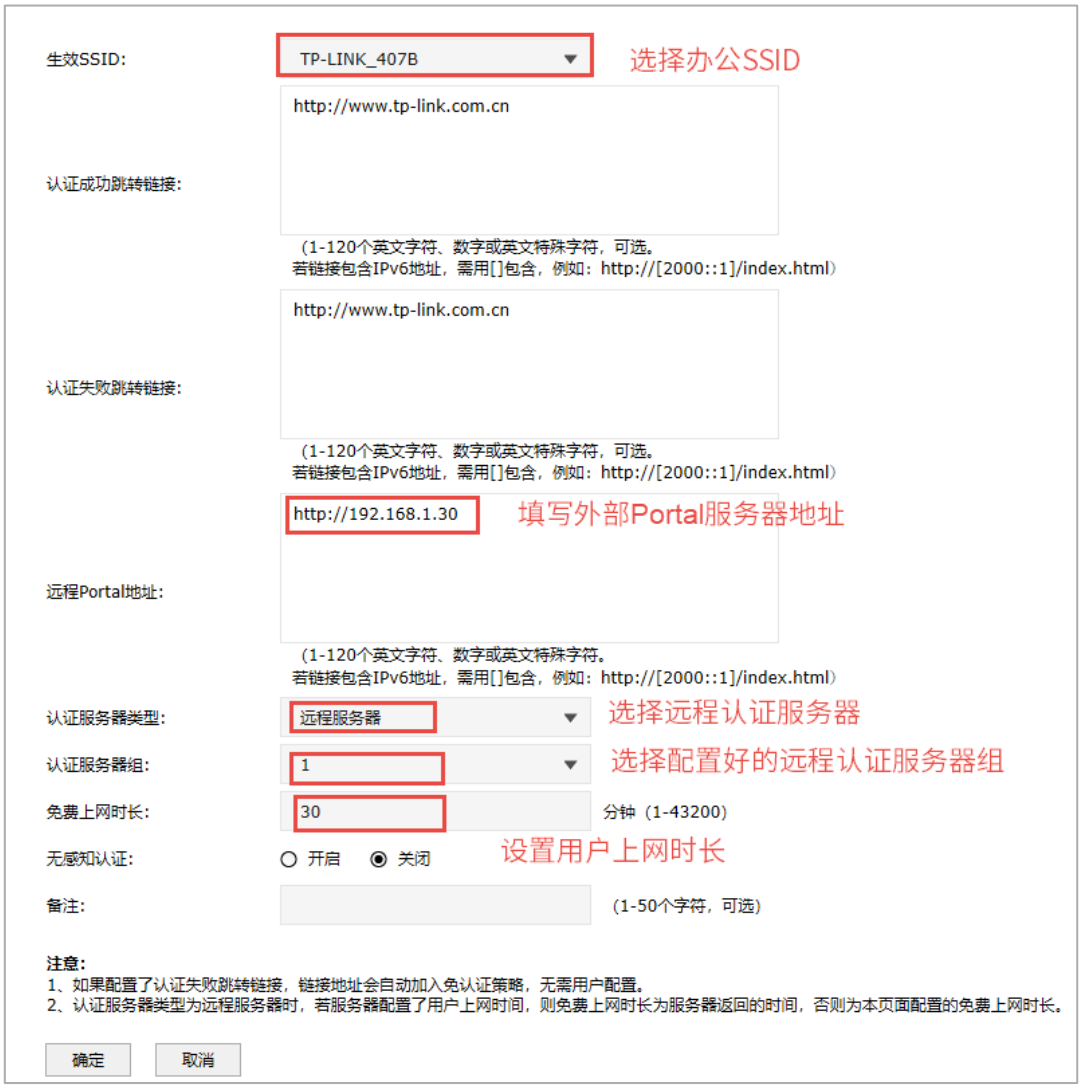
3. 进入页面：认证管理 >> Portal 认证 >> 认证参数， 配置认证老化时间和认证模式，如下图。

