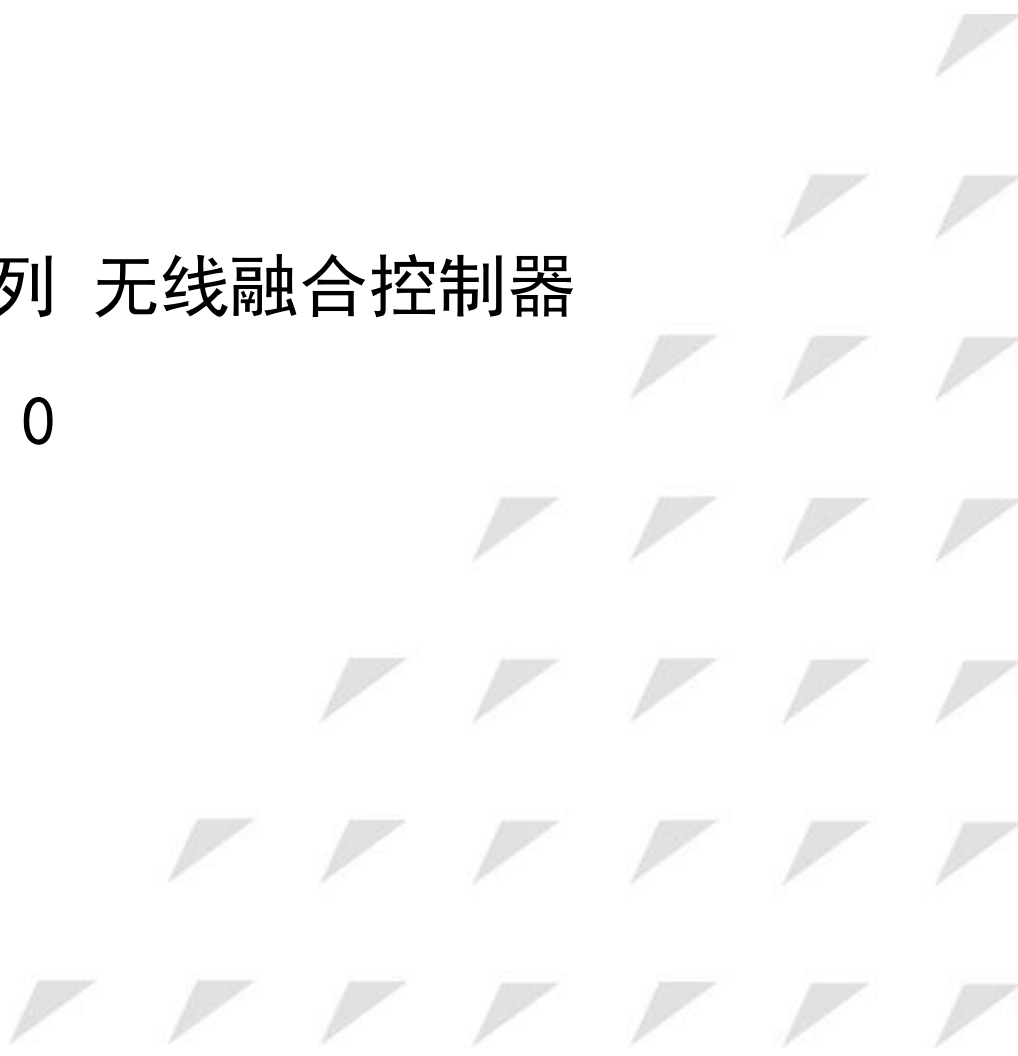


Inspur E 系列 无线融合控制器  
用户手册 V1.0



浪潮思科网络科技有限公司（以下简称“浪潮思科”）为客户提供全方位的技术支持和服务。直接向浪潮思科购买产品的用户，如果在使用过程中有任何问题，可与浪潮思科各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于浪潮思科产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：<http://www.inspur.com/>

技术支持热线：400-691-1766

技术支持邮箱：[inspur\\_network@inspur.com](mailto:inspur_network@inspur.com)

技术文档邮箱：[inspur\\_network@inspur.com](mailto:inspur_network@inspur.com)

客户投诉热线：400-691-1766

公司总部地址：北京市海淀区西北旺东路 10 号院（中关村软件园）东区 20 号

邮政编码：100094

---

## 声 明

**Copyright ©2022**

浪潮思科网络科技有限公司

版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

**inspur** 浪潮 是浪潮思科网络科技有限公司的注册商标。

对于本手册中出现的其它商标，由各自的所有人拥有。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 修订记录

序号	修改时间	责任人	版本	修改说明
1	2021-6-15	无线产品运营处	v1.0	AC&AP 第一版正式版本 1.061.48 用户手册

# 目 录

1	前言 .....	1
1.1	产品版本 .....	1
1.2	通用格式约定 .....	1
1.3	图形界面描述格式约定 .....	1
2	从这开始 .....	2
2.1	AC 系统概述.....	2
2.2	登陆 AC.....	2
2.2.1	登录 AC 的 Web 系统.....	3
2.2.2	登录 AC 命令行（AC XOS 系统） .....	5
2.3	登录注意事项 .....	6
2.3.1	使用 AC Web 系统的注意事项.....	6
2.3.2	使用 AC XOS 系统的注意事项.....	6
2.4	Web 界面介绍 .....	6
2.4.1	界面区域划分 .....	6
2.4.2	用户登录状态区 .....	7
2.4.3	主要菜单导航 .....	8
2.4.4	功能操作区 .....	39
2.4.5	日志和提示功能区 .....	39
2.5	配置命令介绍 .....	41
2.5.1	基础配置命令 .....	41
2.5.2	设备管理命令 .....	42
2.5.3	WLAN 基本业务配置命令.....	44
2.5.4	AP 管理配置命令 .....	46
2.5.5	主备 AC 配置同步（WLAN 部分） .....	47
2.5.1	常用的状态查询命令 .....	48
2.5.2	常用的排障命令 .....	48
2.6	开局向导 .....	50
2.6.1	无线网络规划 .....	50

2.6.2	配置 AP 上线 .....	51
2.6.3	SSID 配置 .....	52
3	配置示例 .....	53
3.1	WLAN 常用业务配置举例 .....	53
3.1.1	配置内部人员接入 WLAN 网络示例（802.1X 认证） .....	53
3.1.2	AC 主备模式配置 .....	73
3.1.3	AC 双链路聚合配置 .....	79

# 1 前言

本文档系统提供了 Inspur E 系列无线融合控制器 WEB 系统功能配置指导。

本文档适用于负责配置和管理 WLAN 的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

## 1.1 产品版本

与本文档相对应的产品版本如下所示。

产品名称	软件版本	适用产品型号
Inspur E 系列无线融合控制器	1.061.48 及 1.061.48 前的所有版本	IAC6020-E、IAC6050-E、IAC6070-E、IAC6080-E、IAC6090-E、IAC7000-E

## 1.2 通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级标题、二级标题、三级标题、。

## 1.3 图形界面描述格式约定

格式	描述
【 】	代表菜单或子菜单名称
>	代表 WEB 系统配置路径：如【系统对象】>【地址簿】，表示“系统对象”菜单下的“地址簿”菜单
<>	代表窗口中的选项或按钮名称

## 2 从这开始

### 2.1 AC 系统概述

为了方便用户对无线融合控制器的维护和使用，无线融合控制器内置一个 Web 服务器，与无线融合控制器相连的终端（以下均以 PC 为例）可以通过 Web 浏览器访问。同时也支持通过 SSH 及串口方式本地连接进行调试和维护。

串口方式连接系统需 PC 与 AC 进行本地串口直连；

Web 和 SSH 方式连接系统的运行环境如下图所示：



### 2.2 登陆 AC

使用有线连接的 Web 或 SSH 方式登录设备前，需完成以下任务：

- AC 设备的接入端口已配置 IP 地址(有默认 IP 即可)。
- PC 终端和 AC 设备网络互通。
- 设备正常运行，HTTP 服务和 HTTPS 服务已正确配置。
- PC 终端已安装浏览器软件或已安装 ssh 连接的客户端工具。

说明：

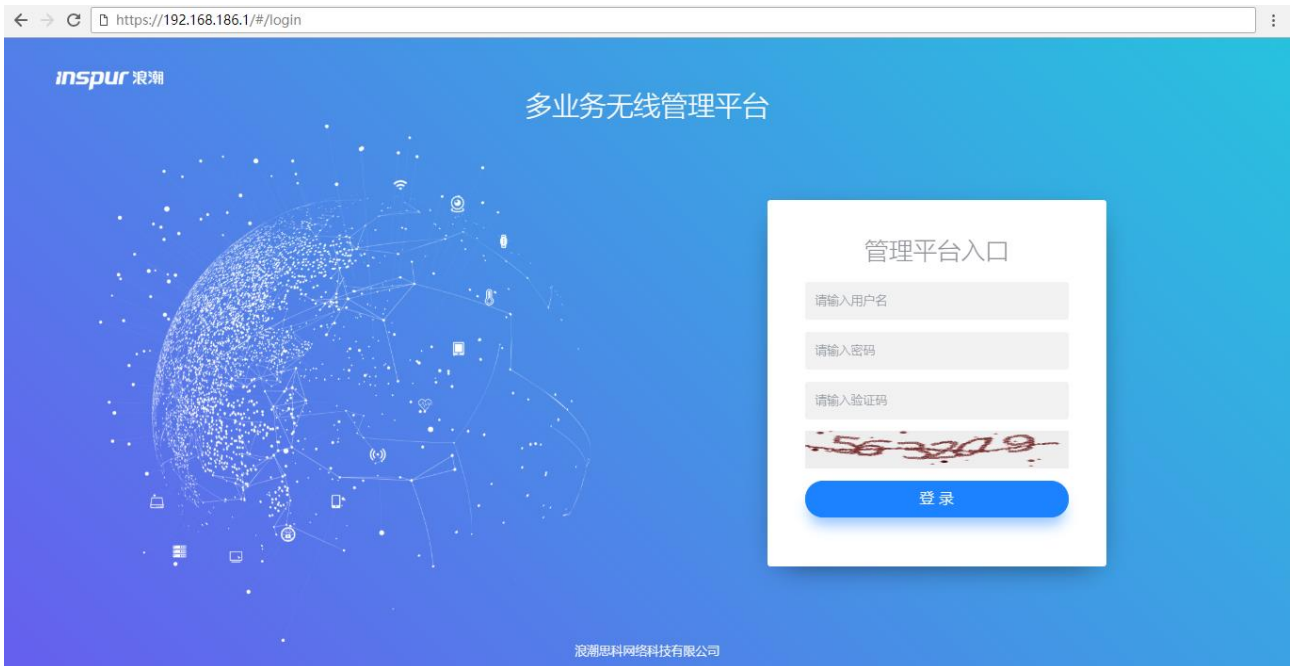
- IAC6020-E、IAC6050-E、IAC6070-E、IAC6080-E、IAC6090-E、IAC7000-E 出厂时在接口“**interface vlan1.1**”（VLAN 1 的接口地址）配置了 IP 地址 192.168.186.1，在所有型号 AC 的物理端口 eth2 及以后的所有电口中缺省已加入 VLAN 1，并默认开启了 DHCP 服务，如 PC 直连时无法获取 IP，则 PC 端需手动配置 192.168.186.0 段的 IP，与 AC 不冲突即可。
- AC 在出厂时已经配置了 SSH 服务，可通过 Shell 工具 SSH 登录至 AC 的命令行。
- 设备在出厂时已经配置了 HTTP 服务和 HTTPS 服务，HTTP 缺省服务端口号为 80，HTTPS 缺省服务端口号为 443。
- 缺省的 Web 和命令行（AC XOS）登录账号与密码为 admin/inspur123。

Web 系统的运行环境如下图所示，用户可以使用 PC 通过 Web +XOS 命令行相结合的方式对设备进行管理和配置。



## 2.2.1 登录 AC 的 Web 系统

1、PC 终端打开浏览器软件（以 Google Chrome 为例），在地址栏中输入“http://192.168.186.1”或“https://192.168.186.1”（192.168.186.1 为默认情况下的示例，如有改动，请以实际配置的接入端口 IP 地址为准），按下回车键，显示 Web 系统的登录页面。（说明：通过 HTTP 方式登录都会强制跳转到 HTTPS 的登录页面。）如下图所示：



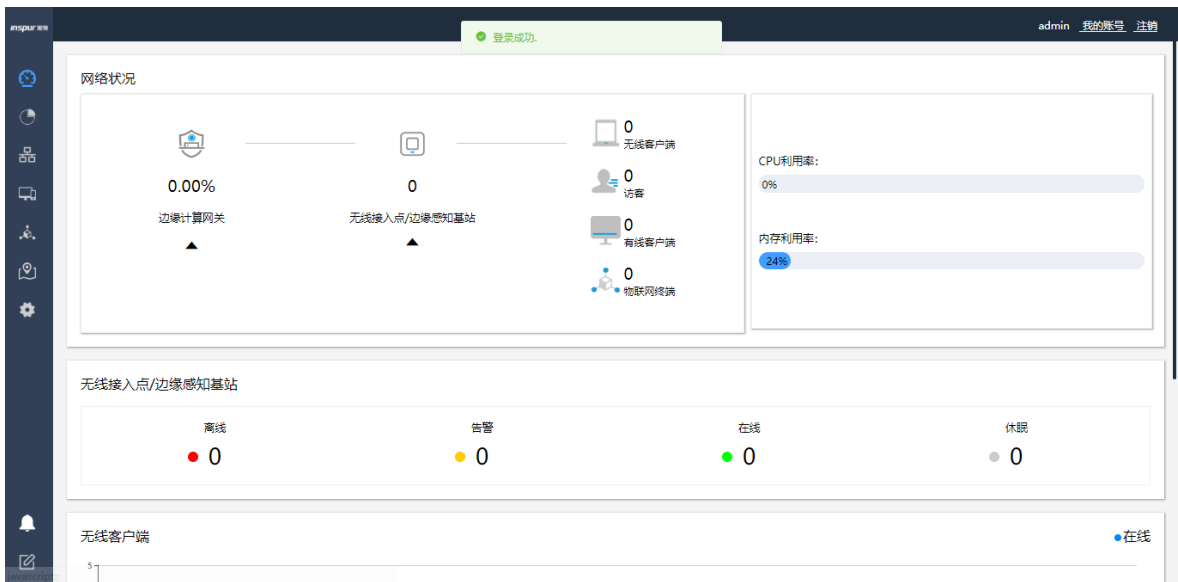
2、输入登录信息。

- a) 输入登用户名和密码（admin/inspur123），以及动态验证码。
- b) 单击“登录”，进入操作页面。
- c) 首次登录 Web 系统时，为确保 Web 系统安全性，可进行密码修改，再重新登录。
- d) 登录失败时，会提示：“用户名或密码无效”或“验证码错误”，表示输入的用户名或密码或验证码不正确。需核实用户名和密码或刷新验证码然后重新输入。
- e) 登录系统过程截图如下所示：

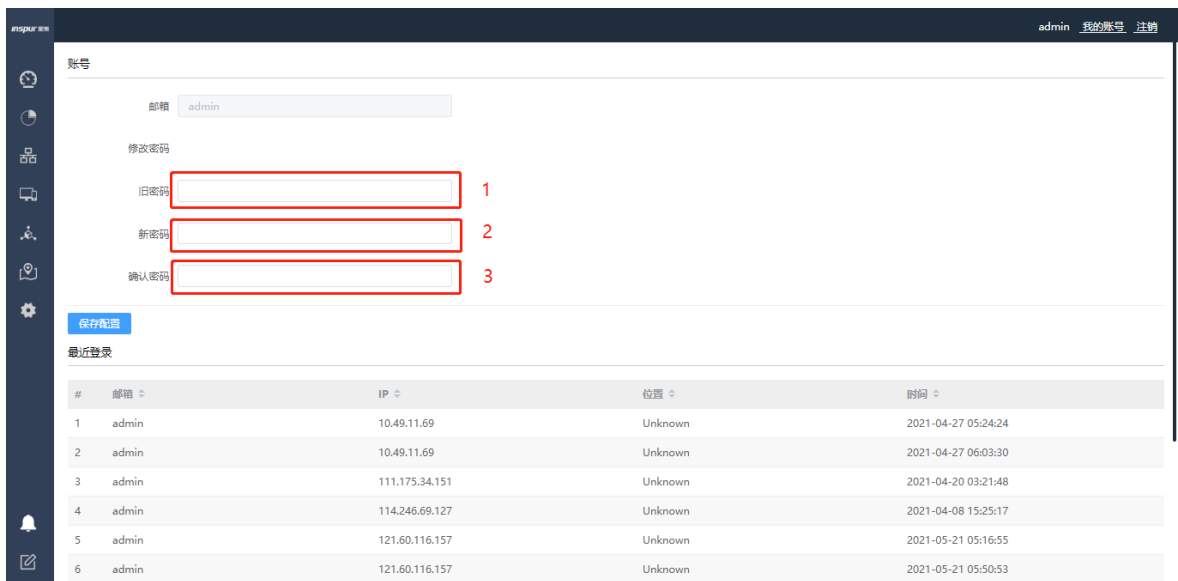




输入登录信息截图



成功登录首页截图



修改账户密码页面截图（成功登录首页→点击右上角<我的账号>按钮）

- 退出当前登录，单击页面右上角的“注销”，重新返回到登录页面。
- 用户登录成功后，在固定时间内未进行任何操作（缺省超时时间为 10 分钟），系统自动注销当前登录，系统重新返回到登录页面。

## 2.2.2 登录 AC 命令行（AC XOS 系统）

### SSH 登录 AC

- PC 终端打开支持 SSH 登录的工具软件（这里以 Windows power shell 为例，用户可根据自行习惯进行选择），在 shell 终端输入“ssh admin@192.168.186.1”（192.168.186.1 为默认情况下的示例，如有改动，请以实际配置的接入端口 IP 地址为准），按下回车键，提示输入 admin 账户的密码 inspur123，回车后登录入 AC；登录过程如下所示：

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell https://aka.ms/pscore6

PS C:\Users\liangbsh> ssh admin@192.168.186.1
admin@192.168.186.1's password:
*****
*      Copyright(c) 2015-2020 Inspur Group Co., Ltd. All rights reserved.      *
*      Without the owner's prior written consent,                               *
*      no decompiling or reverse-engineering shall be allowed.                 *
*****

XOS>
```

- AC 命令行下，可根据需要查询不同的命令来查看设备各类状态信息，修改相应配置。
- 用户登录成功后，在固定时间内未进行任何操作（缺省超时时间为 5 分钟），系统自动注销当前登录。需重新进入命令行系统。

### 串口登录 AC

- 打开 PC 上的终端连接工具，例如 SecureCRT，选择对应的 com 口（串口），参数设置如下：



波特率：115200，数据位：8，奇偶校验：None，停止位：1，流控：不勾选

2、PC 通过串口线与 AC 前面板 console 口连接后，可看到欢迎信息，如下：

```
login[15310]: root login on 'ttys0'

*****
*          Copyright(c) 2015-2020 Inspur Group Co., Ltd. All rights reserved.          *
*          without the owner's prior written consent,                                  *
*          no decompiling or reverse-engineering shall be allowed.                    *
*****

