

华为认证 WLAN 系列教程

HCIP-WLAN

实验指导手册（Web）

版本：2.0



华为技术有限公司

版权所有 © 华为技术有限公司 2023。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、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <https://e.huawei.com>

华为认证体系介绍

华为认证是华为公司基于“平台+生态”战略，围绕“云-管-端”协同的新ICT技术架构，打造的覆盖ICT（Information and Communications Technology，信息技术）全技术领域的认证体系，包含ICT基础设施认证、基础软硬件认证、云平台及云服务认证三类认证。

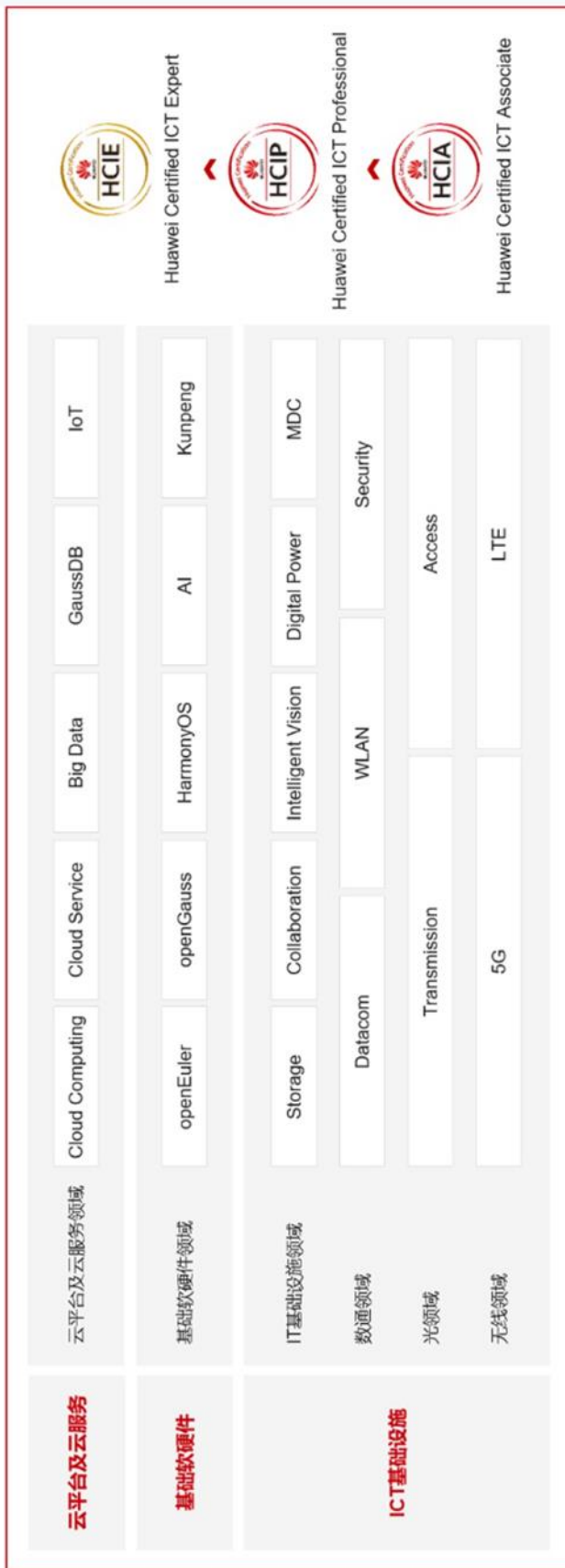
根据ICT从业者的学习和进阶需求，华为认证分为工程师级别、高级工程师级别和专家级别三个认证等级。

华为认证覆盖ICT全领域，符合ICT融合的技术趋势，致力于提供领先的人才培养体系和认证标准，培养数字化时代新型ICT人才，构建良性ICT人才生态。

HCIP-WLAN（Huawei Certified ICT Professional-Wireless Local Area Network，华为认证网络通信高级工程师WLAN方向）主要面向华为公司办事处、代表处一线工程师，以及其他希望学习华为WLAN产品技术人士。HCIP-WLAN认证在内容上涵盖华为WLAN组网架构、WLAN漫游、射频资源管理、接入认证等特性以及WLAN网络规划、WLAN网络优化、故障排除等。

华为认证协助您打开行业之窗，开启改变之门，屹立在WLAN网络世界的潮头浪尖！

华为职业认证



前言

简介

本书为 HCIP-WLAN 认证培训教程，适用于准备参加 HCIP-WLAN 考试的学员或者希望了解 WLAN 组网架构、WLAN 漫游、射频资源管理、接入认证等无线特性以及 WLAN 网络规划、网络优化和故障排除等相关 WLAN 技术的读者。

说明：Web 版实验手册与命令行版实验手册学员可以任选一版学习，两版实验手册所含实验和技术内容均相同，仅在操作方式上有差别。

内容描述

本实验指导书共包含 12 个实验，从设备基本组网开始，逐一介绍了 WLAN 组网、可靠性、云管理、准入认证、漫游、网络规划、运维及故障排查的配置与实现。

本实验指导书共包含如下实验：

- 实验一为 WAC+FIT AP 实验，通过基本的操作与配置，帮助读者熟悉 WAC+FIT AP 组网架构，掌握 AP 上线基本配置。
 - 实验二为 Leader AP 组网实验，通过基本的组网配置，帮助读者掌握 Leader AP 组网架构，掌握 Leader AP 无线业务配置方法。
 - 实验三为 VRRP 热备份实验，针对无线控制器可靠性组网中的 VRRP 热备份组网进行重点讲解，通过本章的实验，使读者掌握 WLAN 可靠性组网架构及搭建方法。
 - 实验四为云管理组网实验，帮助读者熟悉华为云管理方案架构，掌握 WAC 上云及 AP 上云的配置方法。
 - 实验五为 802.1X 认证实验，介绍了 802.1X 认证安全特性，帮助读者熟悉 802.1X 认证的部署方式。
 - 实验六为 Portal 认证实验，介绍了 Portal 认证安全特性，帮助读者熟悉 Portal 认证的部署方式。
 - 实验七为 WLAN 漫游实验，重点介绍 WAC 间三层漫游及其部署方式，帮助读者熟悉 WLAN 的漫游方案。
 - 实验八为射频资源管理实验，着重介绍如何进行 WLAN 射频调优、频谱导航、负载均衡及用户 CAC 功能，帮助读者熟悉网络优化的方法和实现方式。
 - 实验九为室内场景网络规划实验，主要介绍如何设计室内场景 WLAN 网络，帮助读者熟悉网络规划工具的使用以及网络规划细节。
-

- 实验十为室外场景网络规划实验，主要介绍如何设计室外场景 WLAN 网络，帮助读者熟悉网络规划工具的使用以及网络规划细节。
- 实验十一为 CampusInsight 智能运维实验，通过 CampusInsight 平台进行运维管理，帮助读者熟悉 CampusInsight 平台相关功能。
- 实验十二为故障排查综合实验，重点介绍 Portal 认证场景故障的排查方法，帮助读者在实际网络中解决无线故障。

读者知识背景

本课程为华为认证高级课程，为了更好地掌握本书内容，阅读本书的读者应首先具备以下基本条件：

- 具有高级无线局域网知识背景，且需要掌握基础的数通知识。
- 熟悉如何配置华为的软硬件设备，包括交换机、WAC、AP、iMaster NCE-Campus、iMaster NCE-CampusInsight 等。
- 熟悉 WLAN 项目规划流程，了解网络规划工具 WLAN Planner 的基本使用。

本书常用图标



实验环境说明

组网说明：

本实验环境面向准备 HCIP-WLAN 考试的无线网络工程师。每套实验环境包括：无线控制器 3 台，无线接入点 5 台，核心交换机 1 台，接入交换机 1 台，iMaster NCE-Campus 服务器 1 台，iMaster NCE-CampusInsight 服务器一台。每套实验环境适用于一组学员上机操作。

设备介绍:

为了满足 HCIP-WLAN 实验需要, 建议每套实验环境采用以下配置:

设备名称、型号与版本的对应关系如下:

设备名称	设备型号	软件版本
核心交换机	CloudEngine S5732-H24UM2CC	V200R021C00SPC100
接入交换机	CloudEngine S5732-H24UM2CC	V200R021C00SPC100
无线控制器	AirEngine 9700-M1	V200R021C00SPC100
无线接入点	AirEngine 5761-11	V200R021C00SPC200
服务器	iMaster NCE-Campus	V300R021C00SPC110
	iMaster NCE-CampusInsight	V100R021C10SPC100

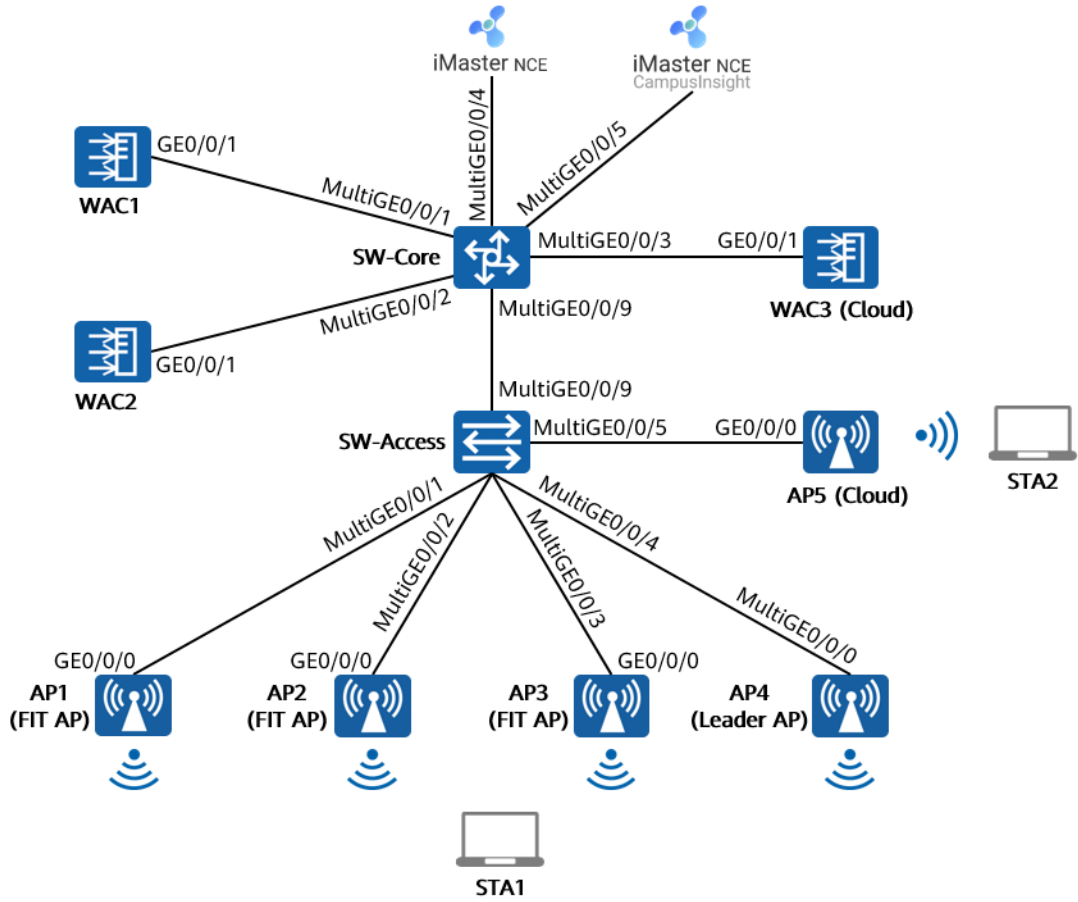
准备实验环境

检查设备

实验开始之前, 请每组学员检查自己的实验设备的登录方式是否齐全, 能否正常登录设备, 实验清单如下。

设备名称	数量	备注
iMaster NCE-Campus	1台	所有实验组共用
iMaster NCE-CampusInsight	1台	所有实验组共用
核心交换机	每组1台	
接入交换机	每组1台	支持PoE供电功能
AirEngine 9700-M1	每组3台	
AirEngine 5761-11	每组4台	
AirEngine 6761-21T	每组1台	此AP作为Leader AP
笔记本	每组2台	用于测试WLAN网络