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。

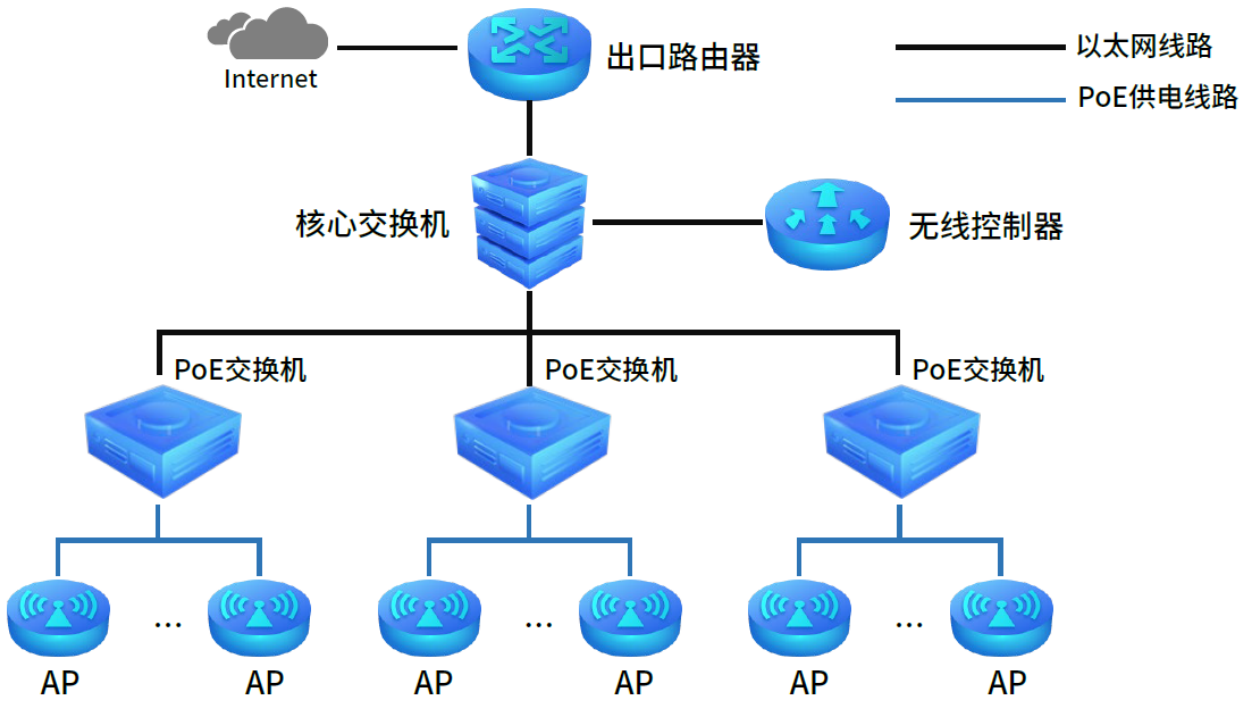
9.6.6 短信认证配置实例

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。

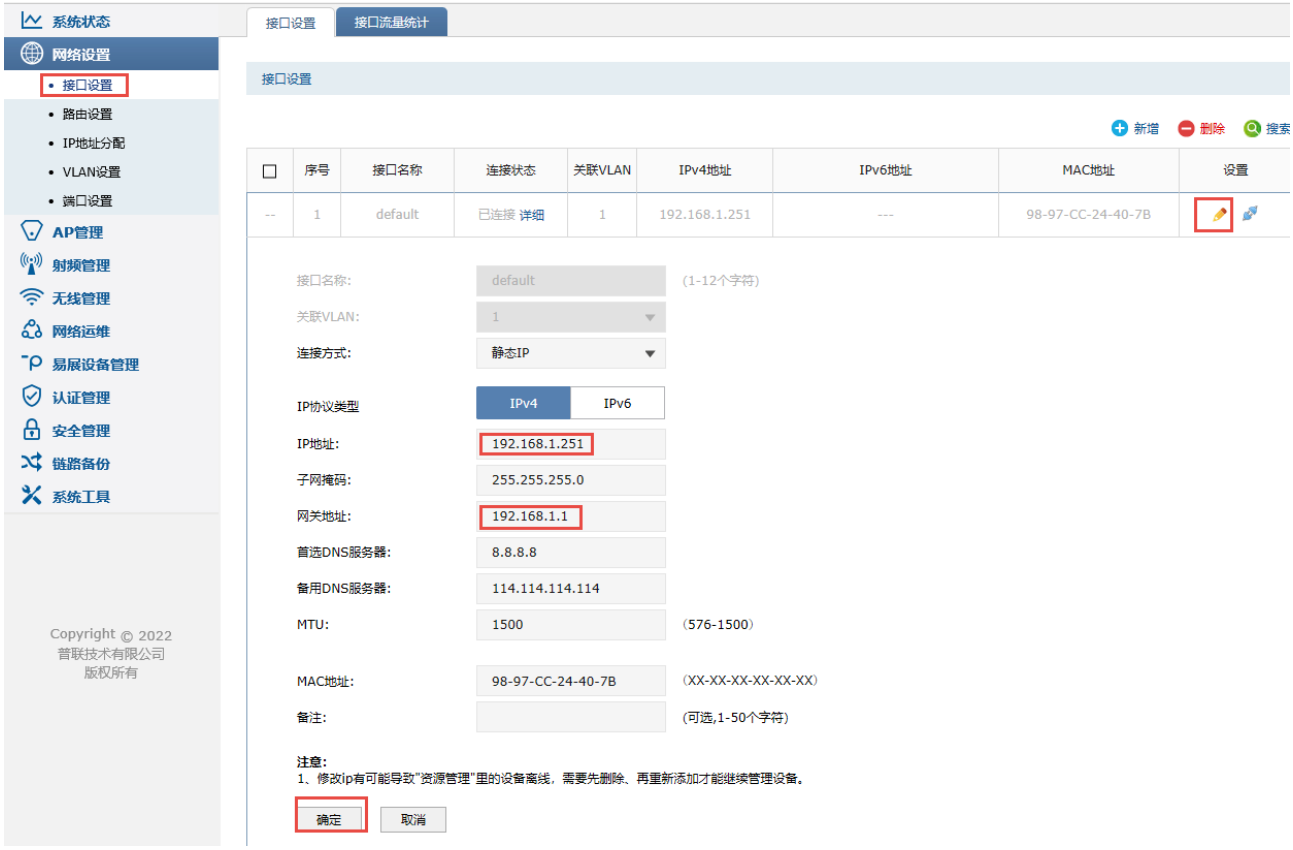
某商场需要实现无线覆盖，为顾客提供无线网络接入，有以下需求：

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。

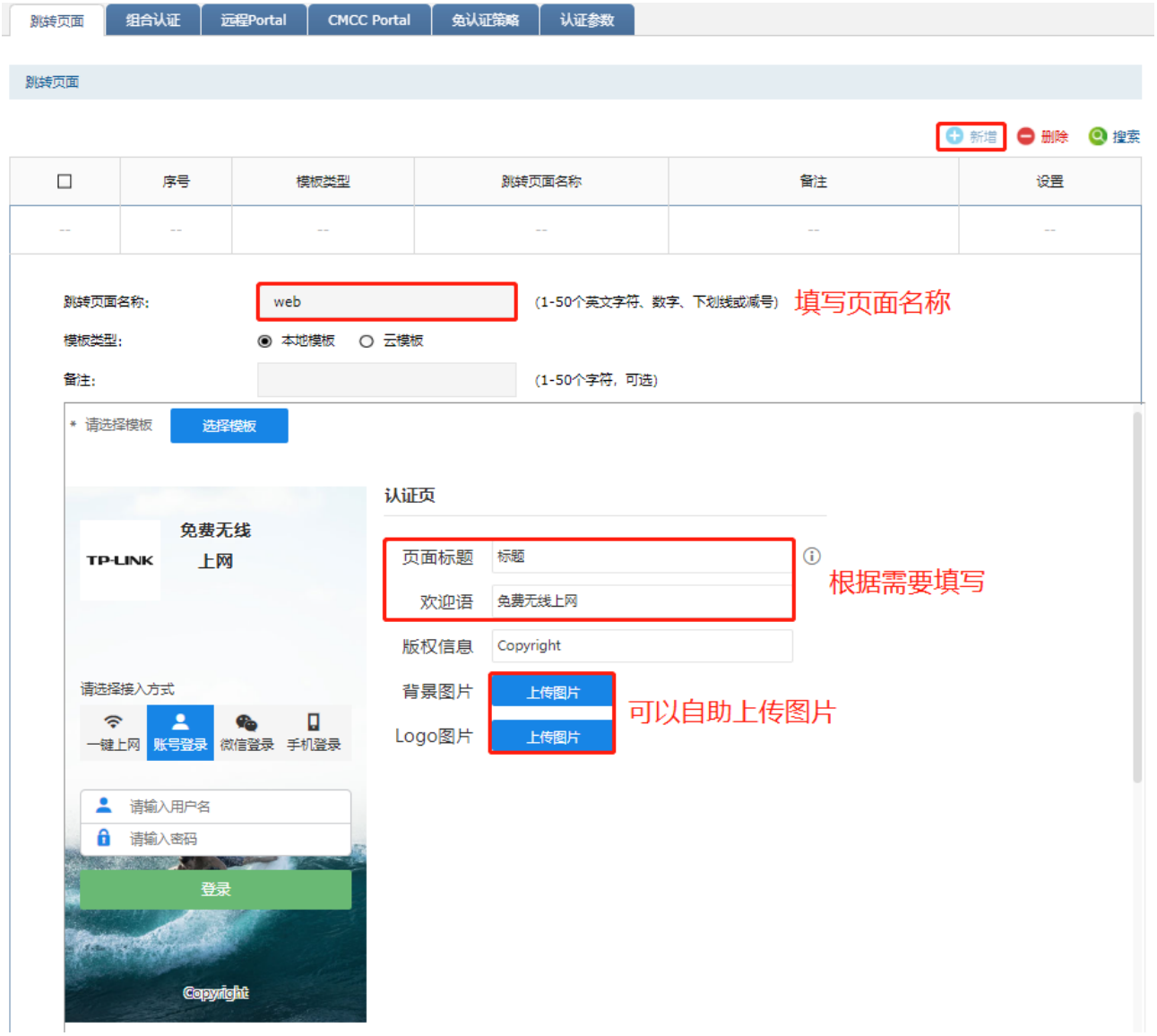
4. 短信设置

（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)

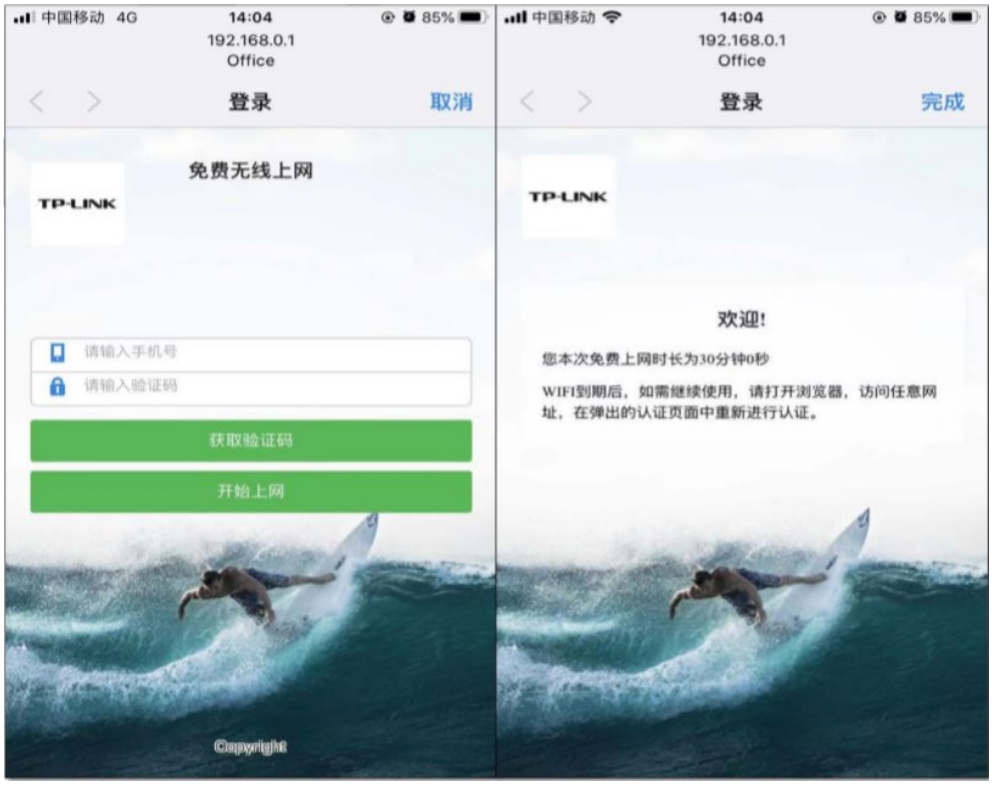
- 百度云


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

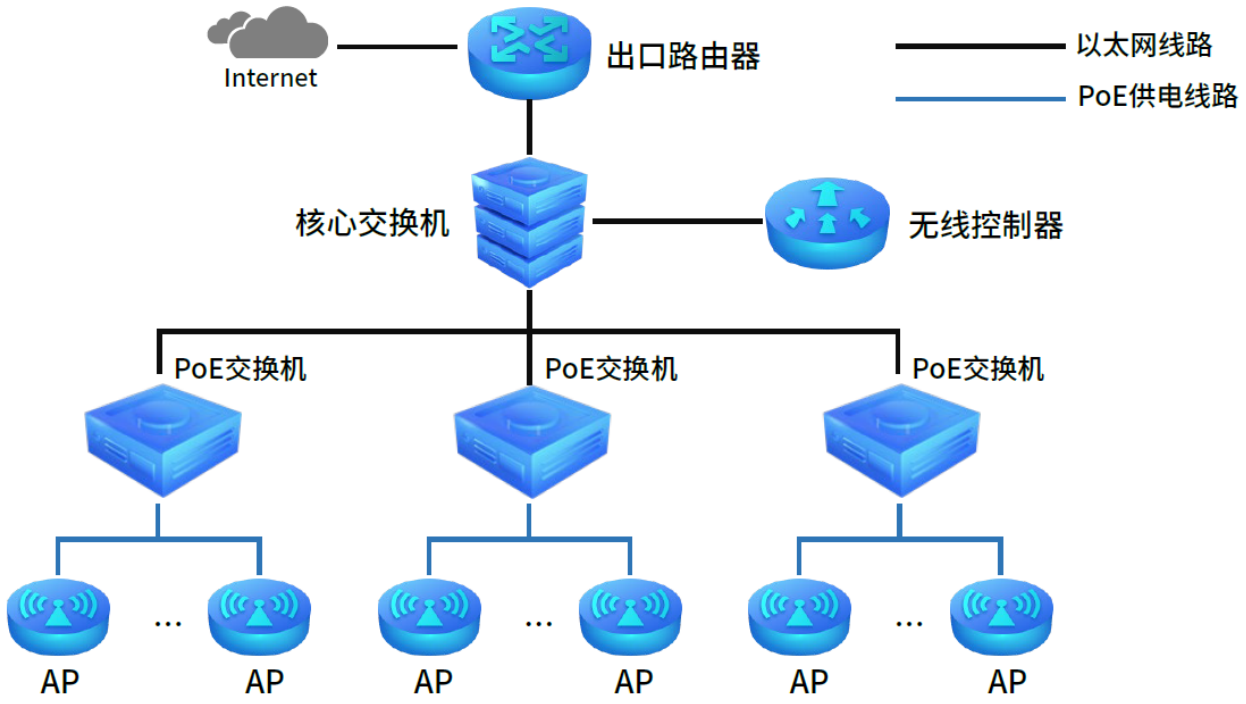
填写完毕点击<确定>，至此短信认证设置完成，顾客连接商场的无线网络 SSID 通过短信认证后即可上网。

效果图如下：



9.6.7 微信认证配置实例

在一些商场、酒店等开放场所，商家在提供免费的 WiFi 服务器的同时需要引导用户关注自己公众号达到推广的目的。TP-LINK 无线控制器的微信认证功能可以满足此类需求，当移动终端无线连接无线网络后，用户需要关注微信公众号并进行指定操作后即可免费上网，可以实现推送广告页面或自动跳转到指定网站的效果。根据用户需求，AC、AP 以及路由器连接参考拓扑，如下图：



➢ **需求介绍**

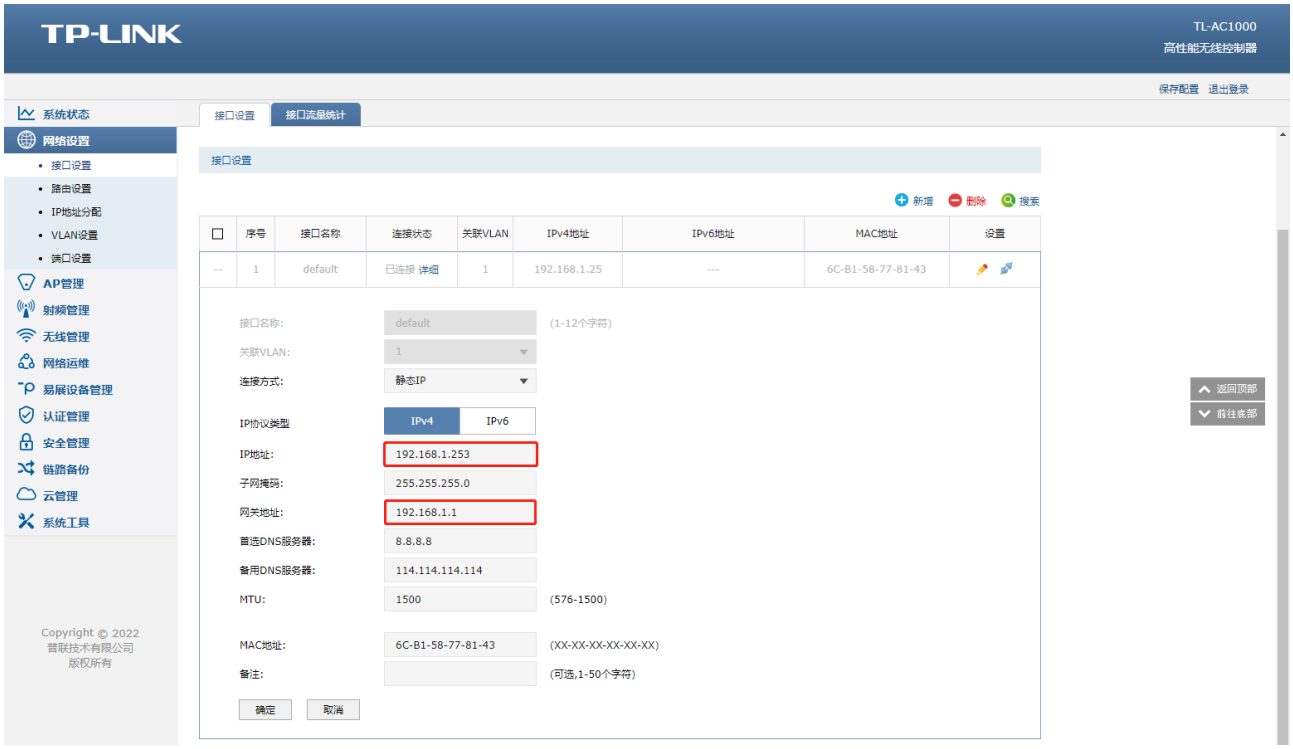
某商场需要实现无线覆盖，为顾客提供无线网络接入，具体需求如下：

某商场希望无线用户通过微信认证之后才能进行浏览网页等上网操作，并且在认证成功以后推送广告页面或者跳转到指定的网站。

➢ **设置方法**

1. AC 控制器基本参数配置

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 ，填写网络中正确的网关（一般是路由器的 IP 地址），如下图：