Please press ENTER
XOS>█
```

按照提示按 enter 键后，即可进入系统。

## 2.3 登录注意事项

### 2.3.1 使用 AC Web 系统的注意事项

登录 Web 系统建议操作系统为 Windows7.0、Windows10.0。Web 系统可适配市面主流浏览器，推荐使用 Chrome 64.0 以上版本。

### 2.3.2 使用 AC XOS 系统的注意事项

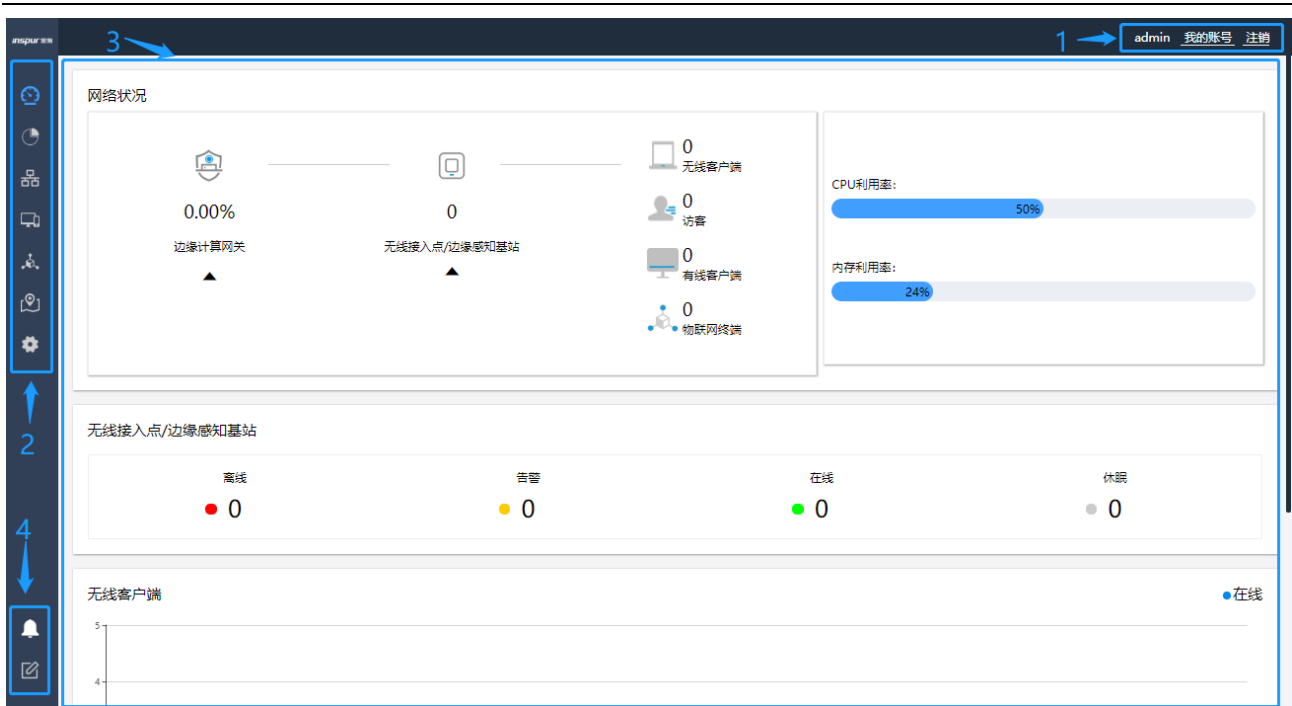
在 Web 系统进行相应功能配置时，命令行中需确保已退出 configure terminal 模式，以保证 Web 配置的下发。

## 2.4 Web 界面介绍

介绍 Web 界面的主要构成部分与相应的菜单功能。

### 2.4.1 界面区域划分

Web 界面布局，主要包含以下几个区域，如下所示。

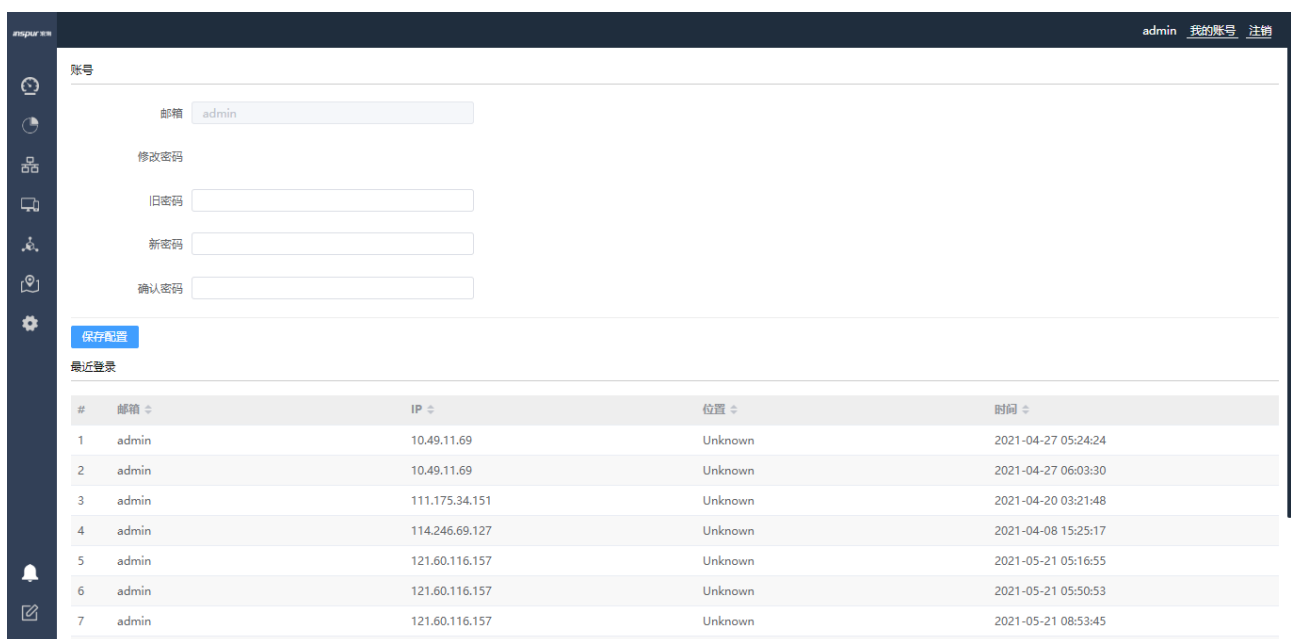


界面区域表:

区域	名称	说明
1	用户登录状态区	用户点击<我的账号>, 可快速进行当前登录账号信息修改、账号登录状态查看, 点注销可退出登录状态。
2	主要菜单导航	以导航树的模式显示各页签下的具体功能分类。 一级菜单导航位于界面左外侧, 二级菜单导航位于界面左内侧。
3	功能操作区	用户可在此区域进行具体的功能配置, 或者查看功能状态。
4	日志和提示功能区	点日志可查看事件、登录、修改日志, 点提示可显示 Web 系统的版本号

## 2.4.2 用户登录状态区

1、点击右上角<我的账号>按钮, 可查看的信息如下所示:



功能描述：可修改当前账号密码，可查看当前账号登录日志；

2、点击【注销】可返回登录页面，如下所示：

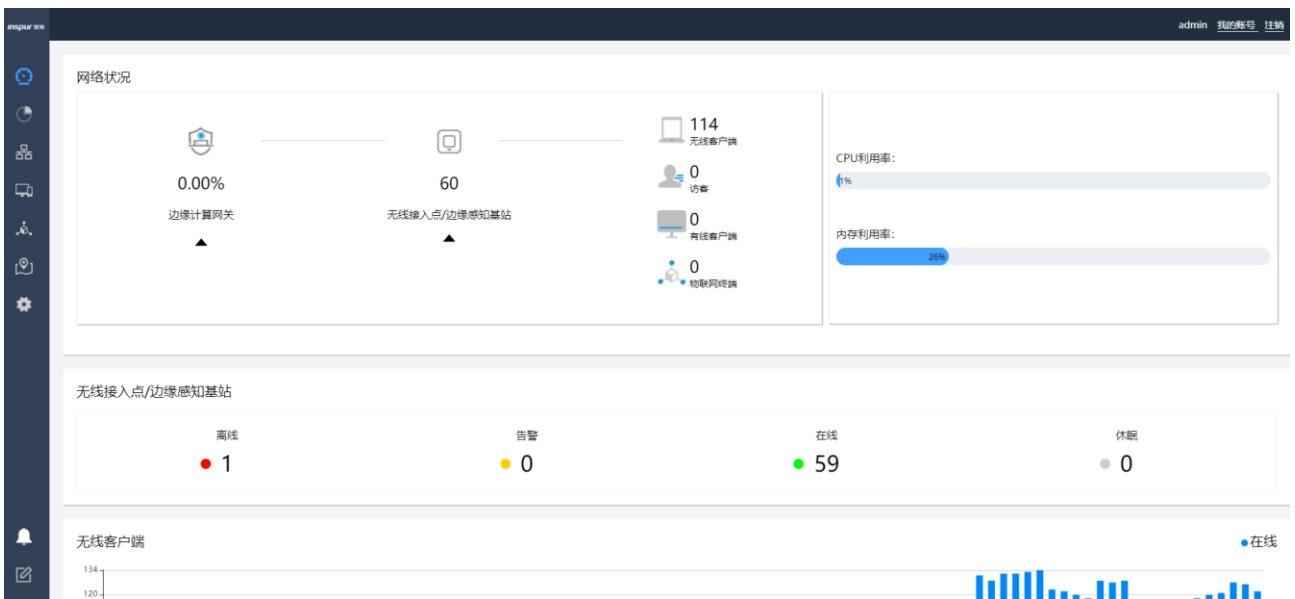
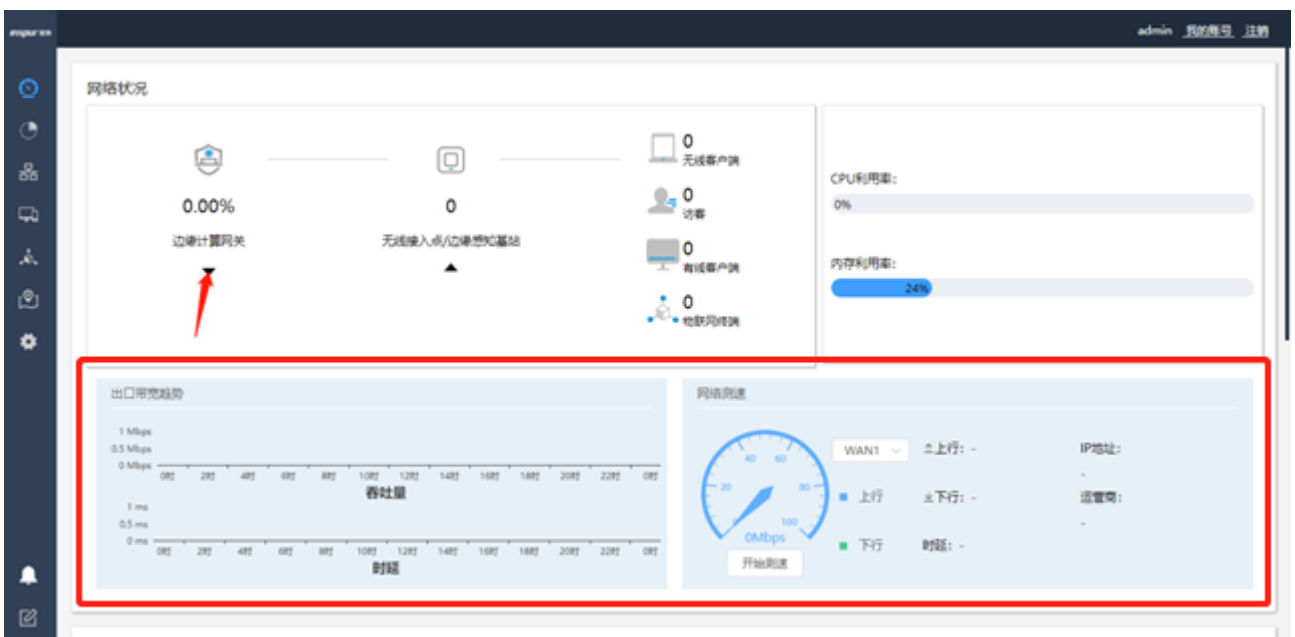
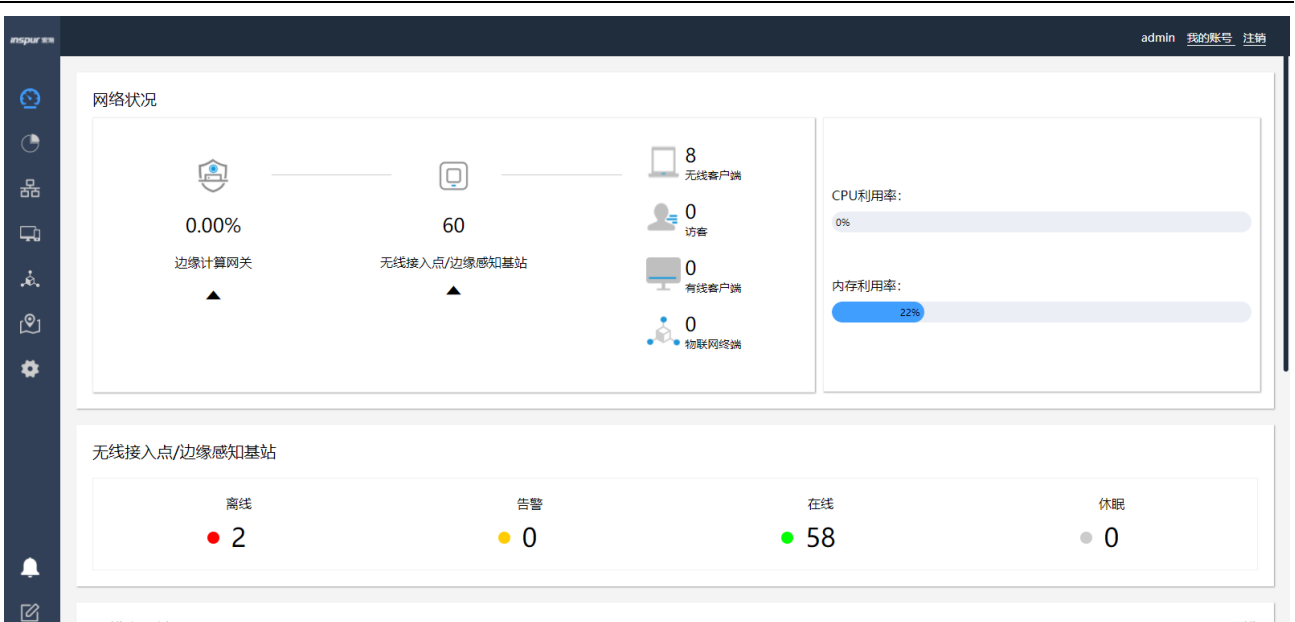


注销后系统将重新返回到用户登录页面。

## 2.4.3 主要菜单导航

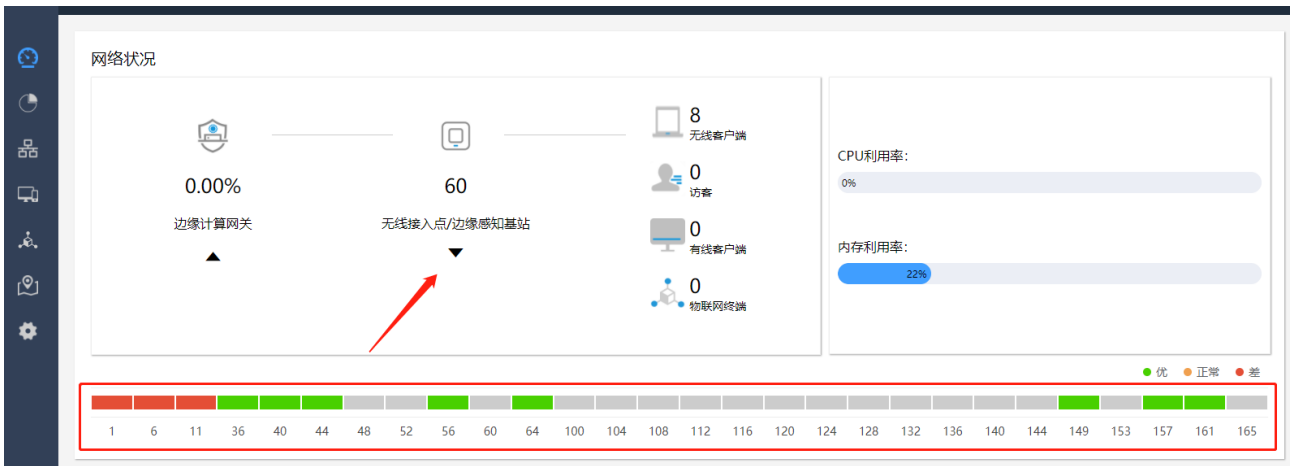
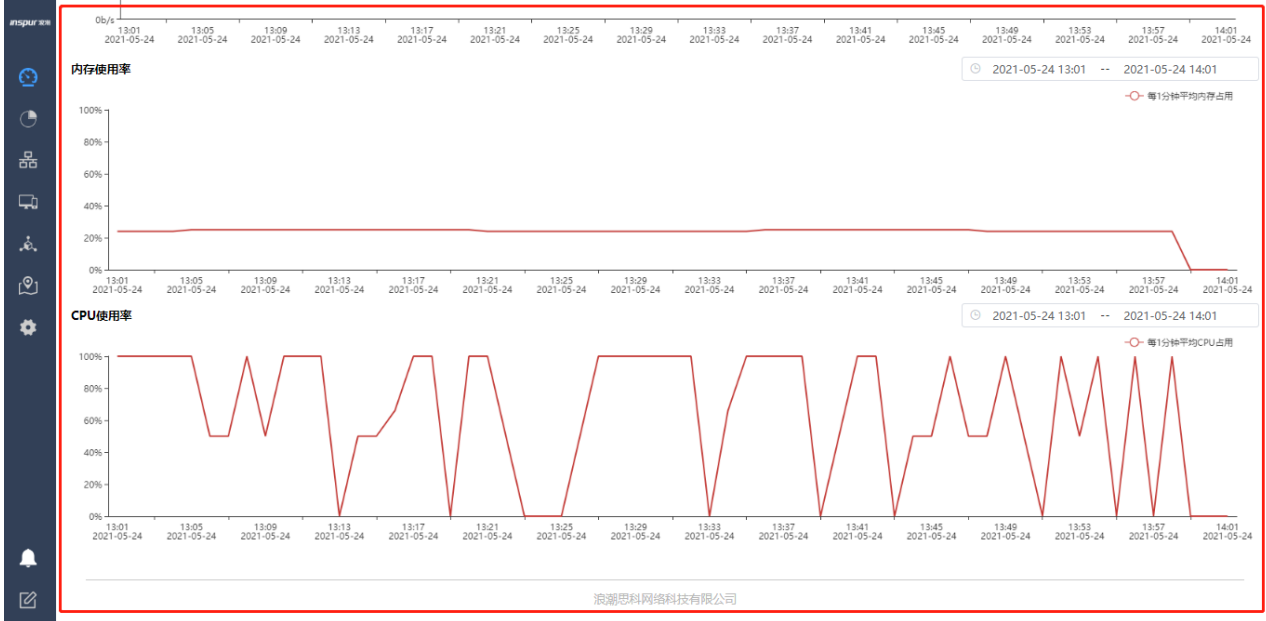
### 2.4.3.1 概览菜单

用户成功登录后的系统首页为【概览】菜单，如下图所示：



通过单击上图选框可进入边缘计算网关详情页，如下三张图所示：





功能描述：通过【概览】菜单可统览系统当前整体状态。包括实时网络流量，CPU、内存利用率，无线接入点/边缘感知基站的状态统计，无线客户端不同时刻在线情况的统计等；

### 2.4.3.2 统计菜单

点击【统计】菜单，如下图所示：



inspur 浪潮
admin 我的账号 注销

无线统计

统计

无线用户 (基于SSID)




- Others
- Unconfigured SSID1
- Unconfigured SSID2
- Unconfigured SSID3

无线用户 (基于射频单元)

- 2.4 GHz
- 5 GHz

无线接入点

- 在线
- 离线
- 休眠
- 警告

无线接入点使用排行 (Top 5)

基于客户端数


无线客户端使用排行 (Top 5)




基于流量

无线接入点流量统计

请选择 2021-05-21 18:14 TO 2021-05-21 19:14

每1分钟平均流量



无线接入点使用排行 (Top 5)

基于客户端数

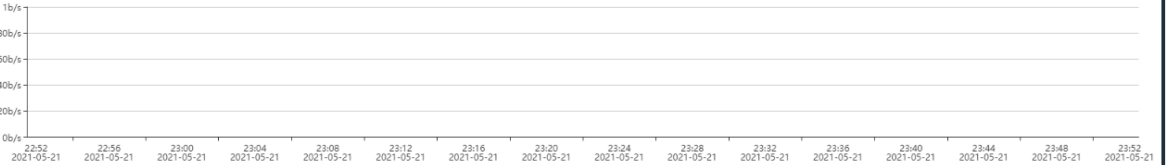
无线客户端使用排行 (Top 5)

基于流量

无线接入点流量统计

请选择 2021-05-21 22:52 TO 2021-05-21 23:52

每1分钟平均流量



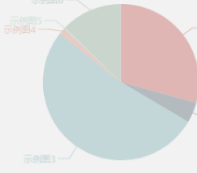
浪潮思科网络科技有限公司

inspur 浪潮
admin 我的账号 注销

应用统计

2021-05-21 23 TO 2021-05-21 23

未获取到当前时间段内该网络的应用数据



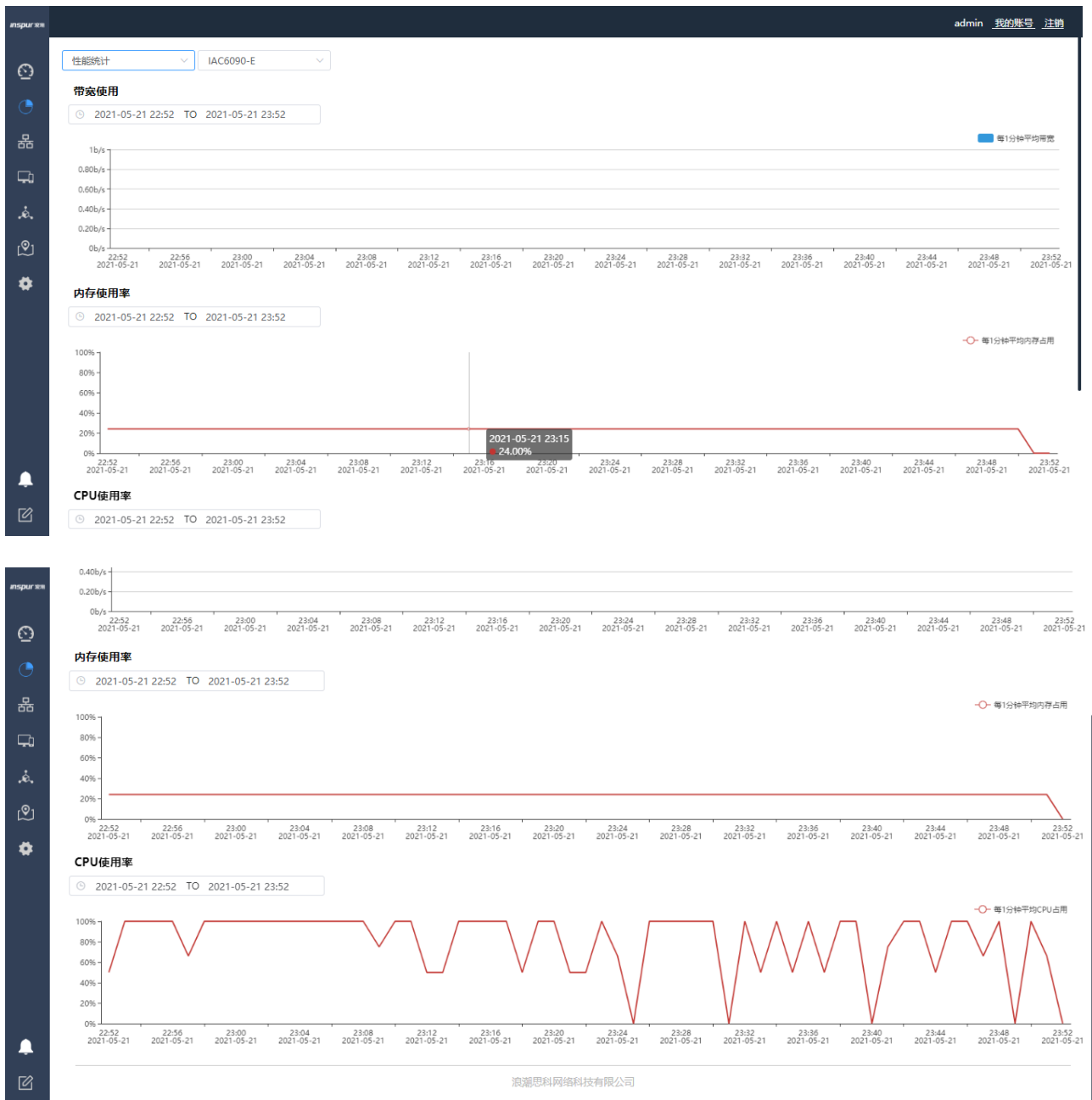
- 示例图1
- 示例图4
- 示例图2
- 示例图3
- 示例图5
- 示例图6

应用 客户端

#	描述	类别	流量	当前使用用户数
暂无数据				

共 0 条 10条/页 1 前往 1 页

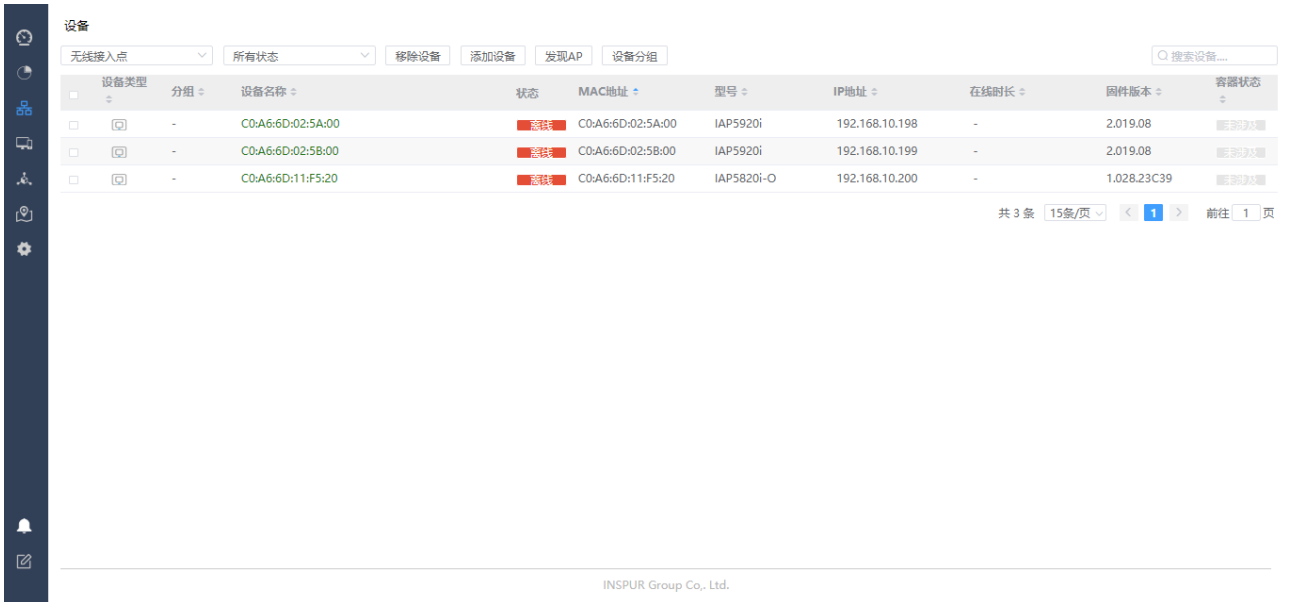
12



功能描述：通过左上角选项框，可对无线、应用、性能等三个维度的相关数据指标进行详细的统计。具体每个维度统计的具体指标类型可在实际登录时进行细致查看，这里不进行一一赘述。

### 2.4.3.3 设备菜单

点击【设备】菜单，如下图所示：

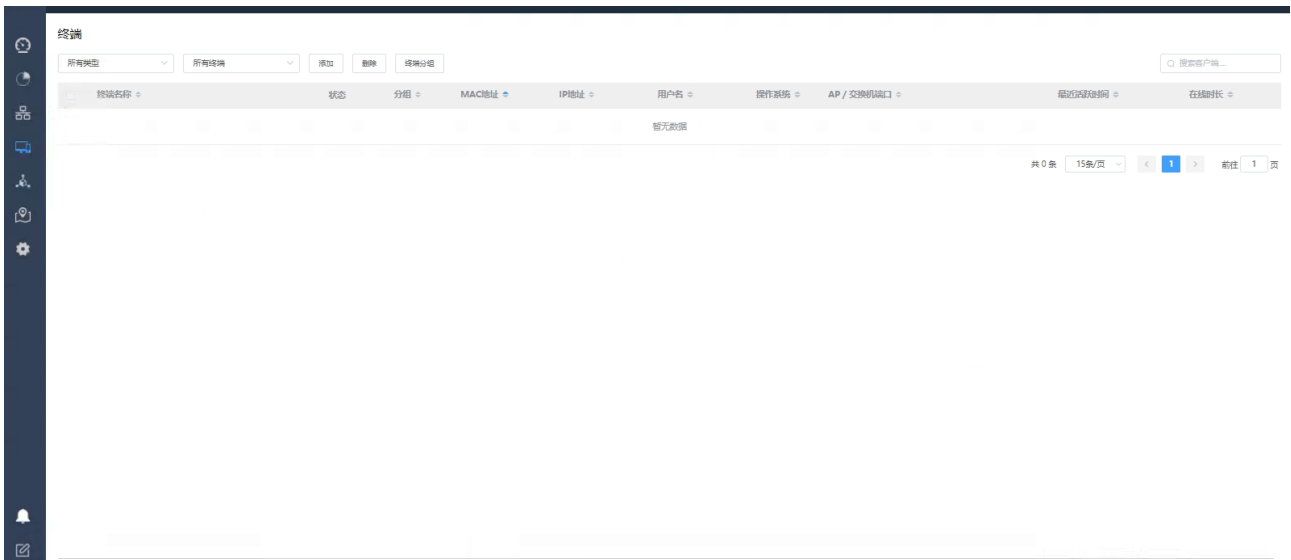


功能描述：主要有三项重点功能可在此菜单下进行操作：

- 1、AP 的添加与删除，在 AP 与 AC 网络连通后，可直接通过<添加设备>功能进行手动添加 AP 设备，或通过<发现 AP>进行自动添加 AP 设备，同时选定任意状态的 AP 进行删除操作；
- 2、AP 状态查看，对已添加 AP 列表中，可实时显示 AP 的在线状态，也可通过点击 AP 进入 AP 详情页中查看 AP 的各类详细状态；
- 3、AP 的批量升级，上传 AP 升级包后，通过批量选定 AP 进行升级；具体的功能操作将在后续配置示例中进行相应介绍。

#### 2.4.3.4 终端菜单

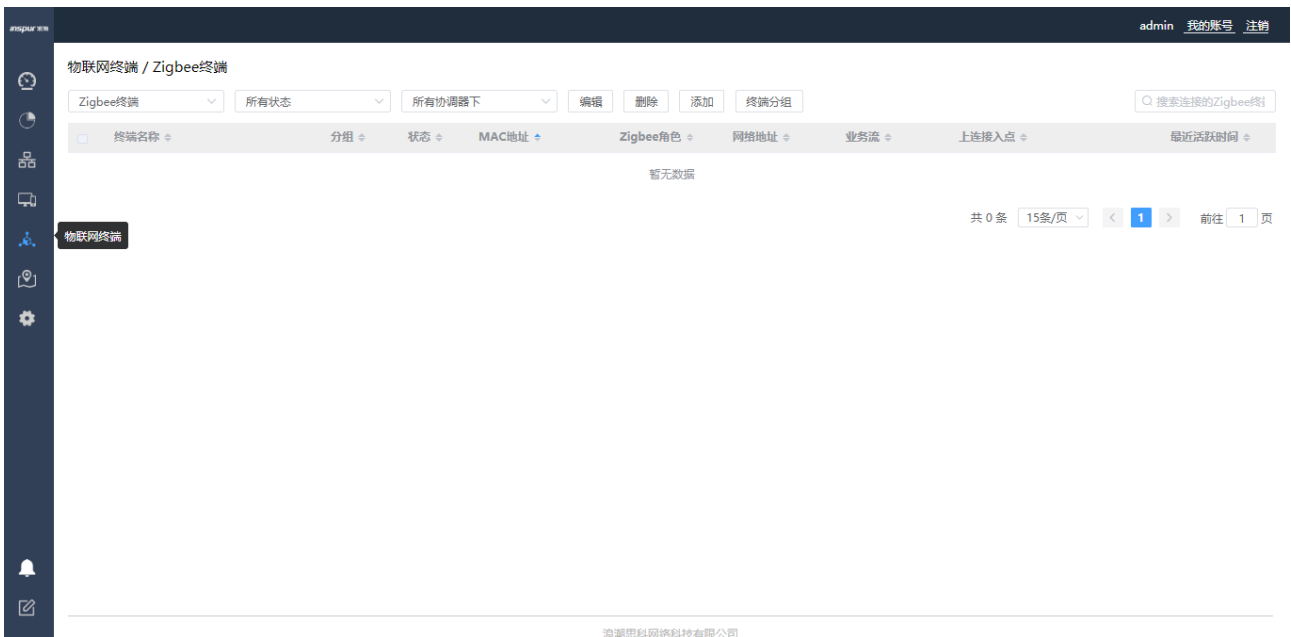
点击【终端】菜单，如下图所示：



功能描述：所有连接过无线网络的终端设备均可显示在此列表中，可任意选定剔除或添加终端设备，能够实时显示终端在线或离线状态；

### 2.4.3.5 物联网终端菜单

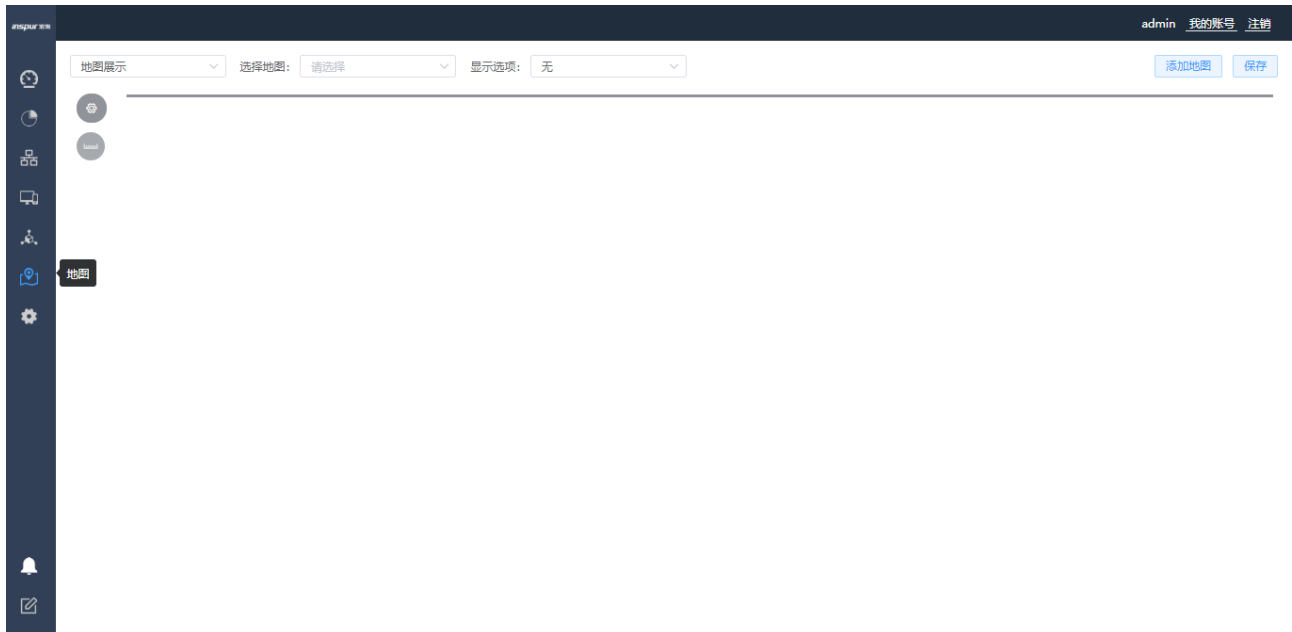
点击【物联网终端】菜单，如下图所示：



功能描述：所有连接过或被扫描到的蓝牙或 Zigbee 的物联终端设备均会显示在此列表中，能够实时显示终端在线或离线状态，添加注册后，可进行统一纳管；

### 2.4.3.6 地图菜单

点击【地图】菜单，如下图所示：



功能描述：需深化开发才能完成此功能；

### 2.4.3.7 设置菜单（业务功能配置菜单）

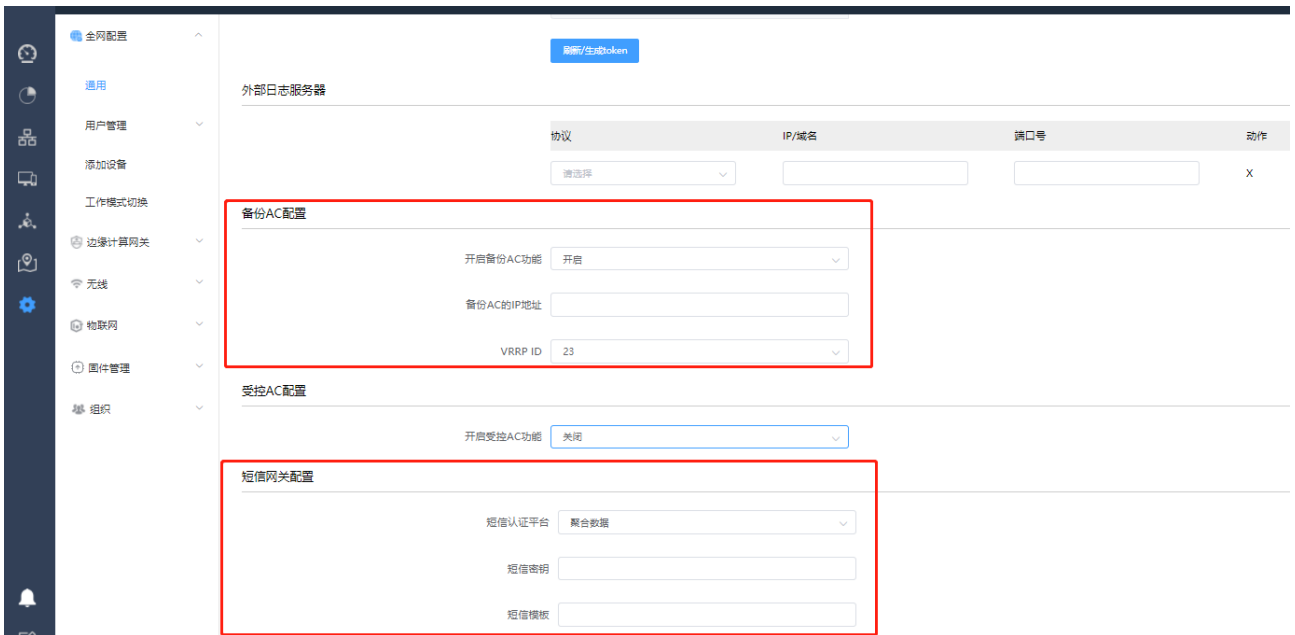
点击【设置】菜单，如下图所示：



功能描述：业务功能的配置几乎都在此菜单中完成，【设置】菜单中包含了有【全网配置】、【边缘计算网关】、【无线】、【物联网】、【固件管理】、【组织】共六个子菜单。

#### 2.4.3.7.1 全网配置菜单

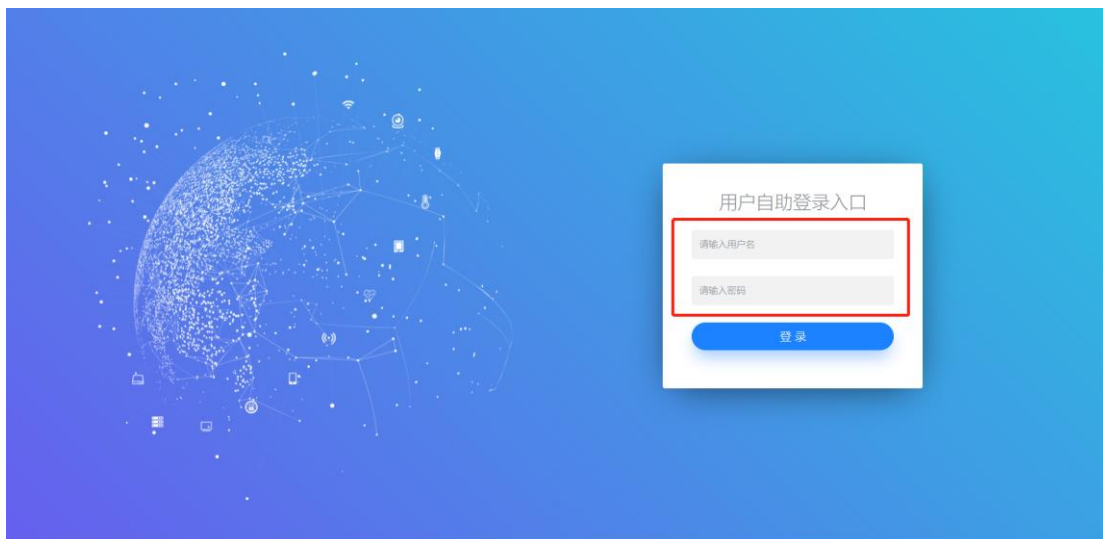
【通用】菜单-主要功能是 VRRP 主备 AC 的绑定功能开启配置，以及短信网关配置，详细内容如下所示：



【用户管理】菜单-主要功能是针对本地 portal、802.1x、mac 认证的用户认证策略模板、用户组、用户的创建及管理，详细配置如下所示：

802.1x 认证支持在线数量限制功能，在创建的认证策略模板中，可选择是否授权 Easy Portal、8020.1x、mac 认证，支持 802.1x 认证的用户自主修改账号密码，修改方法：

电脑端或手机端浏览器输入地址：<http://192.168.186.1/#/localUserLogin?networkname=localhost>，进入用户自助登录入口，使用个人账号和密码登录，显示如下：