实验拓扑



实验拓扑说明如下：

AP1~AP5 与接入交换机 SW-Access 互联，SW-Access 可为 AP 提供 PoE 供电能力。

接入交换机 SW-Access 与核心交换机 SW-Core 通过 MultiGE0/0/9 接口互联。

WAC1~WAC3 旁挂于核心交换机 SW-Core 上。

核心交换机 SW-Core 与 iMaster NCE-Campus、iMaster NCE-CampusInsight 服务器互联，互联网段为 172.21.0.0/17（可根据实际情况进行调整）。

目录

前 言	3
简介.....	3
内容描述.....	3
读者知识背景.....	4
本书常用图标.....	4
实验环境说明.....	4
准备实验环境.....	5
1 WAC+FIT AP 组网实验	14
1.1 实验介绍.....	14
1.1.1 关于本实验.....	14
1.1.2 实验目的.....	14
1.1.3 实验组网介绍.....	14
1.1.4 实验规划.....	15
1.2 实验任务配置.....	16
1.2.1 配置思路.....	16
1.2.2 配置步骤.....	16
1.3 结果验证.....	36
1.3.1 查看 AP 上线状况、SSID 等信息.....	36
1.3.2 终端关联无线信号，测试网络连通性.....	37
1.4 配置参考.....	37
1.4.1 WAC1 配置.....	37
1.4.2 SW-Core 配置.....	40
1.4.3 SW-Access 配置.....	41
1.5 思考题.....	42
2 Leader AP 组网实验	43
2.1 实验介绍.....	43
2.1.1 关于本实验.....	43
2.1.2 实验目的.....	43
2.1.3 实验组网介绍.....	43
2.1.4 实验规划.....	44
2.2 实验任务配置.....	45

2.2.1 配置思路.....	45
2.2.2 配置步骤.....	45
2.3 结果验证.....	54
2.3.1 查看 AP 上线状态、SSID 等信息.....	54
2.3.2 查看射频状态信息.....	55
2.3.3 查看 VLAN 信息.....	55
2.3.4 STA 接入无线网络，测试网络连通性.....	56
2.4 配置参考.....	56
2.4.1 SW-Core 配置.....	56
2.4.2 SW-Access 配置.....	57
2.4.3 Leader AP 配置.....	58
2.5 思考题.....	60
3 VRRP 热备份实验.....	61
3.1 实验介绍.....	61
3.1.1 关于本实验.....	61
3.1.2 实验目的.....	61
3.1.3 实验组网介绍.....	61
3.1.4 实验规划.....	62
3.2 实验任务配置.....	63
3.2.1 配置思路.....	63
3.2.2 配置步骤.....	63
3.3 结果验证.....	71
3.3.1 检查 AP 上线状态.....	71
3.3.2 检查 VAP 信息.....	72
3.3.3 检查 HSB 通道状态.....	73
3.3.4 检查无线配置同步状态信息.....	74
3.3.5 STA 关联无线信号，测试网络连通性.....	75
3.4 配置参考.....	75
3.4.1 WAC1 配置.....	75
3.4.2 WAC2 配置.....	77
3.4.3 SW-Core 配置.....	79
3.4.4 SW-Access 配置.....	80
3.5 思考题.....	81
4 云管理组网实验.....	82
4.1 实验介绍.....	82

4.1.1 关于本实验	82
4.1.2 实验目的.....	82
4.1.3 实验组网介绍.....	82
4.1.4 实验规划.....	83
4.2 实验任务配置	85
4.2.1 配置思路.....	85
4.2.2 配置步骤.....	85
4.3 结果验证	117
4.3.1 在 WAC3 上检查云管理信息	117
4.3.2 STA 接入无线网络，测试网络连通性.....	118
4.3.3 在 NCE 上查看设备运行状态.....	119
4.3.4 在 NCE 上查看终端接入状况.....	119
4.4 配置参考	120
4.4.1 WAC3 配置.....	120
4.4.2 AP5 配置	123
4.4.3 SW-Core 配置.....	126
4.4.4 SW-Access 配置.....	127
4.5 思考题	128
5 802.1X 认证实验.....	129
5.1 实验介绍	129
5.1.1 关于本实验	129
5.1.2 实验目的.....	129
5.1.3 实验组网介绍.....	129
5.1.4 实验规划.....	130
5.2 实验任务配置	132
5.2.1 配置思路.....	132
5.2.2 配置步骤.....	132
5.3 结果验证	153
5.3.1 检查 AP 上线状态	153
5.3.2 检查 VAP 信息	153
5.3.3 STA 通过 802.1X 方式接入无线网络.....	154
5.3.4 查看 NCE 终端认证日志	162
5.3.5 在 WAC1 检查终端认证情况	163
5.4 配置参考	164
5.4.1 WAC1 配置.....	164

5.4.2 SW-Core 配置.....	166
5.4.3 SW-Access 配置.....	167
5.5 思考题	168
6 Portal 认证实验	169
6.1 实验介绍	169
6.1.1 关于本实验	169
6.1.2 实验目的.....	169
6.1.3 实验组网介绍.....	169
6.1.4 实验规划.....	170
6.2 实验任务	172
6.2.1 配置思路配置.....	172
6.2.2 配置步骤.....	172
6.3 结果验证	199
6.3.1 检查 AP 上线状态	199
6.3.2 检查 VAP 信息	199
6.3.3 STA 通过 Portal 认证方式接入无线网络	200
6.3.4 查看 NCE 终端认证日志	201
6.3.5 在 WAC1 上检查终端认证情况.....	202
6.4 配置参考	203
6.4.1 WAC1 配置.....	203
6.4.2 SW-Core 配置.....	206
6.4.3 SW-Access 配置.....	207
6.5 思考题	208
7 WLAN 漫游实验	209
7.1 实验介绍	209
7.1.1 关于本实验	209
7.1.2 实验目的.....	209
7.1.3 实验组网介绍.....	209
7.1.4 实验规划.....	210
7.2 实验任务配置	212
7.2.1 配置思路.....	212
7.2.2 配置步骤.....	212
7.3 结果验证	230
7.3.1 检查 AP 上线	230
7.3.2 检查 VAP 状态	231

7.3.3 检查漫游组状态	232
7.3.4 观察 STA 漫游轨迹	232
7.4 配置参考	233
7.4.1 WAC1 配置	233
7.4.2 WAC2 配置	235
7.4.3 SW-Core 配置	238
7.4.4 SW-Access 配置	238
7.5 思考题	240
8 射频资源管理实验	241
8.1 实验介绍	241
8.1.1 关于本实验	241
8.1.2 实验目的	241
8.1.3 实验组网介绍	241
8.1.4 实验规划	242
8.2 实验任务配置	243
8.2.1 配置思路	243
8.2.2 配置步骤	243
8.3 结果验证	253
8.3.1 查看射频模板和 RRM 模板信息	253
8.3.2 查看当前射频状态信息	255
8.4 配置参考	255
8.4.1 WAC1 配置	255
8.4.2 SW-Core 配置	259
8.4.3 SW-Access 配置	260
8.5 思考题	260
9 室内网络规划实验	261
9.1 实验介绍	261
9.1.1 关于本实验	261
9.1.2 实验目的	261
9.1.3 实验场景介绍	261
9.1.4 前期准备工作	262
9.2 实验任务配置	264
9.2.1 配置思路	264
9.2.2 配置步骤	264
9.3 思考题	289

10 室外网络规划实验	291
10.1 实验介绍.....	291
10.1.1 关于本实验.....	291
10.1.2 实验目的.....	291
10.1.3 实验场景介绍.....	291
10.1.4 前期准备工作.....	292
10.2 实验任务配置.....	294
10.2.1 配置思路.....	294
10.2.2 配置步骤.....	294
10.3 思考题.....	311
11 CampusInsight 智能运维实验	313
11.1 实验介绍.....	313
11.1.1 关于本实验.....	313
11.1.2 实验目的.....	313
11.1.3 实验组网介绍.....	313
11.1.4 实验规划.....	314
11.2 实验任务配置.....	315
11.2.1 配置思路.....	315
11.2.2 配置步骤.....	315
11.3 结果验证.....	335
11.3.1 查看 WAC1 的 SNMP 协议.....	335
11.3.2 查看 WAC1 的 AP 状态和 VAP 信息.....	337
11.4 配置参考.....	338
11.4.1 WAC1 配置.....	338
11.4.2 SW-Core 配置.....	342
11.4.3 SW-Access 配置.....	343
11.5 思考题.....	344
12 故障排查综合实验	345
12.1 实验介绍.....	345
12.1.1 关于本实验.....	345
12.1.2 实验目的.....	345
12.1.3 实验组网介绍.....	345
12.1.4 实验规划.....	346
12.2 实验任务配置.....	348
12.2.1 配置思路.....	348



12.2.2 配置步骤	348
12.3 结果验证.....	363
12.3.1 检查 AP 上线状态.....	363
12.3.2 检查 VAP 信息.....	364
12.3.3 STA 关联无线信号，认证通过	365
12.4 配置参考.....	365
12.4.1 WAC1 配置	365
12.4.2 SW-Core 配置	369
12.4.3 SW-Access 配置	370
12.5 思考题.....	370

1

WAC+FIT AP 组网实验

1.1 实验介绍

1.1.1 关于本实验

本实验通过配置 WAC+FIT AP 组网，使学员能够掌握此组网方式中 AP 上线、STA 上线的原理与配置方法。

1.1.2 实验目的

- 描述 WLAN 业务基本配置流程。
- 配置 AP 上线、STA 上线。
- 阐明 WAC+FIT AP 组网架构。

1.1.3 实验组网介绍

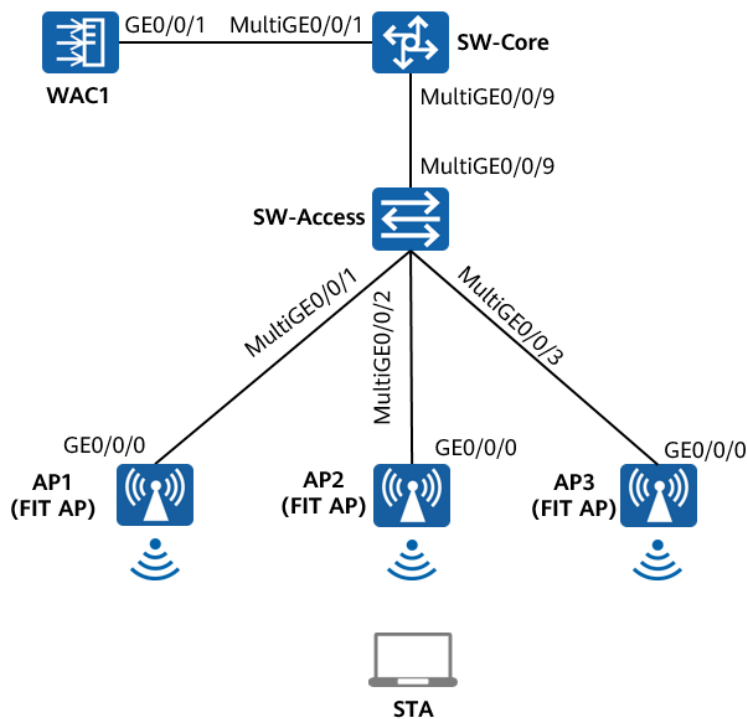


图1-1 WAC+FIT AP 组网实验拓扑图

1.1.4 实验规划

表1-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表1-2 IP 地址规划

设备	端口	IP地址
SW-Core	Vlanif100	10.23.100.254/24
	Vlanif101	10.23.101.254/24
WAC1	Vlanif100	10.23.100.1/24
	MEth0/0/1	172.21.39.4/24