2. 新增无线并进行射频绑定

进入页面：无线管理 >> 无线服务，设置免费 SSID：

3. 认证参数设置

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：

说明：

- 认证老化时间：当已认证客户端断开连接后，对应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：设置 Portal 认证的认证模式，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。

4. 微信认证配置

1) 进入页面：认证管理 >> Portal 认证 >> 跳转页面，点击<新增>，新增一个跳转页面，页面内容根据实际需求进行填写：


跳转页面
组合认证
远程Portal
CMCC Portal
免认证策略
认证参数
跳转页面
1.点击新增
新增
删除
搜索
序号
模板类型
跳转页面名称
备注
设置
2.填写跳转页面名称
跳转页面名称:
weixin
(1-50个英文字符、数字、下划线或减号)
模板类型:
本地模板
云模板
3.选择模板类型
备注:
(1-50个字符，可选)
* 请选择模板
选择模板
TP-LINK
免费无线
上网
请选择接入方式
一键上网
账号登录
微信登录
手机登录
请输入用户名
请输入密码
登录
Copyright
认证页
页面标题
标题
欢迎语
免费无线上网
版权信息
Copyright
背景图片
上传图片
Logo图片
上传图片
4.自定义跳转页面
TP-LINK
欢迎!
您本次免费上网时长为30秒
WIFI到期后，如需继续使用，请打开浏览器，访问任意网址，在弹出的认证页面中重新进行认证。
认证成功页
页面标题
认证成功
公告
欢迎!
背景图片
上传图片
LOGO图片
上传图片
5.自定义认证成功页面
确定
取消
6.点击确定

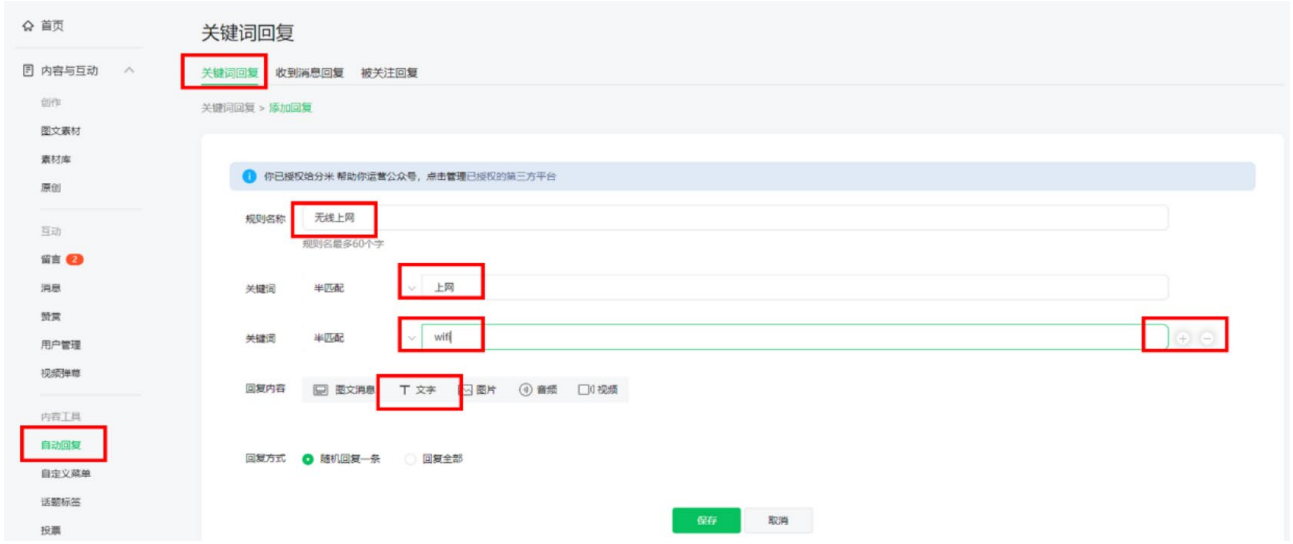
2) 进入页面：认证管理 >>Portal 认证 >> 组合认证，点击<新增>，跳转页面选择之前新增的页面，生效 SSID 选择需要进行微信认证的 SSID，认证成功、失败的跳转链接按需填写。认证方式选择“微信认证”，状态选择“启用”。免费上网时长按需填写或保持默认。填写认证 token，并按照页面提示将相应的连接添加到微信公众号后台即可。

3) 将认证链接 http://ac.tplogin.cn:8080/wechatv2/?auth_token=123456 添加到微信后台被关注自动回复信息中。具体格式为：

点击<ahref="http://ac.tplogin.cn:8080/wechatv2/?auth_token=123456">TP-LINK 免费上网

4) 也可以通过“关键字回复”功能，让用户在微信后台回复关键字获取认证链接，认证上网。首先在页面“自动回复 >> 关键词回复”中点击添加回复：

填写相应的规则名称和关键词，可以通过增加和删减来组合符合需要的关键词，在回复内容中选择文字填写跳转链接：



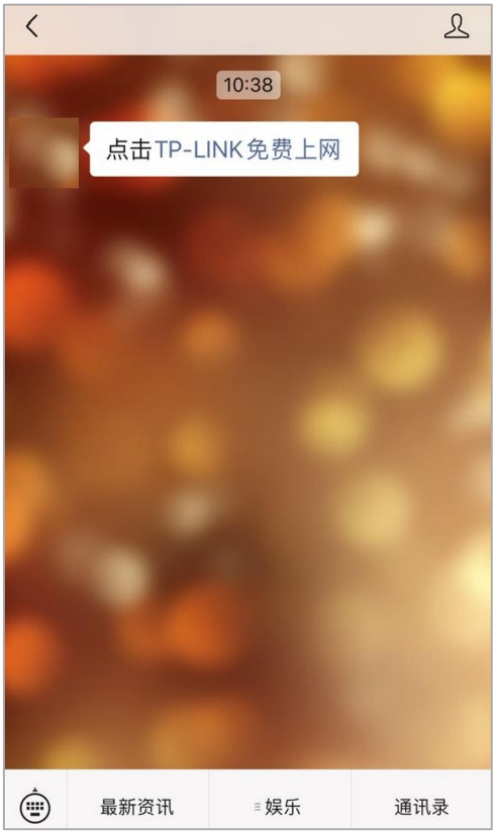
将认证链接“点击<ahref=”http://ac.tplogin.cn:8080/wechatv2/?auth_token=123456”>TP-LINK_免费上网”添加到微信后台关键字自动回复信息中：

填写完成点击<确定>即可。

5. 手机连接无线上网

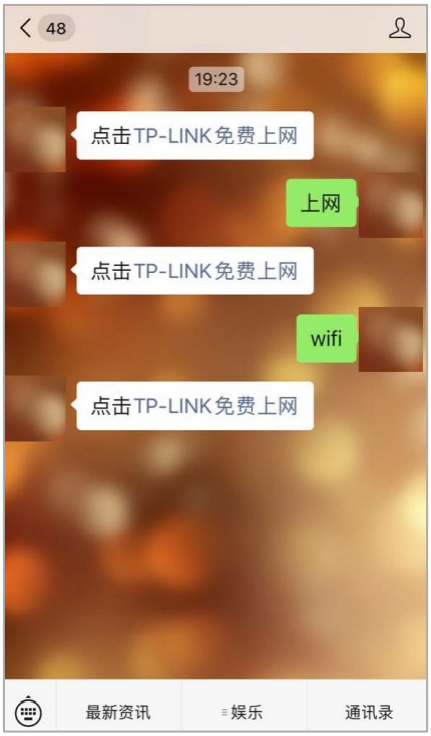
1) 无线终端（手机）连接无线网络后，跳出认证页面如下：

2) 使用手机关注对应的微信公众号，获取公众号返回的认证链接：



3) 点击<TP-LINK 免费上网>后，终端通过认证，就可以实现免费上网。

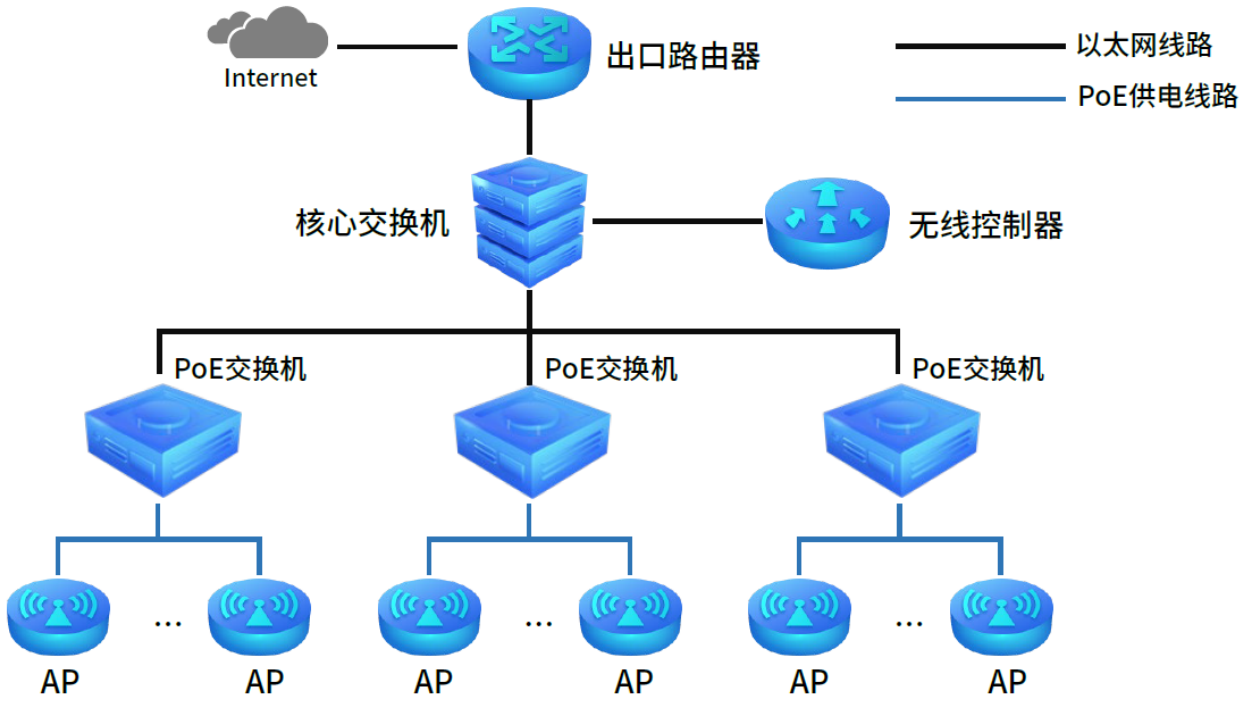
4) 下次接入该无线网络上网，请在该微信公众号中输入包含“上网”、“wifi”等相关词语，收到免费上网消息后，点击即可上网。具体相关词可以在微信公众号后台进行设置。