登陆后在输入新密码，点击“保存配置”即可修改成功。

基本信息

账号名

用户姓名

证件号码

通讯地址

电话

电子邮件

密码

【用户组】页面，可创建用户组，将用户组绑定到认证策略模板及 SSID

用户组

暂无数据

添加新用户组

\* 用户组名

描述

创建者

SSID认证策略

认证策略模板	SSID名称
<input type="text" value="请选择"/>	<input type="text" value="请选择"/>

同步更新本用户组中的用户

用户组

test01

编辑用户组 - test01

\* 用户组名

描述

创建者

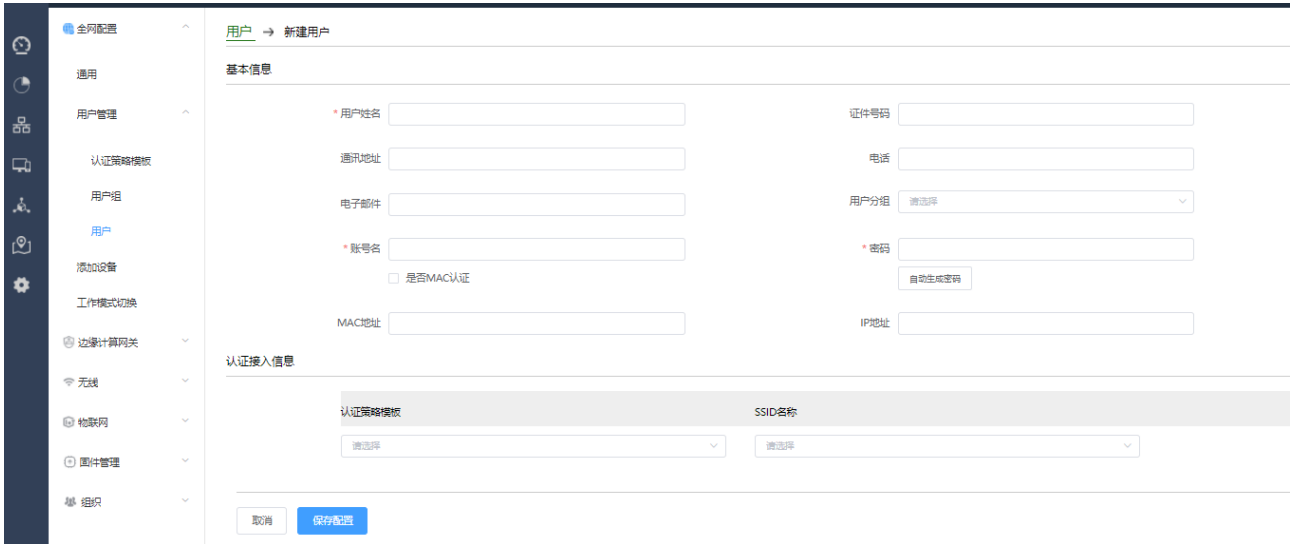
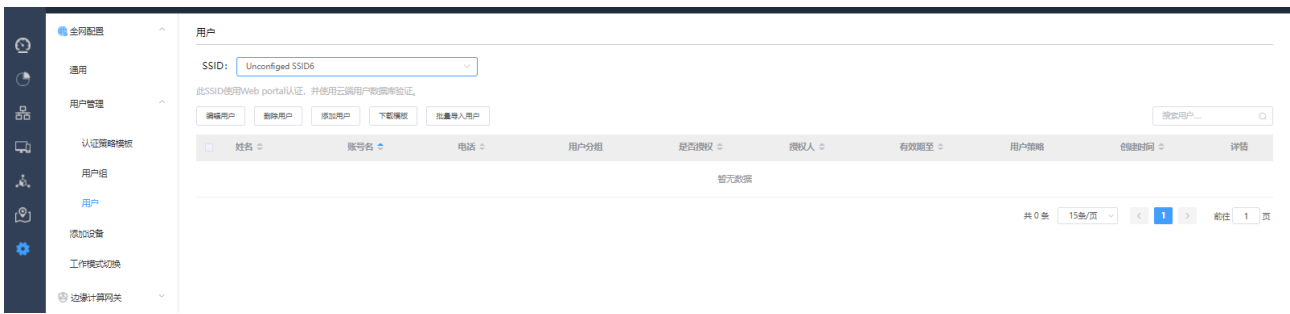
SSID认证策略

认证策略模板	SSID名称
<input type="text" value="test"/>	<input type="text" value="Unconfigured SSID 8"/>

同步更新本用户组中的用户

【用户】页面，选择 SSID，可添加单个用户或通过模板批量导入用户

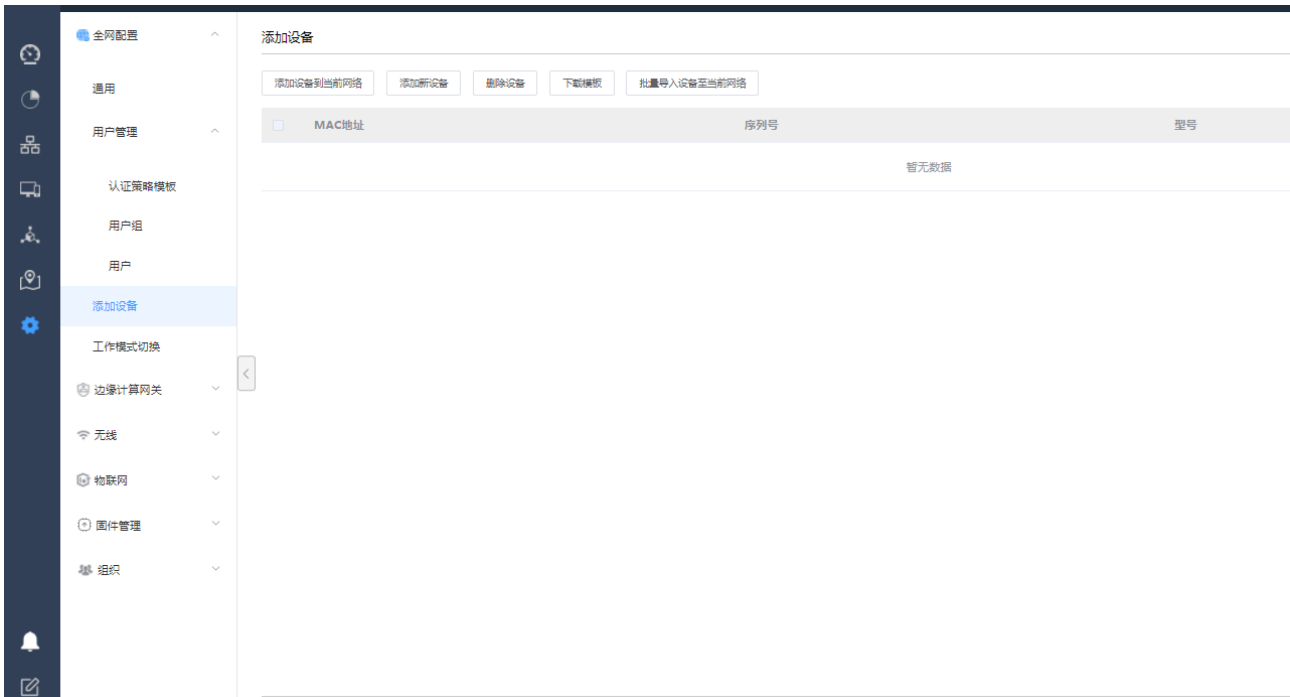


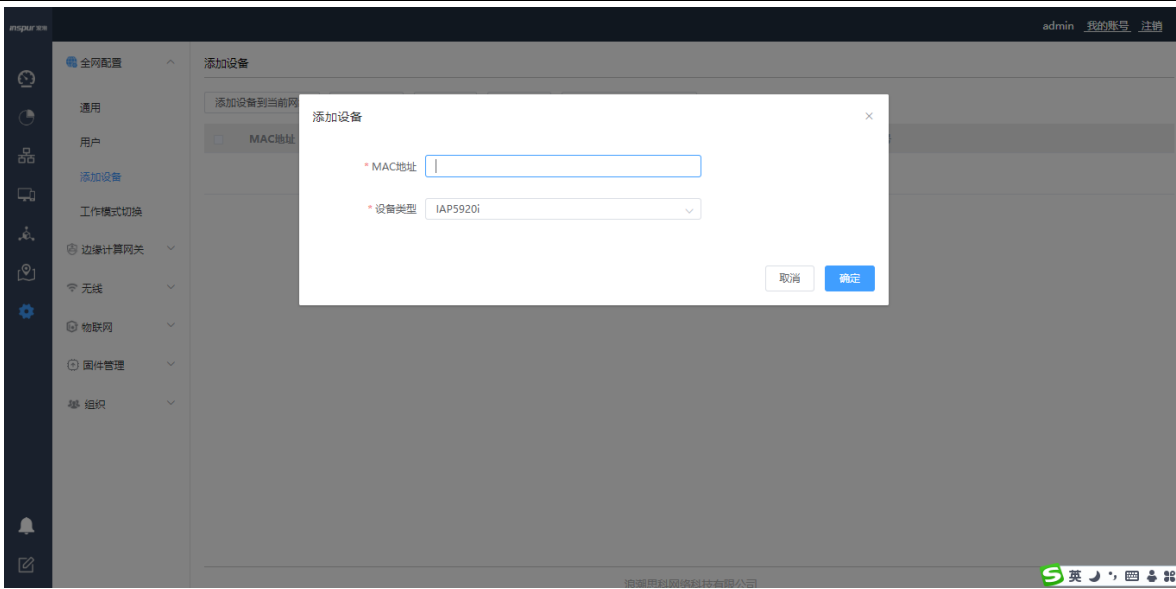


**说明：**当勾选“是否 MAC 认证”，用户名格式将变为 mac 用户名格式：xxxx.xxxx.xxxx（字母为小写）

认证接入信息栏可绑定“认证策略模板”及对应的 SSID

【添加设备】菜单-主要功能是手动添加/删除 AP、下载批量化导入 AP 的模板、批量导入 AP，详细配置内容如下所示：

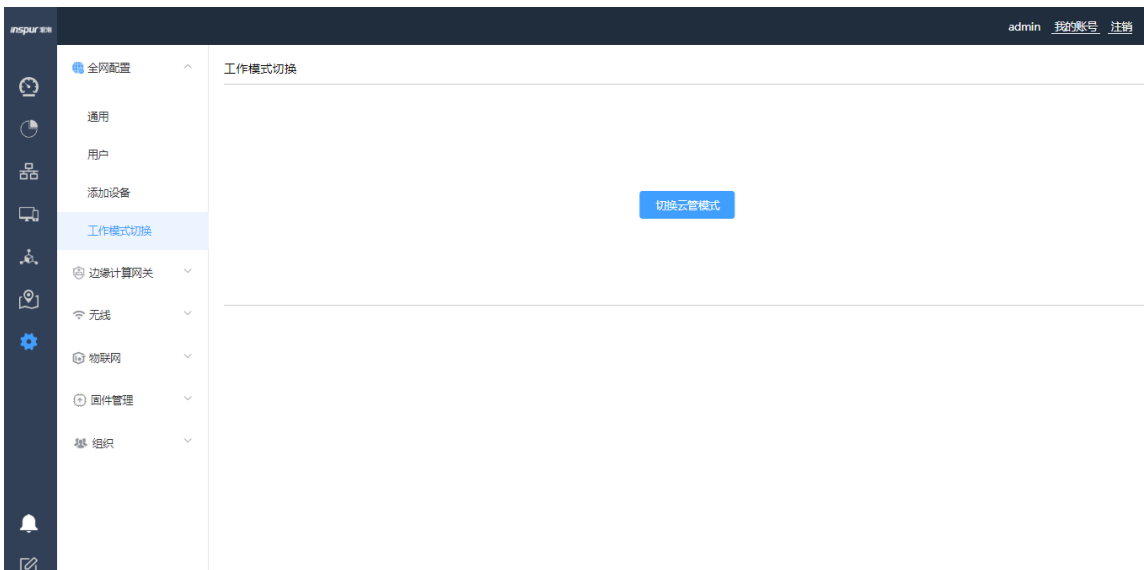




	A	B	C	D	E
1	MacAddr	Model	Name/设备名称 (3-64 characters/字符)	Address/地址 (6-300 characters/字符)	Notes/备注 (6-300 characters/字符)
2					
3					
4					
5					
6					
7					

下载的批量化导入 AP 的模板中，支持批量填写 AP 设备名称后统一导入。

【工作模式切换】菜单-主要功能是 AC 切换无线云管理模式功能的配置，详细如下图所示：

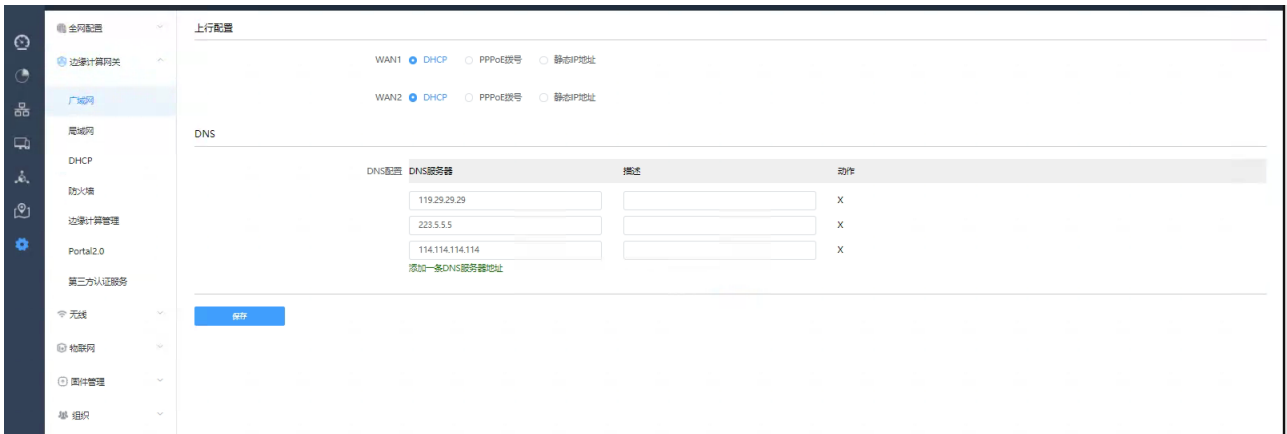


点击<切换云管模式>，工作模式即将切换为云管模式，请确认！

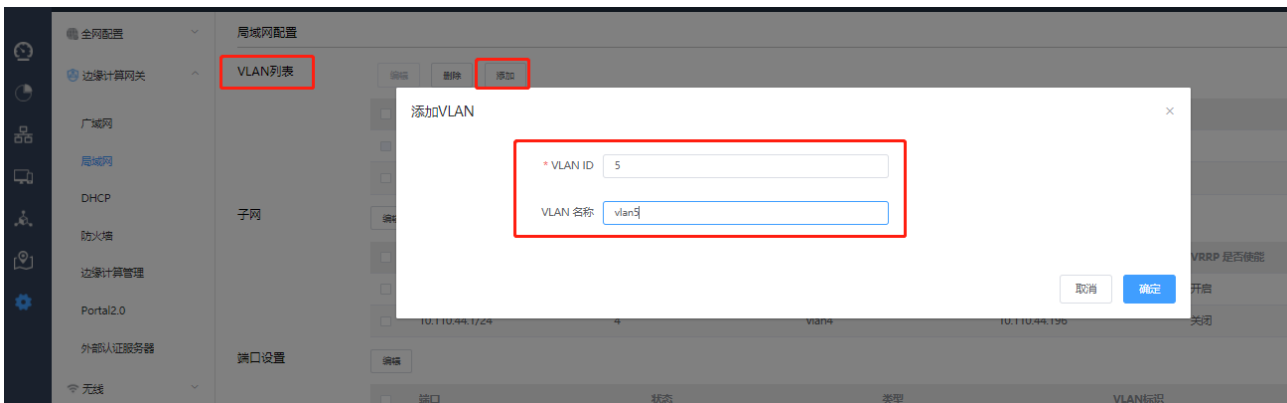
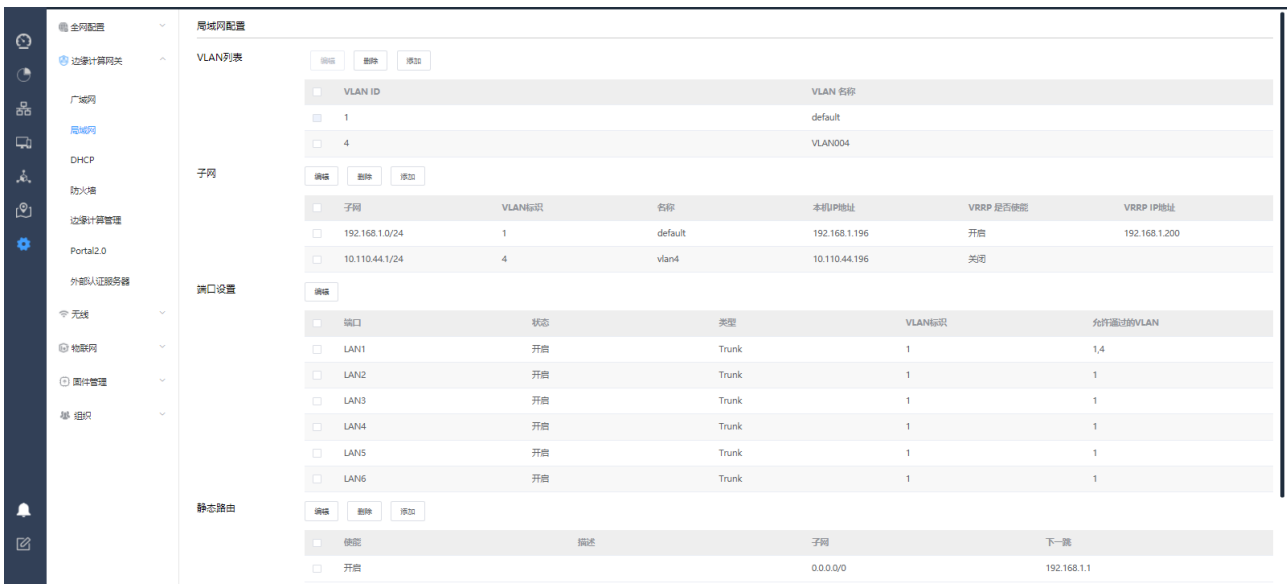
云管模式，需要配置云服务器的主机地址。

### 2.4.3.7.2 边缘计算网关菜单

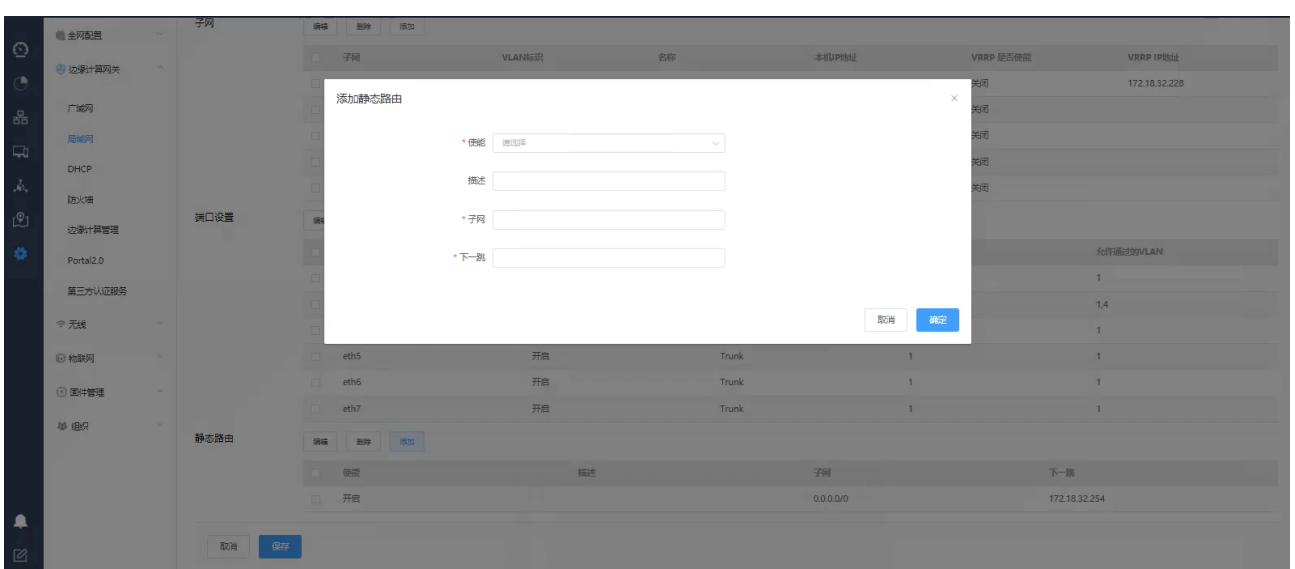
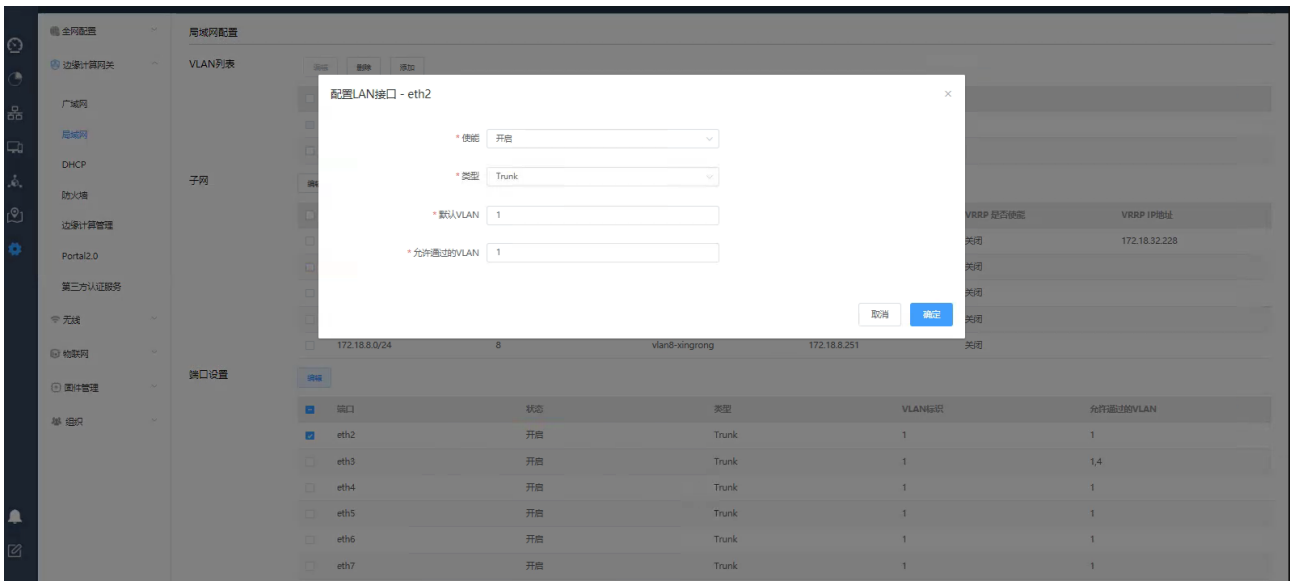
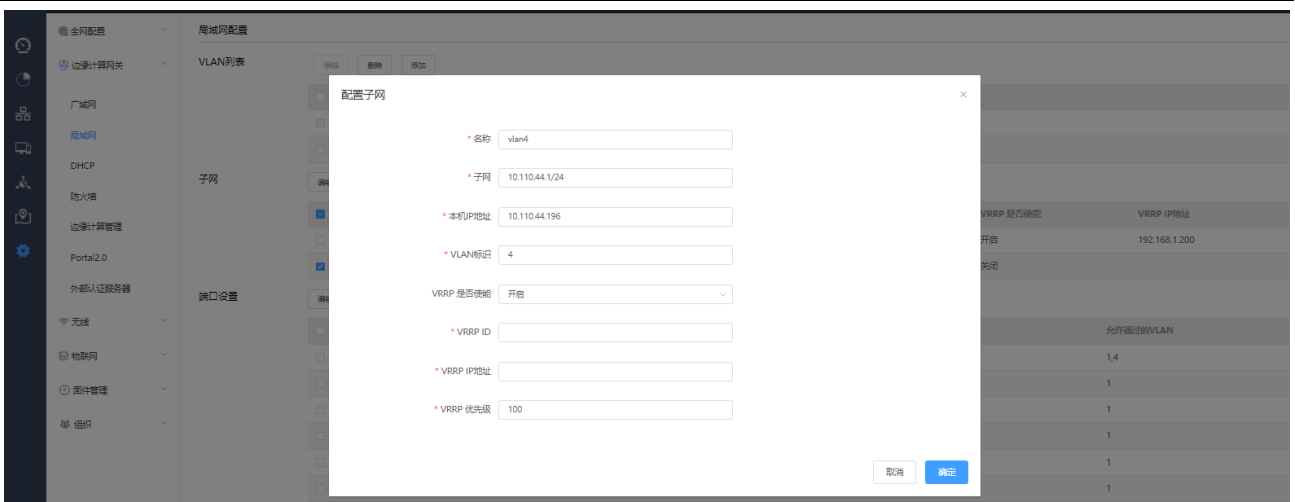
【广域网】菜单-主要功能是 AC 做网关或切换为云管理模式时进行 WAN 口的 IP 信息、DNS 信息的配置，详见如下图所示：



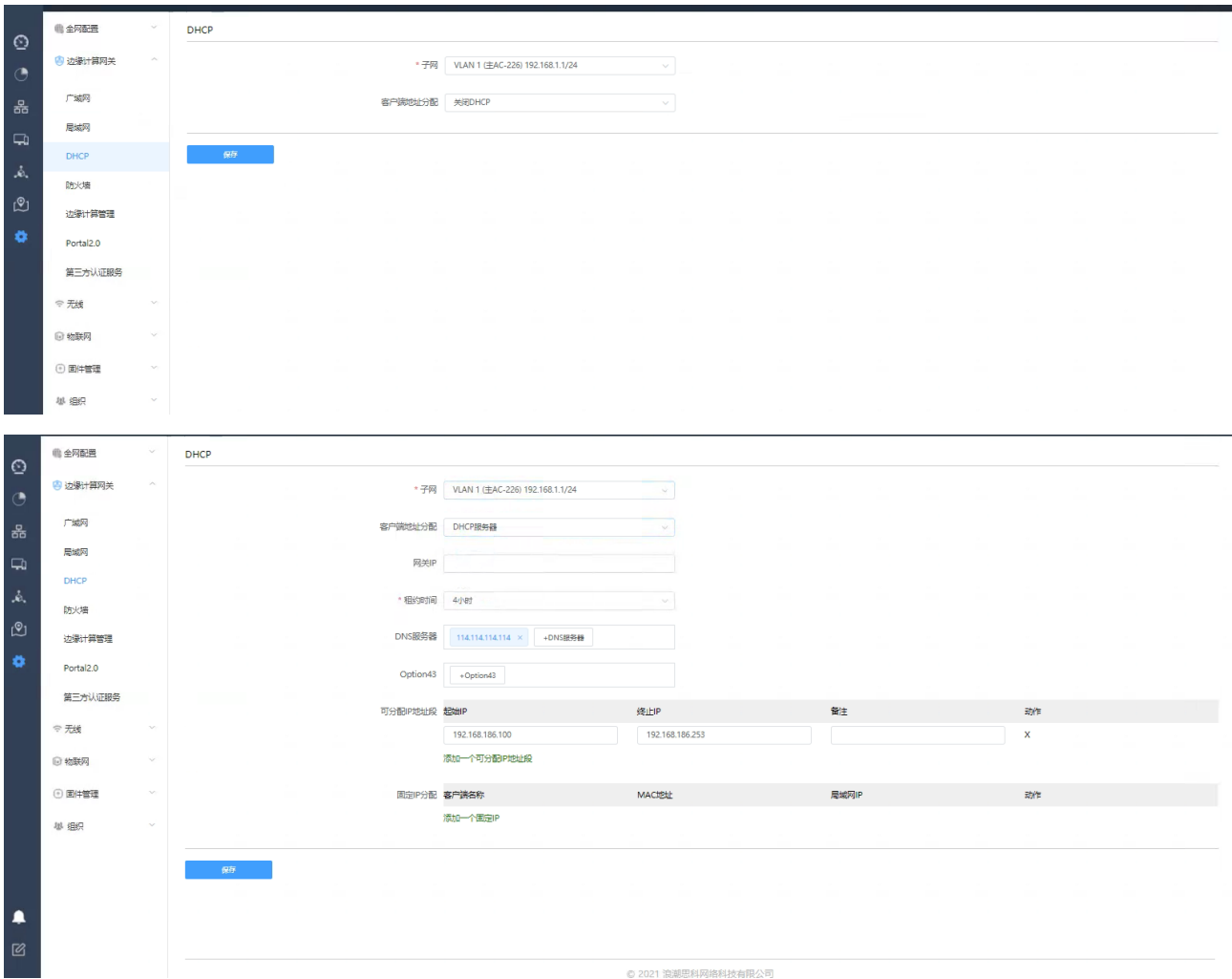
【局域网】菜单-主要功能是 AC 的 VLAN 创建、VLAN 子网创建、VRRP 功能的开启、上下行网络端口、静态路由等功能的配置，详见如下图所示：



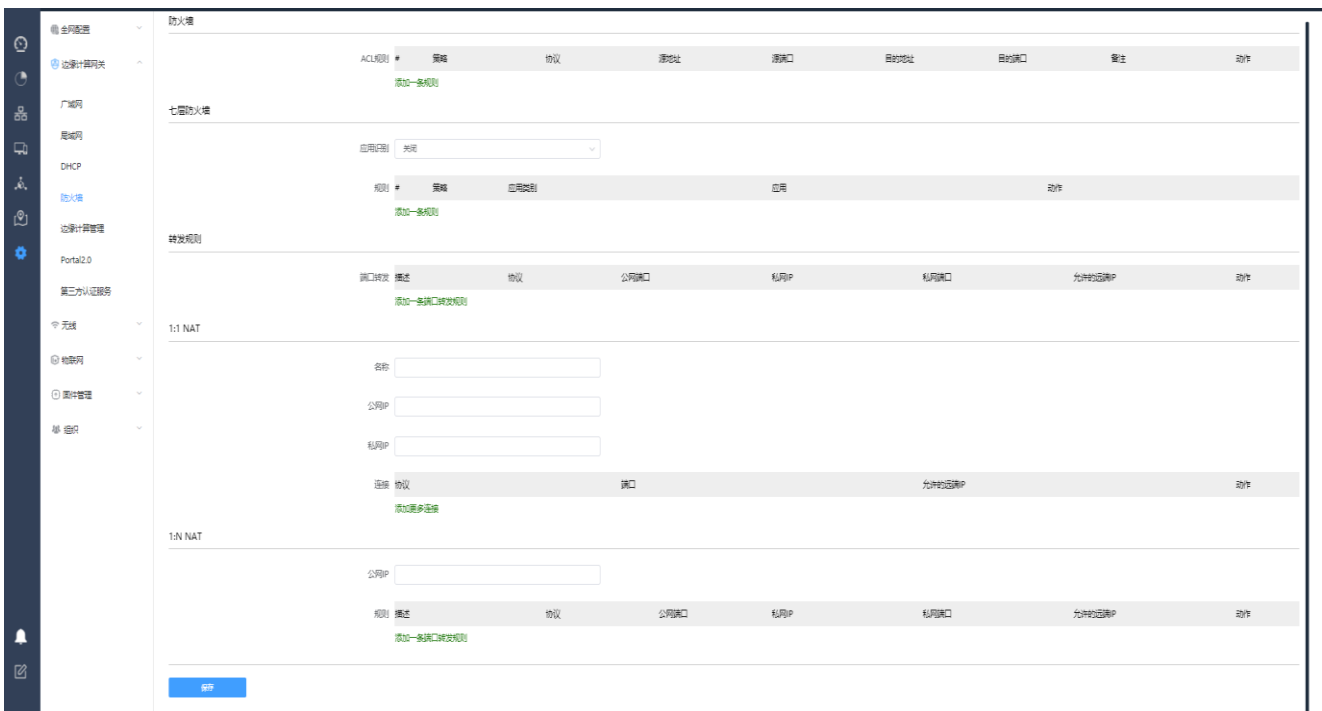
在【VLAN 列表】点击<添加>，可添加 VLAN，VLAN 添加后，在子网模块中可添加该 VLAN 的接口 IP。  
注：portal 认证时需要使用 VLAN IP。



**【DHCP】**菜单-主要功能是 AC 中 DHCP 服务功能配置，包括开启或关闭 DHCP、网关 IP、租约期限、DNS 服务器、地址池起始与结束地址、固定 IP 与 MAC 绑定等配置，详见如下图所示：



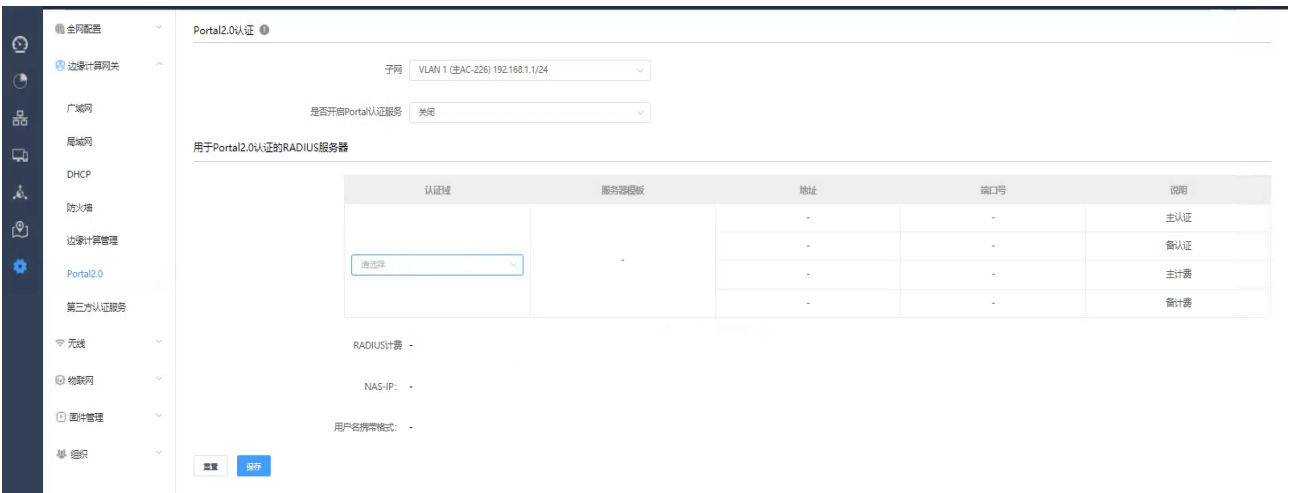
【防火墙】菜单-主要功能是 AC 作为出口网关时实现简单 ACL 控制、NAT 转换等功能的配置，详见如下图所示：



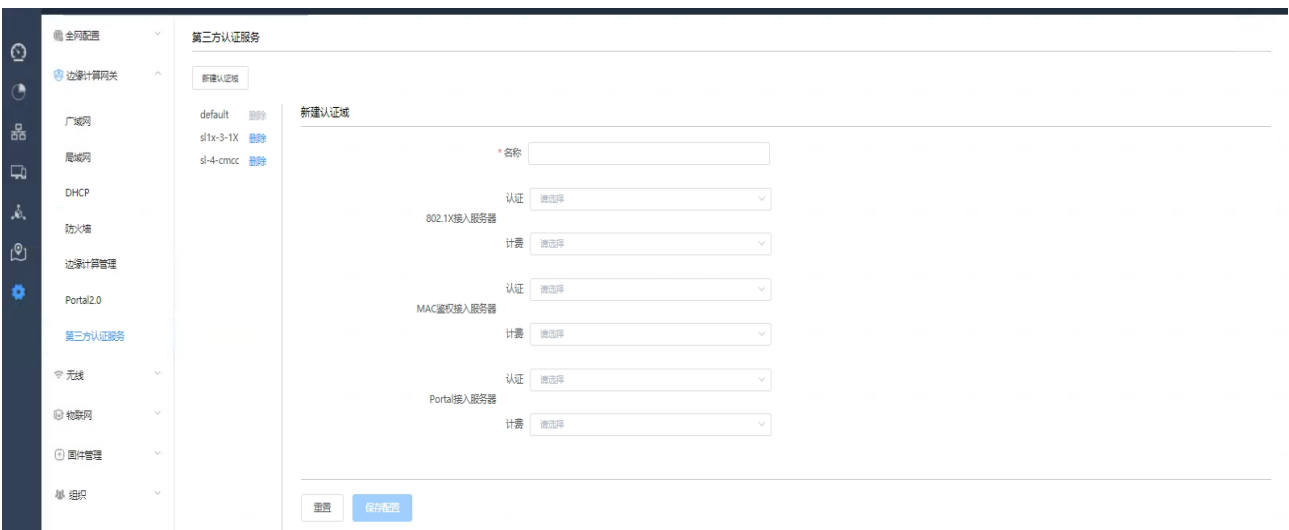
【边缘计算管理】菜单-主要功能是边缘计算的访问控制功能配置，详见如下图所示：



【Portal2.0】菜单-主要功能是 AC 对接第三方 Portal 认证时，在 AC 侧需做的第三方认证平台认证与计费服务信息的配置，详细如下图所示：

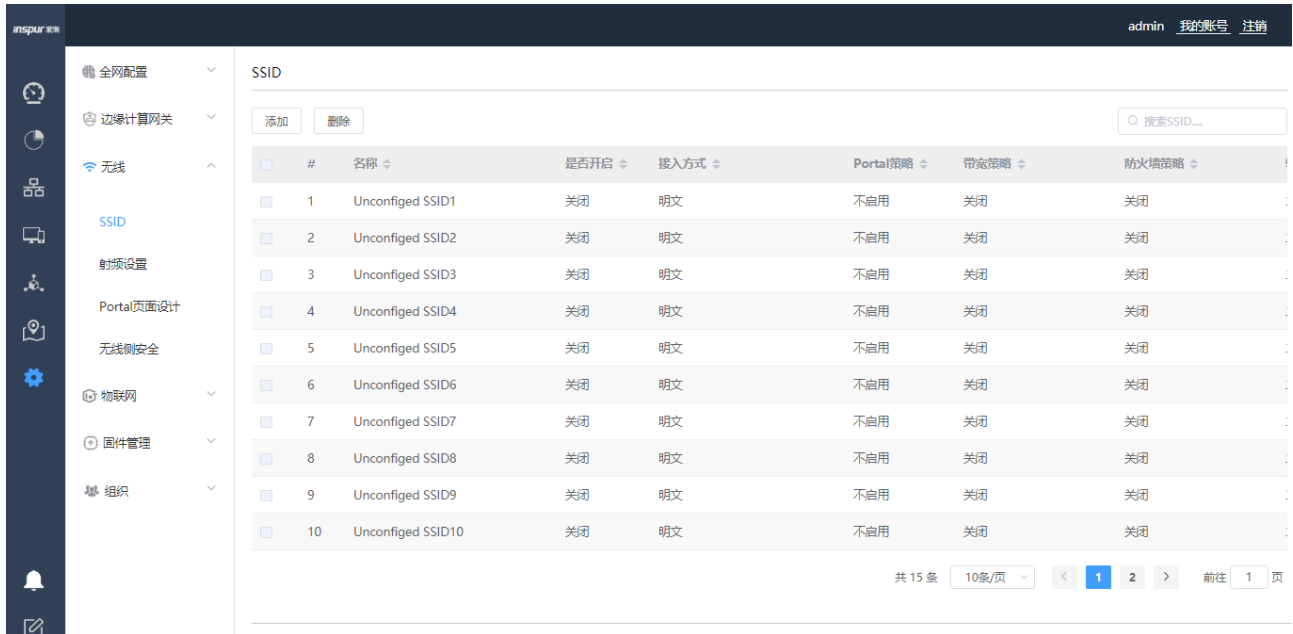


【第三方认证服务】菜单-主要功能是 AC 对接第三方认证服务器时，在 AC 侧需做的第三方认证平台认证与计费服务信息的配置，详细如下图所示：



## 2.4.3.7.3 无线菜单

【SSID】菜单-主要功能是 SSID 模板的配置，有 SSID 名称\使能\是否隐藏 SSID、接入控制选择（本地或第三方）、本地 portal 开启及策略选择、本地\集中转发模式、业务 VLAN 指定、用户逃生模式、带宽策略、快速漫游开关、组播优化开关、定时开\关 SSID、AP 的绑定等功能配置，详见如下图所示：



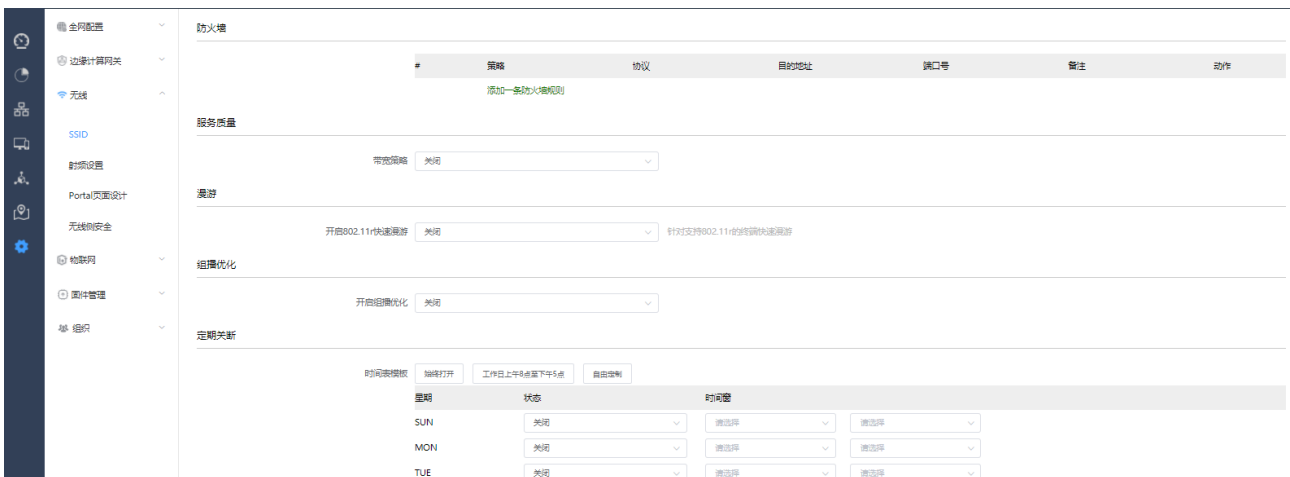
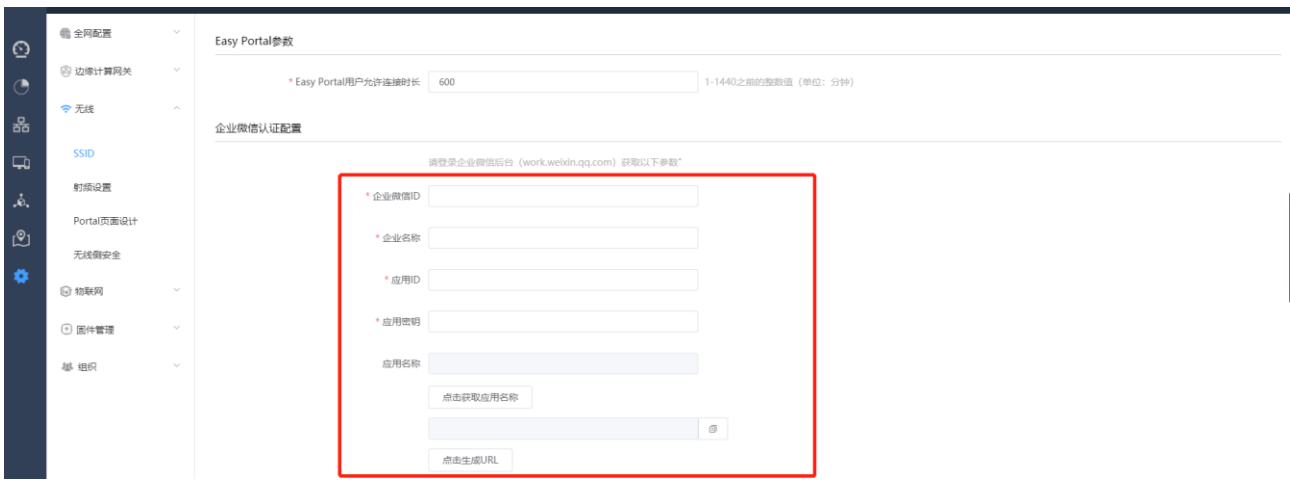
默认有 15 个 SSID 模板，也可再添加，详细的 SSID 模板如下图所示：



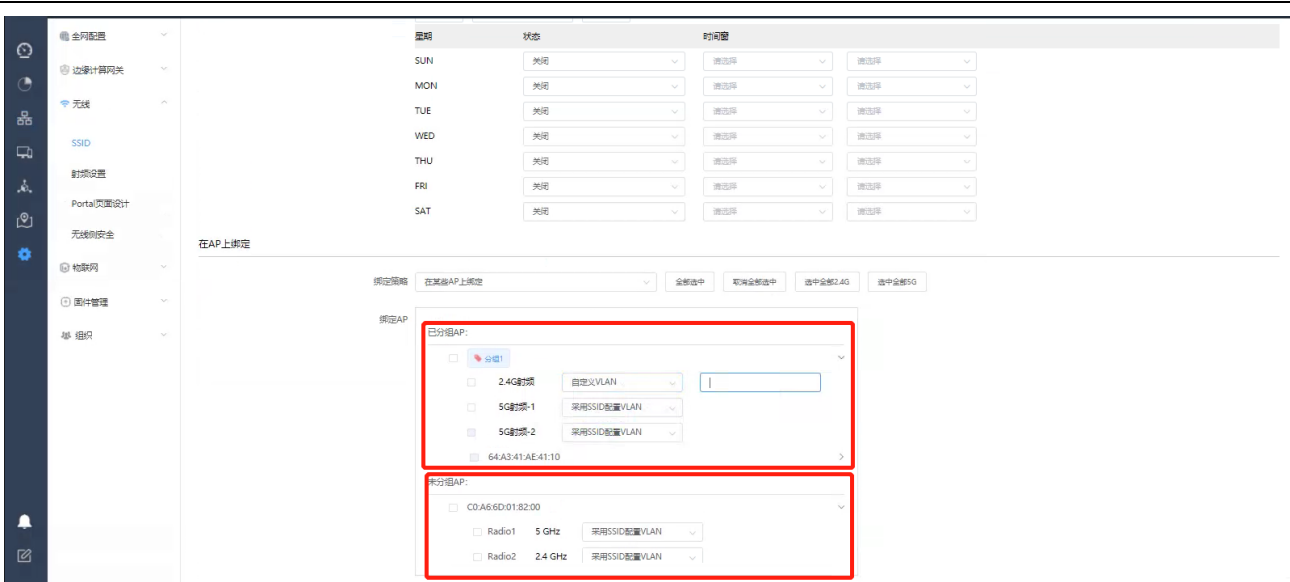


当选择企业微信认证或基于企业微信认证的访客二维码认证时, 会激活企业微信认证配置模块

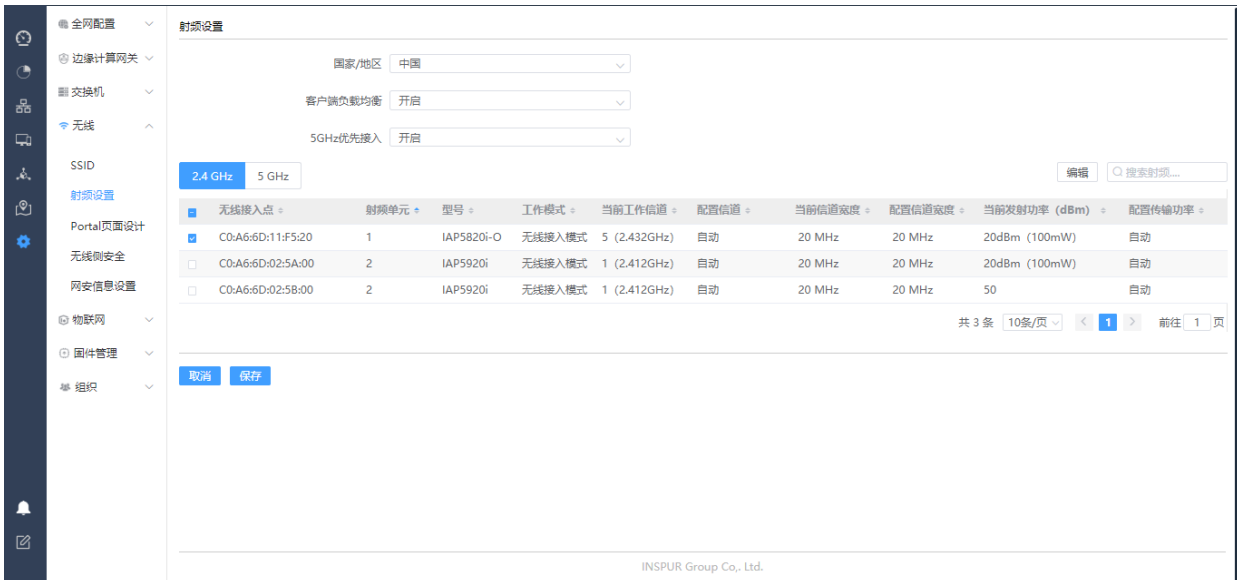




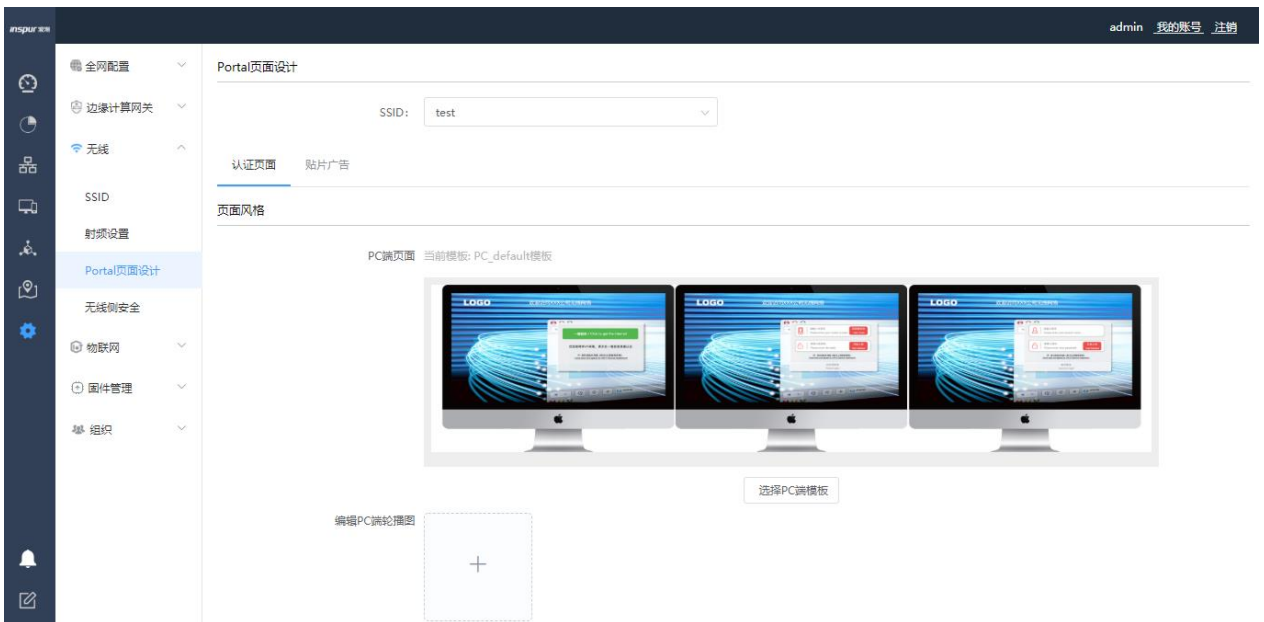
当选择在某些 AP 上绑定时，可以绑定某个分组或其他未分组的 AP，可以基于 2.4G 射频或 5G 射频自定义 VLAN，将 vlan 绑定到 AP 的射频上，该 VLAN 优先级高于 SSID 上绑定的 VLAN，详见如下图所示：



【射频设置】菜单-主要功能是对 AP 的 2.4G/5G 射频的信道、发射功率等功能的配置，详见如下图所示：



【Portal 页面设计】菜单-主要功能是对本地 portal 认证时，重定向页面的风格选择或定制化设计，详见如下图所示：



admin 我的账号 注销

全网配置 边缘计算网关 无线 SSID 射频设置 **Portal页面设计** 无线测安全 物联网 固件管理 组织

内容定制化

PC端页面标题

PC端页面logo

移动端页面标题

移动端页面logo

跳转行为

PC端开启认证前倒计时广告  不开启认证前倒计时广告

admin 我的账号 注销

全网配置 边缘计算网关 无线 SSID 射频设置 **Portal页面设计** 无线测安全 物联网 固件管理 组织

跳转行为

PC端开启认证前倒计时广告  不开启认证前倒计时广告

开启认证前倒计时广告

广告页面展示时间:  秒

PC端页面广告

PC端认证成功后跳转URL

移动端开启认证前倒计时广告  不开启认证前倒计时广告

开启认证前倒计时广告

广告页面展示时间:  秒

移动端页面广告

admin 我的账号 注销