表1-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	100
业务VLAN	101
AP组	ap-group1

VAP模板	wlan-net
安全模板	wlan-net
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	wlan-net
SSID	wlan-net

1.2 实验任务配置

1.2.1 配置思路

- 1.配置 SW-Core、SW-Access 设备的 VLAN 和 IP 地址。
- 2.初始化 WAC1 设备，并修改管理 IP 地址。
- 3.配置 WAC1 设备的 VLAN 和业务 IP 地址，确保网络互通。
- 4.在 SW-Core 上配置 DHCP 服务器，为 AP 及 STA 分配 IP 地址。
- 5.配置 AP 上线。
- 6.配置 WLAN 业务参数，实现 STA 接入 WLAN 网络。

1.2.2 配置步骤

步骤 1 配置交换机 VLAN 信息

配置接入交换机 SW-Access 设备。创建 VLAN 100、101，下行端口允许通过 VLAN 100、101，PVID 为 100，上行端口允许通过 VLAN 100、101，PVID 使用缺省值 VLAN 1。

在 SW-Access 上创建 VLAN 100、101。

```
<Huawei> system-view
[Huawei] sysname SW-Access
[SW-Access] vlan batch 100 101
```

配置 SW-Access 下行端口类型及允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/1
[SW-Access-MultiGE0/0/1] port link-type trunk
[SW-Access-MultiGE0/0/1] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/1] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/1] quit
[SW-Access] interface MultiGE 0/0/2
[SW-Access-MultiGE0/0/2] port link-type trunk
[SW-Access-MultiGE0/0/2] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/2] port trunk pvid vlan 100
```

```
[SW-Access-MultiGE0/0/2] quit
[SW-Access] interface MultiGE 0/0/3
[SW-Access-MultiGE0/0/3] port link-type trunk
[SW-Access-MultiGE0/0/3] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/3] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/3] quit
```

配置 SW-Access 上行端口类型及允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/9
[SW-Access-MultiGE0/0/9] port link-type trunk
[SW-Access-MultiGE0/0/9] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/9] quit
```

配置核心交换机 SW-Core 设备。创建 VLAN 100、101，下行端口允许通过 VLAN 100、101，与 WAC1 互联端口 MultiGE0/0/1 允许通过 VLAN 100、101。

在 SW-Core 上创建 VLAN 100 和 VLAN 101。

```
<Huawei> system-view
[Huawei] sysname SW-Core
[SW-Core] vlan batch 100 101
```

配置 SW-Core 下行端口类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/9
[SW-Core-MultiGE 0/0/9] port link-type trunk
[SW-Core-MultiGE 0/0/9] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE 0/0/9] quit
```

配置 SW-Core 与 WAC1 互联端口的类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/1
[SW-Core-MultiGE 0/0/1] port link-type trunk
[SW-Core-MultiGE 0/0/1] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE 0/0/1] quit
```

步骤 2 配置交换机 IP 地址

配置 SW-Core 的 IP 地址。

```
[SW-Core] interface vlanif 100
[SW-Core-Vlanif100] ip address 10.23.100.254 24
[SW-Core-Vlanif100] quit
[SW-Core] interface vlanif 101
[SW-Core-Vlanif101] ip address 10.23.101.254 24
[SW-Core-Vlanif101] quit
```

步骤 3 初始化 WAC1 设备

AirEngine 9700-M1 出厂时在接口 MEth0/0/1 上配置了 IP 地址 169.254.1.1/24，使用网线将 PC 网卡与此接口进行互联，并配置 PC 网卡地址为 169.254.1.100/24，使用浏览器访问 <https://169.254.1.1> 地址，即可打开 AirEngine 9700-M1 设备的 Web 管理页面。



The image shows the registration page of the Wireless LAN Access Controller. The page has a header with a city skyline and a Wi-Fi icon. The main heading is "Wireless LAN Access Controller". The form contains the following fields and options:

- 用户名: [text input]
- 密码: [password input]
- 确认密码: [password input]
- 串口认证类型: AAA认证 密码认证
- 串口密码: [password input]
- 串口确认密码: [password input]
- 注册按钮: [button]

首次登录 Web 网管时，需要设置用户名和密码，用于 Web 网管和 STelnet 登录。还需要设置串口登录的认证方式和认证信息。

此处设置用户名/密码为：admin/Huawei@123，串口认证类型为密码认证，串口密码为 Huawei@123，然后点击“注册”，如下所示。



The image shows the registration page with the following values entered into the form:

- 用户名: admin
- 密码: (masked)
- 确认密码: (masked)
- 串口认证类型: 密码认证
- 串口密码: (masked)
- 串口确认密码: (masked)
- 注册按钮: [button]

注册成功后，注册用户将用于 STelnet 和 Web 网管登录。然后重新输入用户名和密码，点击“登录”，即可进行 Web 网管。

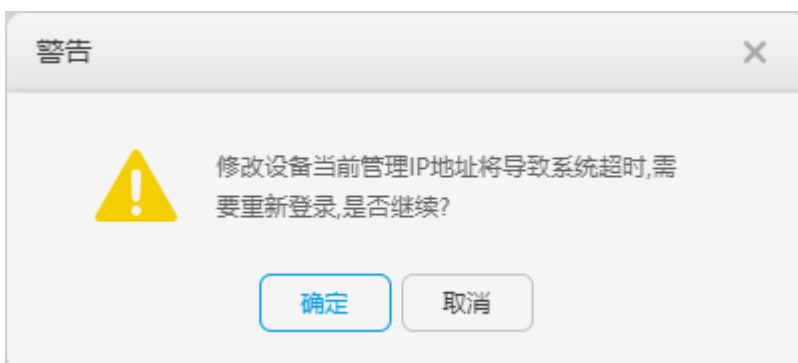


由于在实际的生产网络中，几乎不会使用缺省的管理地址（即 169.254.1.1/24）对设备进行 Web 网管，所以接下来需要对管理地址进行修改。

选择“配置 > AC 配置 > 接口管理”，选择“管理网口”选项卡，配置 WAC1 的 IP 地址为 172.21.39.4，掩码保持不变，最后点击“应用”，如下所示。



修改管理 IP，需要重新登录，点击“确定”。



WAC1 的管理 IP 修改后，需要同步修改 PC 网卡的 IP 地址，本实验中将 PC 网卡地址配置为 172.21.39.100/24，然后使用浏览器访问 https://172.21.39.4，重新进行登录。

登录成功后，发现 WAC1 的管理 IP 已经被成功修改为 172.21.39.4/24，如下所示。



为了实验方便，进一步修改 Web 网管的超时时间，本实验配置为 60 分钟（缺省为 10 分钟），注意，实际的生产网络中出于安全考虑，不建议将 Web 网管的超时时间配置过长。

选择“维护 > AC 维护 > 系统管理”，选择“服务管理”选项卡，将 Web 服务的超时时间修改为 60 分钟，然后点击“应用”，如下所示。



步骤 4 配置 WAC1 设备的 VLAN 和 IP 地址

配置 WAC1 设备。修改 WAC1 设备名称，并创建 VLAN 100、101，修改 GE0/0/1 端口类型为 Trunk，并允许通过 VLAN 100、101。

修改 WAC1 的设备名称。

选择“监控 > AC”，选择“AC 概况”，在“AC 基本信息”中，点击“设备名称”后面的“更改”字样，将设备名称修改为 WAC1。

AC基本信息		
设备型号:	AirEngine9700-M1	
设备名称:	AirEngine9700-M1	[更改]
设备序列号:	102257532103	
MAC地址:	9cb2-e8b5-a224	
系统软件版本:	V200R021C00SPC100	[升级]
License资源已使用数/总数:	0/1024	[查看详情]
AP资源授权license状态:	演示	[查看详情]

重命名 ×

* 设备名称:

在 WAC1 上创建 VLAN 100、101。

选择“配置 > AC 配置 > VLAN”，选择“VLAN”选项卡，点击“批量新建”按钮，新建 VLAN 100、101，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 全局IPv6: OFF

AC配置 **VLAN** VLANIF VLAN Pool

基本配置 新建 删除 **批量新建** 批量删除 刷新

VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan

接口管理

IP 10 共1条

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 AC配置 > VLAN > VLAN > 批量新建VLAN

AC配置 *VLAN ID: (1-4094,格式: 1,3-5,7)

基本配置 **确定** 取消

VLAN

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 全局IPv6: OFF

AC配置 **VLAN** VLANIF VLAN Pool

基本配置 新建 删除 批量新建 批量删除 刷新

VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan
<input type="checkbox"/> 100	VLAN 0100	commonVlan
<input type="checkbox"/> 101	VLAN 0101	commonVlan

接口管理

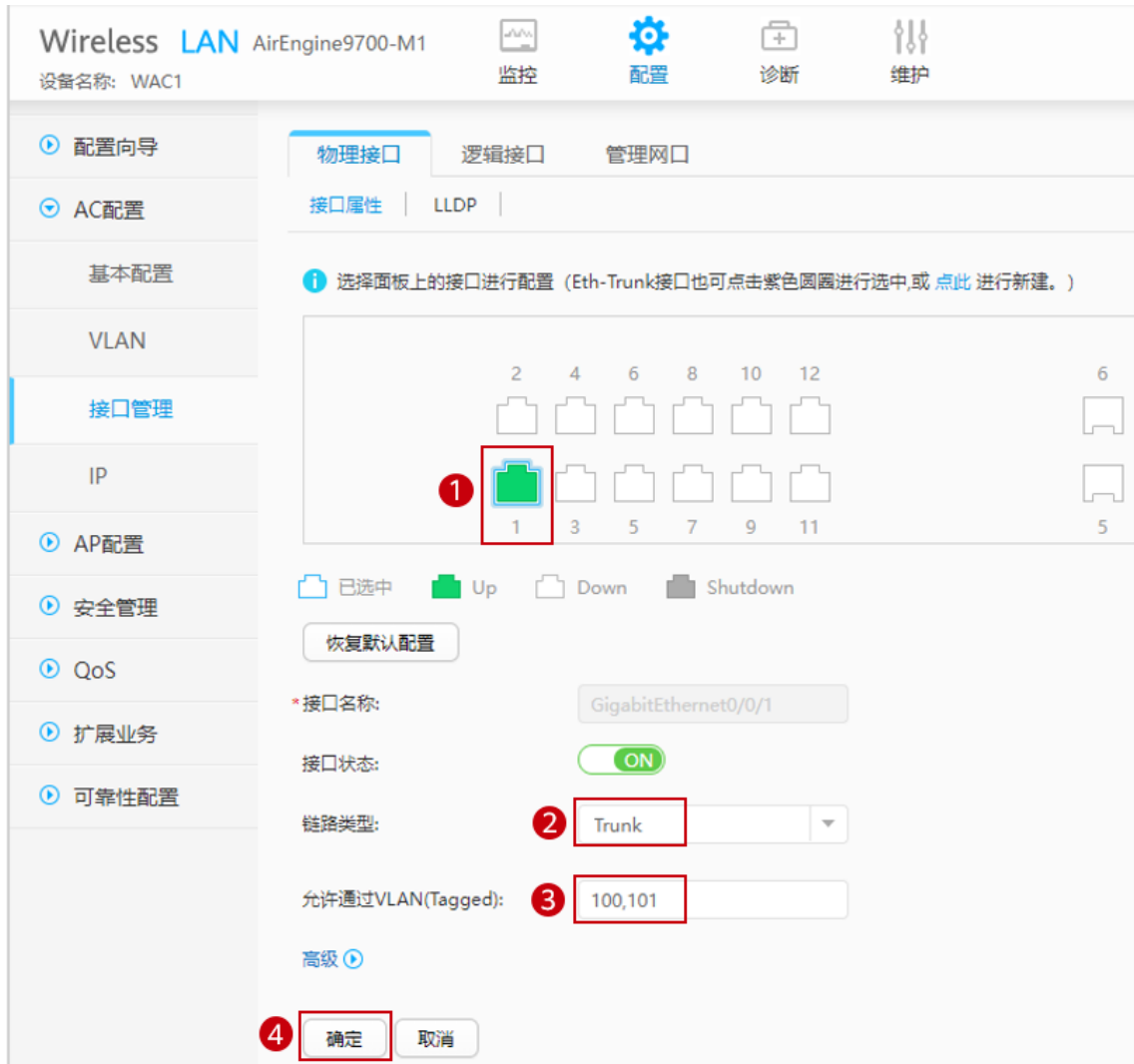
IP 10 共3条

AP配置

安全管理

配置 WAC1 的 GE0/0/1 端口类型及允许通过的 VLAN。

选择“配置 > AC 配置 > 接口管理”，选择“物理接口”选项卡，点击 1 号接口（即 GE0/0/1 接口），配置链路类型为 Trunk，允许通过的 VLAN 为 100 和 101，然后点击“确定”，如下所示。