9.7 一键上网使用方法

9.7.1 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：



9.7.2 需求介绍

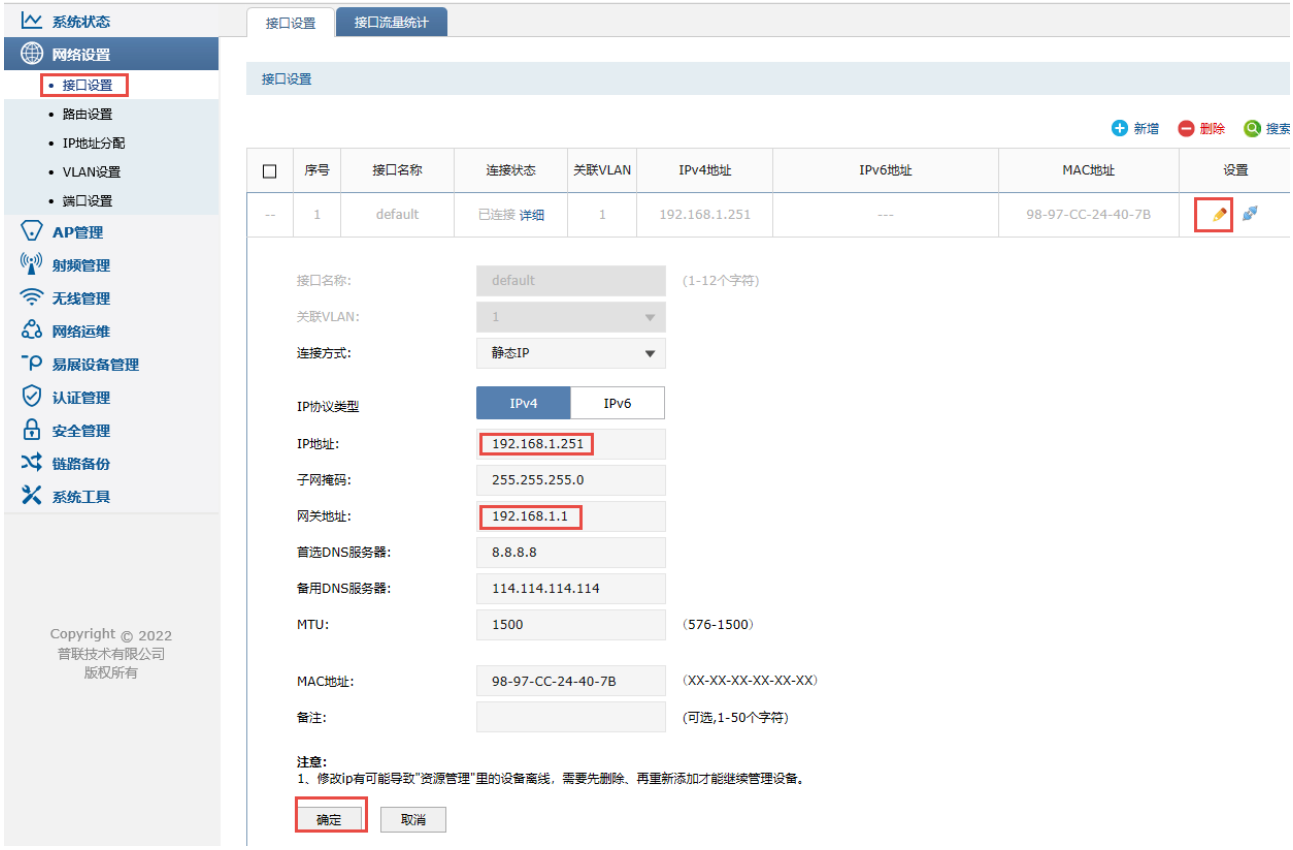
某商场需要实现无线覆盖，为顾客提供无线网络接入，有以下需求：

顾客在商场内都能连接 WIFI，且无需认证即可上网。

9.7.3 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. 配置跳转页面

1) 进入页面：认证管理 >> Portal 认证 >> 跳转页面，根据实际需求设置跳转页面标题、欢迎信息等：

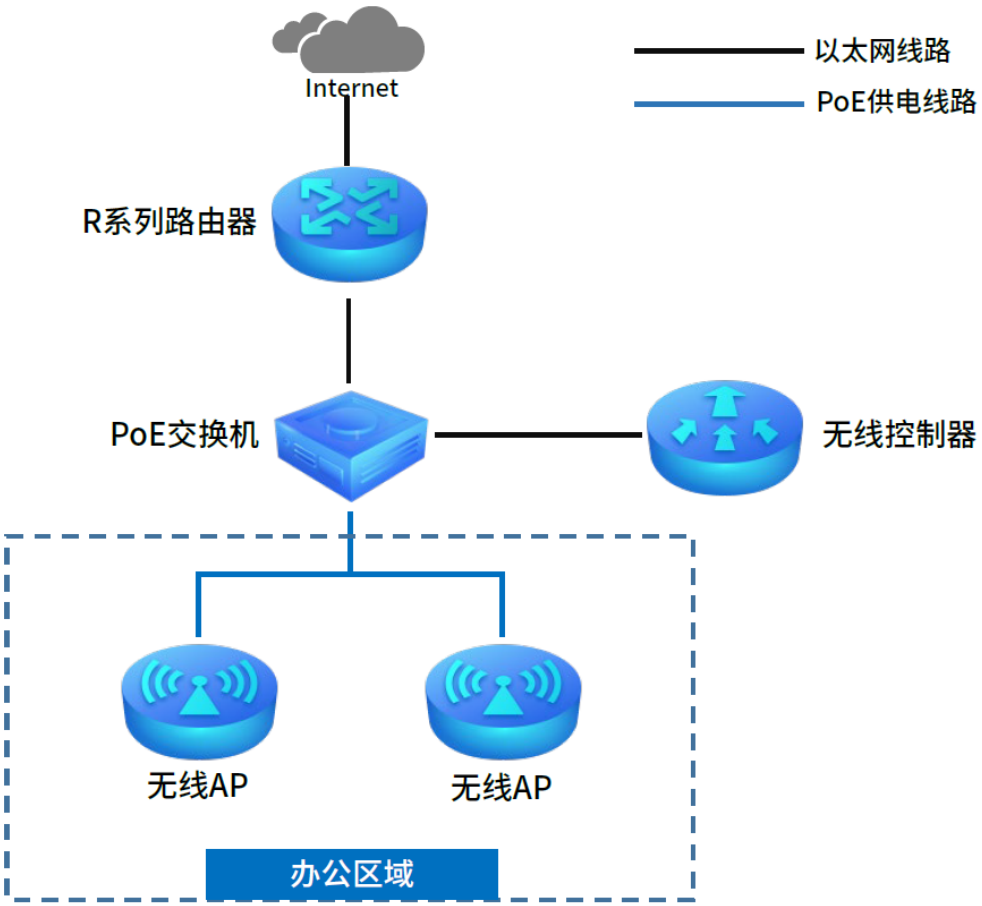
2) 进入页面：认证管理 >> Portal 认证 >> 组合认证， 点击<新增>，启用一键上网功能，如下图。

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：

9.8 免认证策略的使用方法

9.8.1 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：



9.8.2 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；

9.8.3 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。

回目录

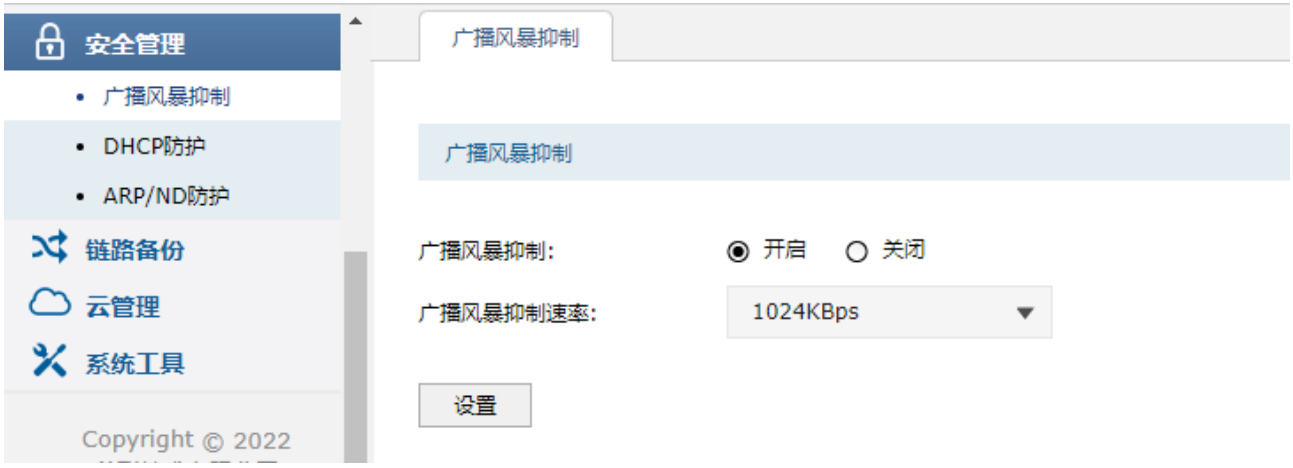
第10章 安全管理

10.1 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。

本页面可开启 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。



10.2 广播风暴抑制配置实例

10.2.1 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。

10.2.2 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。

10.3 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。

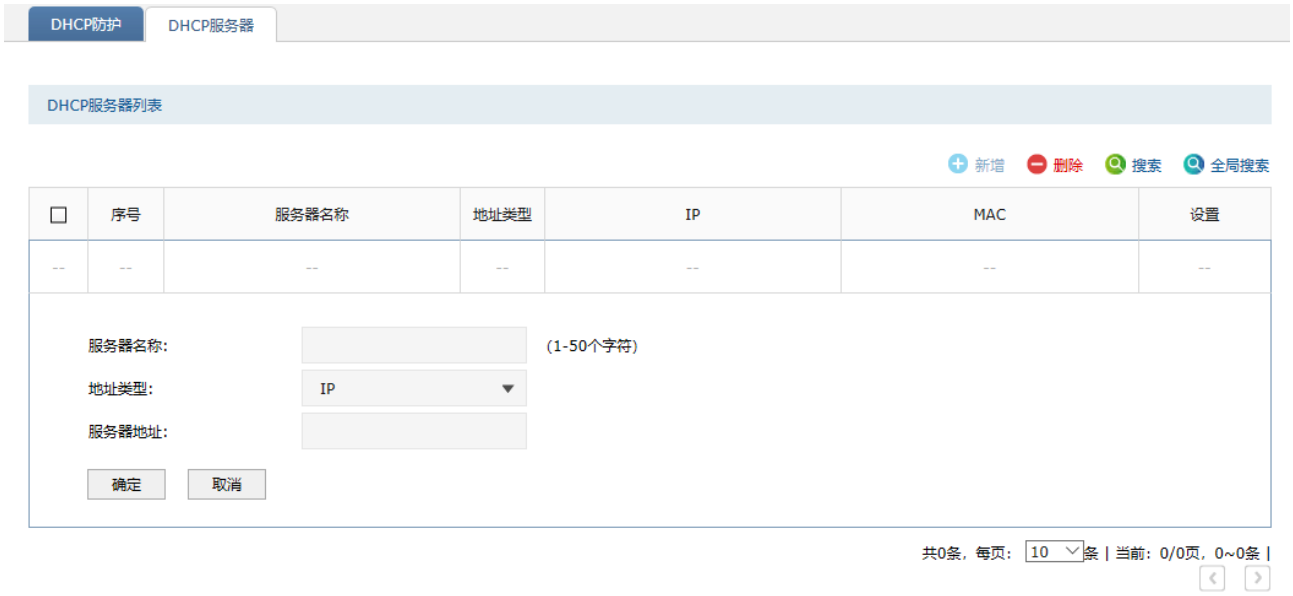
本页面可以查看已关联 AP 的 DHCP 防护设置，单独或批量修改每个 AP 绑定的 DHCP 防护条目。