全网配置 边缘计算网关 无线 SSID 射频设置 **Portal页面设计** 无线测安全 物联网 固件管理 组织

PC端认证成功后跳转URL

移动端开启认证前倒计时广告  不开启认证前倒计时广告

开启认证前倒计时广告

广告页面展示时间:  秒

移动端页面广告

移动端认证成功后跳转URL

[PC端页面效果浏览](#) [移动端页面效果浏览](#)

[取消](#) [保存](#)

浪潮思科网络科技有限公司

inspur admin 我的账号 注销

全网配置 边缘计算网关 无线 SSID 射频设置 Portal页面设计 无线测安全 物联网 固件管理 组织

### Portal页面设计

SSID: test

认证页面 贴片广告

全部 发布 取消发布 增加

名称	移动端图片	移动端图片链接	PC端图片	PC端图片链接	生效时间	失效时间	投放时间	动作
暂无数据								

共 0 条 10条/页 < 1 > 前往 1 页

#### 浮窗广告页面编辑

\* 名称

移动端图片

移动端图片尺寸 146\*146

\* 移动端图片点击跳转URL

PC端图片

PC端图片尺寸 146\*146

\* PC端图片点击跳转URL

\* 有效时间段  开始日期 至 结束日期

投放时间

移动端图片尺寸 146\*146

\* 移动端图片点击跳转URL

PC端图片

PC端图片尺寸 146\*146

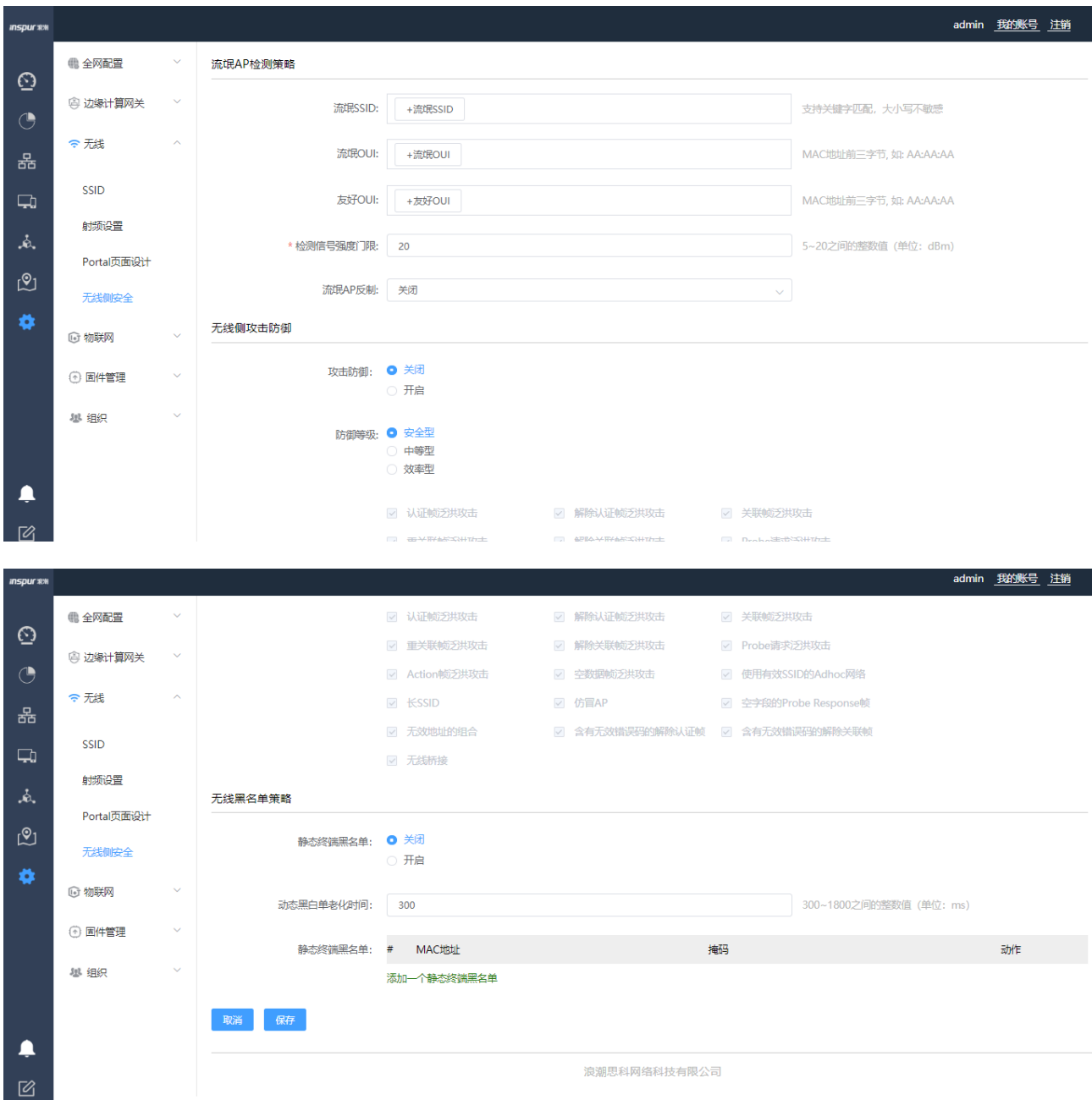
\* PC端图片点击跳转URL

\* 有效时间段  开始日期 至 结束日期

\* 投放时间段  开始日期 至 结束日期

取消 确定

【无线侧安全】菜单-主要功能是流氓 AP 检测策略、无线侧攻击防御、无线黑名单策略的功能配置，详见如下图所示：



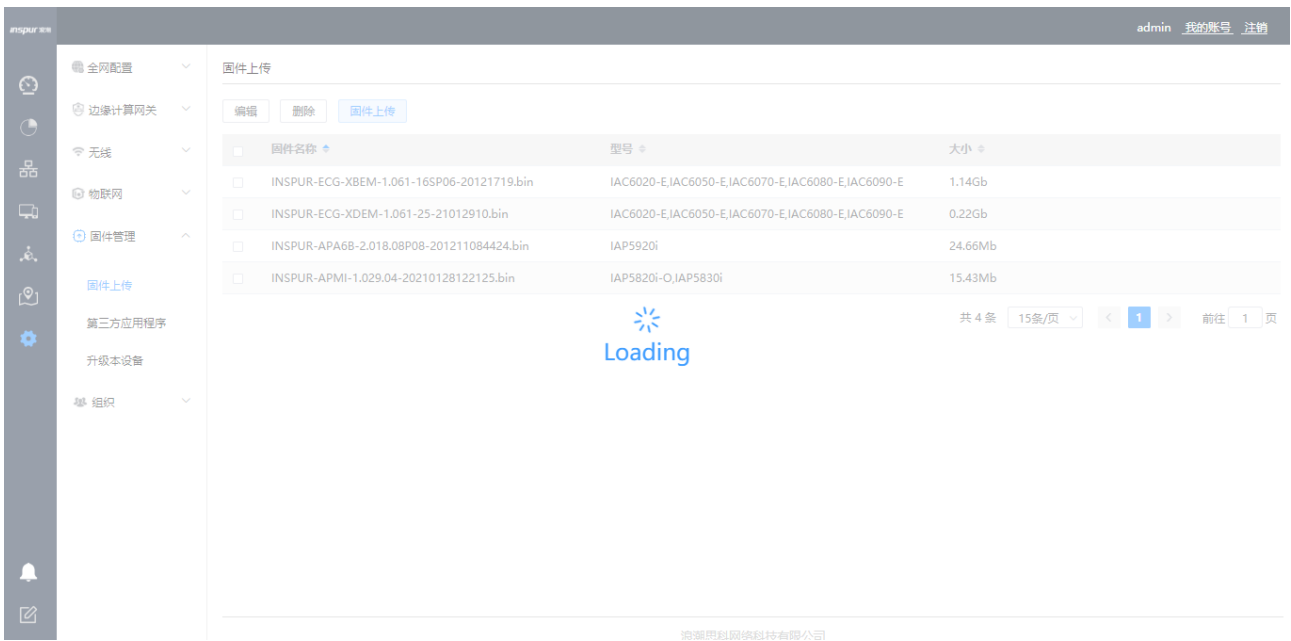
### 2.4.3.7.4 物联网菜单

本次暂略

### 2.4.3.7.5 固件管理菜单

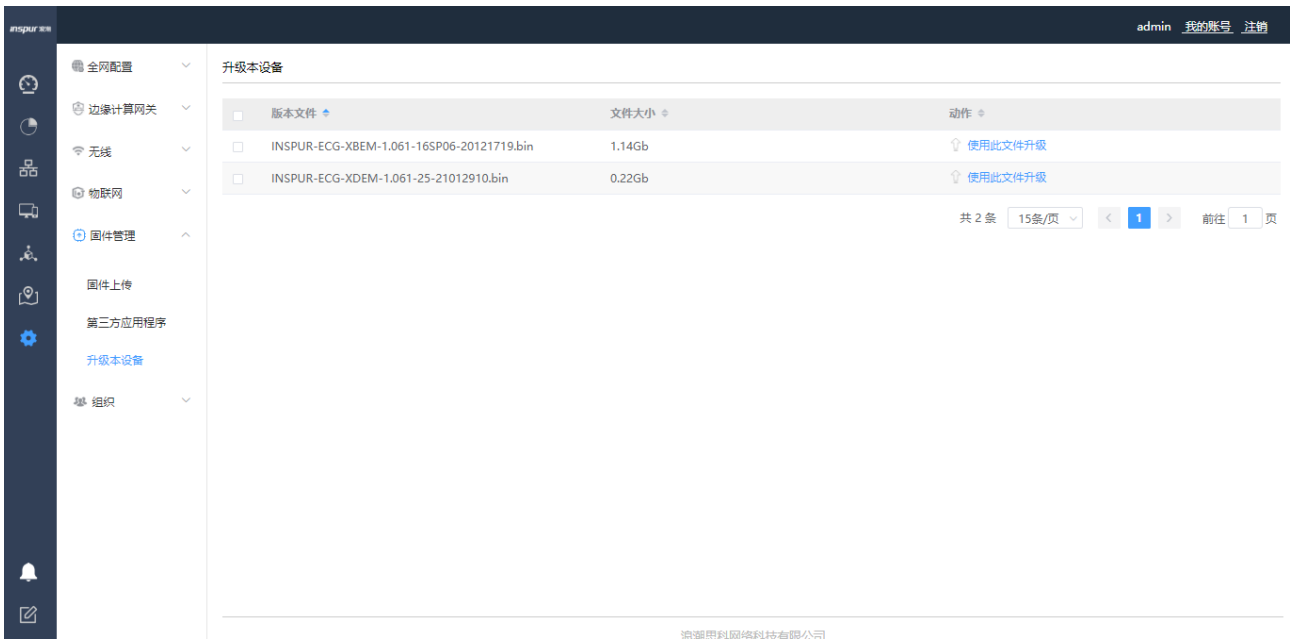
【固件上传】菜单-主要功能是上传 AC、AP 升级包，详见如下图所示：



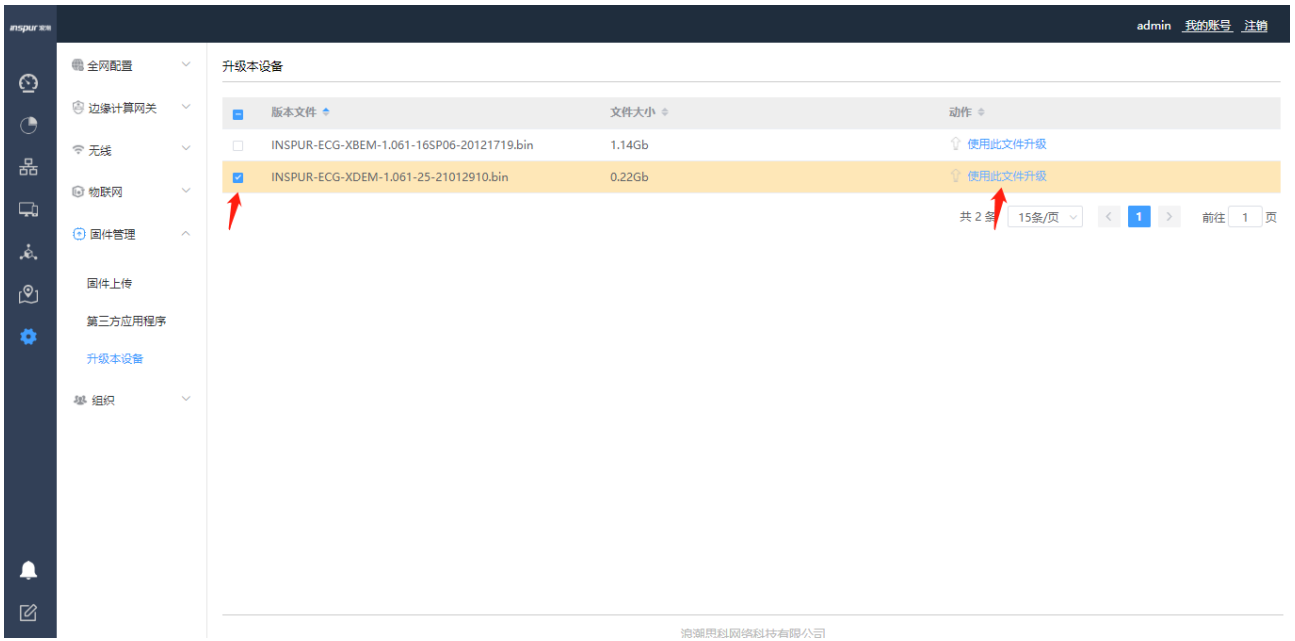


【第三方应用程序】菜单-功能介绍暂略。

【升级本设备】菜单-主要功能是通过 Web 升级直接 AC 设备的版本，详细如下图所示：

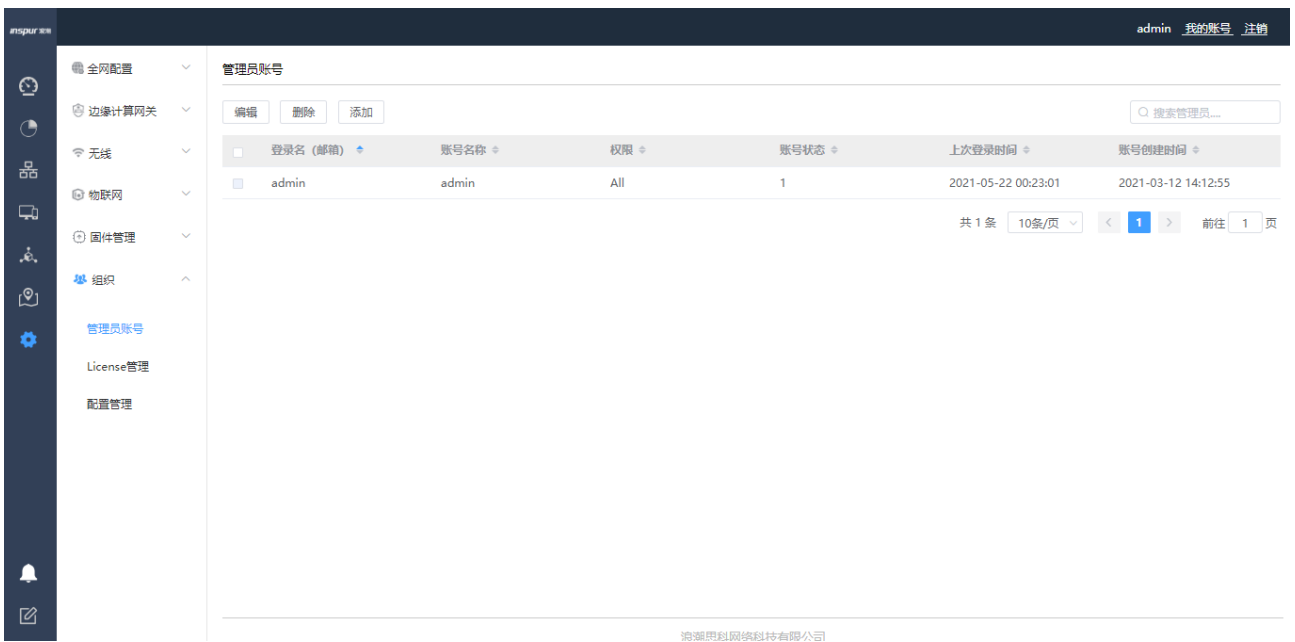


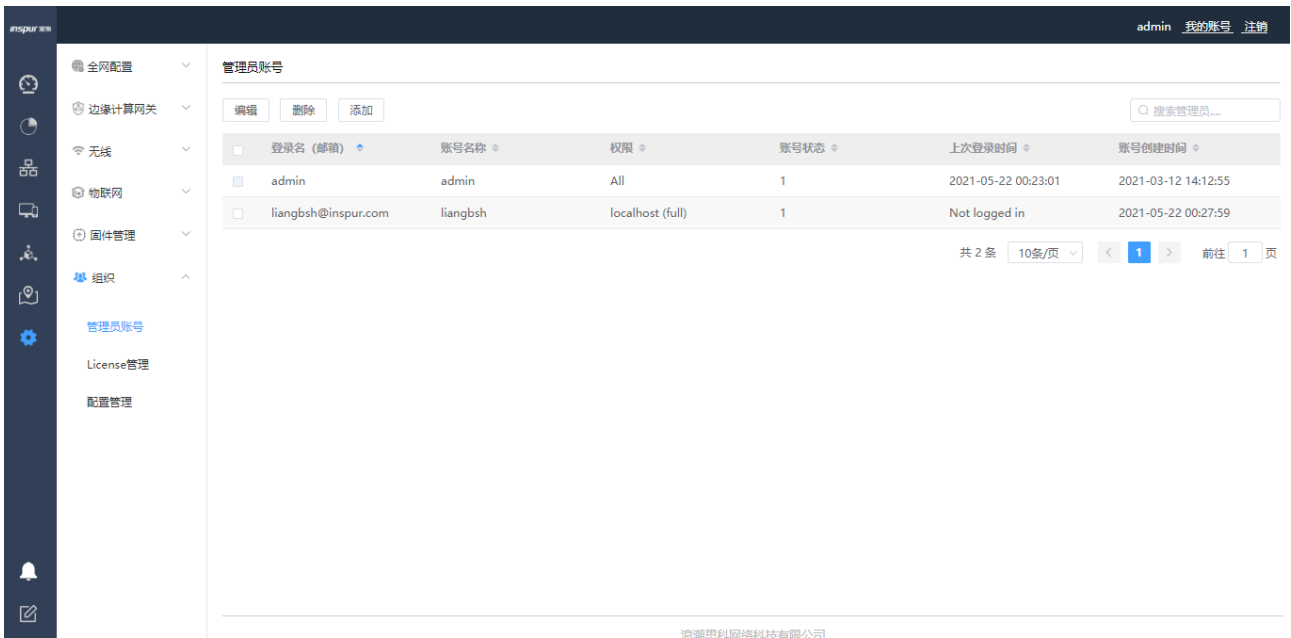
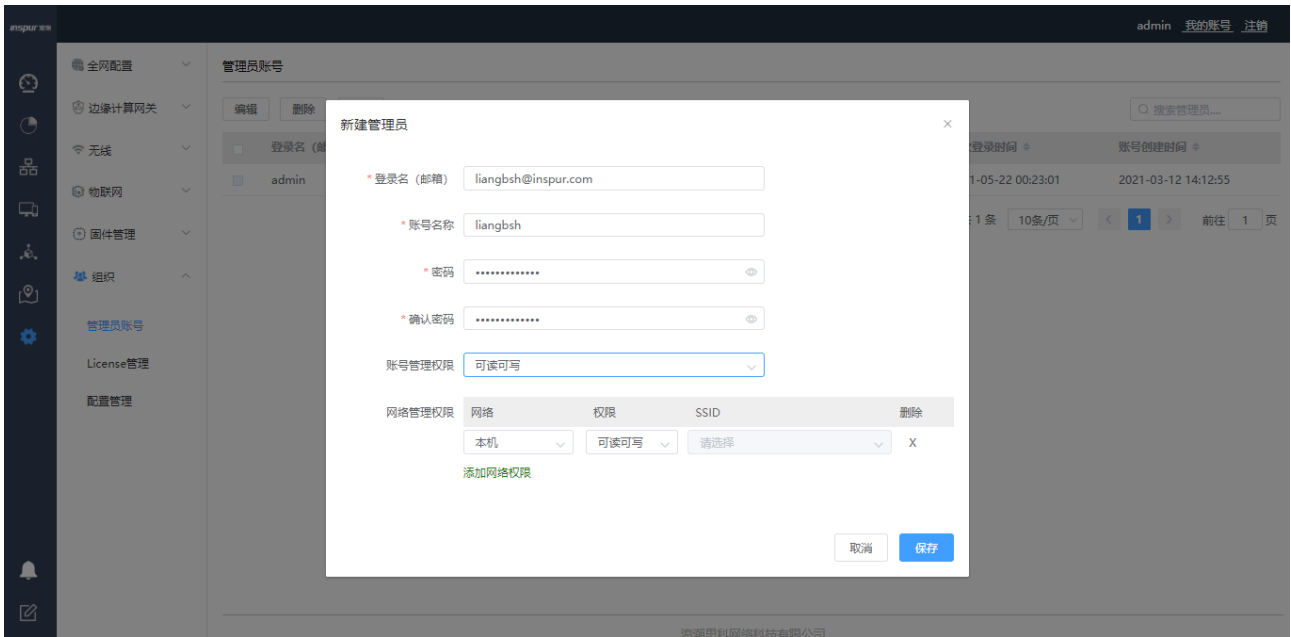




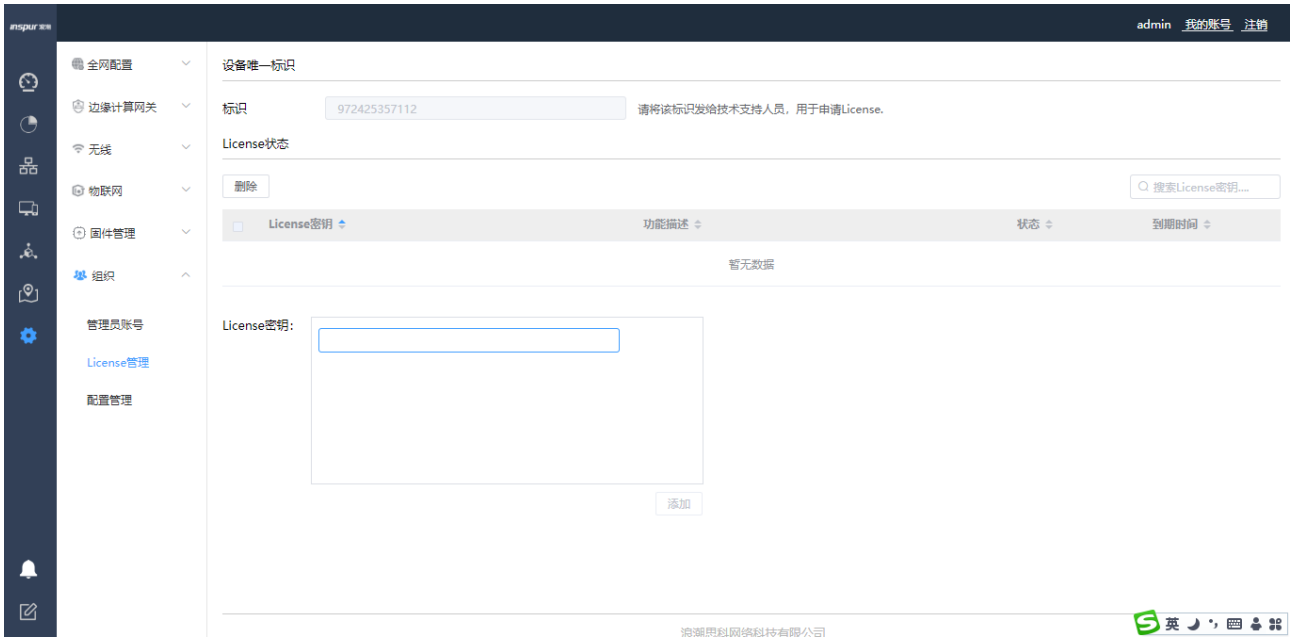
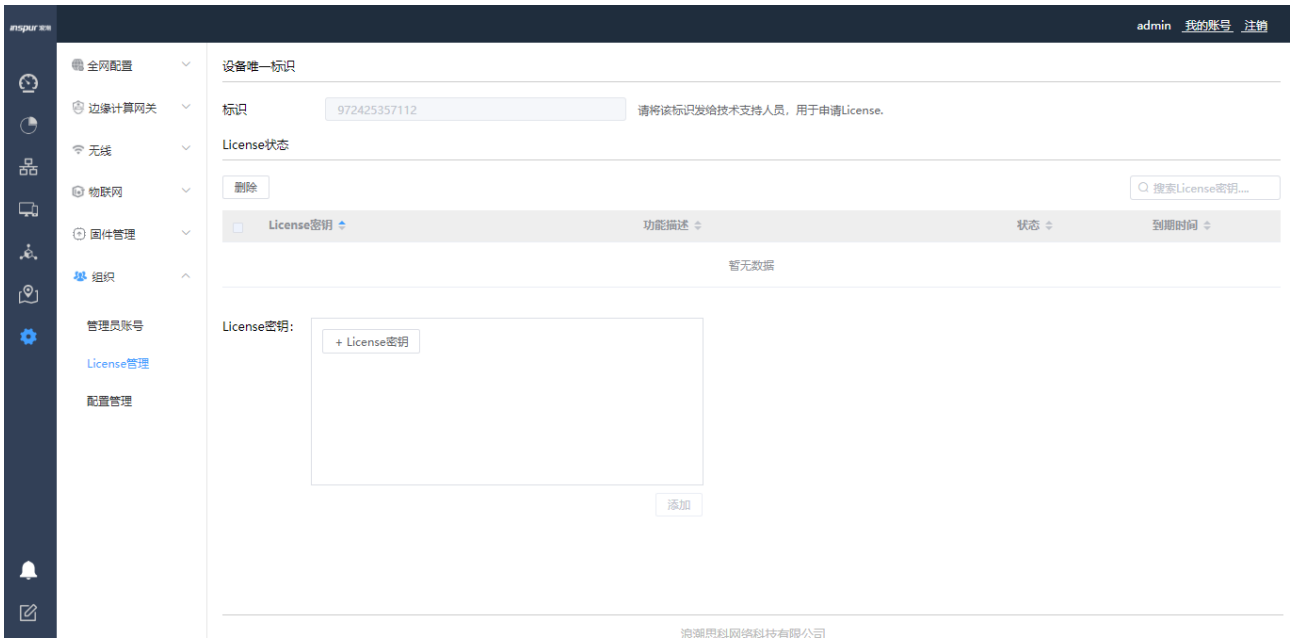
### 2.4.3.7.6 组织菜单

【管理员账号】菜单-主要功能是创建 Web 登录新账号，与 AC 命令行创建用户功能相互独立，详见如下图所示：

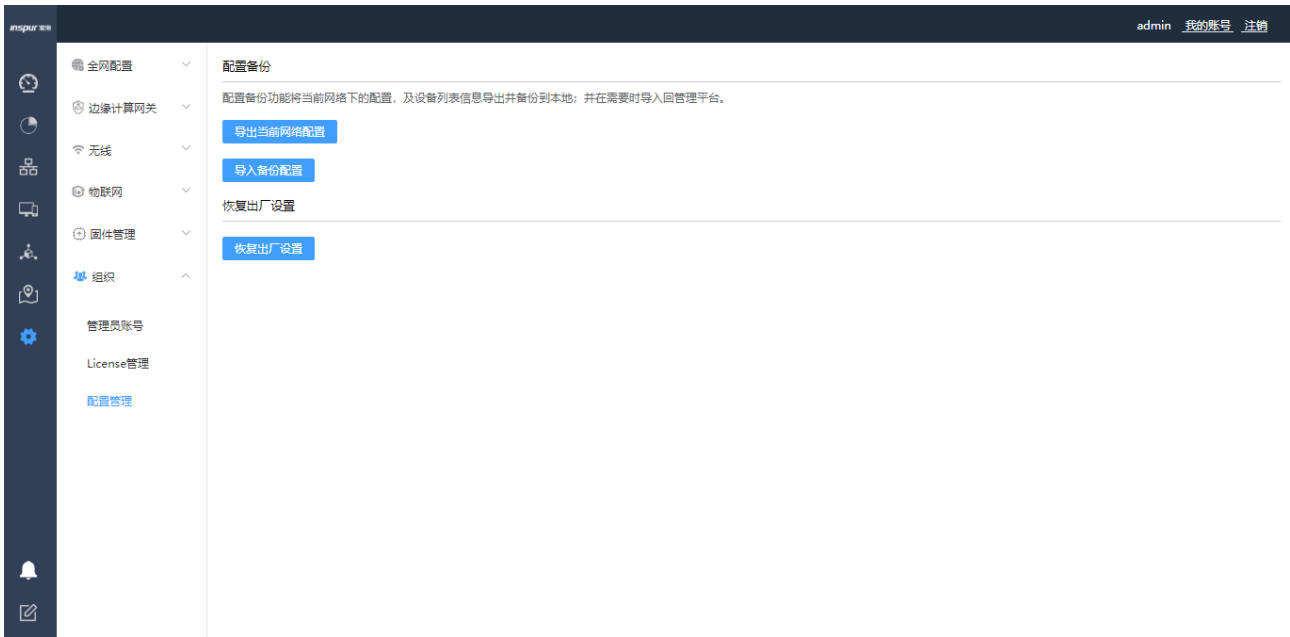




【License 管理】菜单-主要功能是对 AC 进行管理 AP 数据的授权，通过设备唯一标识即 AC 的 device ID，向浪潮产品运营处获取授权，详见如下图所示：



【配置管理】菜单-主要功能是对 AC 业务功能配置进行导入导出，也可进行恢复出厂设置，详见如下图所示：

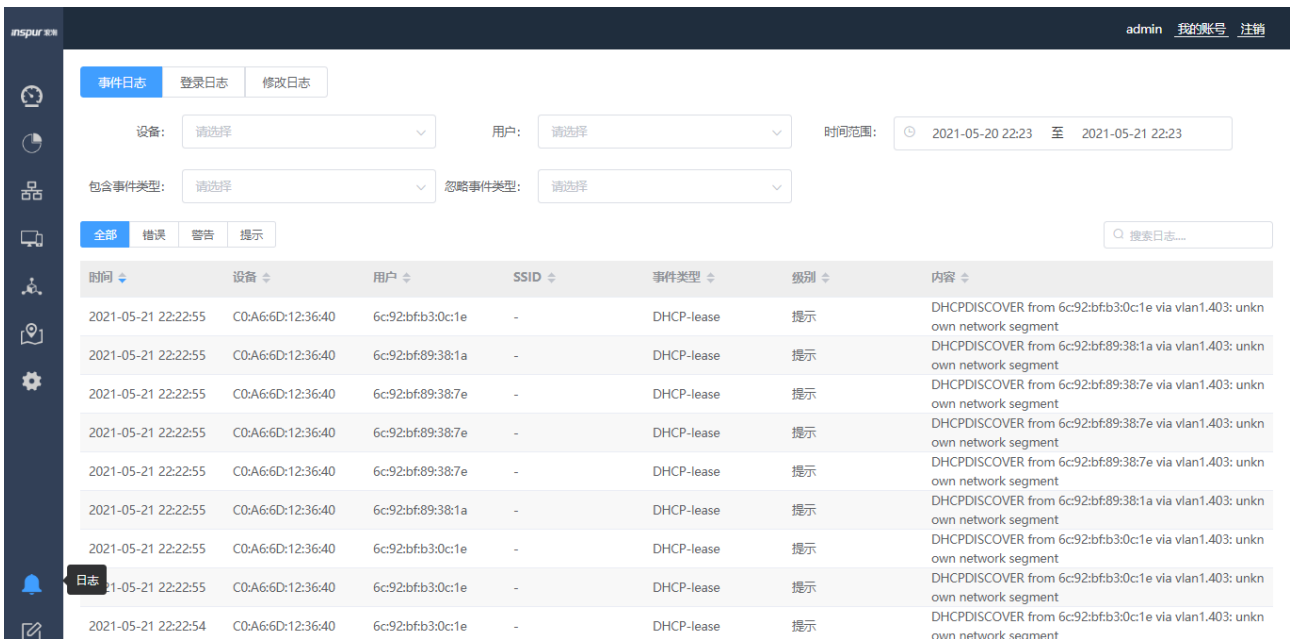


## 2.4.4 功能操作区

主菜单或子菜单中的功能配置或状态查询都在此区域完成，在每个菜单中进行详细介绍；

## 2.4.5 日志和提示功能区

主要分为日志查询和 Web 系统版本查询两个功能，通过<日志>按钮可对系统的事件、登录、修改等日志按不同维度进行查询，如下图所示：



inspur 浪潮 admin 我的账号 注销

事件日志 登录日志 修改日志

Q

名称	IP地址	类型	状态	时间
admin	10.49.11.69	LOGIN	登录成功	2021-04-27 05:24:24
admin	10.49.11.69	LOGIN	登录成功	2021-04-27 06:03:30
admin	111.175.34.151	LOGIN	登录成功	2021-04-20 03:21:48
admin	114.246.69.127	LOGIN	登录成功	2021-04-08 15:25:17
admin	121.60.116.157	LOGIN	登录成功	2021-05-21 05:16:55
admin	121.60.116.157	LOGIN	登录成功	2021-05-21 05:50:53
admin	121.60.116.157	LOGIN	登录成功	2021-05-21 08:53:45
admin	121.60.116.157	LOGIN	登录成功	2021-05-21 10:04:59
admin	121.60.116.157	LOGIN	登录成功	2021-05-21 10:10:21
admin	121.60.116.157	LOGIN	登录成功	2021-05-21 10:34:25

共 20 条 10条/页 < 1 2 > 前往 1 页

浪潮网络科技股份有限公司

inspur 浪潮 admin 我的账号 注销

事件日志 登录日志 修改日志

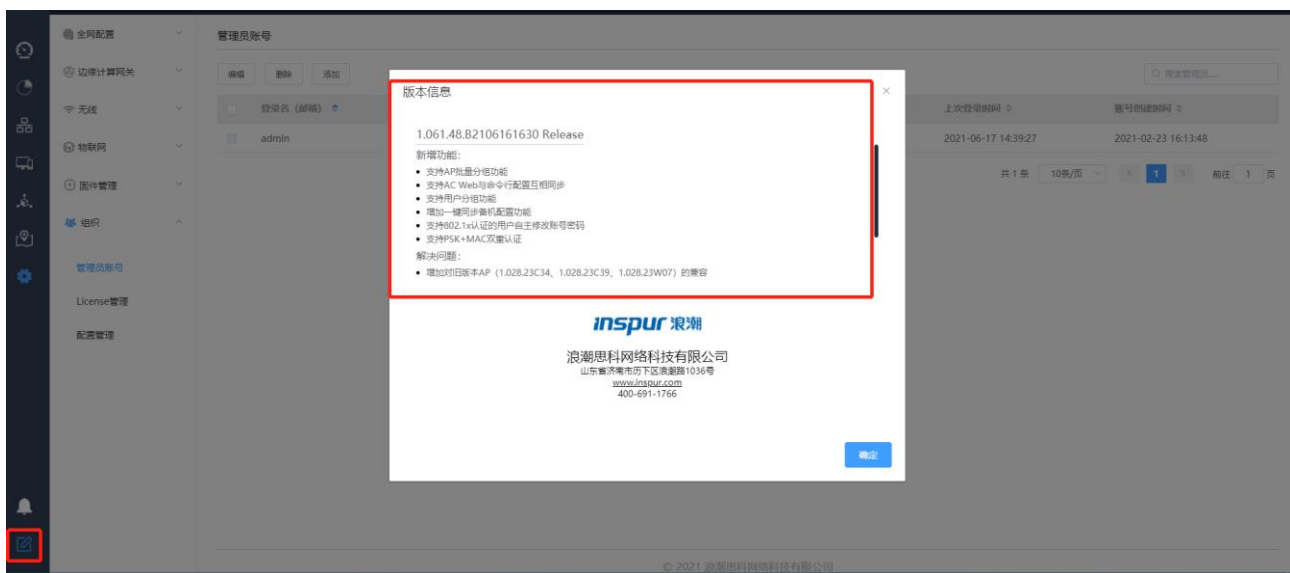
Q

时间	管理员	网络	SSID	页数	标签	历史值	当前值
暂无数据							

共 0 条 10条/页 < 1 > 前往 1 页

浪潮网络科技股份有限公司

通过<提示>按钮可对 Web 系统的版本进行查询，如下图所示：



## 2.5 配置命令介绍

### 2.5.1 基础配置命令

#### 2.5.1.1 获得帮助

使用问号（？）和方向键，可以帮助输入命令：

- 输入一个问号，获得当前可用的命令列表

XOS>?

- 输入若干已知字符，紧接着输入问号（无空格），显示当前可用的已知字符开头的命令列表。

XOS>e?

- 输入命令，紧跟空格和问号，获得命令参数列表

XOS#show ?

- 按下 up 方向键，可显示前面输入的命令。

#### 2.5.1.2 命令模式

AC 命令行界面可分为多种模式。每种命令模式允许在设备上配置不同的组件，当前可用的命令取决于所处的命令模式。输入问号（？）可以在每种命令模式下显示可用的命令列表。下表列出了常用的命令模式：

操作	进入方式	界面提示符	描述
用户模式	登录	XOS>	
特权模式	在用户模式下输入 enable 命令	XOS#	

全局配置模式	在特权模式下输入 configure terminal 命令	configure terminal	
端口配置模式	在全局配置模式下，输入 interface 命令，例如 interface eth2 可进入 eth2 端口；	XOS(config)#interface eth2 XOS(config-if)#	
进入 vlan 接口	在全局配置模式下，输入 interface 命令，例如 interface vlan1.2 可进入 vlan 2 接口	XOS(config)#interface vlan1.2 XOS(config-if)#	

### 2.5.1.3 撤销命令

如果想撤销一个命令或恢复为缺省属性，可以在大多数命令前加关键字 no。

例如，no ip dhcp pool

### 2.5.1.4 保存配置

在特权模式下使用 write 命令可以保存配置。

例如：