The screenshot displays the 'Wireless LAN' configuration page for an AirEngine9700-M1 device. The left sidebar shows the navigation menu with '接口管理' (Interface Management) selected. The main area is divided into '物理接口' (Physical Interface), '逻辑接口' (Logical Interface), and '管理网口' (Management Network Port). Under '物理接口', the '接口属性' (Interface Properties) tab is active. A grid of 12 ports is shown, with port 1 highlighted in green and circled with a red '1'. Below the grid, there are controls for '已选中' (Selected), 'Up', 'Down', and 'Shutdown'. A '恢复默认配置' (Restore Default Configuration) button is present. The configuration fields are as follows:

- *接口名称: GigabitEthernet0/0/1
- 接口状态: ON
- 链路类型: Trunk (circled with a red '2')
- 允许通过VLAN(Tagged): 100,101 (circled with a red '3')

At the bottom, there is an '高级' (Advanced) link and a '确定' (Confirm) button circled with a red '4', along with a '取消' (Cancel) button.

创建 Vlanif100 接口，并配置接口 IP 地址。

选择“配置 > AC 配置 > VLAN”，选择“VLANIF”选项卡，点击“新建”。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 AC配置 基本配置 VLAN 接口管理 IP

全局IPv6: OFF

VLAN **VLANIF** VLAN Pool

新建 删除 刷新

接口名称 连接状态 IPv4地址/掩码

Vlanif1 不可用

10 共1条

在“新建 VLANIF”页面中，配置 VLAN ID 为 100，IP 地址为 10.23.100.1，掩码为 255.255.255.0，然后点击“确定”，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 AC配置 基本配置 VLAN 接口管理 IP AP配置 安全管理 QoS 扩展业务 可靠性配置

AC配置 > VLAN > VLANIF > 新建VLANIF

*VLAN ID: 100

MTU (bytes): 1500

管理接口: OFF

IP地址格式: IPv4 IPv6

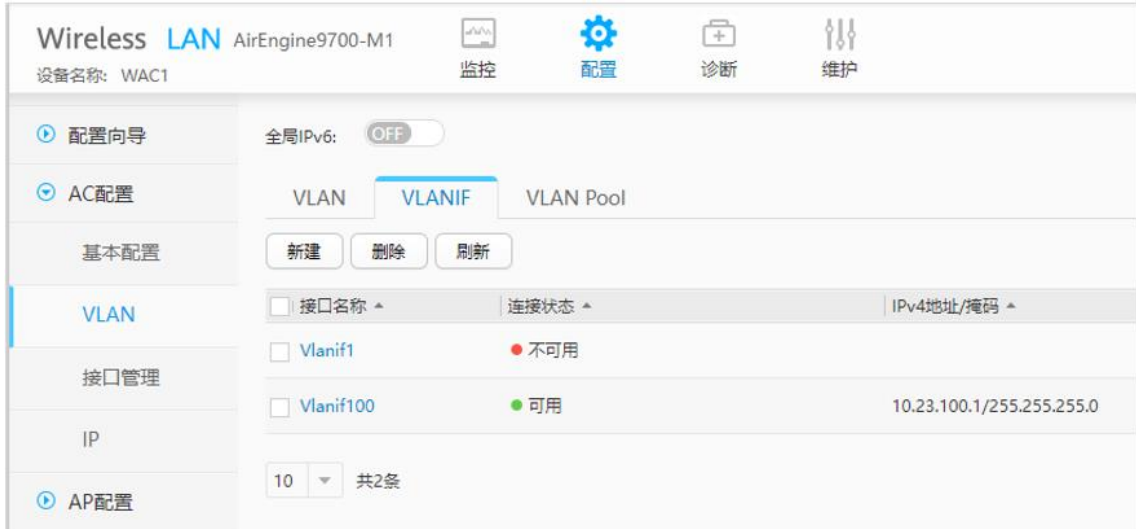
IPv4地址配置

主IP地址/掩码: 10 . 23 . 100 . 1 / 255 . 255 . 255 . 0

从IP地址/掩码: + 添加

高级

确定 取消



步骤 5 配置 DHCP 服务器

启用 DHCP 服务，在 SW-Core 上配置 Vlanif100 端口为 AP 提供 IP 地址。

```
[SW-Core] dhcp enable
[SW-Core] interface vlanif 100
[SW-Core-Vlanif100] dhcp select interface
[SW-Core-Vlanif100] quit
```

在 SW-Core 上配置 Vlanif101 端口为 STA 提供 IP 地址。

```
[SW-Core] interface vlanif 101
[SW-Core-Vlanif101] dhcp select interface
[SW-Core-Vlanif101] quit
```

步骤 6 配置 AP 上线

配置 WAC 基础信息。

选择“配置 > AC 配置 > 基本配置”，选择“AC 基本信息”选项卡，配置 WAC 源地址为 Vlanif100 接口，AP 认证方式为 MAC 认证，如下所示。

展开“高级”选项，配置“CAPWAP 链路配置”，详细配置参数如下所示，此处配置的密码均为 a1234567，然后点击最下方的“应用”按钮。

在弹出的“配置密钥”对话框中，配置 AP 账号的用户名/密码为：admin/Huawei@123，配置离线 VAP 密钥为 a1234567，然后点击“确定”按钮，如下所示。

配置密钥 ✕

i 为提高系统安全性,请完成如下配置。

AP帐号

i 为提高访问AP的安全性,请配置AP的用户名和密码,同时该配置属于全局配置,对所有AP有效。

* 用户名: * 密码:

离线VAP

i AP离线时会发出管理SSID,便于管理员使用无线连接AP,为保证连接的安全性,配置连接管理SSID的密钥。

* 离线VAP密钥:

创建 AP 组。选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“新建”按钮，配置 AP 组名称为 ap-group1，然后点击“确定”，如下所示。

Wireless LAN AirEngine9700-M1 监控 配置 诊断 维护

设备名称: WAC1

配置向导 | **AP组** | 静态负载均衡组

AC配置 | | | |

AP配置

组名称 ^ | VAP模板 ^ | 射频0模板 ^

default | 2.4G-default

AP配置 20 共1条

Wireless LAN AirEngine9700-M1 监控 配置 诊断 维护

设备名称: WAC1

配置向导 | AC配置 | AP配置

AP组配置

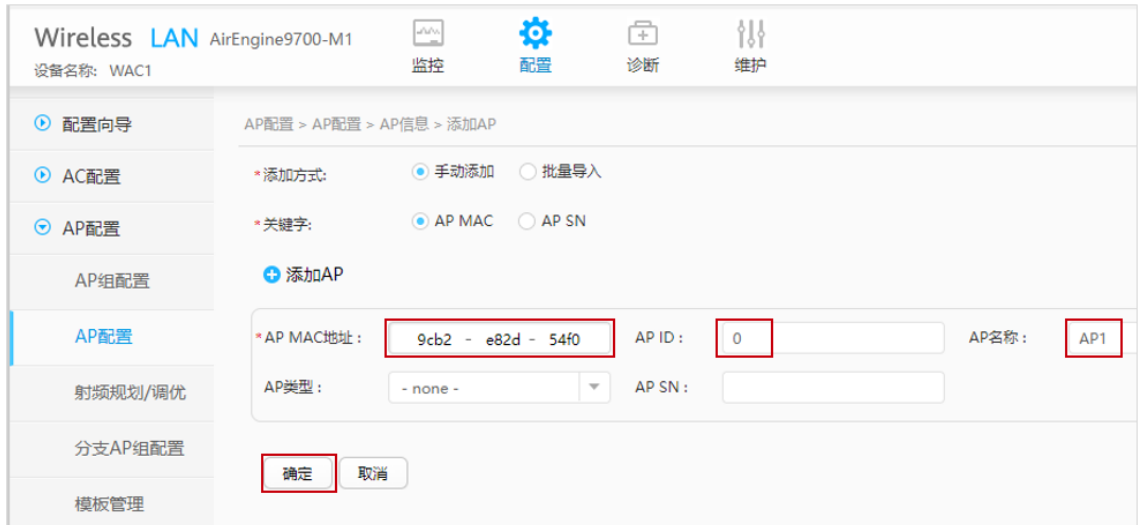
AP配置

AP配置 > AP组配置 > AP组 > 新建AP组

* AP组名称:

在 WAC1 上添加 AP（AP 的 MAC 地址以实际情况为准）。

选择“配置 > AP 配置 > AP 配置”，选择“AP 信息”选项卡，点击“添加”按钮，依次添加 AP1、AP2 和 AP3，此处以添加 AP1 为例进行说明，AP2 和 AP3 的操作步骤类似，不再展示，如下所示。



修改 AP 所属的 AP 组。缺省情况下，新添加的 AP 都位于 default 组，需要将 AP1、AP2 和 AP3 移动至 ap-group1 中。

选择“配置 > AP 配置 > AP 配置”，选择“AP 信息”选项卡，同时选中此三台 AP，点击“修改 AP 配置”按钮，将“AP 组”修改为 ap-group1，然后点击“确定”，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 AC配置 AP配置

AP组配置 AP配置 射频规划/调优 分支AP组配置 模板管理

AP信息 AP白名单 AP黑名单 AP邻居关系 AP设备类型

AP列表

点击AP ID列可进入AP的个性化配置页面。

修改AP配置 添加 替换 删除 加入黑名单 闪灯 清空所有AP 刷新

AP ID	AP MAC地址	AP名称	AP...	IP地址
<input checked="" type="checkbox"/> 0	9cb2-e82d-54f0	AP1	default	10.23.100.174
<input checked="" type="checkbox"/> 1	9cb2-e82d-5410	AP2	default	10.23.100.45
<input checked="" type="checkbox"/> 2	9cb2-e82d-5110	AP3	default	10.23.100.38

10 共3条

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 AC配置 AP配置

AP组配置 AP配置 射频规划/调优 分支AP组配置 模板管理

安全管理 QoS 扩展业务

AP配置 > AP配置 > AP信息 > 修改AP

AP组: ap-group1

AC地址列表: 添加

已选AP列表

AP...	AP MAC地...	AP名称	AP组	IP地址获取方式	IP地址
0	9cb2-e82d-54...	AP1	default	- none -	--
1	9cb2-e82d-54...	AP2	default	- none -	--
2	9cb2-e82d-51...	AP3	default	- none -	--

10 共3条

确定 取消

检查发现，三台 AP 均已属于 ap-group1 组，并且已经获取到 IP 地址，状态为“normal”，AP 上线成功。



The screenshot shows the 'Wireless LAN' configuration page for an AirEngine9700-M1 device. The left sidebar contains navigation options: 配置向导, AC配置, AP配置, AP组配置, AP配置 (selected), 射频规划/调优, 分支AP组配置, and 模板管理. The main content area is titled 'AP信息' and includes a table of APs. A red box highlights the table content.