进入页面：安全管理 >> DHCP 防护，查看已关联 AP 的 DHCP 防护设置，单独或批量绑定 AP 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。

10.4 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。

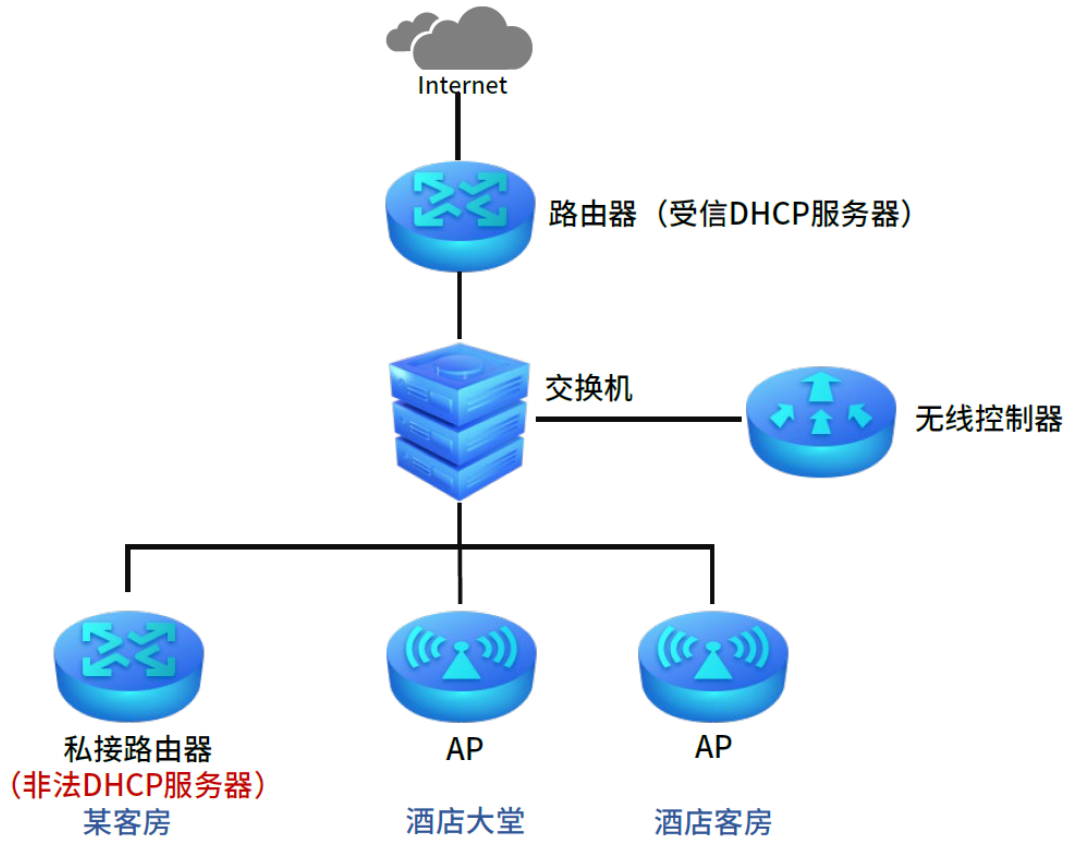


10.5 DHCP 防护配置实例

10.5.1 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。



10.5.2 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。

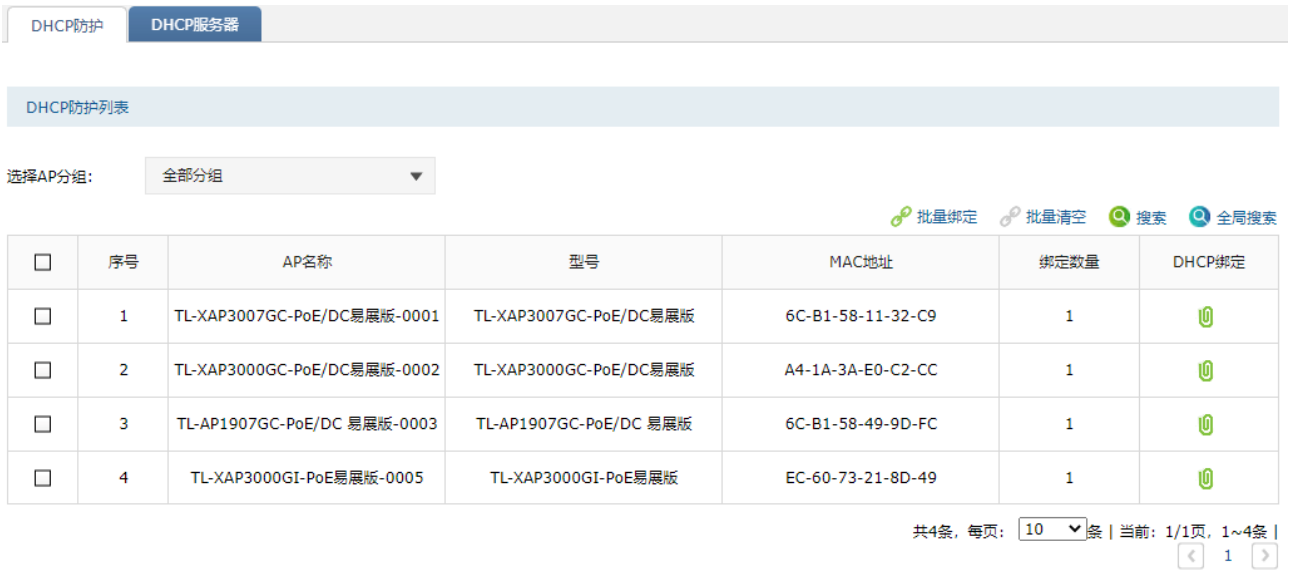
➢ 将 DHCP 服务器绑定到 AP

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

DHCP 绑定到 AP 后，DHCP 防护功能生效。设置完毕，DHCP 防护列表如下：



10.6 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。

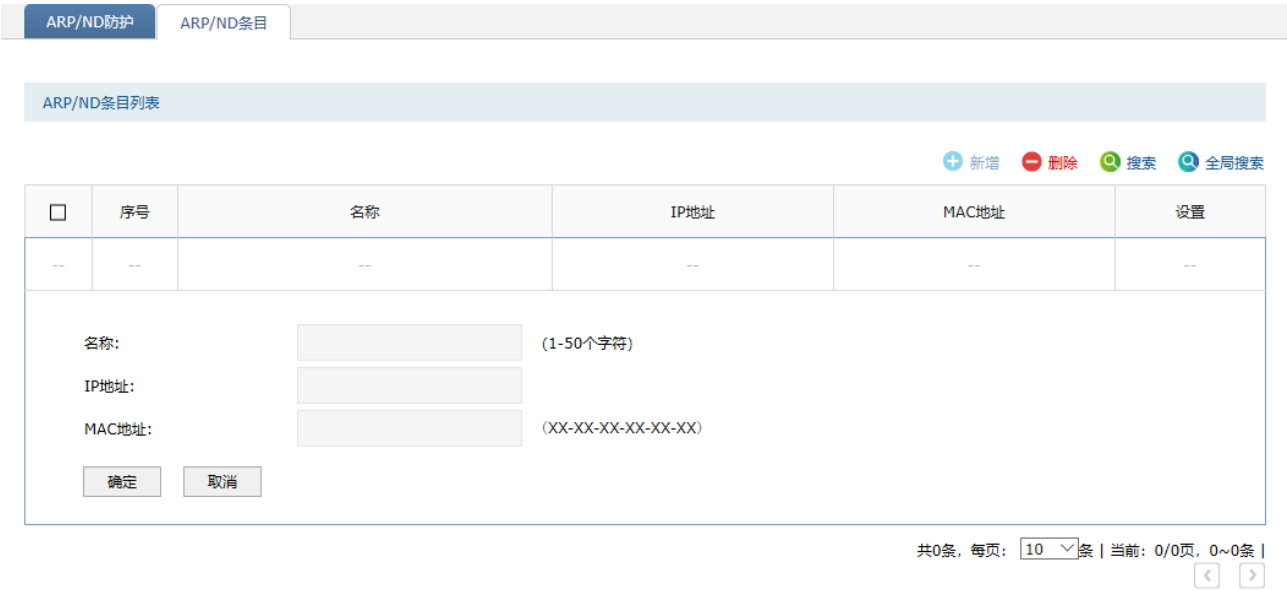
本页面可以查看已关联 AP 的 ARP/ND 防护设置，单独或批量修改每个 AP 绑定的 ARP/ND 防护条目。本页面可以查看已关联 AP 的 DHCP 防护设置，单独或批量修改每个 AP 绑定的 DHCP 防护条目。

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。

10.7 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。



10.8 ARP/ND 防护配置实例

10.8.1 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。

10.8.2 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。

至此，TP-LINK 无线控制器 ARP 防护绑定功能设置完成 。

回目录

第11章 链路备份

11.1 双链路备份

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。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。