```
XOS#write
The current configuration will be written to the device. Are you sure? [Y/N]y
flash:/INSPUR.conf exists, overwrite? [Y/N]:y
Save configuration OK
```

## 2.5.2 设备管理命令

### 2.5.2.1 配置 vlan 接口 ip

配置举例：配置 vlan3 接口 ip 为 192.168.3.1，掩码为 24 位。

```
XOS>enable
XOS# configure terminal /*在特权模式下进入全局配置模式*/
XOS(config)#interface vlan1.3 /*在全局配置模式下，进入 vlan 3 接口配置模式*/
XOS(config-if)#ip address 192.168.3.1/24 /*在 vlan 3 接口配置模式下，vlan 3 的接口地址*/
```

## 2.5.2.2 NAT 配置

### 功能描述

NAT 功能可以根据指定的规则将报文的源地址或目的地址进行替换。这使得用私网地址组建的内网可以通过指定的公网地址访问外网，通过将源地址改为公网 IP 而减少 IP 地址的消耗和减少路由数量。反过来也可以让公网主机访问到私网内的指定主机。

### 配置 NAT

```
XOS>enable
XOS#configure terminal
XOS(config)#interface vlan1.2
XOS(config-if)#ip address 192.168.1.196/24
XOS(config-if)#ip nat outside           //将指定 vlan 口设置为外网口
XOS(config-if)#quit
XOS(config)#ip nat inside source list 4093 interface vlan1.4093 overload     //配置 NAT 规则
```

## 2.5.2.3 静态路由配置

### 功能描述

静态路由允许管理员在设备上配置静态路由信息。若没有特别指定的话，静态路由信息的优先级是除了直连路由外最高的，比动态路由信息具有更高的优先级。在小型网络中，配置静态路由可以为网络提供很好的稳定性。

### 配置静态路由

静态路由信息可以在配置视图下直接配置，但配置是否生效要根据配置是否满足下一跳 IP 是否在本地网段内和路由优选两个判断条件。此外静态路由配置命令支持为路由配置优先级。涉及以下命令。

配置举例：

配置到网关 192.168.1.1 的默认路由。

```
XOS>enable
XOS#configure terminal
XOS(config)#ip route 0.0.0.0/0 192.168.1.1
```



## 2.5.2.4 端口配置

配置举例：将 eth2 口配置为 trunk 类型，允许通过的 vlan 为 1-9，默认 vlan 为 1。

```
XOS>enable
XOS#configure terminal
XOS(config)# interface eth2
XOS(config-if)# switchport mode trunk //端口类型为 trunk
XOS(config-if)# switchport trunk allowed vlan add 1 to 9 //允许通过的 vlan
XOS(config-if)# switchport trunk pvid 1 //默认 vlan
```

## 2.5.3 WLAN 基本业务配置命令

### 2.5.3.1 终端在线状态

配置举例：查看所有终端状态

```
XOS>enable
XOS#show wlan client all
Total Number of Clients      : 1
MacAddr      BSSID      IP      State      Online Time
-----
6c6a.7751.f586  1c88.795b.0031  10.110.33.93  Associated  49h33m46s
```

可查看终端的当前在线的终端数量、MAC 地址、所关联的 BSSID、终端的 IP 地址、关联状态、在线时间。

### 2.5.3.2 wlan 服务模板配置

配置举例：将 wlan 服务模板 1 配置 ssid 名称为 test，限制 ssid 接入终端数为 50，psk 认证密码为 11111111，二层桥接（本地转发）模式，业务 vlan 为 3，开启 ssid 下行限速 10Mbps，上行限速 5Mbps。

```
XOS>enable
XOS#configure terminal
XOS(config)#wlan service-profile 1 //对应 web 上第一个 ssid
```

```

XOS(wlan-service-profile)#max-client-count 50 //限制 ssid 接入终端数 ( 默认为 64 )

XOS(wlan-service-profile)#service disable //配置时应先去掉使能

XOS(wlan-service-profile)#ssid test //ssid 名称

XOS(wlan-service-profile)#air-security-policy wpa2-psk //关联接入方式为预共享密钥 wpa2-psk

XOS(wlan-service-profile)#cipher-suite ccmp //加密类型

XOS(wlan-service-profile)#client-forwarding-mode local-data //本地转发

XOS(wlan-service-profile)#pre-shared-key pass-phrase 11111111 //密钥

XOS(wlan-service-profile)#vlan-pool 3 //对应 WEB 中寻址和流量策略-VLAN 标记中配置的 VLAN

XOS(wlan-service-profile)#traffic-limit ssid-based inbound 5120 //上行限速 5Mbps ( ssid-based 为每 ssid
限速 , user-based 为每终端宽带限速 )

XOS(wlan-service-profile)#traffic-limit ssid-based outbound 10240 //下行限速 10Mbps( ssid-based 为每 ssid
限速 , user-based 为每终端宽带限速 )

XOS(wlan-service-profile)#service enable //使能

```

### 2.5.3.3 DHCP 配置

配置举例：地址池名称为 vlan100，子网为 192.168.100.0/24，可分配 IP 地址段为 192.168.100.101-192.168.100.200，默认网关为 192.168.100.1，租约时间为 1 天，DNS 服务器为 114.114.114.114。

```

XOS>enable

XOS#configure terminal

XOS(config)#service dhcp //开启 DHCP

XOS(config)#ip dhcp pool vlan100 //地址池名称

XOS(dhcp-config)#network 192.168.100.0/24 //子网

XOS(dhcp-config)#range 192.168.100.101 192.168.100.200 //可分配 IP 地址段

XOS(dhcp-config)#default-router 192.168.100.1 //默认网关

```

```
XOS(dhcp-config)#lease-time 1 0 0 0 //租约时间
XOS(dhcp-config)#dns-server 114.114.114.114 //DNS 服务器
```

### 2.5.3.4 射频配置

配置举例：针对型号为 IAP5820i-E、name 为 C0A66D01E500 的 AP，配置 2.4GHz 信道为 6，发射功率为 20dBm，5GHz 信道和发射功率为默认配置

```
XOS>enable
XOS#configure terminal
XOS(config)#wlan ap C0A66D01E500 model iap5820i-e apid 1 //包含 AP 名称、型号、apid
XOS(config)#mac-address c0a6.6d01.e500 //AP mac 地址为 mac-address c0a6.6d01.e500
XOS(wlan-ap)# radio 1 type 80211gn //radio 1 为 2.4GHz 802.11gn
XOS(wlan-ap-radio)# channel 6 //信道为 6
XOS(wlan-ap-radio)# max-power 20 //发射功率为 20dBm ( 100mW )
XOS(wlan-ap-radio)# enable //开启使能
XOS(wlan-ap-radio)# radio 2 type 80211ac //radio 2 为 5GHz 802.11ac
XOS(wlan-ap-radio)#enable //开启使能，信道和发射功率为自动
```

## 2.5.4 AP 管理配置命令

### 2.5.4.1 查看 AP 在线状态

配置举例：

```
XOS>enable
XOS#show wlan ap all //可以查看当前 AP 在线状态
NA:Never Assoc NI:No Ip I:Idle J:Join ID:Image Download C:Config
DC:Data Check R:Running RS:Reset M:Master S:Slave
Running/Total APs :0/2
ID Name MAC IP Model Time State
-----
```

1	C0A66D01E500	c0a6.6d01.e500	192.168.1.191	iap5820i-e	1h0m0s	R/M
2	111111111111	1111.1111.1111	0.0.0.0	iap5820i-e	0h0m0s	NA

状态说明:

NA:Never Assoc	//AP 未关联 AC
NI:No Ip	//无 IP 地址
I:Idle	//空闲状态, 当前 AP 为离线状态
J:Join	//CAPWAP 连接建立状态
ID:Image Download	//版本下载状态
C:Config	//初始化配置下载状态
DC:Data Check	//数据校验状态
R:Running	//运行状态, 表示 AP 与 AC 成功建立 CAPWAP 隧道
RS:Reset	//不涉及
M:Master	//主用状态, 表示当前 AC 为 AP 的主 AC
S:Slave	//备用状态, 表示当前 AC 为 AP 的备 AC

## 2.5.4.2 重启 AP

配置举例: 可以在 AC 的命令行中通过 `clear wlan ap [all][name]` 命令重启所有 AP 或具体某个 AP。

```
XOS>enable

XOS#clear wlan ap all //重启所有 AP

XOS#clear wlan ap name C0A66D01E500 //重启 Name 为 C0A66D01E500 的 AP
```

## 2.5.5 主备 AC 配置同步 (WLAN 部分)

配置方法: 登录主 AC, 输入 `hot-backup sync config` 命令进行配置同步。