AP ID	AP MAC地址	AP名称	AP组	IP地址
0	9cb2-e82d-54f0	AP1	ap-group1	10.23.100.174
1	9cb2-e82d-5410	AP2	ap-group1	10.23.100.45
2	9cb2-e82d-5110	AP3	ap-group1	10.23.100.38

步骤 7 配置 WLAN 业务

通过域管理模板配置国家码，缺省国家码为中国（如果设备在中国以外地区，则需要改为设备所在地对应的国家码）。

选择“配置 > AP 配置 > 模板管理 > 射频管理 > 域管理模板”，点击“新建”，配置模板名称为 domain1，然后点击“确定”。



The screenshot shows a dialog box titled '新建域管理模板'. It has a text input field for the template name, which contains 'domain1'. Below the input field are two buttons: '确定' (OK) and '取消' (Cancel).

然后选中 domain1 模板，配置国家码为中国，点击“应用”，如下所示。



域管理模板: 展示模板引用关系

模板介绍信息: 域管理模板提供对国家码、调优信道集合和调优带宽等的配置。

国家码:

4.9G频段使能: ?

[→ 2.4GHZ DCA信道集合](#)

[→ 5GHZ DCA信道集合](#)

在 AP 组中引用域管理模板。

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组的配置界面。



Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置 监控 诊断 维护

配置向导 | AC配置 | AP配置 | AP组配置 | AP配置 | 射频规划/调优

AP组 静态负载均衡组

修改 新建 删除 刷新

组名称 ^	VAP模板 ^	射频0模板 ^
<input type="checkbox"/> default		2.4G-default
<input type="checkbox"/> ap-group1		2.4G-default

20 共2条

在 AP 组配置界面中，选择“射频管理 > 域管理模板”，配置域管理模板为“domain1”，然后点击“应用”，如下所示。（注意：缺省域管理模板为 default）



创建名为“wlan-net”的安全模板，并配置安全策略。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > 安全模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



选择“wlan-net”安全模板，配置如下参数（密钥为 a12345678），点击“应用”。



创建名为“wlan-net”的 SSID 模板，并配置 SSID 名称为“wlan-net”。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > SSID 模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



选择“wlan-net” SSID 模板，配置 SSID 名称为“wlan-net”，点击“应用”。



创建名为“wlan-net”的 VAP 模板，配置业务数据转发模式、业务 VLAN，并且引用安全模板和 SSID 模板。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > VAP 模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



选择“wlan-net” VAP 模板，配置转发模式为直接转发，业务 VLAN 为 101，点击“应用”。

VAP模板: 展示模板引用关系

模板介绍信息: 在VAP模板下配置各项参数,然后在AP组或AP中引用VAP模板,AP上就会生成VAP,VAP用来为STA提供无线接入服务。通过配置VAP模板下的参数,使A

基础配置 高级配置

使能状态: ON

转发模式: ▼

业务VLAN: 单个VLAN VLAN Pool 业务VLAN ID:

配置“wlan-net” VAP 模板所关联的 SSID 模板为“wlan-net”，点击“应用”。

模板管理

- 无线业务
 - VAP模板
 - default
 - wlan-net
 - SSID模板 [default]**
 - 安全模板 [default]
 - 流量模板 [default]
 - 认证模板
 - 终端黑白名单模板
 - 智能应用控制模板
 - UCC模板

* SSID模板: ▼

模板介绍信息: SSID用来指定不同的无线网络。在STA上搜索可

基础配置 高级配置

* SSID名称:

最大用户数:

配置“wlan-net” VAP 模板所关联的安全模板为“wlan-net”，点击“应用”。

模板管理

- 无线业务
 - VAP模板
 - default
 - wlan-net
 - SSID模板 [wlan-ne...]
 - 安全模板 [default]**
 - 流量模板 [default]
 - 认证模板
 - 终端黑白名单模板
 - 智能应用控制模板
 - UCC模板
 - Hotspot2.0模板
 - 攻击防御模板
 - CPE隧道模板
 - SSID模板
 - default
 - wlan-net
 - default-wds
 - default-mesh
 - 流量模板

* 安全模板: ▼

模板介绍信息: 配置WLAN安全策略,可以对无线终端进行身

基础配置 高级配置

Open认证方式存在一定的安全风险,建议采用其他认证方式

* 安全策略: WPA3 WPA2-WPA3 WAPI

认证方式: Dot1x DPSK PPS

WPA加密方式: AES AES-TKIP TK

WPA2加密方式: AES AES-TKIP TK

密钥类型: PASS-PHRASE HEX

* 密钥:

配置 AP 组引用 VAP 模板。

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组的配置界面。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 | AC配置 | AP配置 | **AP组配置** | AP配置 | 射频规划/调优

AP组 | 静态负载均衡组

修改 | 新建 | 删除 | 刷新

组名称	VAP模板	射频0模板
default		2.4G-default
ap-group1		2.4G-default

20 共2条

在 AP 组配置界面中，选择“VAP 配置”，在“VAP 模板列表”中，点击“添加”。

AP配置 > AP组配置 > AP组

AP组配置: ap-group1 查看成员

显示所有模板 配置模型介绍

- VAP配置**
- 射频管理
- AP
- WIDS

VAP 模板列表

相关配置

新建 | **添加** | 移除 | 展示模板引用关系

模板名称

配置 VAP 模板名称为“wlan-net”，WLAN ID 为 1，射频为 0 和 1，点击“确定”。

添加VAP模板

+ 添加

*VAP模板名称: wlan-net *WLAN ID: 1 *射频: 0,1

高级

确定 取消

然后查看“VAP 模板列表”如下。

VAP 模板列表

相关配置

新建 添加 移除 展示模板引用关系

模板名称	SSID模板	认证模板	安全模板	WLAN ID	射频	转发模式	业务VLAN	使能状...
<input type="checkbox"/> wlan-net	wlan-net		wlan-net	1	0	直接转发	101	● 开启
<input type="checkbox"/> wlan-net	wlan-net		wlan-net	1	1	直接转发	101	● 开启

10 共2条

1.3 结果验证

1.3.1 查看 AP 上线状况、SSID 等信息

选择“监控 > AP”，选择“AP 统计”选项卡，可以查看 AP 的状态信息，其中“normal”代表 AP 已正常上线。

AP列表

智能诊断 上线失败记录 下线记录 SoftGRE隧道状态 导出信息 IoT插卡信息

AP ID	AP名称	AP组	状态名称
0	AP1	ap-group1	● normal
1	AP2	ap-group1	● normal
2	AP3	ap-group1	● normal

10 共3条

总AP数 : 3 normal : 3

AirEngine5761-11 : 3

选择“监控 > SSID”，选择“VAP”选项卡，可以查看 VAP 关联的 AP 名称、SSID 名称、BSSID 名称、认证方式、状态等信息。

SSID VAP

自动刷新: OFF

AP型VAP列表

应用统计清零

AP ID ▲	AP名称 ▲	射频ID ▲	WLAN ID ▲	SSID ▲	BSSID ▲	认证方式 ▲	接入用户数 ▲	状态 ▲
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA/WPA2-PSK	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA/WPA2-PSK	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA/WPA2-PSK	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA/WPA2-PSK	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA/WPA2-PSK	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA/WPA2-PSK	0	on

10 共6条

注: 选择列表中的VAP,查看该VAP应用统计信息。

1.3.2 终端关联无线信号，测试网络连通性

STA 扫描接入无线网络“wlan-net”。



测试 STA 与业务网关的网络连通性。

```
C:\Windows\system32>ping 10.23.101.254

正在 Ping 10.23.101.254 具有 32 字节的数据:
来自 10.23.101.254 的回复: 字节=32 时间=4ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=8ms TTL=254

10.23.101.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 4ms, 最长 = 8ms, 平均 = 6ms
```

1.4 配置参考

1.4.1 WAC1 配置

Software Version V200R021C00SPC100

```
#
 sysname WAC1
#
 http secure-server ssl-policy default_policy
 http server enable
#
 vlan batch 100 to 101
#
 stp enable
#
 authentication-profile name default_authen_profile
 authentication-profile name dot1x_authen_profile
 authentication-profile name mac_authen_profile
 authentication-profile name macportal_authen_profile
 authentication-profile name portal_authen_profile
#
 ssl policy default_policy type server
  pki-realm default
  version tls1.2
  ciphersuite ecdhe_rsa_aes128_gcm_sha256 ecdhe_rsa_aes256_gcm_sha384
#
 aaa
 authentication-scheme default
  authentication-mode local
 authentication-scheme radius
  authentication-mode radius
 authorization-scheme default
  authorization-mode local
 accounting-scheme default
  accounting-mode none
 local-aaa-user password policy administrator
 domain default
  authentication-scheme default
  accounting-scheme default
  radius-server default
 domain default_admin
  authentication-scheme default
  accounting-scheme default
 local-user admin password irreversible-cipher
 $1a$Z#*{";)lk6$LUMXJS;VWR$p7mWZtx|EN3q#M`}27Bg+[8<)ELp.$
 local-user admin privilege level 15
 local-user admin service-type telnet ssh http
#
 interface Vlanif100
  ip address 10.23.100.1 255.255.255.0
#
 interface MEth0/0/1
  ip address 172.21.39.4 255.255.255.0
```

```
#
interface Ethernet0/0/47
 ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
capwap source interface vlanif100
capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%#
capwap dtls inter-controller psk %^%#tc.5LFZ\o]^\bM8'*YYv#<te,1Oq8kAL.}J+v{puP%^%#
capwap message-integrity psk %^%#eJ&eRx\$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x*%^%#
capwap sensitive-info psk %^%#;,L1<.L'e+li6MX,^QxH{6z#&#z[v4Oe"pCPrFJ'%^%#
capwap inter-controller sensitive-info psk %^%#ji6gT7>2y3dm}n~Bb"%8z$0]B62~|NkD,WJF[n2U%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
wlan
 temporary-management psk %^%#PwFE@vw_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
 ap username admin password cipher %^%#PBMhAQ{[@]1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)I%^%#
 traffic-profile name default
 security-profile name default
 security-profile name wlan-net
   security wpa-wpa2 psk pass-phrase %^%#51sYLQj@,Ph}m2@A1j:Of3n/)t5j=+!"K+9yB{.%%^%# aes
 security-profile name default-wds
 security-profile name default-mesh
 ssid-profile name default
 ssid-profile name wlan-net
   ssid wlan-net
 vap-profile name default
 vap-profile name wlan-net
   service-vlan vlan-id 101
   ssid-profile wlan-net
   security-profile wlan-net
 wds-profile name default
 mesh-handover-profile name default
 mesh-profile name default
 regulatory-domain-profile name default
 regulatory-domain-profile name domain1
 air-scan-profile name default
 rrm-profile name default
 radio-2g-profile name default
 radio-5g-profile name default
 wids-spoof-profile name default
 wids-whitelist-profile name default
 wids-profile name default
 wireless-access-specification
 ap-system-profile name default
```

```
port-link-profile name default
wired-port-profile name default
ap-group name default
ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
    vap-profile wlan-net wlan 1
  radio 1
    vap-profile wlan-net wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0
  ap-name AP1
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410
  ap-name AP2
  ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110
  ap-name AP3
  ap-group ap-group1
provision-ap
#
return
```