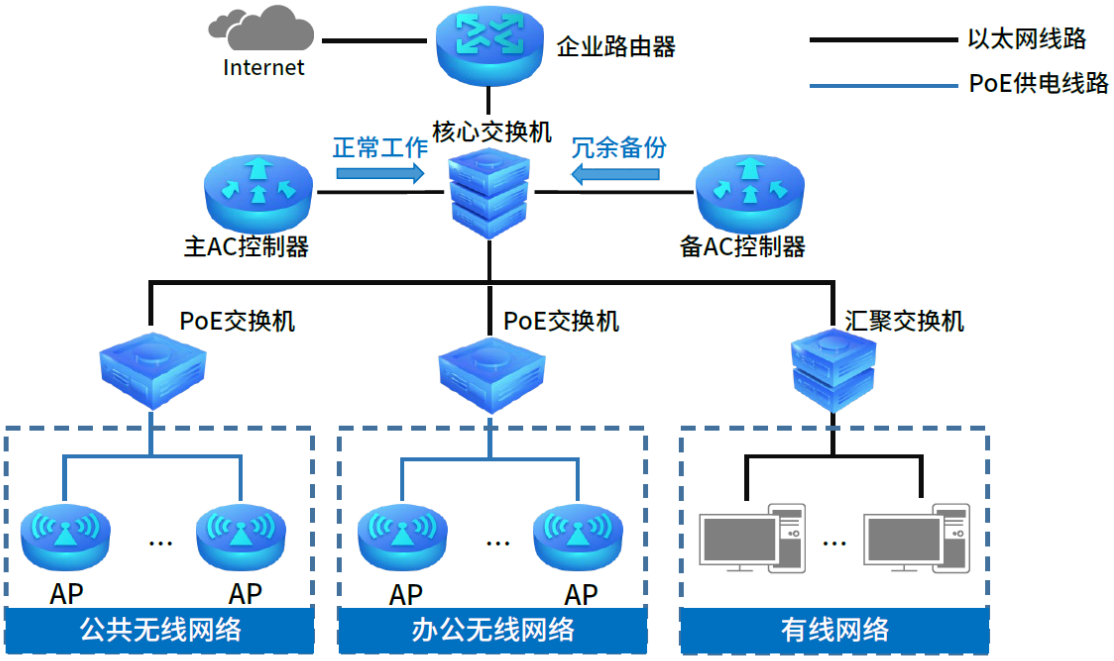
11.2 双链路备份配置实例

11.2.1 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。

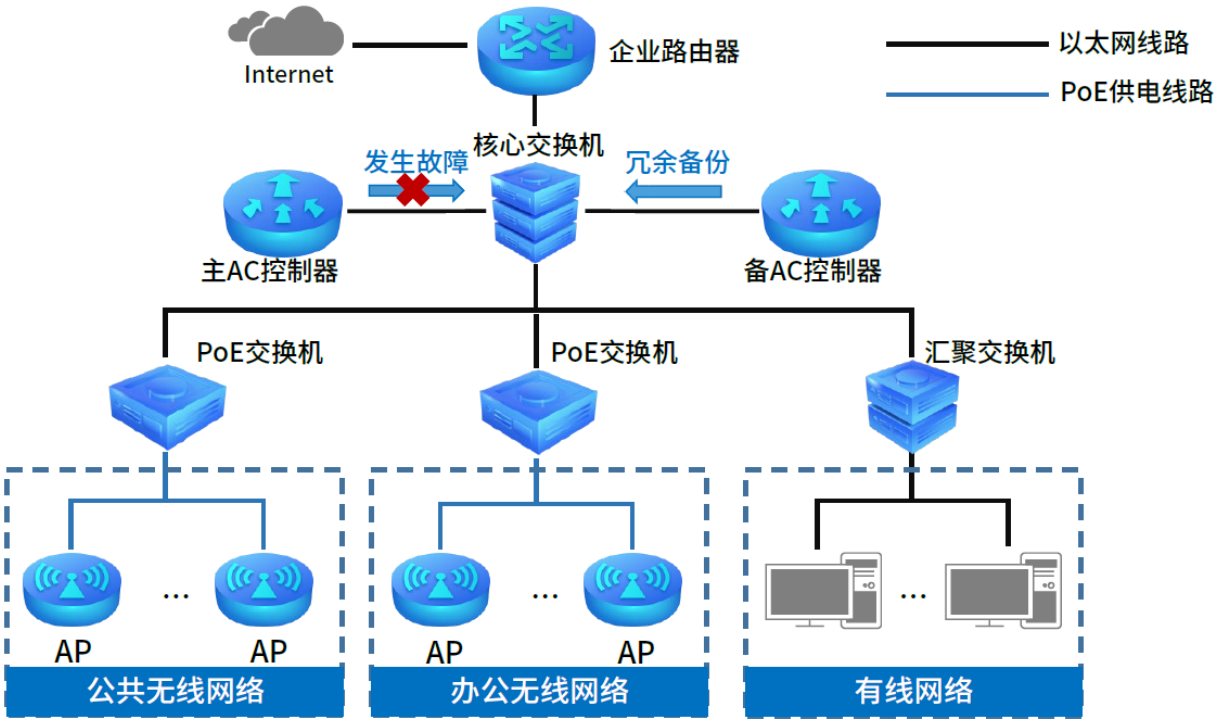
- AC 链路备份

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。

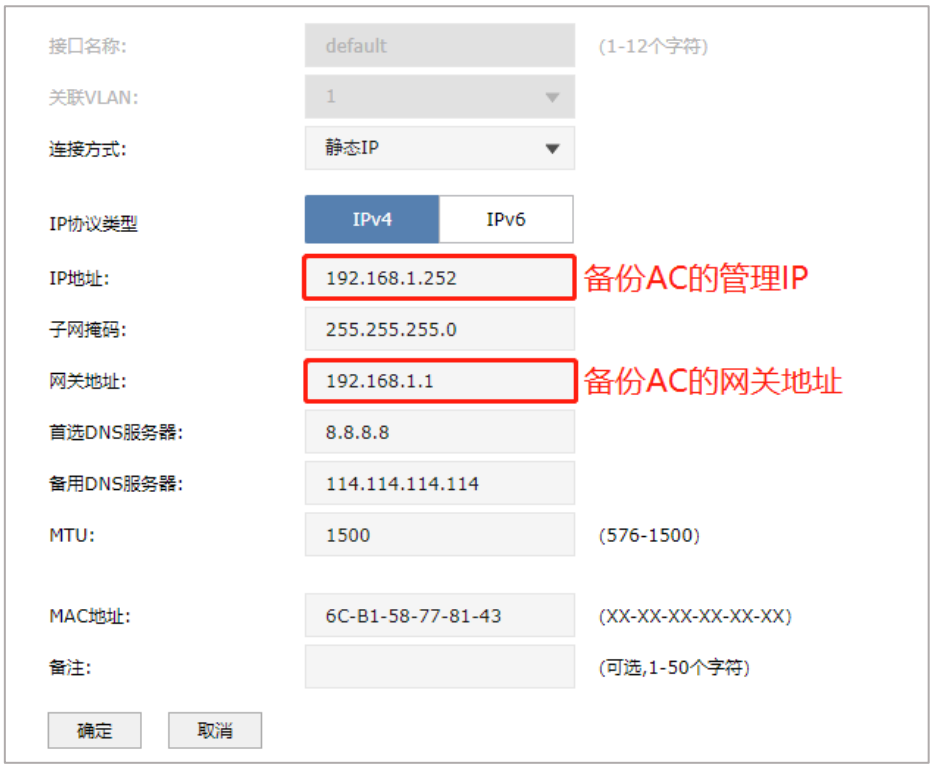


11.2.2 链路备份设置

➢ 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。

进入备用 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:

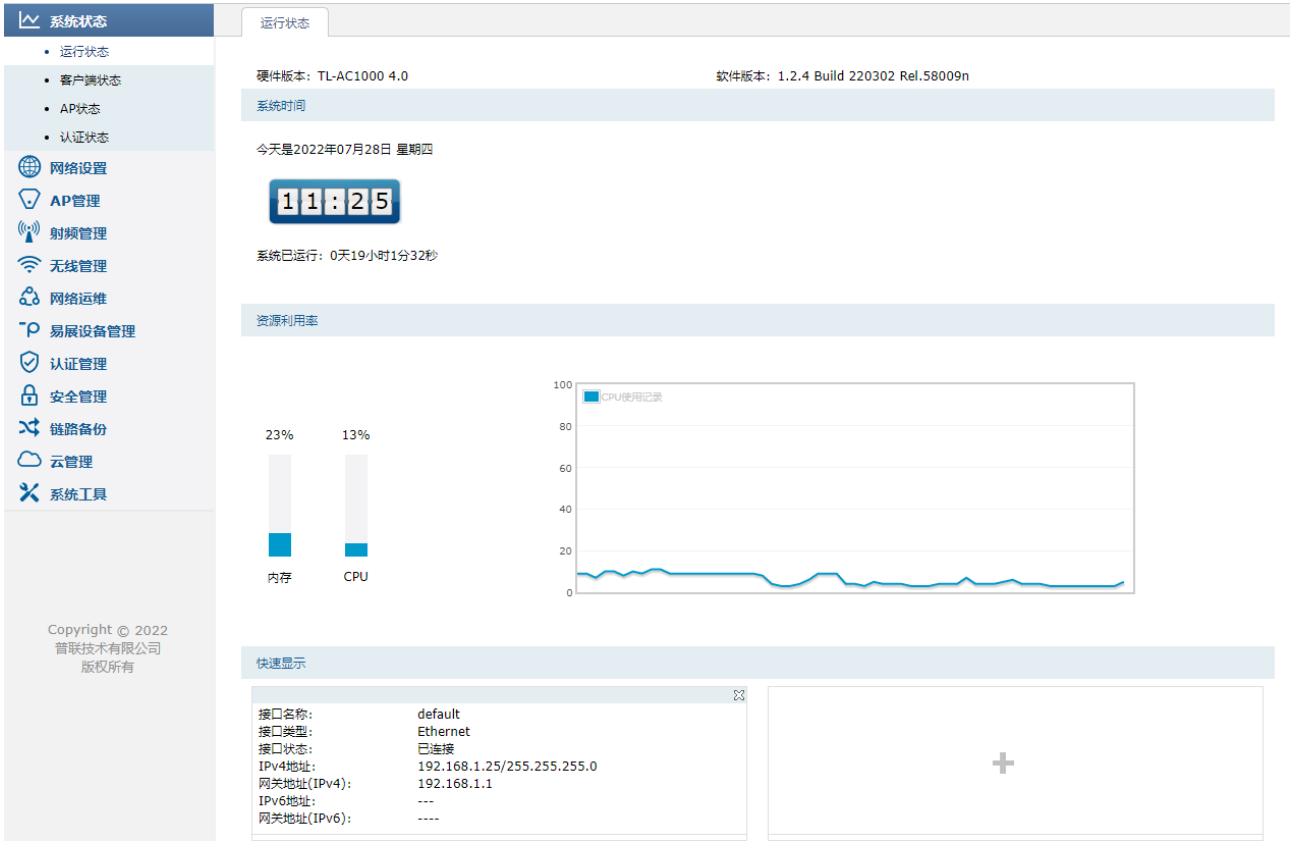
- 修改双链路配置将使所有处于主链路状态的 AP 重启，处于备链路状态下的 AP 断开与本机的连接。
- 当 AP 与 AC 重新建立连接之后，就会按照新的链路优先级重新选择主用 AC 和备份 AC。
- 当 AP 从主 AC 切换至备份 AC 时，已认证的无线客户端需要重新认证。
- 使用双链路备份时，用户需自行确保主、备 AC 之间配置的一致性

回目录

第12章 系统

12.1 系统状态

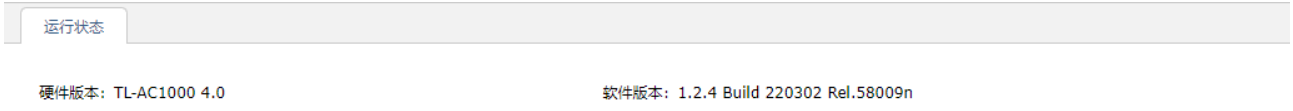
通过无线控制器的管理 IP 地址登录到 Web 管理页面后，可查看设备当前的运行状态、客户端状态、AP 状态和认证状态。