```
XOS>enable //进入特权模式

XOS#hot-backup sync config //下发配置同步操作指令
```

注意:

- 1、配置同步需要在主 AC 下进行
- 2、当前支持的配置同步内容:
  - (1) WLAN 配置同步 (使能和关闭、外接 RADIUS 服务器认证方式时 mac 认证模板的增加、删除或修改)
  - (2) 射频配置同步 (信道、功率等)
  - (3) ap 配置同步 (AP 的增加与删除)

## 2.5.1 常用的状态查询命令

### 1、查看 Device ID

```
XOS#show device id
Device ID:1039165640027
```

### 2、查看设备型号、MAC、SN 等信息

```
XOS#show device manuinfo
```

### 3、查看 License 许可数量

```
XOS#show license wlan
```

### 4、查看接口状态

```
XOS#show interface brief
```

### 5、查看设备运行状态

```
XOS#start-shell
~ # top //可查看内存、CPU 使用情况
Mem: 770008K used, 2182620K free, 0K shrd, 2232K buff, 268044K cached
CPU:  0.0% usr  0.3% sys  0.0% nic 98.8% idle  0.0% io  0.3% irq  0.2% sirq
Load average: 0.00 0.00 0.00 1/90 19354
  PID  PPID  USER      STAT   VSZ  %VSZ CPU  %CPU COMMAND
19354 19353 root       R      2564  0.0  0  0.3 top
```

## 2.5.2 常用的排障命令

### 1、抓包命令

操作方法：进入 start-shell，通过 tcpdump 命令抓包

```
tcpdump tcp -i eth2 -t -s 0 -c 100 and dst port ! 22 and src net 192.168.1.0/24 -w ./target.pcap
```

(1)tcp: ip icmp arp rarp 和 tcp、udp、icmp 这些选项等都要放到第一个参数的位置，用来过滤数据报的类型

(2)-i eth2：只抓经过接口 eth2 的包

(3)-t：不显示时间戳

(4)-s 0：抓取数据包时默认抓取长度为 68 字节。加上-S 0 后可以抓到完整的数据包

(5)-c 100：只抓取 100 个数据包

(6)dst port ! 22：不抓取目标端口是 22 的数据包

(7)src net 192.168.1.0/24：数据包的源网络地址为 192.168.1.0/24

(8)-w ./target.pcap：保存成 pcap 文件，方便使用 wireshark 分析

```
~ # tcpdump tcp -i eth2 -t -s 0 -c 100 and dst port ! 22 and src net 192.168.1.0/24
```

```

tcpdump: WARNING: eth2: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
IP 192.168.1.251.58726 > 192.168.1.196.2222: Flags [P.], seq 870525834:870525950, ack 2129546362, win 16652, options [nop,nop,TS val 300326066 ecr 145403849], length 116, RPKI-RTR
IP 192.168.1.196.2222 > 192.168.1.251.58726: Flags [P.], seq 1:293, ack 116, win 423, options [nop,nop,TS val 145406350 ecr 300326066], length 292, RPKI-RTR
IP 192.168.1.251.58726 > 192.168.1.196.2222: Flags [.], ack 293, win 16579, options [nop,nop,TS val 300326086 ecr 145406350], length 0
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel

```

## 2、debug 日志信息收集

命令：

XOS#debug wlan all //开启 wlan 模块的 debug 功能（命令前加 no 可关闭 debug）

XOS#terminal monitor //输出调试信息

以终端关联 psk 认证的 ssid 的过程为例：

```

XOS#debug wlan all
XOS#terminal monitor
XOS#2021/06/22 10:49:27 informational: WMAC_AC: Receiving authentication frame from station
f8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 informational: WMAC_AC: New STA
2021/06/22 10:49:27 informational: WMAC_AC: Authentication OK (Open-System) with bssid
64:a3:41:ae:41:22 .
2021/06/22 10:49:27 errors : WMAC_AC: Receiving association request from sta f8:95:ea:a5:6f:5c
2021/06/22 10:49:27 errors : WMAC_AC: Receiving association request from sta f8:95:ea:a5:6f:5c,
seq [0x807f]
2021/06/22 10:49:27 errors : WMAC_AC: IEEE 802.11 element parse ignored unknown element
(id=127 elen=8)
2021/06/22 10:49:27 errors : WMAC_AC: IEEE 802.11 element parse ignored unknown element
(id=191 elen=12)
2021/06/22 10:49:27 errors : WMAC_AC: Unknown vendor specific information element ignored
(vendor OUI 00:17:f2 len=11)
2021/06/22 10:49:27 errors : WMAC_AC: Unknown Broadcom information element ignored (type=4
len=5).
2021/06/22 10:49:27 errors : WMAC_AC: Unknown vendor specific information element ignored
(vendor OUI 00:10:18 len=9)
2021/06/22 10:49:27 informational: WMAC_AC: Station association succeed with AID: 1, SSID: Unconfigd
SSID7, BSSID: 64:a3:41:ae:41:22.
2021/06/22 10:49:27 notifications: WMAC_AC: [IPC] Sending ADD-STATION to AP by CAPWAP with
station MAC f8:95:ea:a5:6f:5c, AID 1 and APID 61 RID 2. assoseq [0x807f]
2021/06/22 10:49:27 informational: WMAC_AC: STA f8:95:ea:a5:6f:5c - event 1 notification
2021/06/22 10:49:27 informational: WMAC_AC: Unauthorizing port for station f8:95:ea:a5:6f:5c.

```

```

2021/06/22 10:49:27 informational: WMAC_AC: Sending 1/4 msg of 4-Way Handshake.
2021/06/22 10:49:27 informational: WMAC_AC: Receiving EAPOL-Key frame (2/4 Pairwise) from
stationf8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 notifications: WMAC_AC: WPA: PTK derivation A1 : 64:a3:41:ae:41:22 A2 :
f8:95:ea:a5:6f:5c
2021/06/22 10:49:27 informational: WMAC_AC: Success to verify key MIC.
2021/06/22 10:49:27 informational: WMAC_AC: Recving 2/4 msg of 4-Way Handshake
2021/06/22 10:49:27 informational: WMAC_AC: Sending 3/4 msg of 4-Way Handshake
2021/06/22 10:49:27 informational: WMAC_AC: STA f8:95:ea:a5:6f:5c - sending 3/4 msg of 4-Way
Handshake
2021/06/22 10:49:27 informational: WMAC_AC: Receiving EAPOL-Key frame (4/4 Pairwise) from
stationf8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 informational: WMAC_AC: Updating station key for station f8-95-ea-a5-6f-5c .
2021/06/22 10:49:27 notifications: WMAC_AC: [IPC] Sending ADD-STATION to AP by CAPWAP with
station MAC f8:95:ea:a5:6f:5c, AID 1 and APID 61 RID 2. assoseq [0x807f]
2021/06/22 10:49:27 informational: WMAC_AC: Updateing group key for BSS 64-a3-41-ae-41-22 .
2021/06/22 10:49:27 notifications: WMAC_AC: Updating WLAN Group key with key index 1.
2021/06/22 10:49:27 notifications: WMAC_AC: [IPC] Sending UPDATE-WLAN to AP by CAPWAP with
ssid Unconfigd SSID7 and APID 61.
2021/06/22 10:49:27 informational: WMAC_AC: AP-STA-CONNECTED f8:95:ea:a5:6f:5c
2021/06/22 10:49:27 informational: WMAC_AC: Authorizing port for station f8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 informational: WMAC_AC: STA f8:95:ea:a5:6f:5c - Pairwise key handshake
completed (RSN)

```

## 2.6 开局向导

### 2.6.1 无线网络规划

无线项目开局前，与客户确定网络拓扑及网络规划，AC 通常旁挂在核心/汇聚交换机，由 DHCP 服务器提供 AP 及终端的地址。

配置项	规划说明
管理 VLAN	管理 VLAN 用于设备管理使用，建议和业务 VLAN 分开。
业务 VLAN	终端业务 VLAN，该 VLAN 在 ssid 中配置，可根据不同的业务划分多个不同的业务 VLAN
AC 的源接口	VLANIF 管理_vlan: x.x.x.x/x (192.168.1.0/24) AC 上配置到网关的静态路由
DHCP 服务器	通常由核心、汇聚、DHCP SERVER 等为 AP 和终端分配 IP 地址
AP 的 IP 地址池	AP 的管理地址池规划：与 AC 同网段或跨三层（跨三层时需要在 dhcp 中配置 option43 选项）

STA 的 IP 地址池	终端的业务地址池规划，需充分考虑到可能连接的终端数量，预留足够的地址
AC 接口配置	AC 与核心互联口需要透传管理 VLAN 和业务 VLAN
核心/AC 接口配置	核心与 AC 互联口需要透传管理 VLAN 和业务 VLAN
POE 交换机接口配置	上行口透传管理 VLAN 和业务 VLAN 下行口透传管理 VLAN 和业务 VLAN，native VLAN 为管理 VLAN
SSID 规划	<p>一般可分为内部办公、物联终端、运维及访客等几类，可根据不同的场景进行区分；</p> <p><b>要点：</b></p> <ol style="list-style-type: none"> <li>1、认证接入方式选择，本地 psk、本地 portal、本地 mac+psk、dot.1x、与第三方统一认证平台适配等；</li> <li>2、转发方式的选择，一般建议选择本地转模式（业务流量不经过 AC），业务需要时才进行选择选择集中模式（业务流量经过 AC），一般选择集中转发时，需根据流量大小评估设备性能是否满足要求；</li> <li>3、根据实际的业务场景对终端带宽进行限定；</li> <li>4、对 AP 进行合理分组，选择相应的分组，下发匹配的 SSID；</li> </ol>

## 2.6.2 配置 AP 上线

### 1、AC 侧局域网配置

路径：【设置】>子菜单【边缘计算网关】>子菜单【局域网】，进入“局域网配置”页面。

The screenshot displays the '局域网配置' (LAN Configuration) page with four main sections highlighted by red boxes:

- VLAN列表 (VLAN List):** Shows a table with columns for VLAN ID and VLAN Name. Existing entries include VLAN 1 (default), VLAN 4 (VLAN004), and VLAN 10 (VLAN10).
- 子网 (Subnet):** Shows a table with columns for Subnet, VLAN ID, Name, Local IP Address, VRRP Status, and VRRP IP Address. Existing entries include 192.168.1.0/24 (VLAN 1, default, 192.168.1.199, enabled) and 10.110.44.1/24 (VLAN 4, vlan4, 10.110.44.199, disabled).
- 端口设置 (Port Settings):** Shows a table with columns for Port, Status, Type, VLAN ID, and Allowed VLANs. Existing entries include eth2, eth3, eth4, and eth5, all with '开启' (Enabled) status and 'Trunk' type, associated with VLAN 1.
- 静态路由 (Static Route):** Shows a table with columns for Status, Description, Subnet, and Next Hop. Existing entries include '启用' (Enabled) with description '描述', subnet 0.0.0.0, and next hop 192.168.1.1.



- a、根据规划表，创建 AC 的管理 VLAN 及子网 ip、创建业务 VLAN  
(注：当使用 portal 认证方式时，需要为该业务 VLAN 配置子网 ip)
- b、配置 AC 与核心/汇聚的互联端口，trunk 模式，透传管理和业务 VLAN
- c、配置 AC 到网关的默认路由

## 2、核心汇聚交换机配置

- a、配置无线管理 VLAN、业务 VLAN 及地址池
- b、配置与 AC 互联端口，trunk 模式，透传管理和业务 VLAN
- c、配置与 POE 交换机互联端口，trunk 模式，透传管理和业务 VLAN

## 3、POE 交换机配置

- a、配置无线管理 VLAN、业务 VLAN
- b、配置与核心\汇聚互联端口，trunk 模式，透传管理和业务 VLAN
- c、配置连接 AP 的下行口，trunk 模式，透传管理和业务 VLAN，PVID 或 native vlan 配置为管理 VLAN

## 4、测试网络连通性

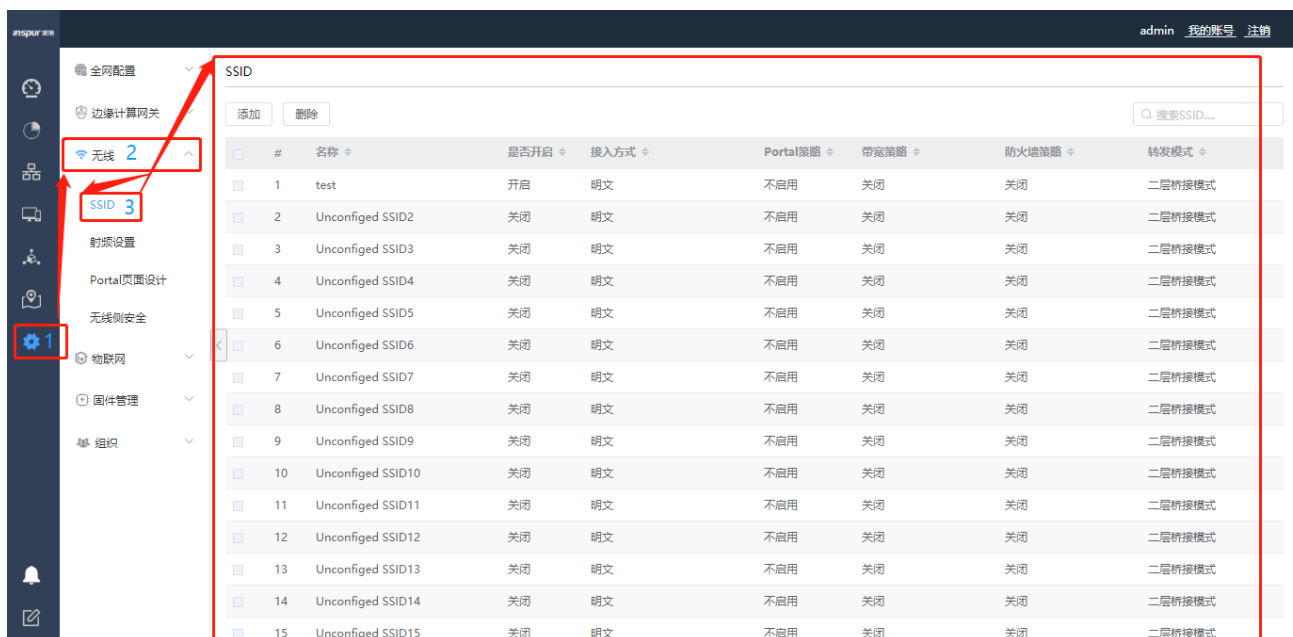
网络配置完成后，检查 AP 是否获取到管理 IP，测试 AP 与 AC 网络连通性。

## 5、导入 AP

可通过模板批量导入 AP，若 AP 出厂版本较老而无法上线，核实 AC 版本是否低于 1.061.48，如低于可直接升级至 1.061.48 或以上版本即可完成 AP 上线，并可对 AP 进行批量升级。

## 2.6.3 SSID 配置

路径：**【设置】** > 子菜单**【无线】** >子菜单**【SSID】**，进入 WLAN 业务配置页面，选择模板配置 SSID。





### 3.1.1.3 组网需求

组网需求：

- AC 组网方式：旁挂二层组网。
- DHCP 部署方式：AC 作为 DHCP 服务器为 AP 分配 IP 地址，SwitchB 作为 DHCP 服务器为 STA 分配 IP 地址。
- 业务数据转发方式：本地转发。
- WLAN 认证方式：WPA-WPA2+802.1X。

### 3.1.1.4 网络规划

配置项	规划数据
管理 VLAN	VLAN100
业务 VLAN	VLAN101
AC 的源接口	VLANIF100: 10.23.100.254/24
DHCP 服务器	AC 作为 DHCP 服务器为 AP 分配 IP 地址，SwitchB 作为 DHCP 服务器为 STA 分配 IP 地址
AP 的 IP 地址池	10.23.100.1~10.23.100.200/24
STA 的 IP 地址池	10.23.101.1~10.23.101.200/24
RADIUS 认证 RADIUS 服务器参数	IP 地址：10.23.103.1 认证端口号：1812 共享密钥：inspur@123
802.1X 接入模板	认证方式：EAP
SSID 名称	SSID 名称：WLAN_test
安全策略	安全策略：WPA-WPA2+802.1X+AES
VAP 模板	转发模式：本地转发 业务 VLAN：VLAN101

### 3.1.1.5 配置思路

- ◇ 配置 AP、AC 和周边网络设备之间实现网络互通。

- ✧ 配置 AC 局域网
- ✧ 配置 AP 在 AC 上线。
- ✧ 在 AC 上配置 WLAN 相关业务（SSID）。
- ✧ 配置第三方认证服务器。

### 3.1.1.6 操作步骤

#### 3.1.1.6.1 配置周边设备

# 配置接入交换机 SwitchA 的接口 GE0/0/1 和 GE0/0/2 加入 VLAN100 和 VLAN101。

```
inspur# enable

inspur# configure terminal

inspur(config)# hostname SwitchA

SwchA(config)# vlan database

SwchA(config-vlan)# vlan 100-101

SwchA(config-vlan)# quit

SwchA(config)# interface eth-0-1

SwchA(config-if)# switchport mode trunk

SwchA(config-if)# switchport trunk native vlan 100

SwchA(config-if)# switchport trunk allowed vlan add 100-101

SwchA(config-if)# quit

SwchA(config)# interface eth-0-2

SwchA(config-if)# switchport mode trunk

SwchA(config-if)# switchport trunk allowed vlan add 100-101

SwchA(config-if)# quit
```

# 配置汇聚交换机 SwitchB 的接口 GE0/0/1 加入 VLAN100 和 VLAN101, GE0/0/2 加入 VLAN100 和 VLAN102, GE0/0/3 加入 VLAN103, GE0/0/4 加入 VLAN104, 创建 VLANIF102、VLANIF103 和 VLANIF104 接口, 并配置下一跳为 Router 的缺省路由。

```
inspur# enable

inspur# configure terminal

inspur(config)# hostname SwitchB
```

```
SwchB(config)# vlan database
SwchB(config-vlan)# vlan 100-104
SwchB(config-vlan)# quit
SwchB(config)# interface eth-0-1
SwchB(config-if)# switchport mode trunk
SwchB(config-if)# switchport trunk allowed vlan add 100-101
SwchB(config-if)# quit
SwchB(config)# interface eth-0-2
SwchB(config-if)# switchport mode trunk
SwchB(config-if)# switchport trunk allowed vlan add 100
SwchB(config-if)# switchport trunk allowed vlan add 102
SwchB(config-if)# quit
SwchB(config)# interface eth-0-3
SwchB(config-if)# switchport mode trunk
SwchB(config-if)# switchport trunk native vlan 103
SwchB(config-if)# switchport trunk allowed vlan add 103
SwchB(config-if)# quit
SwchB(config)# interface eth-0-4
SwchB(config-if)# switchport mode trunk
SwchB(config-if)# switchport trunk native vlan 104
SwchB(config-if)# switchport trunk allowed vlan add 104
SwchB(config-if)# quit
SwchB(config)# interface vlan 102
SwchB(config-if)# ip address 10.23.102.1/24
SwchB(config-if)# quit
SwchB(config)# interface vlan 103
SwchB(config-if)# ip address 10.23.103.2/24
SwchB(config-if)# quit
SwchB(config)# interface vlan 104
SwchB(config-if)# ip address 10.23.104.1/24
SwchB(config-if)# quit
```

```
SwchB(config)# ip route 0.0.0.0 0.0.0.0 10.23.104.2
```

# 配置 Router 的接口 GE0/0/1 的 IP 地址，并配置指向 STA 网段的静态路由。

```
<Inspur> system-view
[Inspur] sysname Router
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] ip address 10.23.104.2 24
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.23.101.0 24 10.23.104.1
```

### 3.1.1.6.2 配置 DHCP 服务器为 STA 分配 IP 地址

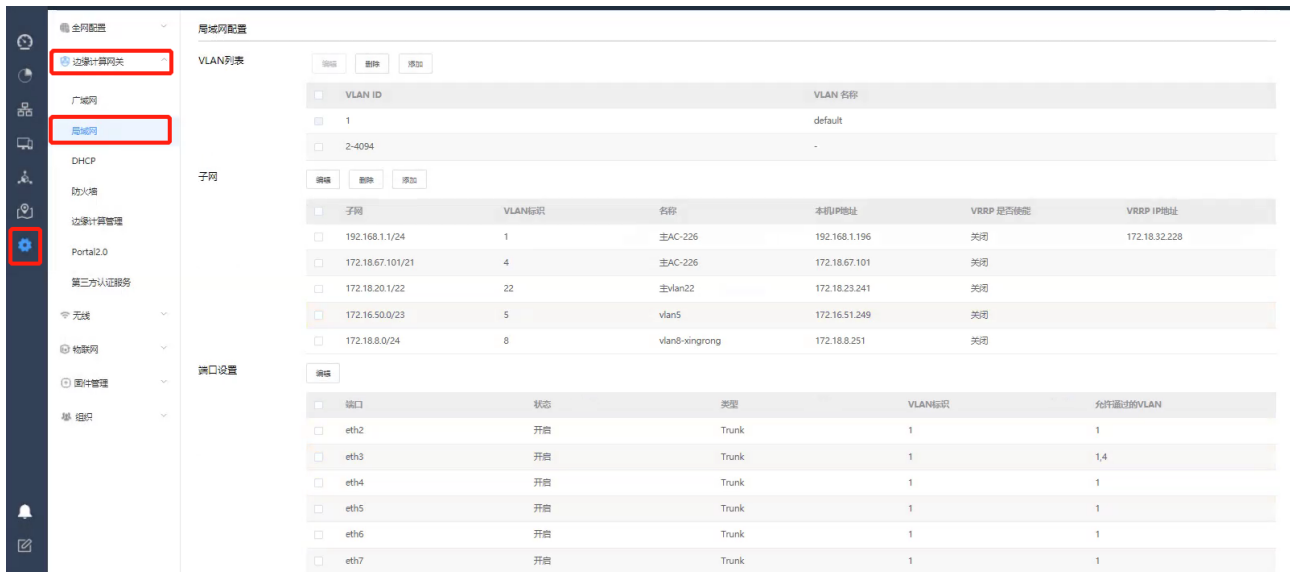
# 在 SwitchB 上配置 Interface Vlan 101 接口为 STA 提供 IP 地址。