1.4.2 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 100 to 101
#
dhcp enable
#
interface Vlanif1
#
interface Vlanif100
  ip address 10.23.100.254 255.255.255.0
  dhcp select interface
#
interface Vlanif101
  ip address 10.23.101.254 255.255.255.0
  dhcp select interface
#
interface MEth0/0/1
  ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
```

```
#
interface MultiGE0/0/4
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

1.4.3 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
port link-type trunk
```

```
port trunk allow-pass vlan 100 to 101
#
return
```

1.5 思考题

在无线控制器上配置无线业务时，通常将 AP 进行分组，然后基于 AP 组进行业务配置，请思考以下问题：为什么不推荐基于单 AP 配置无线业务？

参考答案：

基于单个 AP 配置 WLAN 业务，则管理员需要在每个 AP 上分别配置 WLAN 业务参数，当 AP 数量较多时，配置工作量随之增加；且当配置变更时，也需要逐一修改每个 AP 的配置，不易于运维管理。而基于 AP 组进行配置，可以很好的解决此问题。

2 Leader AP 组网实验

2.1 实验介绍

2.1.1 关于本实验

本实验通过 Leader AP 组网场景的配置与结果验证，实现 AP 和 STA 上线，让学员能够掌握 Leader AP 组网的部署方法。

2.1.2 实验目的

- 描述 Leader AP 的组网架构。
- 掌握 Leader AP 组网的 WLAN 业务配置方法。
- 了解 Leader AP 的业务检查方法。

2.1.3 实验组网介绍

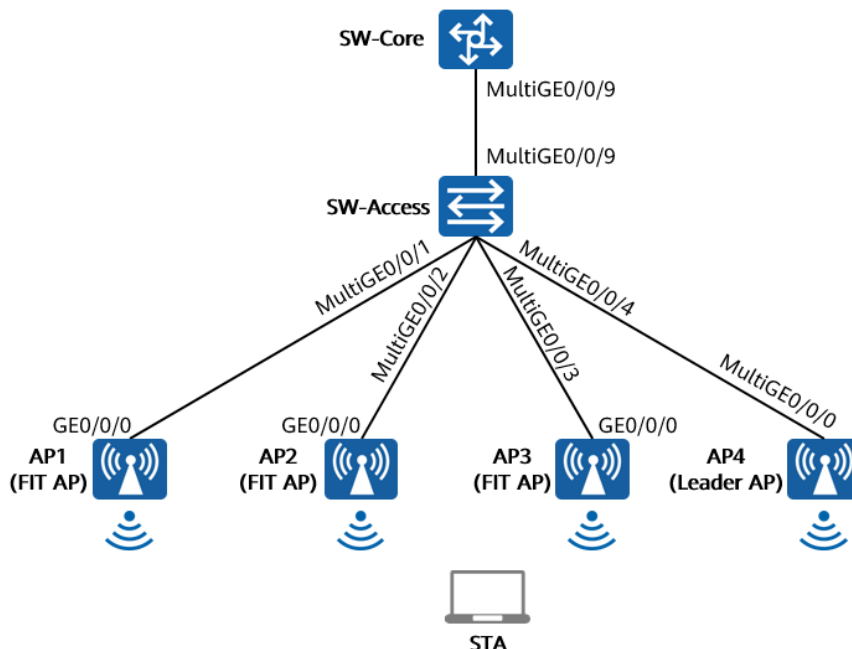


图2-1 Leader AP 组网实验拓扑图

在 Leader AP 组网拓扑图中，AP1、AP2、AP3 为 FIT AP，AP4 为 Leader AP，Leader AP 统一管理无线网络。

SW-Core 是核心交换机，同时作为 DHCP 服务器，为 AP 和 STA 分配 IP 地址。SW-Access 是接入交换机，为 AP 提供 PoE 供电服务。

2.1.4 实验规划

表2-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/4	Trunk	PVID:100 Allow-pass: VLAN 100 101

表2-2 IP 地址规划

设备	端口	IP地址
SW-Core	VLANif 100	10.23.100.254/24
	VLANif 101	10.23.101.254/24
Leader AP	VLANif 100	DHCP动态获取

表2-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	100
业务VLAN	101
AP组	default
VAP模板	系统自动生成

安全模板	系统自动生成
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	系统自动生成
SSID	wlan-net
AP Zone	default

2.2 实验任务配置

2.2.1 配置思路

- 1.配置 SW-Core、SW-Access 的 VLAN 信息、端口模式。
- 2.配置 SW-Core 作为 DHCP 服务器，确保 AP 能够获取 IP 地址。
- 3.设置 AP4 的工作模式为 FAT 模式。
- 4.配置 AP4 的名称及系统时间，并检查 AP 上线情况。
- 5.配置 WLAN 业务参数，实现 STA 访问 WLAN 网络。

2.2.2 配置步骤

步骤 1 配置 VLAN 信息

- # 配置接入交换机 SW-Access 设备，创建 VLAN 100、101，下行接口允许 VLAN 100、101，PVID 为 100，上行接口允许 VLAN 100、101，PVID 使用缺省值 VLAN 1。
- # 在 SW-Access 上创建 VLAN 100、101。

```
<Huawei> system-view
[Huawei] sysname SW-Access
[SW-Access] vlan batch 100 101
```

- # 配置 SW-Access 下行端口类型及允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/1
[SW-Access-MultiGE0/0/1] port link-type trunk
[SW-Access-MultiGE0/0/1] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/1] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/1] quit
[SW-Access] interface MultiGE 0/0/2
[SW-Access-MultiGE0/0/2] port link-type trunk
[SW-Access-MultiGE0/0/2] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/2] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/2] quit
```

```
[SW-Access] interface MultiGE 0/0/3
[SW-Access-MultiGE0/0/3] port link-type trunk
[SW-Access-MultiGE0/0/3] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/3] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/3] quit
[SW-Access] interface MultiGE 0/0/4
[SW-Access-MultiGE0/0/4] port link-type trunk
[SW-Access-MultiGE0/0/4] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/4] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/4] quit
```

配置 SW-Access 上行端口类型及允许通过的 VLAN。

```
[[SW-Access] interface MultiGE 0/0/9
[SW-Access-MultiGE0/0/9] port link-type trunk
[SW-Access-MultiGE0/0/9] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/9] quit
```

配置核心交换机 SW-Core，创建 VLAN 100、101，下行接口允许 VLAN 100、101。

在 SW-Core 上创建 VLAN 100 和 VLAN 101。

```
<Huawei> system-view
[Huawei] sysname SW-Core
[SW-Core] vlan batch 100 101
```

配置 SW-Core 下行端口类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/9
[SW-Core-MultiGE 0/0/9] port link-type trunk
[SW-Core-MultiGE 0/0/9] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE 0/0/9] quit
```

步骤 2 配置 DHCP 服务器

配置 SW-Core 作为 DHCP 服务器为 STA 和 AP 分配 IP 地址。

启用 DHCP 服务，在 SW-Core 上配置 Vlanif100 接口为 AP 提供 IP 地址。

```
[SW-Core] dhcp enable
[SW-Core] interface vlanif 100
[SW-Core-Vlanif100] ip address 10.23.100.254 24
[SW-Core-Vlanif100] dhcp select interface
[SW-Core-Vlanif100] quit
```

在 SW-Core 上配置 Vlanif101 接口为 STA 提供 IP 地址。

```
[SW-Core] interface vlanif 101
[SW-Core-Vlanif101] ip address 10.23.101.254 24
[SW-Core-Vlanif101] dhcp select interface
[SW-Core-Vlanif101] quit
```

在 SW-Core 上查看 AP1、AP2、AP3、AP4 获取到的 IP 地址。

```
[SW-Core] display ip pool interface Vlanif100 used
Pool-name      : Vlanif100
```

```

Pool-No      : 0
Lease       : 1 Days 0 Hours 0 Minutes
Domain-name  : -
DNS-server0 : -
NBNS-server0 : -
Netbios-type : -
Position    : Interface
Status     : Unlocked
Gateway-0   : -
Network    : 10.23.100.0
Mask       : 255.255.255.0
VPN instance : --
Logging     : Disable
Conflicted address recycle interval: -
Address Statistic: Total      :254      Used      :4
                   Idle       :250      Expired   :0
                   Conflict    :0       Disabled  :0
-----
Network section
      Start      End      Total      Used Idle(Expired) Conflict Disabled
-----
      10.23.100.1 10.23.100.254 254      4      250(0)      0      0
-----
Client-ID format as follows:
DHCP   : mac-address           PPPoE   : mac-address
IPSec  : user-id/portnumber/vrf PPP      : interface index
L2TP   : cpu-slot/session-id   SSL-VPN : user-id/session-id
-----
Index      IP      Client-ID      Type      Left      Status
-----
116  10.23.100.117  9cb2-e82d-5110  DHCP      86299  Used
170  10.23.100.171  eca1-d1f7-7dd0  DHCP      86299  Used
213  10.23.100.214  9cb2-e82d-5410  DHCP      86329  Used
224  10.23.100.225  9cb2-e82d-54f0  DHCP      86304  Used
-----
    