12.1.1 运行状态

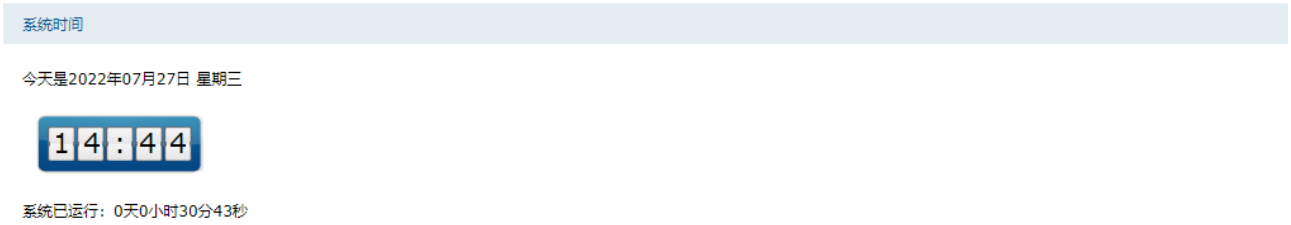
进入页面：系统状态 >> 运行状态，可查看以下信息：

- **软硬件版本**



- **系统时间**

本栏用于实时显示设备的系统时间和运行时间。

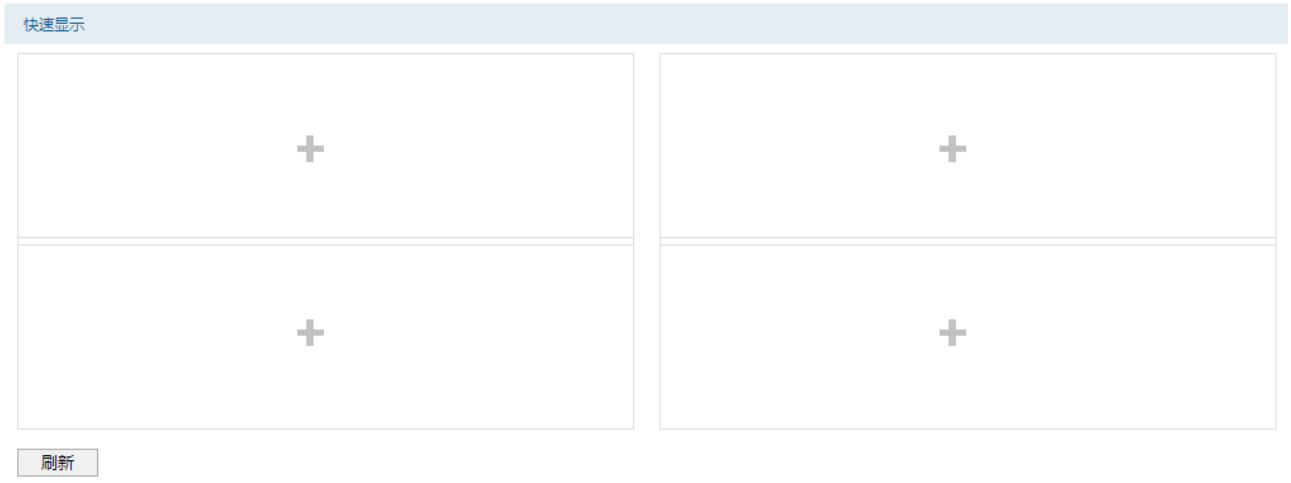


- **资源利用率**

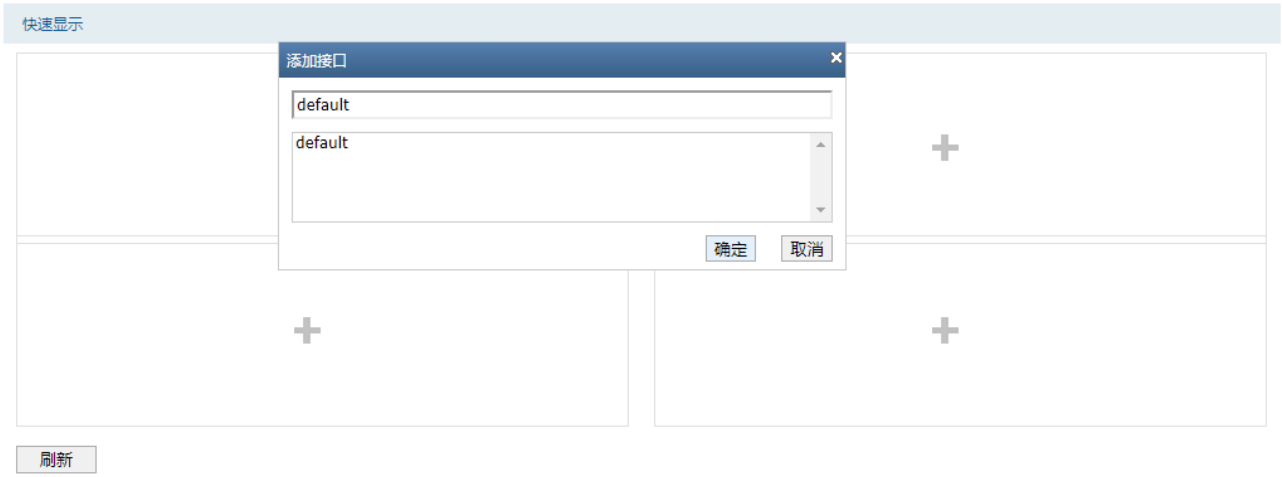
本栏用于实时显示设备的内存和 CPU 利用率。

- **快速显示**

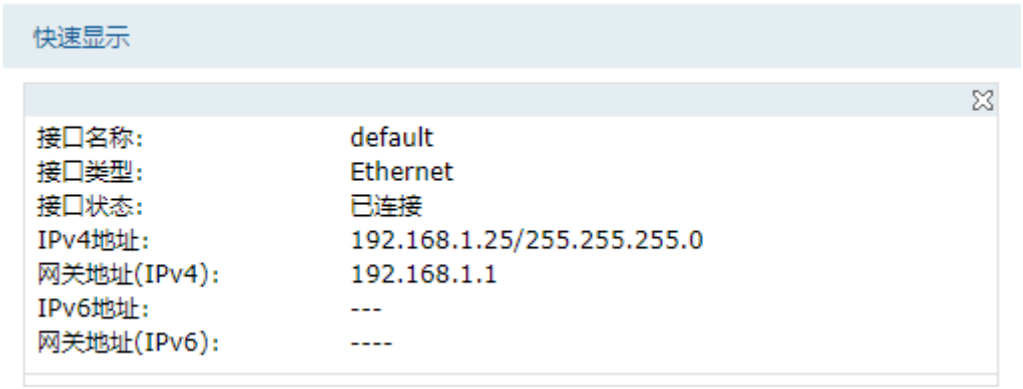
本栏用于显示接口信息。



选择一个窗口点击<+>，添加接口，点击<确定>。



添加完成后，该窗口中将显示接口信息，包括接口名称、类型、连接状态、IP 地址等。



12.1.2 客户端状态

进入页面：系统状态 >> 客户端状态，可根据分组查看并设置 AP 的客户端信息，包括 MAC 地址、AP 名称、射频单元、SSID，IPv4/IPv6 地址、VLAN ID、接入时间、信号强度等。

点击<🔗>或<断开连接>，可断开客户端连接；点击<备份>可将客户端信息.csv 文件下载到本地。

➢ **设置**

点击<✏>，可设置客户端名称。

➢ **搜索**

点击<全局搜索>，可基于列名和内容对客户端进行搜索。

点击<搜索>，可基于列名、内容对当前页进行搜索，可选“在结果中搜索”及“在所有条目中搜索”两种方式。

12.1.3 认证状态

进入页面：系统状态 >> 认证状态，可查看并编辑认证用户和无感知认证用户信息。

点击<全局搜索>，可基于列名和内容对列表进行搜索。

点击<搜索>，可基于列名、内容对当前页进行搜索，可选“在结果中搜索”及“在所有条目中搜索”两种方式。

- **认证用户列表**

点击<备份>，可备份所有认证用户条目至 ANSI 编码格式的 CSV 文件中。点击<断开连接>，将删除已认证用户条目，用户需要重新认证。

认证方式	用户登录所使用的认证方式。
SSID	当前登录用户所在的无线服务。
认证时间	用户登录时间。
认证剩余时间	用户认证过期的剩余时间。

- **无感知认证用户列表**

SSID	无感知认证用户认证时所属的无线服务。
MAC 地址	无感知认证用户认证时的 MAC 地址。
认证时间	无感知认证用户最后一次认证的时间。
断开连接	删除该无感知认证用户。

12.2 云管理

TP-LINK 无线控制器支持 TP-LINK 商用网络云平台和 TP-LINK 本地 NMS 管理平台管理。

TP-LINK 本地 NMS 管理平台是基于企业私有云管理架构的 TP-LINK 网络设备管理服务，可部署至企业本地物理服务器或虚拟机。

TP-LINK 商用网络云平台是基于公有云管理架构的 TP-LINK 网络设备云管理平台。

12.2.1 TP-LINK 本地 NMS 管理平台

进入页面：云管理 >> 基本配置，在“云类型”选择 TP-LINK 本地 NMS 管理平台，进行服务器及端口设置。

云平台绑定状态	显示当前设备是否已经绑定到本地 NMS 管理平台或 TP-LINK 商用网络云平台项目中。如未绑定，可登录本地 NMS 管理平台或 TP-LINK 商用网络云平台进行设备绑定。如云类型选择 TP-LINK 商用网络云平台，还可使用 TP-LINK 商云 APP 进行设备绑定。

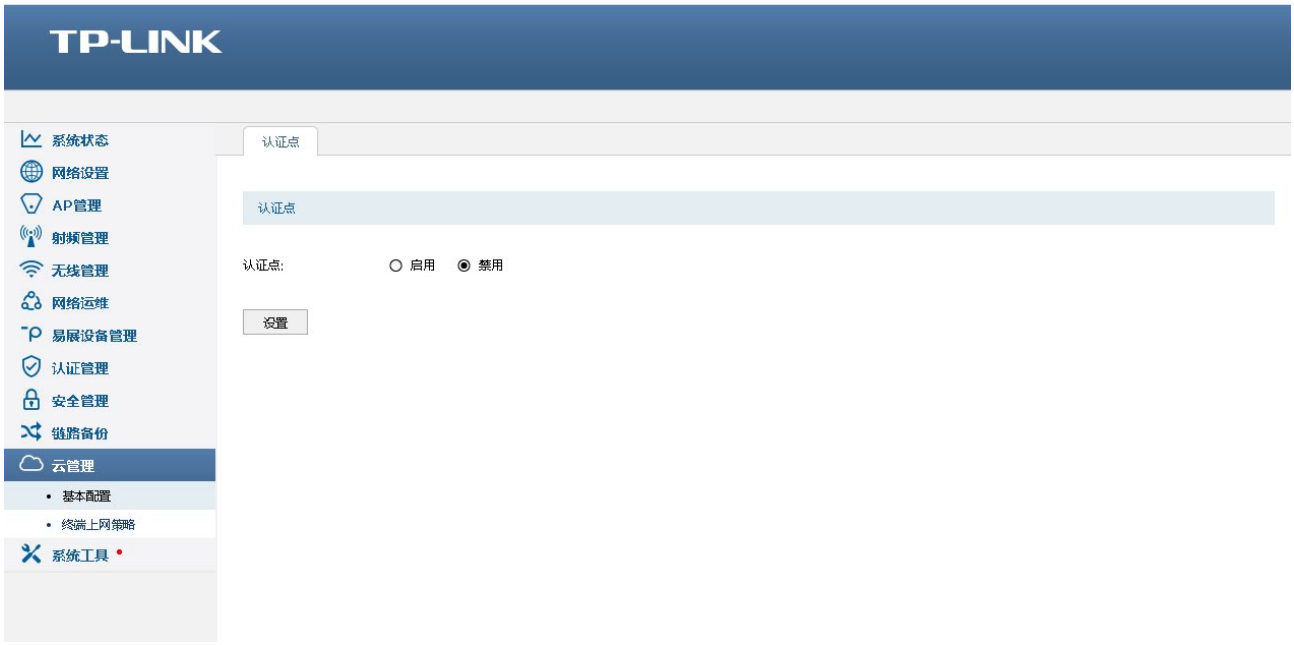
12.2.2 TP-LINK 商用网络云平台

进入页面：云管理 >> 基本设置，可将设备绑定到 TP-LINK 商用云平台。详情见 **2.2TP-LINK 商用网络云平台管理**。

12.2.3 终端上网策略

启用云管理功能后，可进入页面：云管理 >> 终端上网策略 >> 认证点，配置认证点。

开启认证点，并将设备绑定到 TP-LINK 本地 NMS 管理平台，终端上网策略的认证点功能将生效。



12.3 管理账号

12.3.1 管理账号

进入页面：系统工具 >> 管理账号 >> 管理账号，可修改管理账户用户名及密码。

12.3.2 系统管理设置

进入页面：系统工具 >> 管理账号 >> 系统管理设置，可进行服务端口和会话超时时间的管理。

Http 服务	Http 服务默认打开，当取消勾选该项时，将无法通过 Http 的方式对 WEB 进行管理。
Http 服务端口	用于 Web 管理界面的 Http 服务端口，默认为 80 端口。不能与其他的服务端口重复。
Https 服务端口	用于 Web 管理界面的 Https 服务端口，默认为 443 端口。不能与其他的服务端口重复。
Web 会话超时时间	如果在会话超时时间内都没有进行操作，系统将自动退出登录，以保证设备和网络的安全。
最大登录尝试次数	当连续尝试登陆失败达到该次数时，将会在一段时间内锁定设备不允许继续登录。
登录锁定时长	当连续登陆失败次数达到最大登录尝试次数后，将会在锁定时长期间无法进行登录。