```
SwchB# enable
SwchB# configure terminal
SwchB(config)# dhcp server
SwchB(config)# interface vlan 101
SwchB(config)# ip address 10.23.101.254/24
SwchB(config-if)# dhcp server enable
SwchB(config-if)# dhcp excluded-address 10.23.101.251 10.23.101.254
SwchB(config)# dhcp pool yewu_101
SwchB(dhcp-config)# network 10.23.101.0/24
SwchB(dhcp-config)# dns-server 114.114.114.114
SwchB(dhcp-config)# gateway 10.23.101.254
SwchB(dhcp-config)# lease 1 0 0
SwchB(config-if)# quit
```

### 3.1.1.6.3 配置 AC 局域网

1. 进入 AC 局域网配置页面。

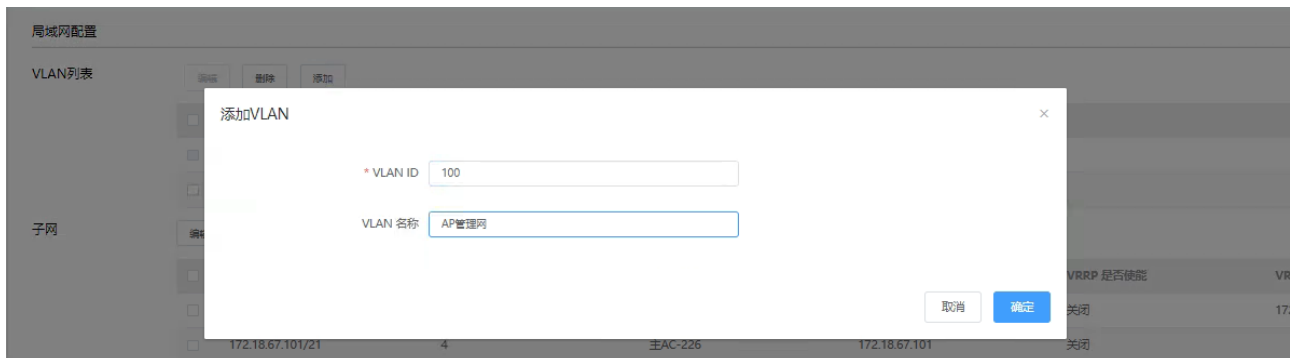
# 登录 AC Web 系统，单击菜单【设置】>子菜单【边缘计算网关】>子菜单【局域网】，进入“局域网配置”页面。



2. 配置网络互联。

a. 首先配置 AP 管理平面接口地址。

# 在“VLAN 列表”，单击选择<添加>按钮，添加 AP 管理平面的 VLAN 100



# 在“子网”中，单击选择<添加>按钮，创建 AP 管理平面的配置虚拟接口 Interface VLAN 100 接口地址 10.23.100.254。

添加子网

\* 名称 AP管理网

\* 子网 10.23.100.0/24

\* 本机IP地址 10.23.100.254

\* VLAN标识 100

VRRP 是否使能 关闭

取消 确定

# 单击<确定>按钮，AP 管理平面接口地址配置完成。

网络配置

边缘计算网关

广域网

局域网

DHCP

防火墙

边缘计算管理

Portal2.0

第三方认证服务

无线

局域网配置

VLAN列表

VLAN ID	VLAN 名称
1	default
2-99	
100	AP管理网
101-4094	

子网

子网	VLAN标识	名称	本机IP地址	VRRP 是否使能	VRRP IP地址
192.168.1.1/24	1	主AC-226	192.168.1.196	关闭	172.18.32.228
10.23.100.0/24	100	AP管理网	10.23.100.254	关闭	

# 以“AP 管理平面接口地址配置”同样的方式创建业务 vlan102 及配置 VLAN 102 接口地址 10.23.102.2/24。

## b.配置 VLAN 及端口

# 选择旁挂核心交换机的连接端口“eth2”，单击<编辑>按钮，选择“接口类型”为“Trunk”，将“eth2”加入 VLAN100（管理 VLAN）和 VLAN101。（如果 AC 直接连接 AP（AP 单独供电或 POE 模块供电时），需要在 AC 直连 AP 的接口上配置缺省 VLAN 为管理 VLAN100）

配置LAN接口 - eth2

\* 使能 开启

\* 类型 Trunk

\* 默认VLAN 1

\* 允许通过的VLAN 100,101

取消 确定



# 单击<确定>，完成配置。

### c.配置静态路由。

# 继续在【局域网】菜单下划鼠标，单击“静态路由”下的<添加>按钮，进入“添加静态路由表”页面。

# 配置“子网”为“10.0.0.0/0”，“下一跳”为“10.23.102.1”。

接口	状态	类型	VLAN标识	允许通过的VLAN
<input checked="" type="checkbox"/> eth2	开启	Trunk	1	100,102
<input type="checkbox"/> eth3	开启	Trunk	1	1,4
<input type="checkbox"/> eth4	开启	Trunk	1	1
<input type="checkbox"/> eth5	开启	Trunk	1	1
<input type="checkbox"/> eth6	开启	Trunk	1	1
<input type="checkbox"/> eth7	开启	Trunk	1	1

使能	描述	子网	下一跳
<input checked="" type="checkbox"/> 开启		0.0.0.0/0	10.23.102.1

# 单击“确定”，完成静态路由表的配置。

# 【局域网】下的所有配置生效需单击页面最下方的<保存>按钮来完成。（**重要提醒!!!**）

## 3. 配置 AP 在 AC 上线

### a.配置 AP 管理网 DHCP 服务:

# 单击菜单【设置】>子菜单【边缘计算网关】>子菜单【DHCP】，进入 DHCP 服务配置页面。

inspur admin 我的账号 注销

全网配置

边缘计算网关

广域网

局域网

DHCP

防火墙

边缘计算管理

Portal2.0

无线

物联网

固件管理

组织

DHCP

\*子网 VLAN 1 (default) 192.168.186.0/24

客户端地址分配 DHCP服务器

网关IP

\*租约时间 4小时

DNS服务器 114.114.114.114 × +DNS服务器

Option43 +Option43

可分配IP地址段	起始IP	终止IP	备注	动作
	192.168.186.100	192.168.186.253		X

添加一个可分配IP地址段

固定IP分配	客户名称	MAC地址	局域网IP	动作

添加一个固定IP

保存

# 选择子网 VLAN 100（AP 管理网）10.23.100.0/24。

inspur admin 我的账号 注销

全网配置

边缘计算网关

广域网

局域网

DHCP

防火墙

边缘计算管理

Portal2.0

无线

物联网

固件管理

组织

DHCP

\*子网 VLAN 100 (AP管理网) 10.23.100.0/24

客户端地址分配 关闭DHCP

保存

浪潮思科网络科技有限公司

# 开启 DHCP 服务器，在“客户端地址分配”选项框选择“DHCP 服务器”。



# 配置 DHCP 服务器各项参数，“租约”、“可分配地址段”为必填项，其余参数可根据需要进行选择配置，点击<保存>按钮完成配置。

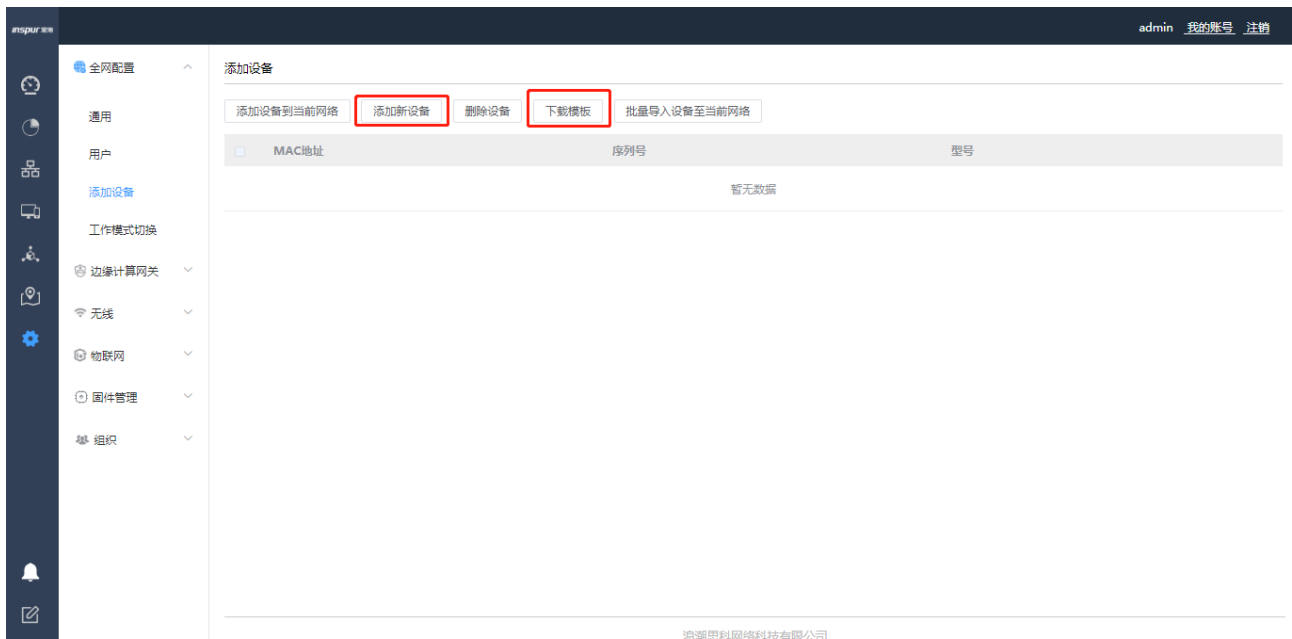


## b.手动添加 AP:

# 单击菜单【设置】>子菜单【全网配置】>子菜单【添加设备】，进入 AP 设备添加界面。



# 通过<添加设备>按钮、或<下载模板>按钮 + <批量导入设备至当前网络>按钮，可进行单个或批量添加 AP 到 AC。



### 添加设备

\* MAC地址

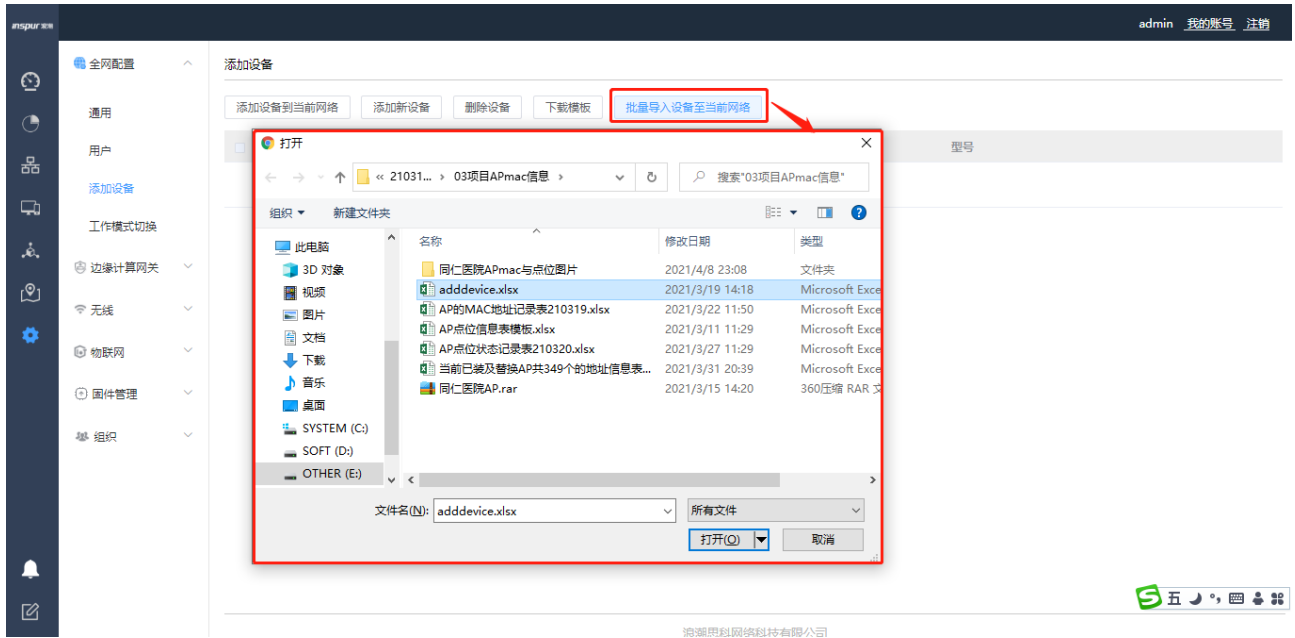
\* 设备类型

# 在 AP 模板文件中填写 AP 信息，示例如下。“MACAddr: 60:de:44:76:e3:60”，“Model: 5920i”，设备类型根据实际进行选择。

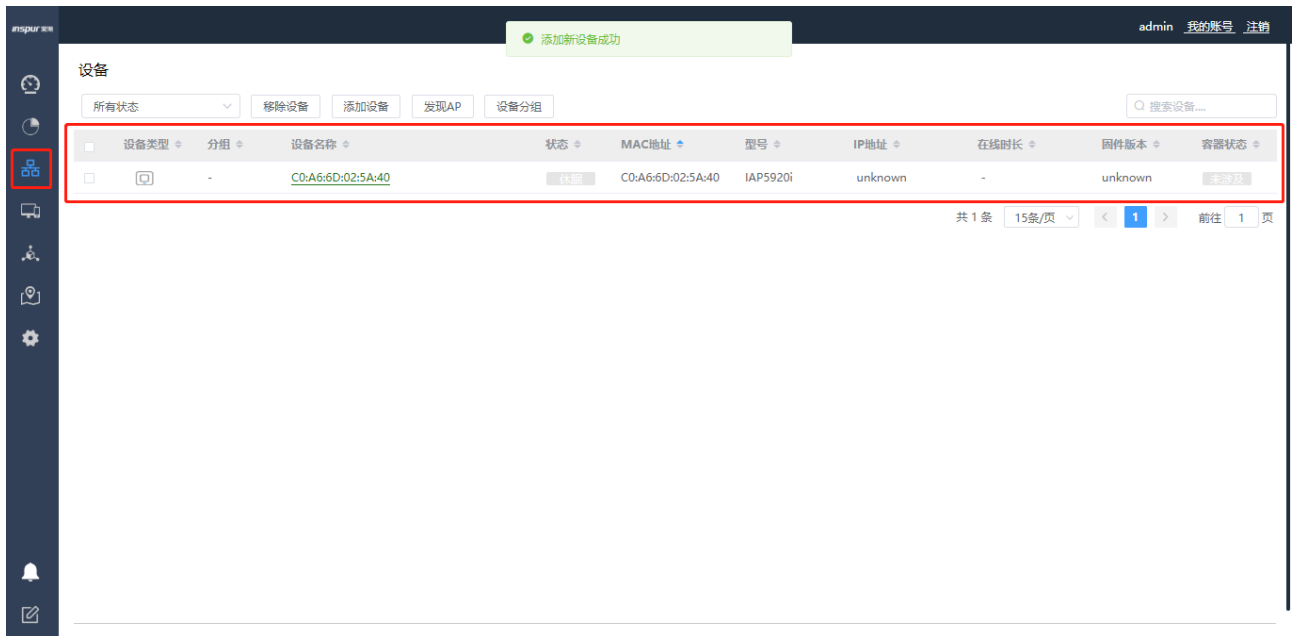
	A	B	C	D	E
1	MacAddr	Model	Name/设备名称 (3-64 characters/字符)	Address/地址 (6-300 characters/字符)	Notes/备注 (6-300 characters/字符)
2					
3					
4					
5					
6					

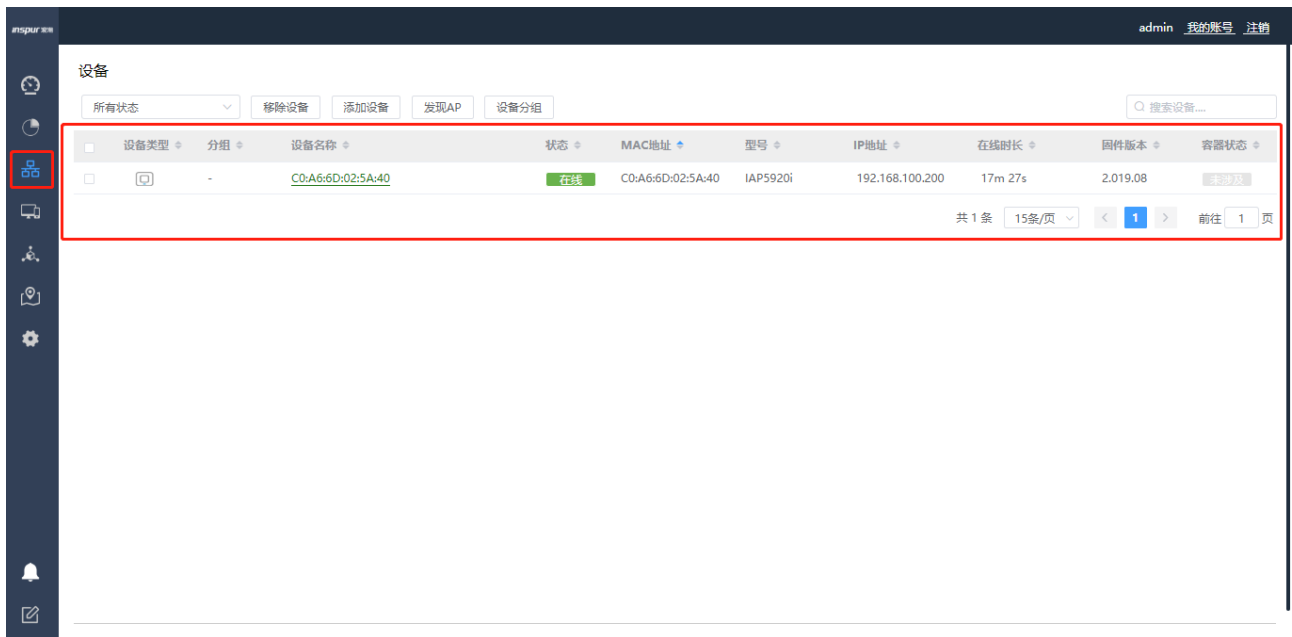
# 如需添加多个 AP，可以参照以上表格及示例在 AP 模板文件中填写多条 AP 信息。

# 单击<批量导入设备至当前网络>按钮，选择填写后的模板文件，单击“打开”。



# 导入完成后，单击菜单【设备】，可查看添加的全部 AP 列表。

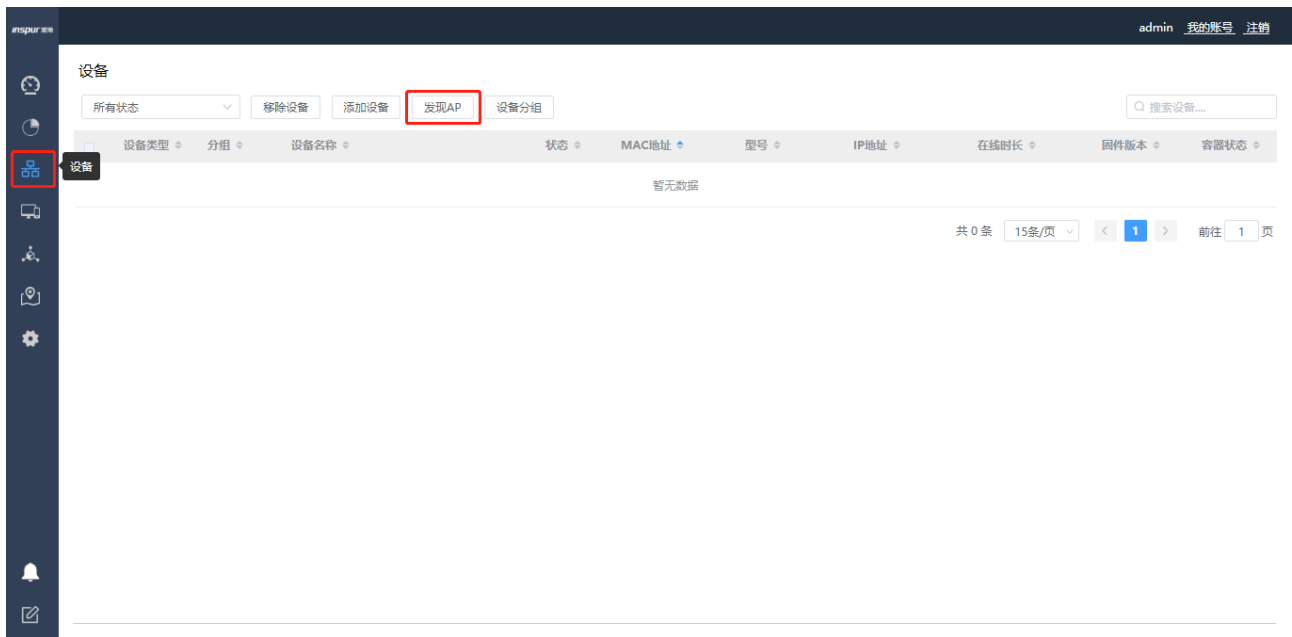




# 网络无异常情况下，几分钟后，AP 将依次上线。

### c.自动添加 AP:

# 单击菜单【设备】，单击<发现 AP>按钮，可进入自动发现 AP 设备界面。



# 在 AP 与 AC 网络连通后，AP 自动获取到 AP 管理网 IP，单击<发现 AP>按钮，可立即发现在线的 AP 设备。

设备

所有状态 移除设备 添加设备 发现AP 设备分组

设备类型 分组 设备名称 状态 MAC地址 型号 IP地址 在线时长 固件版本 容器状态

暂无数据

共 0 条 15条/页 < 1 > 前往 1 页

发现AP 添加AP 刷新 取消

#	MAC地址	IP地址	型号	最近发现时间
1	C0:A6:6D:02:5A:40	192.168.100.200	IAP5920i	2021-05-25 13:04

# 选定发现的 AP，单击<添加>按钮，将 AP 设备添加至 AP 设备列表，刷新 Web 页面，AP 状态变动为在线状态，自动添加 AP 成功。（注意：）

设备

所有状态 移除设备 添加设备 发现AP 设备分组

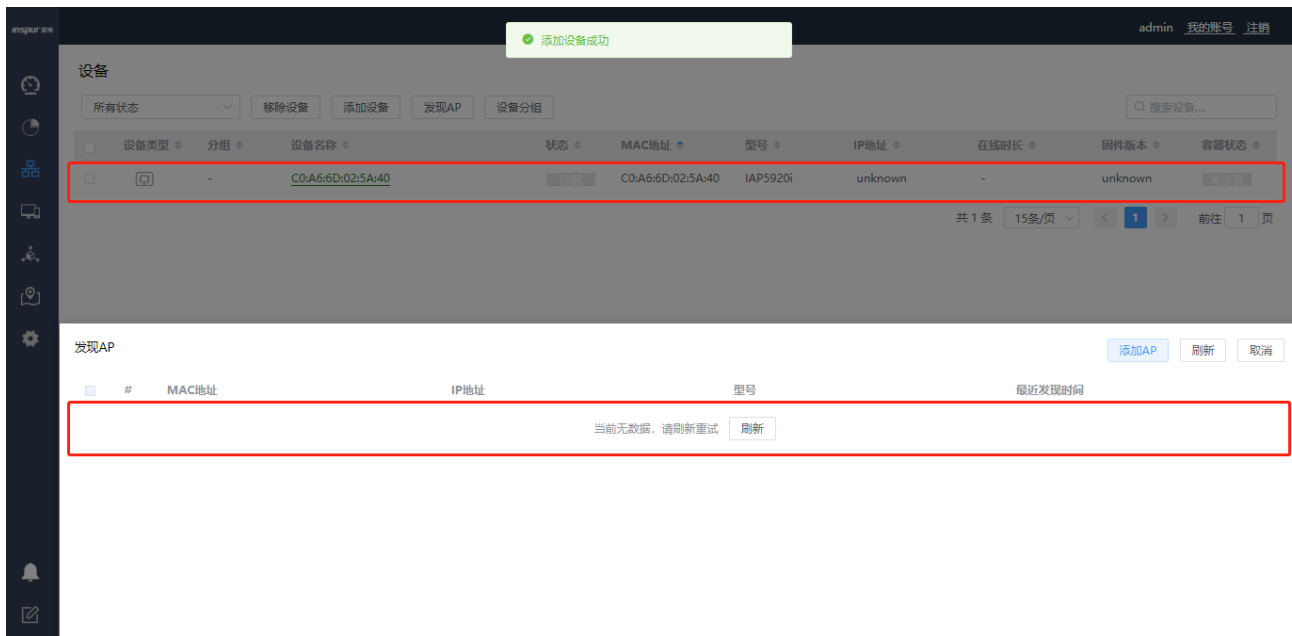
设备类型 分组 设备名称 状态 MAC地址 型号 IP地址 在线时长 固件版本 容器状态

暂无数据

共 0 条 15条/页 < 1 > 前往 1 页

发现AP 添加AP 刷新 取消

#	MAC地址	IP地址	型号	最近发现时间	
<input checked="" type="checkbox"/>	1	C0:A6:6D:02:5A:40	192.168.100.200	IAP5920i	2021-05-25 13:04



inspur 浪潮 admin 我的账号 注销

添加设备成功

设备

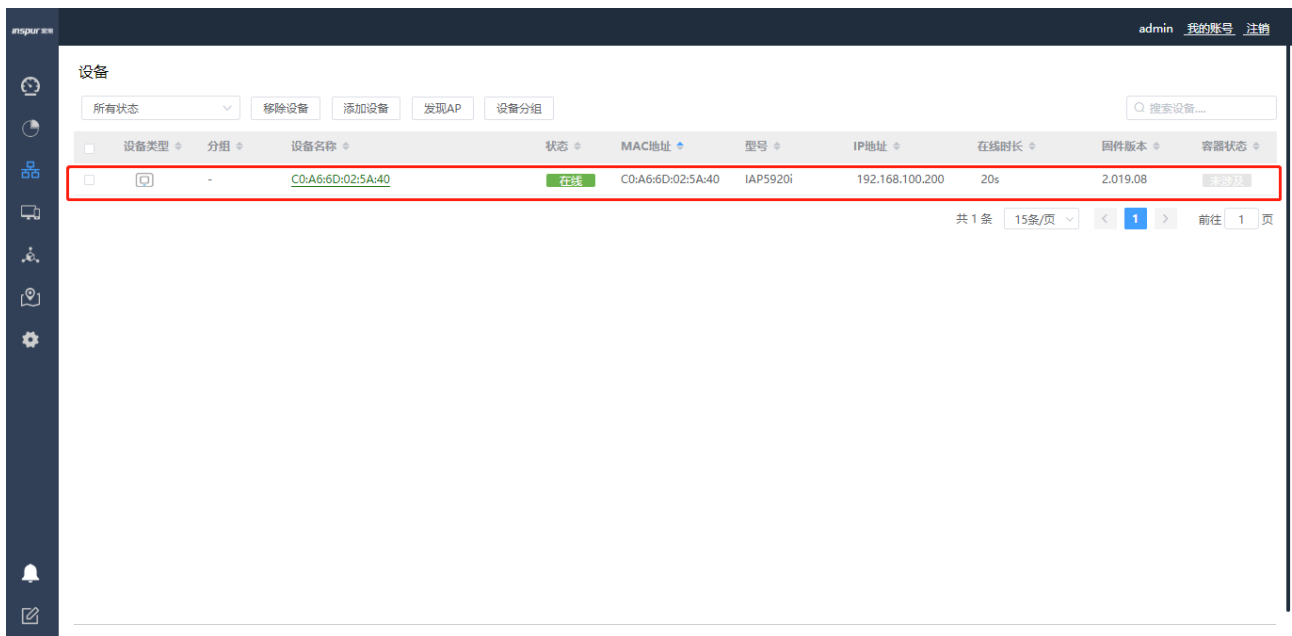
所有状态 移除设备 添加设备 发现AP 设备分组 搜索设备...

设备类型	分组	设备名称	状态	MAC地址	型号	IP地址	在线时长	固件版本	容器状态
			未知	C0:A6:6D:02:5A:40	IAP5920i	unknown	-	unknown	

共 1 条 15条/页 < 1 > 前往 1 页

发现AP 添加AP 刷新 取消

#	MAC地址	IP地址	型号	最近发现时间
当前无数据, 请刷新重试 刷新				



inspur 浪潮 admin 我的账号 注销

设备

所有状态 移除设备 添加设备 发现AP 设备分组 搜索设备...

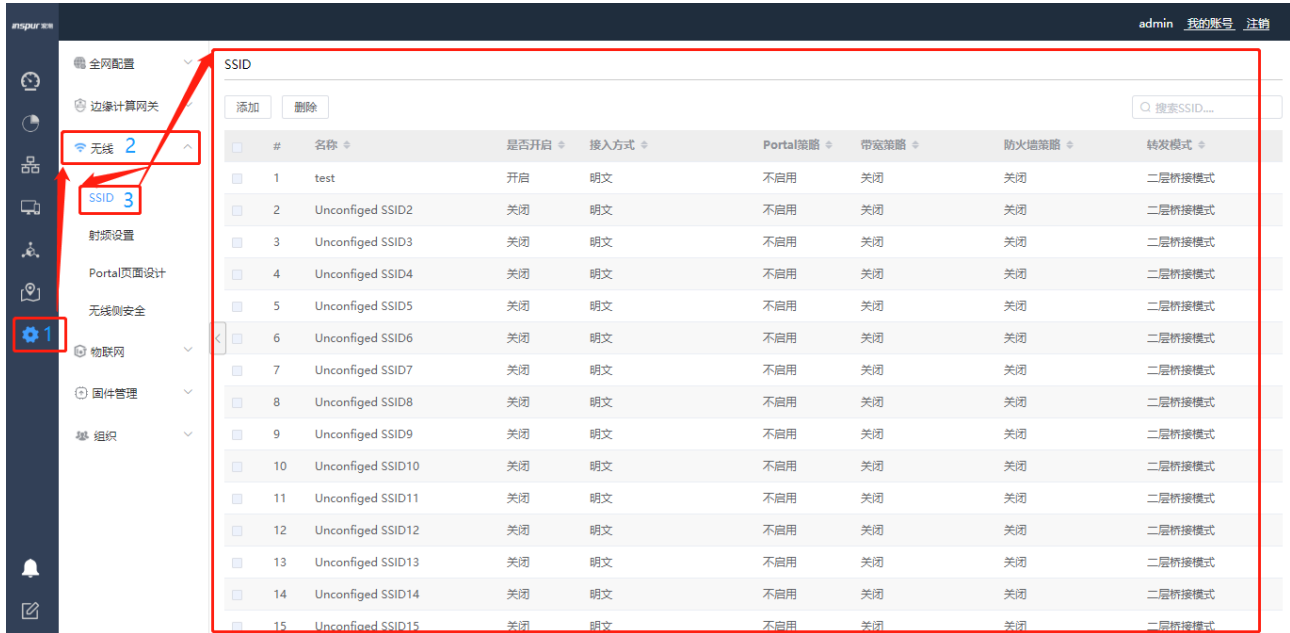
设备类型	分组	设备名称	状态	MAC地址	型号	IP地址	在线时长	固件版本	容器状态
			在线	C0:A6:6D:02:5A:40	IAP5920i	192.168.100.200	20s	2.019.08	非沙箱

共 1 条 15条/页 < 1 > 前往 1 页

### 3.1.1.6.4 配置 WLAN 业务

# 单击菜单【设置】>子菜单【无线】>子菜单【SSID】，进入 WLAN 业务配置页面。





# 系统默认提供 15 个 SSID 模板，可任意选择一个进行修改，也可自行创建新模板；

# 单击任意 SSID 可进入配置 SSID 名称、开关 SSID、是否隐藏、接入控制（开放、预共享密钥、MAC 认证、无感知认证、企业级 WPA2 等）、寻址和流量策略（转发模式、业务 VLAN ID、用户逃生）、防火墙策略、QoS、快速漫游、组播优化、定期关断、在 AP 上绑定等功能。

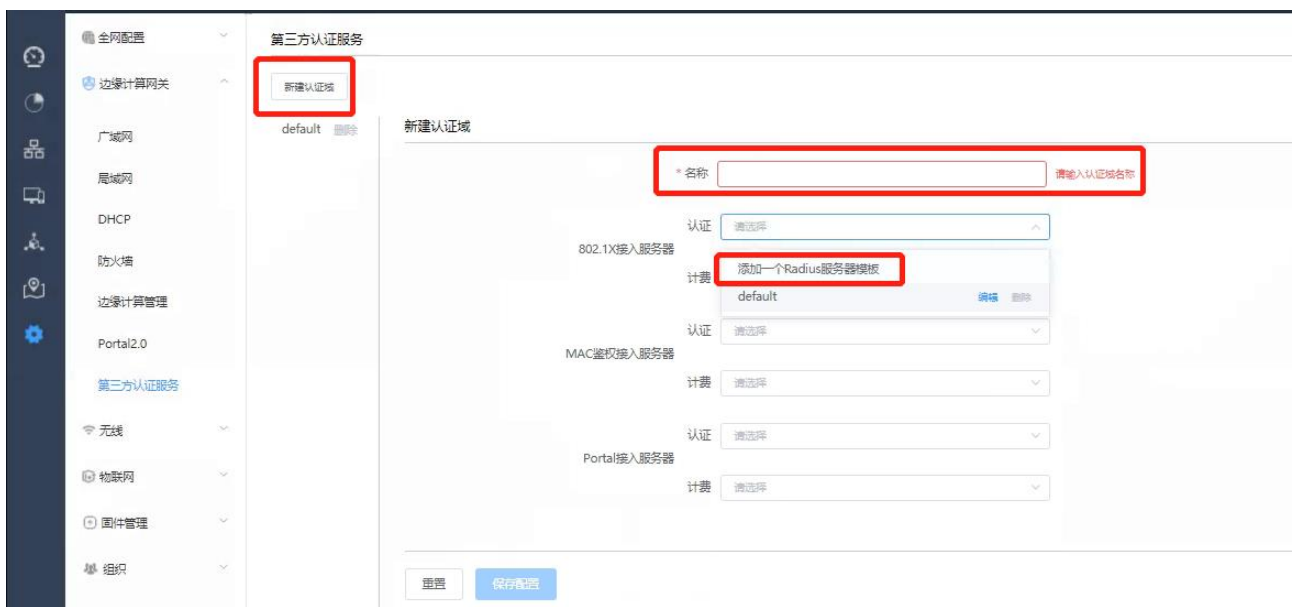
# 配置第三方认证服务器认证域

位置：【设置】>【边缘计算网关】>【第三方认证服务器】配置第三方认证服务器的认证域。

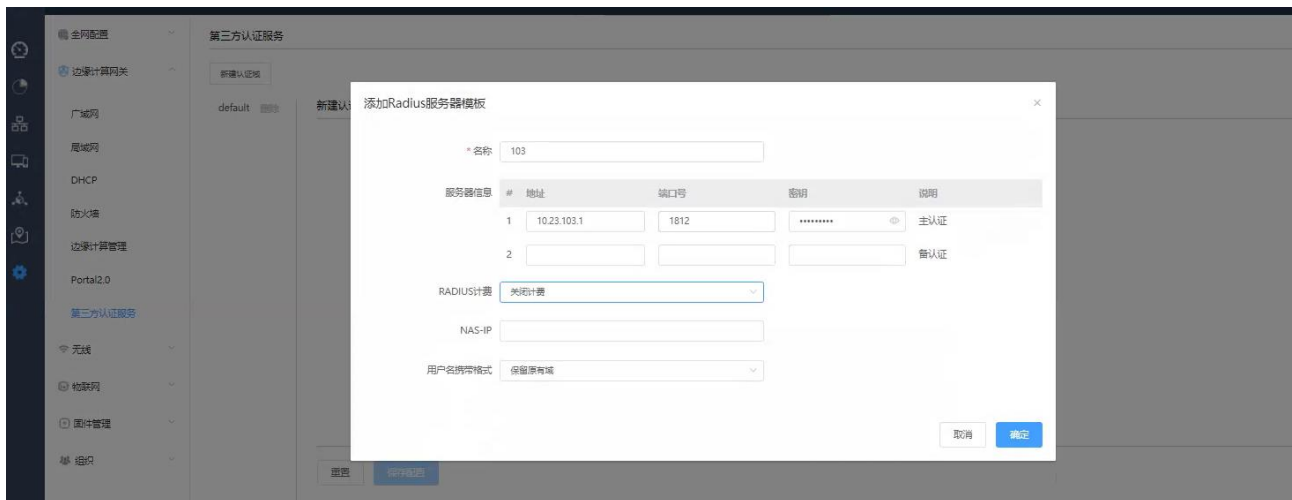


本例配置 1x 认证的认证域设置如下：

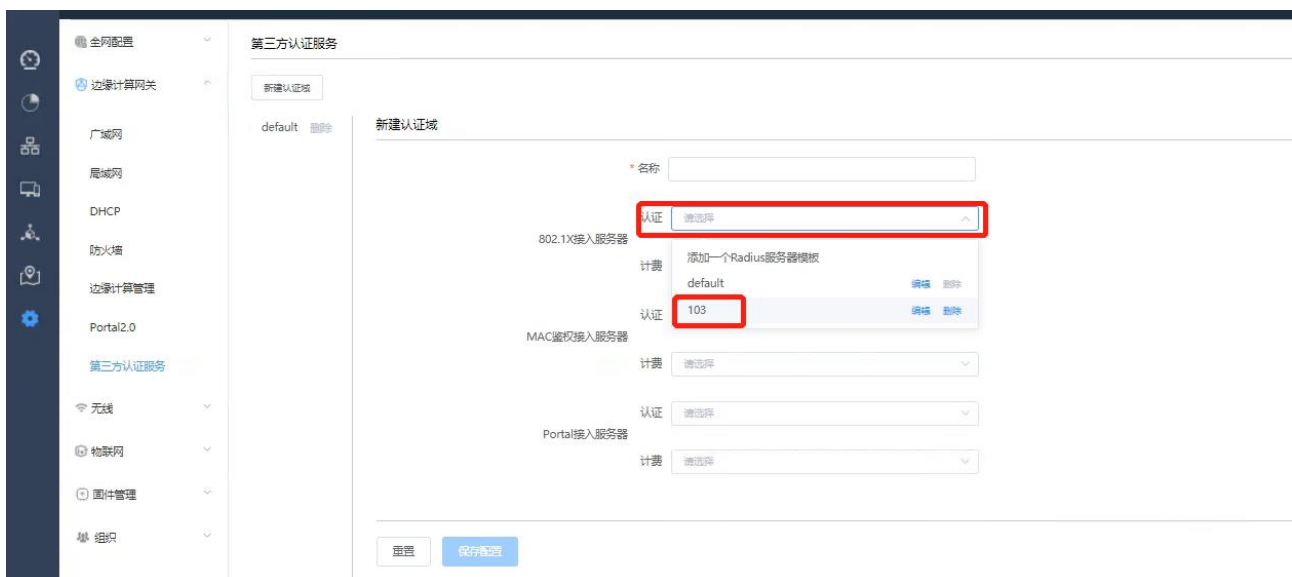
点击<新建认证域>，输入认证域“名称”，在 802.1X 接入服务器栏选择“添加一个 Radius 服务器模板”



输入认证服务器的地址、端口号和密钥，点击<确定>



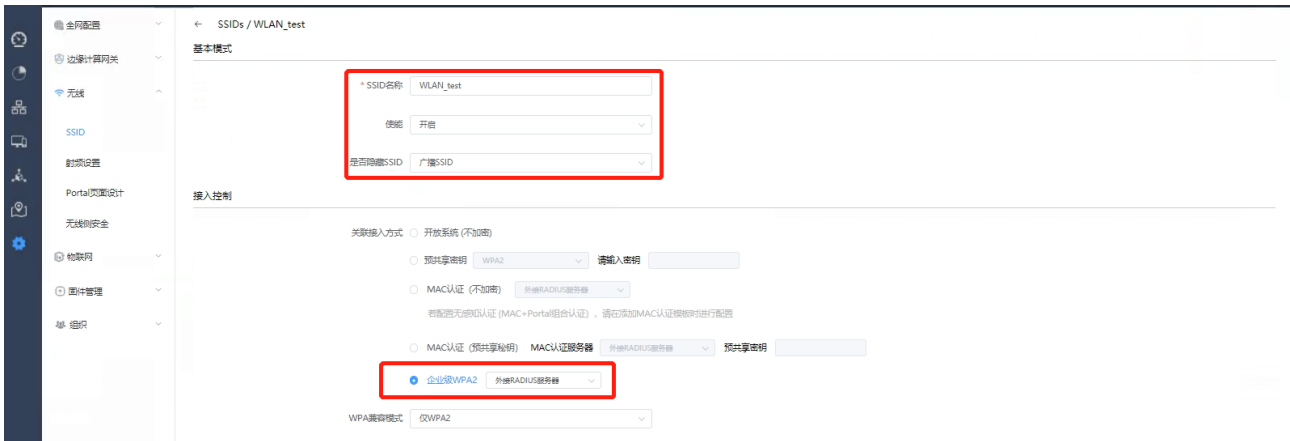
选择刚才创建的 Radius 服务器模版并保存配置，完成第三方服务器认证域配置。



# 创建 SSID

【设置】>【无线】>【SSID】选择 SSID 模版进入编辑模式

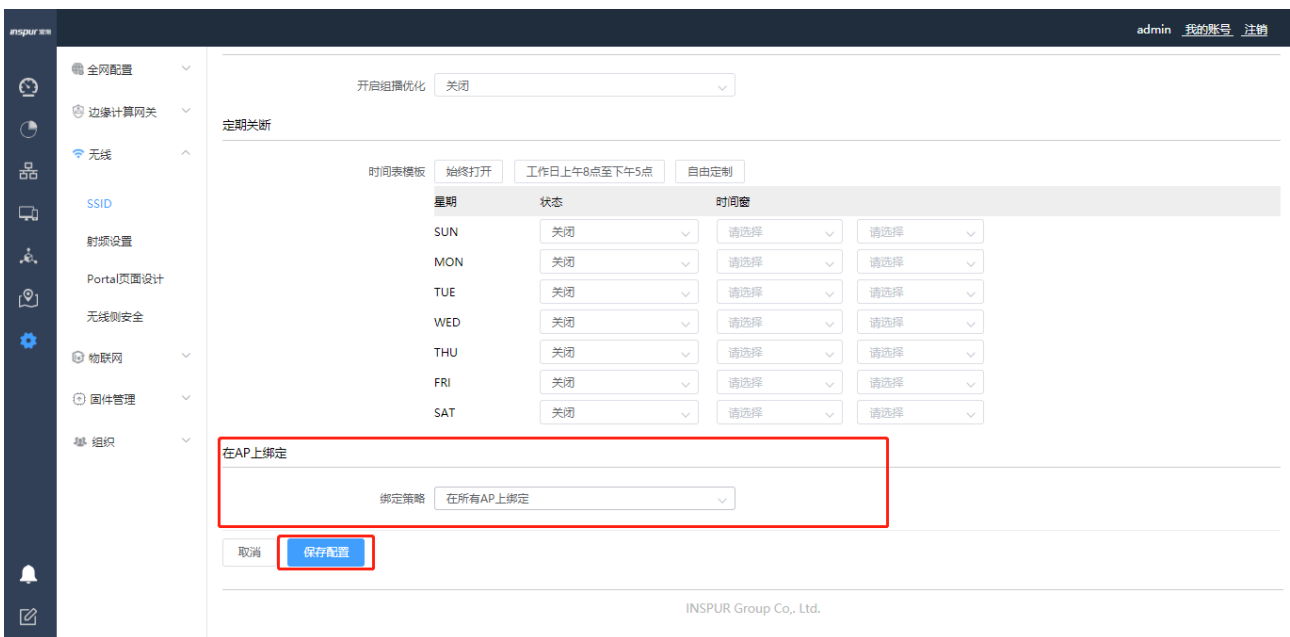
输入 SSID 名称，开启使能，广播 SSID，关联接入方式选择“企业级 WPA2（外置 RADIUS 服务器）”



在“用于 WPA2 认证的 RADIUS 服务器”框选择刚才创建的认证域  
#设置业务数据转发模式及业务网 VLAN，如下所示：



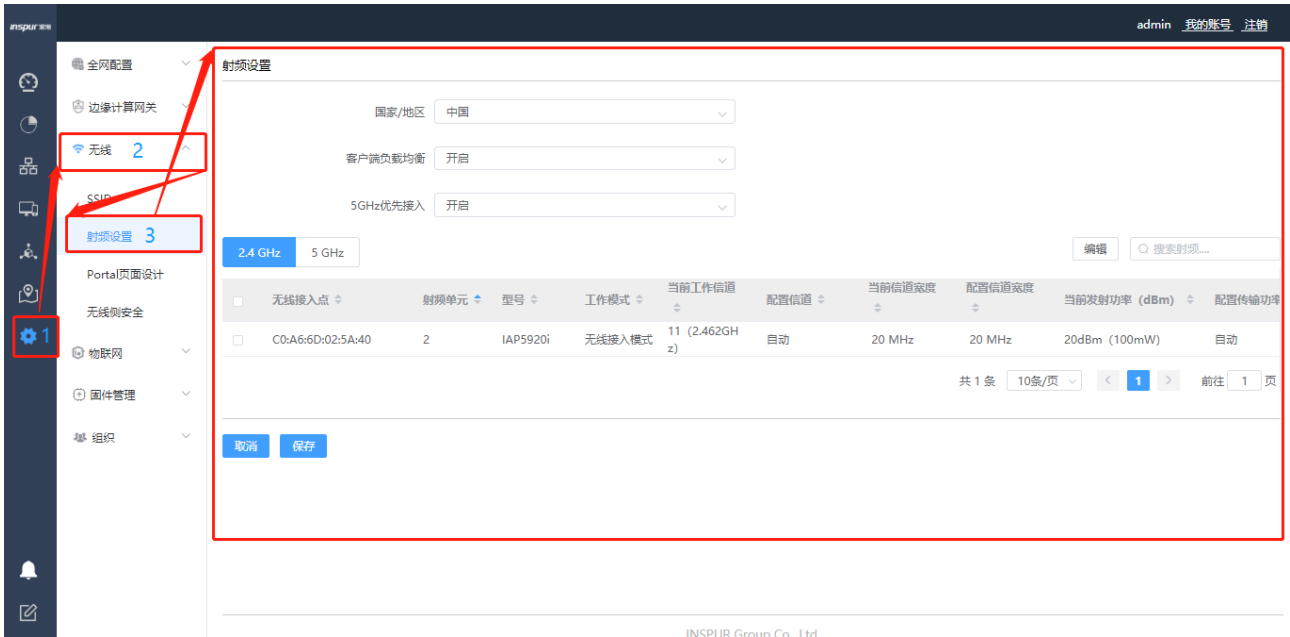
# 通过滑动鼠标配置好的策略应用至相应的 AP，如下所示：



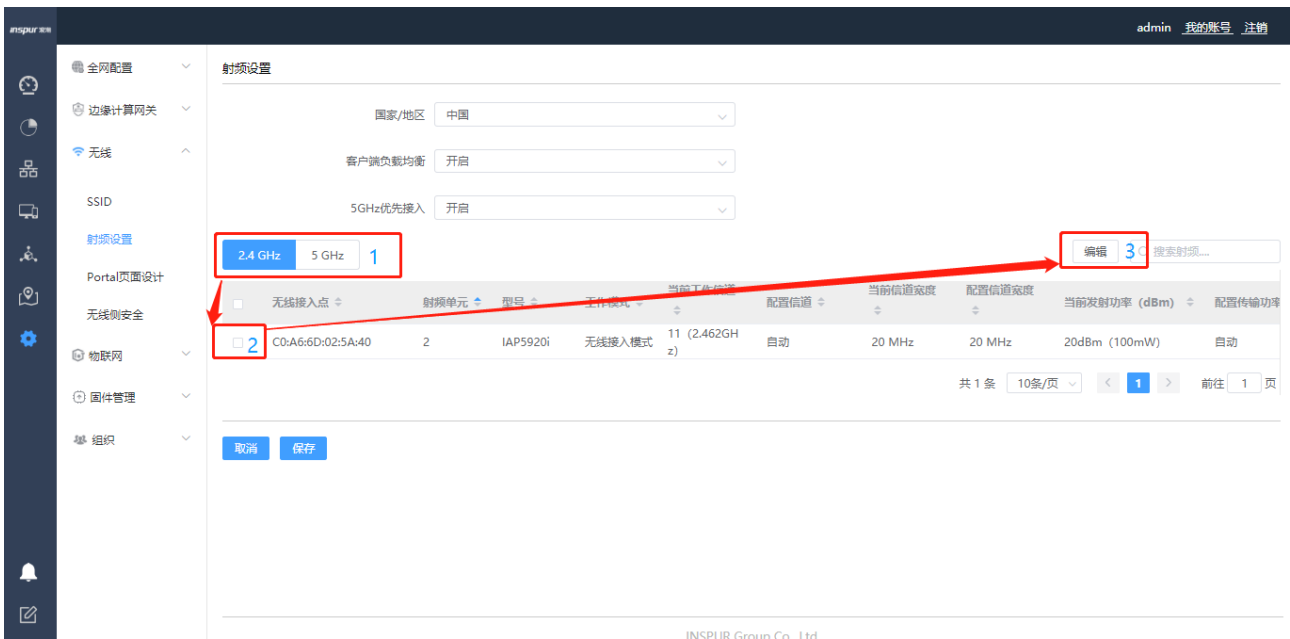
# 单击<保存配置>完成 WLAN 业务网络的配置。

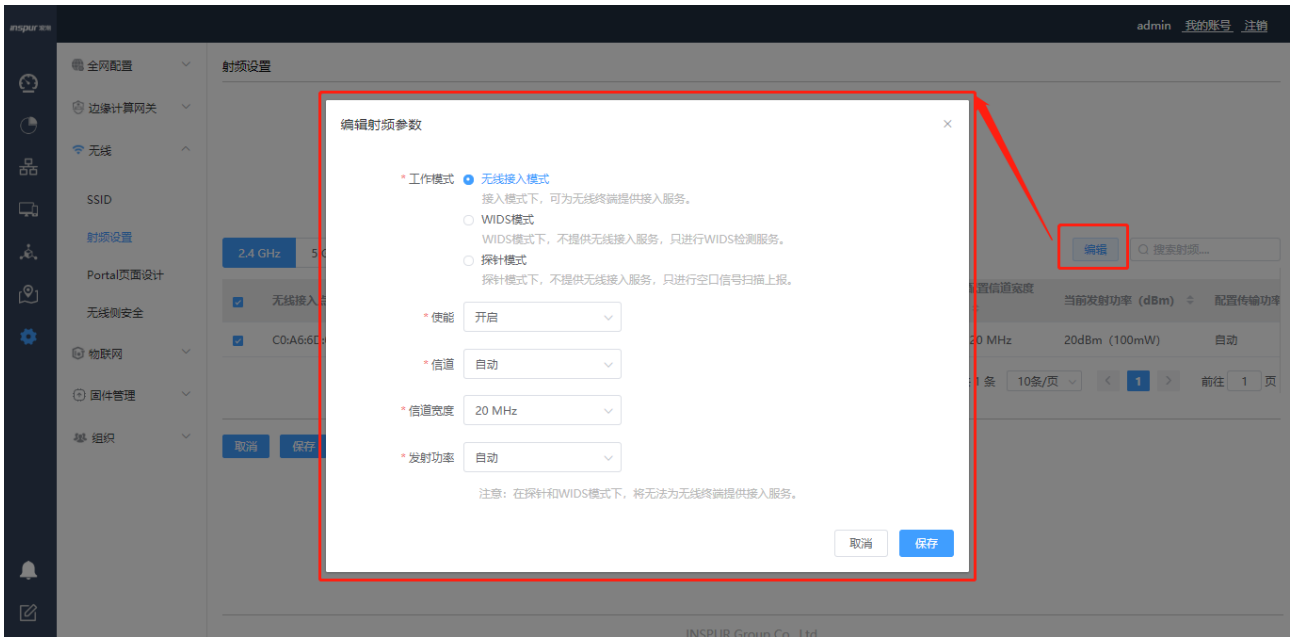
#### 4. 配置 AP 的信道和功率

# 单击菜单【设置】>子菜单【无线】>子菜单【射频设置】，进入 AP 的信道和功率配置页面。



# 单击“射频设置”中<2.4G>或<5G>射频的选项按钮，选定需要进行编辑的 AP，点击右上方的<编辑>按钮，进入 AP 的信道、功率、频率宽度等参数的配置页面。





# AP 信道的设定需根据整体周围信道情况进行统一考虑，2.4G 中有 1、6、11 三个信道相互之间是不重叠的，5G 频段相邻信道之间不重叠；

# 初期一般以默认配置为主，如后续验证测试时，需手动调整再进行统一优化。

## 5. 配置第三方服务器

# 具体配置方法建议参考相应的产品手册。

## 6. 检查配置结果

# 完成配置后，用户可通过无线终端搜索到 SSID 为 **WLAN\_test** 的无线网络。

# 用户关联到无线网络后，无线 PC 能够被分配相应的 IP 地址。

# 在 STA 上使用 802.1X 客户端进行认证，输入正确的用户名和密码后，STA 认证成功，正常访问 WLAN 网络。需要根据设置的认证方式 **PEAP** 对客户端进行相应的配置。

### Windows xp 系统下的配置

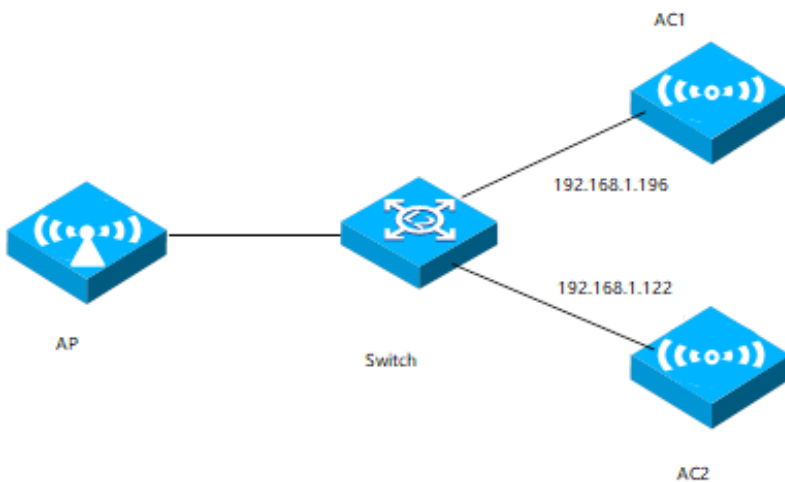
- a) 首先在无线网络属性中，添加 SSID 为 **WLAN\_test**，并选择认证方式为 **WPA2**，加密使用的算法 **AES**。
- b) 在“验证”选项卡中，选择 EAP 类型为 **PEAP**，单击“属性”，去掉验证服务器证书选项（此处不验证服务器证书），单击“配置”，去掉自动使用 Windows 登录名和密码选项，然后单击“确定”。

### Windows 7 系统下的配置

- a) 进入管理无线网络页面，单击“添加”，选择手动创建网络配置文件，添加 SSID 为 **WLAN\_test**，并选择认证方式为 **WPA2-企业**，加密使用的算法 **AES**，单击“下一步”。
- b) 单击“更改连接设置”，进入“无线网络属性”界面，选择“安全”页签，单击“设置”，取消勾选“验证服务器证书”（此处不验证服务器证书），单击“配置”，取消勾选“自动使用 Windows 登录名和密码”，单击“确定”。
- c) 单击“确定”，返回“无线网络属性”界面，单击“高级设置”，在“高级设置”界面，勾选“指定身份验证模式”，并选择身份验证模式为“用户身份验证”，单击“确定”。

### 3.1.2 AC 主备模式配置

#### 3.1.2.1 网络拓扑示意



#### 3.1.2.2 组网规划

配置项	规划数据
管理 VLAN	VLAN10
主 AC 管理 ip	192.168.1.196
备 AC 管理 ip	192.168.1.122
VRRP IP	192.168.1.100

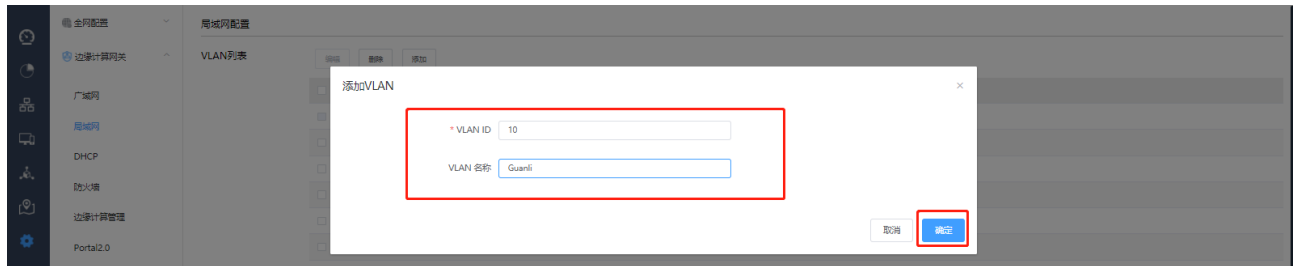
### 3.1.2.3 操作步骤

1) 如拓扑图所示，AC1 和 AC2 都在 vlan10 内， AC1 的 vlan10 的三层接口地址是 192.168.1.196，AC2 的三层接口地址是 192.168.1.122。

#### AC1 上的配置

【设置】>【边缘计算网关】>【局域网】，进入局域网配置页面。

在【VLAN 列表】点击<添加>，添加 VLAN10



在【子网】点击<添加>配置子网设置如下：

#### 配置子网

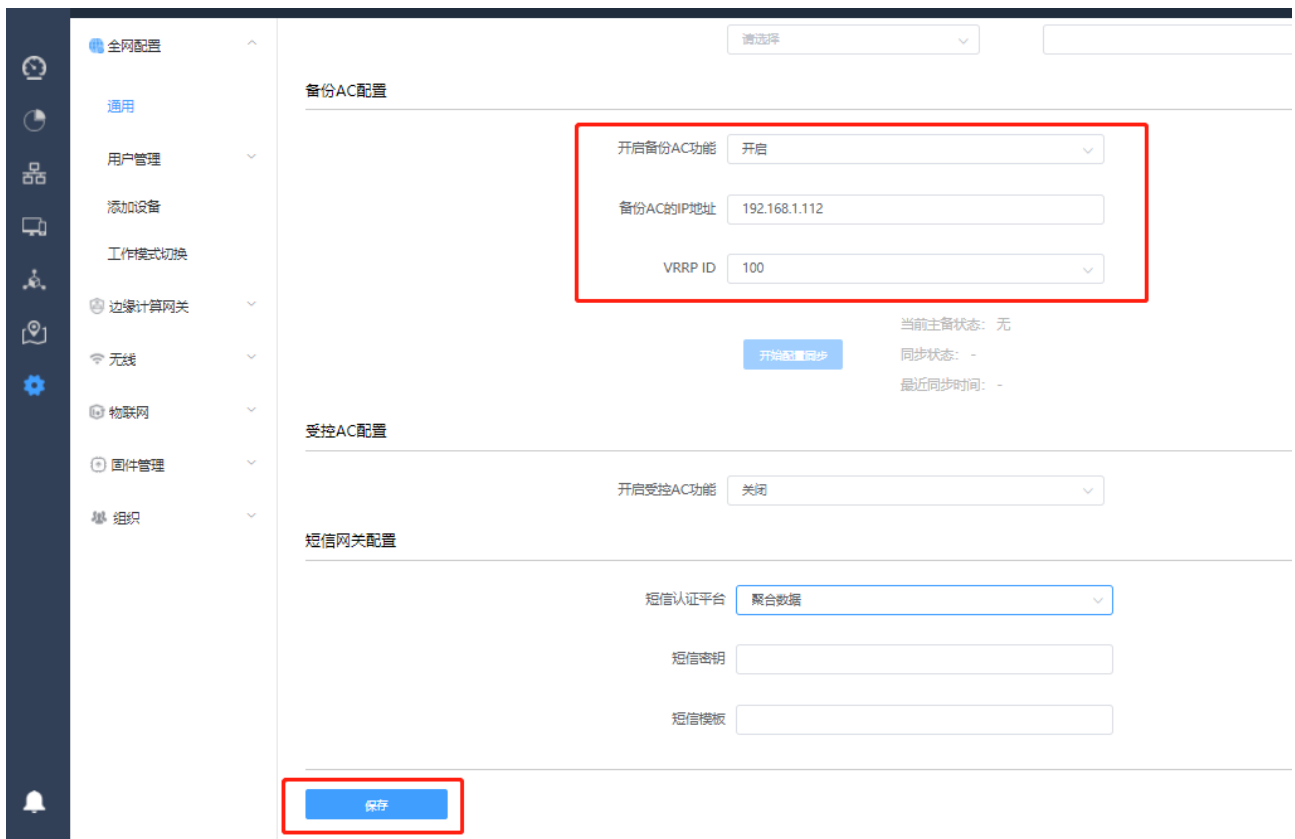
* 名称	default
* 子网	192.168.1.0/24
* 本机IP地址	192.168.1.196
* VLAN标识	10
VRRP 是否使能	开启
* VRRP ID	100
* VRRP IP地址	192.168.1.100
* VRRP 优先级	100

在【端口设置】将 VLAN10 加入端口

端口设置

端口	状态	类型	VLAN标识	允许通过的VLAN
<input type="checkbox"/> eth2	开启	Trunk	1	1,4,10
<input type="checkbox"/> eth3	开启	Trunk	1	1
<input type="checkbox"/> eth4	开启	Trunk	1	1
<input type="checkbox"/> eth5	开启	Trunk	1	1

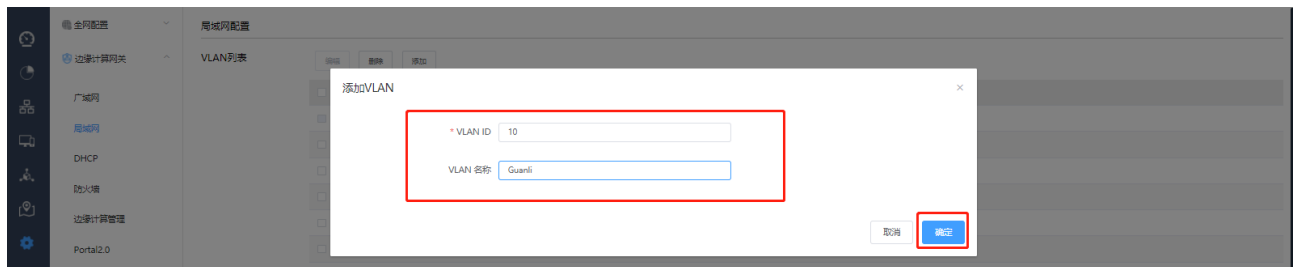
【设置】>【全局配置】>【通用】，设置备份 AC 配置，备份 AC 的 IP 地址为 AC2 的 IP，设置 VRRP ID 并保存。



### AC2 上的配置

【设置】>【边缘计算网关】>【局域网】，进入局域网配置页面。

在【VLAN 列表】点击<添加>，添加 VLAN10



在【子网】点击<添加>配置子网设置如下：



## 配置子网

* 名称	default
* 子网	192.168.1.1/24
* 本机IP地址	192.168.1.122
* VLAN标识	10
VRRP 是否使能	开启
* VRRP ID	100
* VRRP IP地址	192.168.1.100
* VRRP 优先级	100

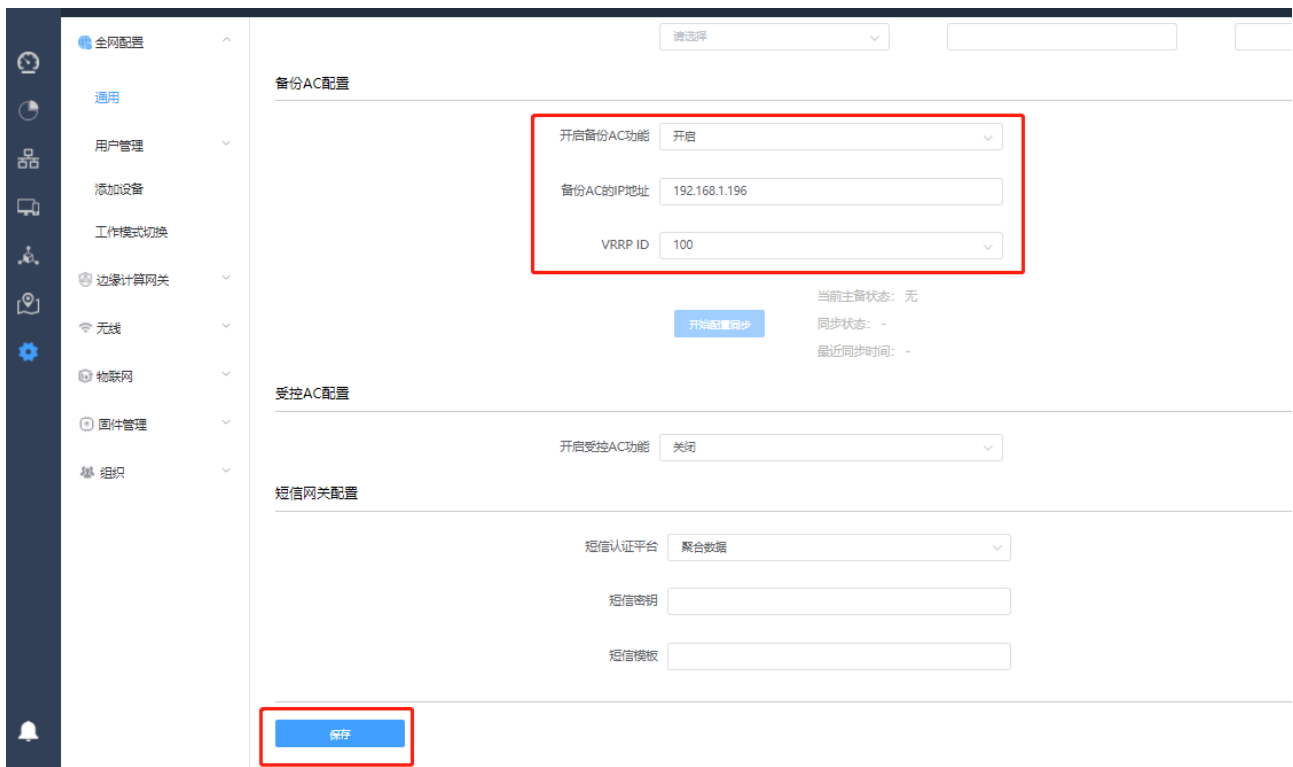
在【端口设置】将 VLAN10 加入端口

端口设置

编辑

端口	状态	类型	VLAN标识	允许通过的VLAN
<input checked="" type="checkbox"/> eth2	开启	Trunk	1	1,4,10
<input type="checkbox"/> eth3	开启	Trunk	1	1
<input type="checkbox"/> eth4	开启	Trunk	1	1
<input type="checkbox"/> eth5	开启	Trunk	1	1

【设置】>【全局配置】>【通用】，设置备份 AC 配置，备份 AC 的 IP 地址为 AC2 的 IP，设置 VRRP ID 并保存。



#在 AC1 上通过 show vrrp 命令查看 vrrp 状态