```

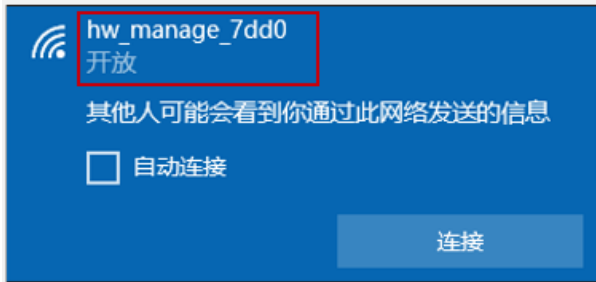
可以看到 AP1~AP4 均获取到 IP 地址（获取地址以实际情况为准）。

步骤 3 切换 AP4 工作模式

缺省情况下，AP 的工作模式为 FIT AP 模式，需要首先将 AP4 切换至 FAT AP 模式。

本实验中 AP4 的 MAC 地址为 eca1-d1f7-7dd0，Leader AP 的缺省 IP 地址为 169.254.2.1/24。

使用管理 PC 搜索附近 SSID 为 “hw_manage_7dd0” 的无线信号并连接，管理 PC 的无线网卡会自动获取到 169.254.2.0/24 网段的 IP 地址（若无法自动获取，可手动配置管理 PC 地址，如：169.254.2.100/24），如下所示。



使用浏览器访问 <https://169.254.2.1>，对 AP4 进行管理。初次登录 AP4，需要配置用户名/密码，本实验配置用户名为 admin，密码为 Huawei@123，如下所示。





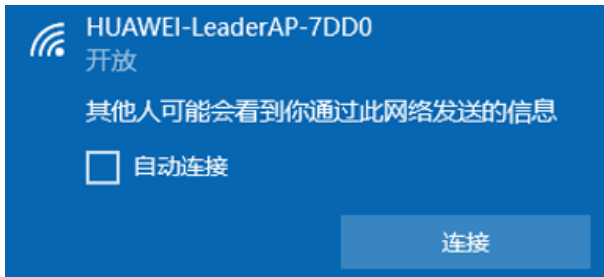
重新登录 AP4，如下所示。



修改 AP4 的模式为 FAT AP，然后 AP4 将会自动重启。



AP4 重启后，搜索名称为“HUAWEI-LeaderAP-7DD0”的 SSID 并连接，若 AP 版本为 V200R021C00 及之前版本，AP 访问地址为 https://192.168.1.1；若 AP 版本为 V200R021C01 及之后版本，AP 访问地址为 https://169.254.2.1。



初次登录 Leader AP，需要配置用户名/密码、串口认证等基本信息。本实验密码均配置为“Huawei@123”。



在弹出的页面中，配置 FIT AP 账号、离线 VAP，密码均配置为“Huawei@123”。



步骤 4 配置 AP 名称及系统时间

登录 AP4 后，系统会自动提示配置 AP 名称及系统时间。

AP 设备名称配置为“Leader AP”，所在国家、时区请根据实际情况配置，此处配置国家为“中国”，时区为“UTC + 08:00:00”，系统时间选择“手动设置”，并点击“使用 PC 当前时间”，最后点击“应用”。

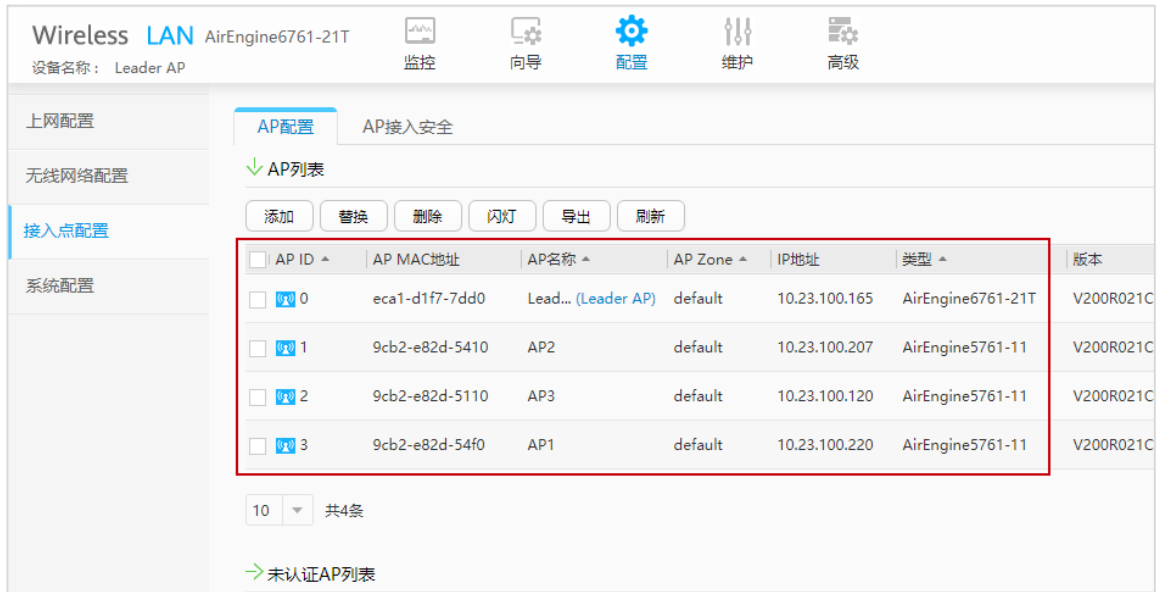


步骤 5 检查 AP 上线情况

由于 Leader AP 缺省的 AP 认证方式为不认证，所以 AP1、AP2、AP3 获取到 IP 地址后，会自动在 Leader AP 中上线，无需任何配置。

选择“配置 > 接入点配置”，可以看到 AP 均已正常上线，其中 AP ID 为 0 的 AP 代表 Leader AP 自身。缺省情况下，所有 AP 均位于“default” AP Zone 中。

在“AP 配置”界面中，点击“修改”按钮，可以修改 AP 的名称。修改后如下所示。



AP ID	AP MAC地址	AP名称	AP Zone	IP地址	类型	版本
0	eca1-d1f7-7dd0	Lead... (Leader AP)	default	10.23.100.165	AirEngine6761-21T	V200R021C
1	9cb2-e82d-5410	AP2	default	10.23.100.207	AirEngine5761-11	V200R021C
2	9cb2-e82d-5110	AP3	default	10.23.100.120	AirEngine5761-11	V200R021C
3	9cb2-e82d-54f0	AP1	default	10.23.100.220	AirEngine5761-11	V200R021C

步骤 6 配置 WLAN 业务参数

使用配置向导配置 WLAN 业务参数。选择“向导 > 配置向导”，点击“多 AP 配置向导”，如下所示。



单AP配置向导

适用于您只有一个AP的情况,可使用该AP作为网关或者作为现有网络的拓展。

多AP配置向导

适用于门店、办公室等场景。由其中一个AP作为Leader AP,其他AP作为FitAP进行管理。

上网模式配置为“桥接模式”。本实验中 AP 网关及业务网关均位于 SW-Core 上，AP 的管理 VLAN 为 VLAN 100，业务 VLAN 为 VLAN 101。

Wireless LAN AirEngine6761-21T
设备名称： Leader AP

监控 向导 配置 维护 高级

配置向导

*上网模式：
桥接模式



上网连接设置

MultiGE0 GE0

已选中 Up Down Shutdown

配置 Wi-Fi 信号设置。无线网络名称设置为“wlan-net”，业务 VLAN ID 为 101，加密方式为“密码认证”，密钥为“a12345678”，生效射频全部勾选，点击“应用”。

Wi-Fi信号设置

*无线网络名称：
wlan-net

业务VLAN ID：
101

加密方式：
密码认证

*密钥：

生效射频：
 2.4GHz 5GHz(Radio1) 5G/6GHz(Radio2)

单用户上行限速(Kbps)：
不限速

单用户下行限速(Kbps)：
不限速

终端黑白名单：
 终端白名单 终端黑名单 关闭

应用

2.3 结果验证

2.3.1 查看 AP 上线状态、SSID 等信息

在 Web 页面中，点击“监控”，可以查看 AP 上线状态、SSID、设备状态等信息。



The screenshot displays the 'Wireless LAN' management interface for an AirEngine6761-21T device. The page is divided into two main sections: '接入点' (Access Points) and '网络' (Networks).

接入点 (Access Points) Section:

- Navigation: 接入点 (selected), 向导, 配置, 维护, 高级
- Table Columns: 接入点, 用户数, AP Zone, 状态
- Table Data:

接入点	用户数	AP Zone	状态
Leader... (Leader AP)	1	default	● normal
AP1	0	default	● normal
AP2	0	default	● normal
AP3	0	default	● normal
- Footer: 5 共4条

网络 (Networks) Section:

- Navigation: SSID名称
- Table Columns: SSID名称, 用户数
- Table Data:

SSID名称	用户数
wlan-net	0
HUAWEI-LeaderAP-7DD0	1
- Footer: 5 共2条



2.3.2 查看射频状态信息

选择“高级 > 射频配置 > 射频规划”，可以查看当前射频状态信息。

Wireless LAN AirEngine6761-21T
设备名称: Leader AP

监控 向导 配置 维护 高级

AP配置
射频配置
射频规划
射频参数
接口管理
IP业务
安全管理

→ 2.4GHZ DCA信道集合
→ 5GHZ DCA信道集合

射频列表

立即调优 导入配置 导出配置 刷新 识别冗余射频

AP ID	AP名称	射频ID	频段	工作模式	射频状态	频宽 / 信道
2	AP3	0	2.4G	正常模式	on	自动 20M/11
2	AP3	1	5G	正常模式	on	自动 20M/48
1	AP2	0	2.4G	正常模式	on	自动 20M/11
1	AP2	1	5G	正常模式	on	自动 20M/40
3	AP1	0	2.4G	正常模式	on	自动 20M/6
3	AP1	1	5G	正常模式	on	自动 20M/153
0	Leader AP	0	2.4G	正常模式	on	自动 20M/6
0	Leader AP	1	5G	正常模式	on	自动 20M/161
0	Leader AP	2	5G	正常模式	on	自动 20M/48

10 共9条

2.3.3 查看 VLAN 信息

在配置 Leader AP 时，管理 VLAN 及业务 VLAN 均会自动创建，无需单独配置。

选择“高级 > 接口管理 > VLAN”，可以查看 VLAN 信息。



2.3.4 STA 接入无线网络，测试网络连通性

STA 扫描接入无线网络 “wlan-net”。



测试 STA 与业务网关的网络连通性。

```
C:\Windows\system32>ping 10.23.101.254

正在 Ping 10.23.101.254 具有 32 字节的数据:
来自 10.23.101.254 的回复: 字节=32 时间=4ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=8ms TTL=254

10.23.101.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 4ms, 最长 = 8ms, 平均 = 6ms
```

2.4 配置参考

2.4.1 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
```

```
vlan batch 100 to 101
#
dhcp enable
#
interface Vlanif1
#
interface Vlanif100
 ip address 10.23.100.254 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.254 255.255.255.0
 dhcp select interface
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
return
```

2.4.2 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
```

```
interface MultiGE0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
return
```

2.4.3 Leader AP 配置

```
Software Version V200R021C00SPC200
#
 http secure-server ssl-policy default_policy
 http secure-server server-source -i Vlanif1
 http server enable
#
vlan batch 100 to 101
#
dhcp enable
#
acl name nat 2000
 rule 1 permit
#
interface Vlanif1
 nat outbound 2000
 ip address dhcp-alloc unicast
#
interface Vlanif100
 ip address 169.254.2.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 169.254.2.1
#
interface Vlanif101
#
interface Ethernet0/0/47
```



```
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/0
port hybrid tagged vlan 2 to 4094
dhcp snooping trusted
#
interface MultiGEO/0/0
port hybrid tagged vlan 2 to 4094
dhcp snooping trusted
#
interface NULL0
#
interface LoopBack1023
ip address 192.168.254.254 255.255.255.255
#
capwap dtls control-link encrypt off
#
wlan
temporary-management psk %^%#G6e>(-F%#0224pAP=ww-{d9uW99'GH<=Ls829jd2%^%#
ap username admin password cipher %^%#2:|"2joHRTx#3S:3RhXG.C)-HN+d--t@^y<1i8E,%^%#
traffic-profile name default
traffic-profile name huawei-leaderap
traffic-profile name webf0BpYGRa8w7E
security-profile name default
security-profile name huawei-leaderap
security open
security-profile name webf0BpYGRa8w7E
security wpa-wpa2 psk pass-phrase %^%#.F}COC([W0!x-j"1FZJK),9M<:!]KL1%8NY)]i65%^%# aes
ssid-profile name default
ssid-profile name huawei-leaderap
ssid HUAWEI-LeaderAP-7DD0
ssid-profile name webf0BpYGRa8w7E
ssid wlan-net
vap-profile name huawei-leaderap
service-vlan vlan-id 100
ssid-profile huawei-leaderap
security-profile huawei-leaderap
traffic-profile huawei-leaderap
type leaderap-management
radio 0 1 2
vap-profile name webf0BpYGRa8w7E
service-vlan vlan-id 101
ssid-profile webf0BpYGRa8w7E
security-profile webf0BpYGRa8w7E
traffic-profile webf0BpYGRa8w7E
ap-zone default
radio 0 1 2
regulatory-domain-profile name default
```