12.4 设备管理

12.4.1 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。

12.4.2 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。

12.4.3 重启设备

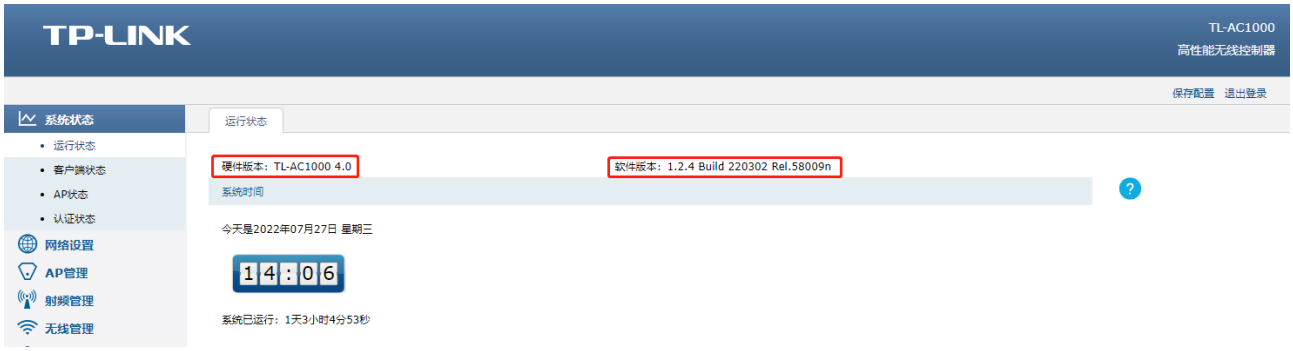
进入页面：系统工具 >> 设备管理 >>重启设备，点击<重启设备>，可对设备进行重启，如下图。

说明：

- 在重启设备过程中，请不要将设备断电！

12.4.4 软件升级

进入页面：系统状态 >> 运行状态，可查看当前设备硬件版本及软件版本。



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。

12.4.5 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。

12.5 诊断工具

12.5.1 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。

12.5.2 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！

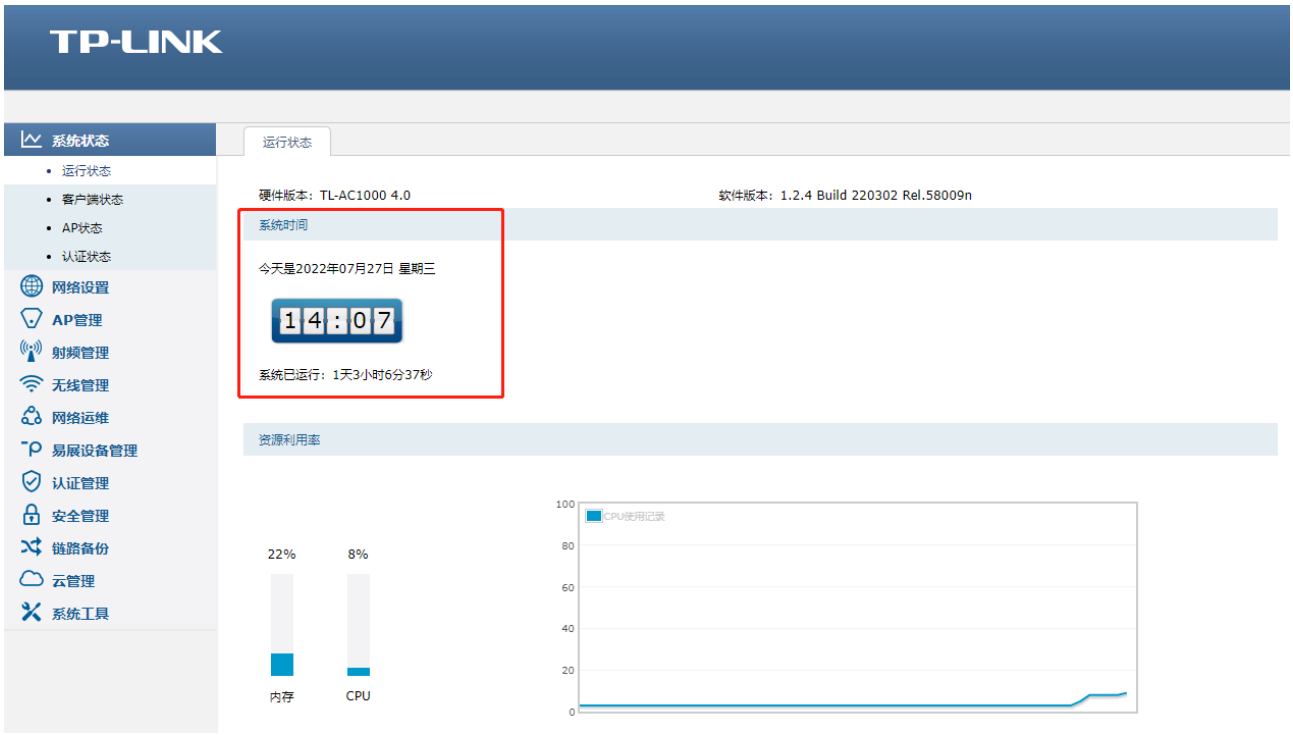
说明:

请在技术支持人员指导下使用故障诊断功能!

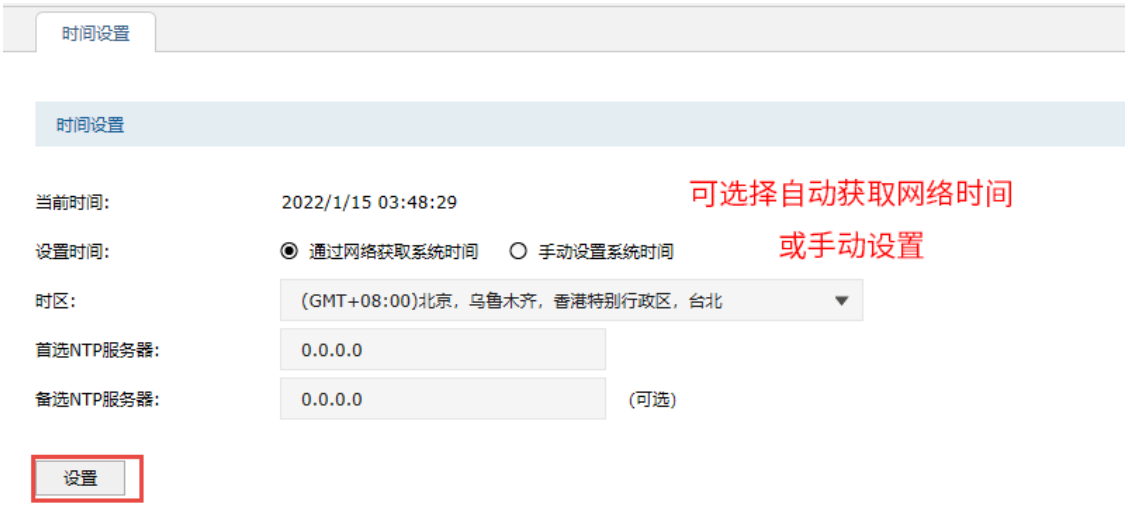
12.6 时间设置

12.6.1 系统时间设置

进入页面：系统状态 >> 运行状态，可查看实时显示设备的系统时间和运行时间。



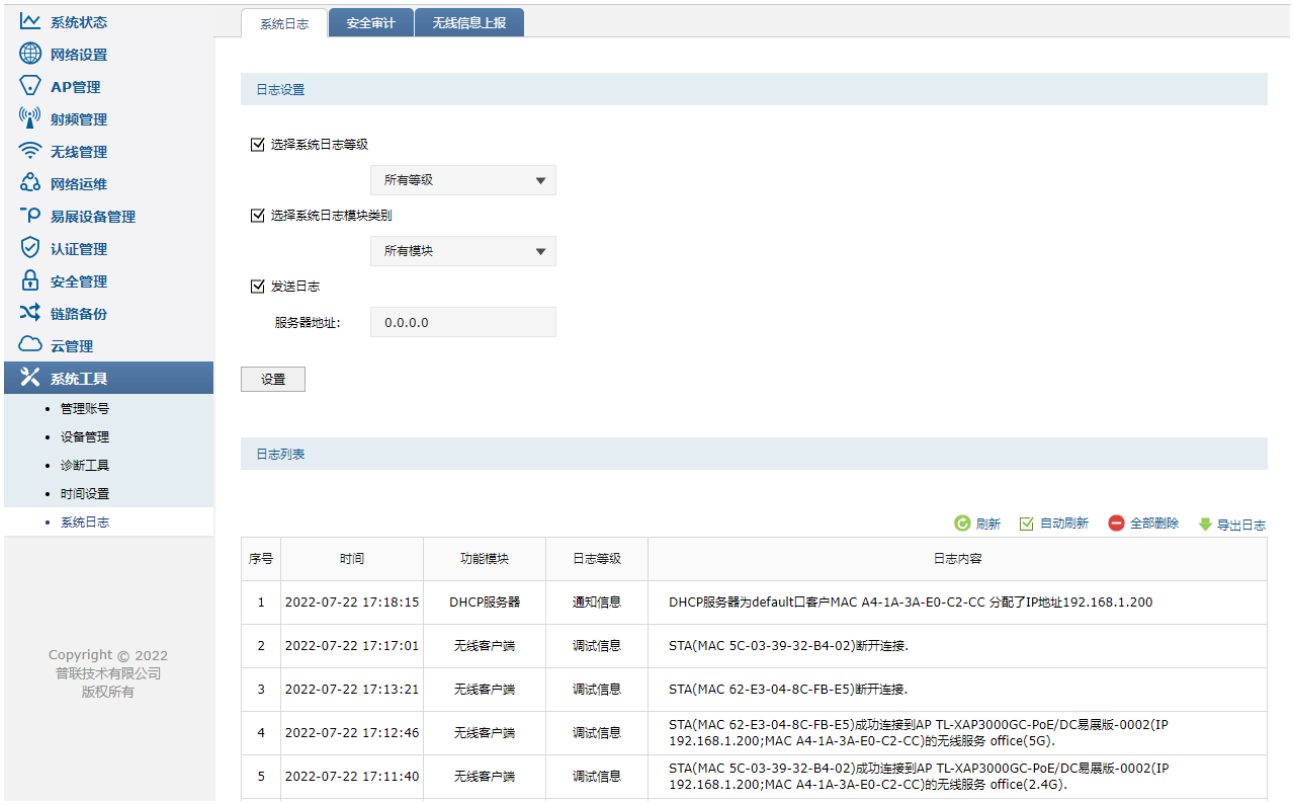
进入页面：系统工具 >> 时间设置，可查看和设置系统时间，如下图。



12.7 系统日志

12.7.1 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。



12.7.2 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。

12.7.3 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。

回目录