```
XOS#show vrrp
IPv4 standby Information:
  Run Method    : Real MAC
Total number of virtual routers : 1
Interface      VRID  state      Run   Adver   Auth   Virtual
                Pri   Timer     Type  IP
-----
vlan1.10       100  Master    100   1000 ms  --    192.168.1.100 (Not IP owner)
```

#在 AC2 上通过 show vrrp 命令查看 vrrp 状态

```
XOS#show vrrp
IPv4 standby Information:
  Run Method    : Real MAC
Total number of virtual routers : 1
Interface      VRID  state      Run   Adver   Auth   Virtual
                Pri   Timer     Type  IP
-----
vlan1.10       100  Backup    100   1000 ms  --    192.168.1.100 (Not IP owner)
```

#可以看到 AC1 协商为 vrrp 的主设备，AC2 协商为 vrrp 的备设备（在优先级相同的情况下，IP 地址大的会协商为主设备）

### 主备配置同步

【设置】>【全局配置】>【通用】>【备份 AC 设置】点击<开始配置同步>将主 AC 配置同步到备 AC 上，同步状态会显示为配置同步完成。AC 主备模式配置完成



### 验证结果

配置完成后，分别在主备 AC 上查看 vrrp 信息和 ap 信息，应该看到 vrrp 状态和 ap 的状态一致。

#在 AC1 命令行查看

```
XOS#show wlan ap all
NA:Never Assoc NI:No Ip I:Idle J:Join ID:Image Download C:Config
DC:Data Check R:Running RS:Reset M:Master S:Slave
Running/Total APs :1/1
ID Name MAC IP Model Time State
-----
1 C0A66D018200 c0a6.6d01.8200 192.168.1.118 iap5920i 0h8m21s R/M
XOS#show vrrp detail
IPv4 standby Information:
Run Method : Real MAC
Total number of virtual routers : 1
Interface vlan1.10
VRID : 100 Adver Timer : 1000 msec
Admin Status : UP State : Master
Config Pri : 100 Running Pri : 100
Preempt Mode : FALSE Delay Time : 0 msec
Auth Type : -- Key : --
Virtual IP : 192.168.1.100 (Not IP owner)
Virtual MAC : 0000-5e00-0164
Master IP : 192.168.1.196
VRRP Track Information:
```

#在 AC2 命令行查看

```
XOS#show wlan ap all
NA:Never Assoc NI:No Ip I:Idle J:Join ID:Image Download C:Config
DC:Data Check R:Running RS:Reset M:Master S:Slave
Running/Total APs :1/1
ID Name MAC IP Model Time State
-----
1 C0A66D018200 c0a6.6d01.8200 192.168.1.118 iap5920i 0h11m23s R/S
XOS#show vrrp detail
IPv4 standby Information:
```

```

Run Method      : Real MAC
Total number of virtual routers : 1
Interface vlan1.10
VRID           : 100                Adver Timer   : 1000 msec
Admin Status   : UP                 State          : Backup
Config Pri     : 100                Running Pri    : 100
Preempt Mode   : FALSE              Delay Time     : 0 msec
Auth Type      : --                 Key            : --
Virtual IP     : 192.168.1.100 (Not IP owner)
Virtual MAC    : 0000-5e00-0164
Master IP      : 192.168.1.122
VRRP Track Information:

```

在 down 掉 AC1 的链路后，AC2 会成为主 AC，其上的 ap 状态也由 Slave 转变为 Master。

### 3.1.3 AC 双链路聚合配置

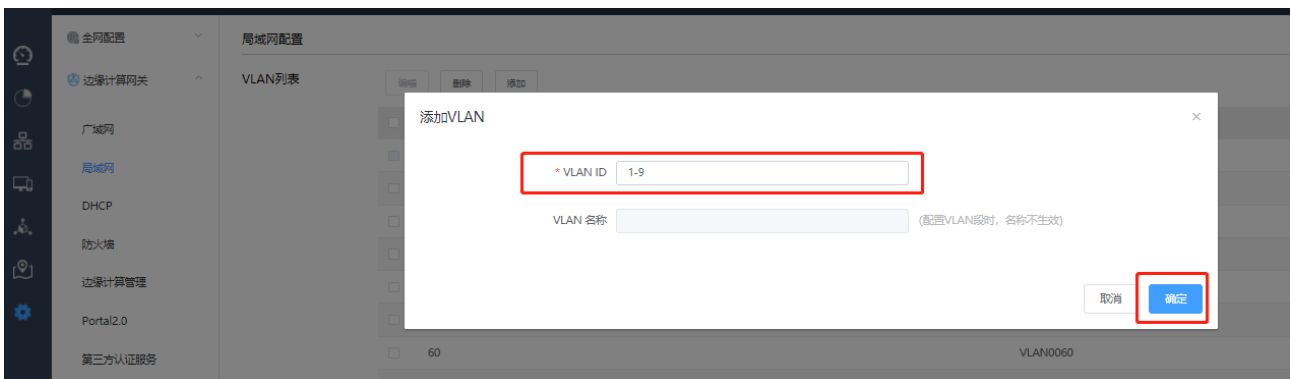
#### 3.1.3.1 组网需求

将 AC 的 eth4 和 eth5 端口加入聚合组 1，配置 trunk，通过 vlan 1-9

#### 3.1.3.2 操作步骤

【设置】>【边缘计算网关】>【局域网】，进入局域网配置页面。

在【VLAN 列表】点击<添加>，添加 VLAN1-9，点击<确定>



在【端口设置】将 VLAN1-9 加入 eth4 和 eth5 端口并保存

配置LAN接口 - eth4

\* 使能

\* 类型

\* 默认VLAN

\* 允许通过的VLAN

取消 确定

配置LAN接口 - eth5

\* 使能

\* 类型

\* 默认VLAN

\* 允许通过的VLAN

取消 确定

接口设置

编辑

端口	状态	类型	VLAN标识	允许通过的VLAN
<input type="checkbox"/> eth2	开启	Trunk	1	1,4,10
<input type="checkbox"/> eth3	开启	Trunk	1	1
<input type="checkbox"/> eth4	开启	Trunk	1	1-9
<input type="checkbox"/> eth5	开启	Trunk	1	1-9

静态路由

编辑 删除 添加

使能	描述	子网	下一跳
<input type="checkbox"/> 开启		0.0.0.0/0	192.168.1.1

取消 保存

登录 AC 命令行，将 eth4 和 eth5 加入到静态聚合组 1：

```
XOS(config)#interface eth4
XOS(config-if)#static-channel-group 1
XOS(config-if)#quit
XOS(config)#interface eth5
XOS(config-if)#static-channel-group 1
XOS(config-if)#quit
```

show static-channel-group 可查看当前聚合组信息如下：

```
XOS(config)#show static-channel-group
% Static Aggregator: sa1
% Member:                Status:
```

```
eth4          INACTIVE
eth5          INACTIVE
```

配置聚合接口根据源 ip 和目的 ip 进行负载分担:

```
XOS(config)#interface sa1
```

```
XOS(config-if)#port-channel load-balance src-dst-ip //缺省的负载分担模式是基于源 MAC 和目的 MAC
```

## 检验结果

# 查看 AC 上聚合组的信息

```
XOS# show static-channel-group
```

```
% Static Aggregator: sa1
```

```
% Member:          Status:
eth4                ACTIVE
eth5                ACTIVE
```

# 查看接口状态

```
XOS#show interface brief
```

```
The brief information of interface(s) under bridge mode:
```

```
Status: ADM - administratively down
```

```
Duplex: A - auto;H - half;F - full
```

```
Type:A - access;T - trunk;H - hybrid
```

Interface	Status	Speed	Duplex	Type	PVID	Description
eth0	DOWN	1g	F	A	4093	
eth1	DOWN	1g	F	A	4094	
eth2	DOWN	1g	F	T	1	
eth3	DOWN	1g	F	T	1	
eth4	UP	1g	F	T	1	
eth5	UP	1g	F	T	1	
sa1	UP	2g	F	T	1	

# 查看负载分担模式

```
XOS# show etherchannel load-balance
```

```
% LACP Aggregator: sa1
```

```
Source and Destination IP address
```