```
dca-channel 5g bandwidth 20mhz
dca-channel 6g bandwidth 20mhz
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-whitelist-profile name default
wids-profile name default
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
ap-group name default
ap-id 0 type-id 151 ap-mac eca1-d1f7-7dd0
  ap-name Leader-AP
ap-id 1 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
  ap-name AP1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
  ap-name AP2
ap-id 3 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
  ap-name AP3
provision-ap
#
return
```

2.5 思考题

Leader AP 组网中桥接模式与网关模式的区别是什么？

参考答案：

桥接模式是指 Leader AP 不做网关，起桥接作用，上行方向使用一台独立的网关设备，Leader AP 和 FIT AP 在一个二层网络内互通。由独立网关开启 DHCP 服务给用户和 AP 分配 IP 地址，业务的转发方式使用直接转发，流量不会全部经过 Leader AP 处理。

网关模式是指 Leader AP 作为网关，不使用独立网关设备，Leader AP 和 FIT AP 在一个二层网络内互通。Leader AP 上行连接外网，开启 NAT，下行连接交换机，Leader AP 开启 DHCP 服务给 FIT AP 和用户分配 IP 地址，组网比桥接模式简单。业务的转发方式为隧道转发，流量都会经过 Leader AP 处理。

3 VRRP 热备份实验

3.1 实验介绍

3.1.1 关于本实验

本实验通过 WLAN 可靠性组网的调试与配置，让学员掌握华为 WLAN 可靠性组网方案的部署方式。

3.1.2 实验目的

- 描述 WLAN 可靠性组网方式。
- 掌握 VRRP 双机热备组网配置。

3.1.3 实验组网介绍

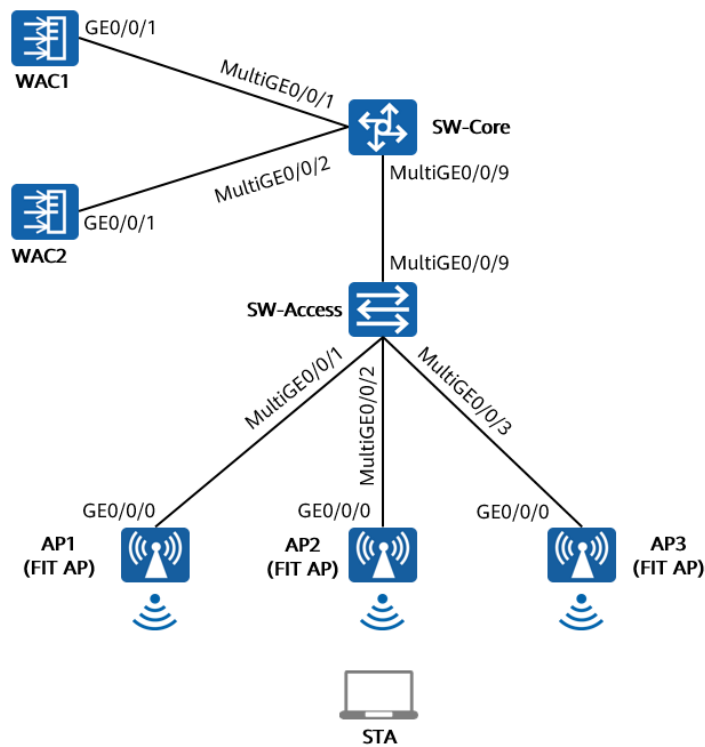


图3-1 VRRP 热备份实验拓扑图

3.1.4 实验规划

表3-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
WAC2	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表3-2 IP 地址规划

设备	端口	IP地址	备注
WAC1	Vlanif100	10.23.100.1/24	用于无线配置同步
WAC2	Vlanif100	10.23.100.2/24	用于无线配置同步
SW-Core	Vlanif100	10.23.100.254/24	管理VLAN, DHCP启用
	Vlanif101	10.23.101.254/24	业务VLAN, DHCP启用
VRRP虚地址	/	10.23.100.33	与AP建立CAPWAP隧道

表3-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	100
业务VLAN	101
HSB通道VLAN	100
AP组	ap-group1
VAP模板	wlan-net
安全模板	wlan-net
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	wlan-net
SSID	wlan-net
无线配置同步PSK	Huawei@123

3.2 实验任务配置

3.2.1 配置思路

- 1.配置 WAC1、WAC2、AP、SW-Core、SW-Access 设备网络互通。
- 2.配置 DHCP 服务器。
- 3.配置 VRRP 双机热备。
- 4.配置无线配置同步功能。
- 5.配置 WLAN 业务。

3.2.2 配置步骤

步骤 1 配置交换机 VLAN 及 IP 地址

- # 配置核心交换机 SW-Core 设备，创建 VLAN 100、101，配置端口模式并放行相应 VLAN。
- # 在 SW-Core 上创建 VLAN 100 和 VLAN 101。

```
<Huawei> system-view
[Huawei] sysname SW-Core
```

```
[SW-Core] vlan batch 100 101
```

配置 SW-Core 下行端口类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/9
[SW-Core-MultiGE 0/0/9] port link-type trunk
[SW-Core-MultiGE 0/0/9] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE 0/0/9] quit
```

配置 SW-Core 与 WAC1、WAC2 互联端口类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/1
[SW-Core-MultiGE 0/0/1] port link-type trunk
[SW-Core-MultiGE 0/0/1] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE 0/0/1] quit
[SW-Core] interface MultiGE 0/0/2
[SW-Core-MultiGE 0/0/2] port link-type trunk
[SW-Core-MultiGE 0/0/2] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE 0/0/2] quit
```

配置接入交换机 SW-Access 设备，创建 VLAN 100、101，下行端口允许通过 VLAN 100、101，PVID 为 100，上行端口允许通过 VLAN 100、101，PVID 使用缺省值 VLAN 1。

在 SW-Access 上创建 VLAN 100、101。

```
<Huawei> system-view
[Huawei] sysname SW-Access
[SW-Access] vlan batch 100 101
```

配置 SW-Access 下行端口类型及允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/1
[SW-Access-MultiGE0/0/1] port link-type trunk
[SW-Access-MultiGE0/0/1] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/1] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/1] quit
[SW-Access] interface MultiGE 0/0/2
[SW-Access-MultiGE0/0/2] port link-type trunk
[SW-Access-MultiGE0/0/2] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/2] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/2] quit
[SW-Access] interface MultiGE 0/0/3
[SW-Access-MultiGE0/0/3] port link-type trunk
[SW-Access-MultiGE0/0/3] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/3] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/3] quit
```

配置 SW-Access 上行端口类型及允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/9
[SW-Access-MultiGE0/0/9] port link-type trunk
[SW-Access-MultiGE0/0/9] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/9] quit
```

配置 SW-Core 的 IP 地址。

```
[SW-Core] interface vlan 100
[SW-Core-Vlanif100] ip address 10.23.100.254 24
[SW-Core-Vlanif100] quit
[SW-Core] interface vlan 101
[SW-Core-Vlanif101] ip address 10.23.101.254 24
[SW-Core-Vlanif101] quit
```

步骤 2 初始化 WAC 设备

- # 初始化 WAC1 和 WAC2 的配置过程请参考 1.2.2 步骤 3，不再赘述。
- # WAC1 的管理地址配置为 172.21.39.4/24，WAC2 的管理地址配置为 172.21.39.5/24。

步骤 3 配置 WAC 的 VLAN 及 IP 地址

- # WAC1、WAC2 的 VLAN 及 IP 地址配置过程请参考 1.2.2 步骤 4，不再赘述。
- # WAC1 的 Vlanif100 接口地址配置为 10.23.100.1/24，WAC2 的 Vlanif100 接口地址配置为 10.23.100.2/24。

步骤 4 配置 DHCP 服务器

- # SW-Core 作为 DHCP 服务器为 STA 和 AP 分配 IP 地址。在 SW-Core 上启用 DHCP 服务，配置 Vlanif100 端口为 AP 提供 IP 地址，并排除掉部分 IP 地址（WAC 接口地址、VRRP 协议虚地址等），以避免 IP 地址冲突。

```
[SW-Core] dhcp enable
[SW-Core] interface vlanif 100
[SW-Core-Vlanif100] dhcp select interface
[SW-Core-Vlanif100] dhcp server excluded-ip-address 10.23.100.1 10.23.100.3
[SW-Core-Vlanif100] dhcp server excluded-ip-address 10.23.100.33
[SW-Core-Vlanif100] quit
```

- # 在 SW-Core 上配置 Vlanif101 端口为 STA 提供 IP 地址。

```
[SW-Core] interface vlanif 101
[SW-Core-Vlanif101] dhcp select interface
[SW-Core-Vlanif101] quit
```

步骤 5 配置 VRRP 双机热备（WAC1）

- # 选择“配置 > 可靠性配置 > VRRP/BFD”，配置 VRRP 备份组的状态恢复响应延迟时间为 60 秒，点击“应用”使配置生效。同时在 VRRP 列表中点击“新建”，创建一个 VRRP 组，并按照如下参数进行配置。
- # 注意：WAC1 为主用设备，VRRP 虚地址配置为 10.23.100.33，优先级配置为 120。

Wireless LAN AirEngine9700-M1

设备名称: WAC1

监控
配置
诊断
维护

- 配置向导
- AC配置
- AP配置
- 安全管理
- QoS
- 扩展业务
- 可靠性配置
- VRRP/BFD

VRRP列表
BFD

高级配置

状态恢复响应延迟时间(秒):

VRRP协议版本: 版本2 版本3

免费ARP报文发送: ON

应用

VRRP VRRP6

i VRRP基于IPv4类型进行配置。

VRRP列表

新建 删除 刷新

VRID ▲ | ▲ | ▲ | ▲

新建VRID
✕

i 普通VRRP组的主备状态可以跟随管理VRRP组的主备状态,建议先创建管理VRRP组。

* VLANIF/IP: /

* VRID: VRRP类型:

* 虚拟IP地址: + 添加 ✕ 优先级:

抢占模式: ON ?

抢占延迟时间(秒):

绑定VRRP组

管理VRID: 管理VRRP接口:

绑定BFD

高级 ▶

确定 取消

配置 HSB 通道，使能双机热备功能。

选择“配置 > 可靠性配置 > 可靠性配置”，按照如下参数配置，然后点击“应用”。



步骤 6 配置 VRRP 双机热备 (WAC2)

选择“配置 > 可靠性配置 > VRRP/BFD”，配置 VRRP 备份组的状态恢复响应延迟时间为 60 秒，点击“应用”使配置生效。同时在 VRRP 列表中点击“新建”，创建一个 VRRP 组，并按照如下参数进行配置。

注意：WAC2 为备用设备，VRRP 虚地址配置为 10.23.100.33，优先级配置为 100。



配置 HSB 通道，使能双机热备功能。

选择“配置 > 可靠性配置 > 可靠性配置”，按照如下参数配置，然后点击“应用”。

步骤 7 配置 CAPWAP 源地址

配置 WAC1 基本信息。

选择“配置 > AC 配置 > 基本配置”，选择“AC 基本信息”选项卡，配置 WAC 源地址为 VRRP 虚地址 10.23.100.33，AP 认证方式为 MAC 认证，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 | AC基本信息 | AC间漫游 | Navi-AC

AC配置

- AC源地址IP类型: IPv4 IPv6 IPv4&IPv6
- AC源地址:
 - VLANIF LoopBack IP地址
 - IPv4: [. . .]
 - 接口 | IPv4地址 | IPv6地址
 - | 10.23.100.33
- AP数据缓存: OFF
- AP认证方式: MAC认证 [添加AP]
- 无线用户IPv6业务: OFF
- 高级
- 应用

展开“高级”选项，配置“CAPWAP 链路配置”，详细配置参数如下所示，此处配置的密码均为 a1234567，然后点击最下方的“应用”按钮。

高级

CAPWAP链路配置

AC - AP

- AC到AP的CAPWAP管理报文优先级: 7
- AP到AC的CAPWAP管理报文优先级: 7
- 允许AP以预置证书与AC进行DTLS会话: ON
- 允许AP以不认证方式与AC进行DTLS会话: ON
- AC-AP间控制隧道DTLS加密: 自动
- AC-AP间数据隧道DTLS加密: OFF
- *AC-AP间DTLS加密预共享密钥: [*****]
- AC-AP间敏感信息加密预共享密钥: [*****]
- 报文完整性校验: ON
- 报文完整性预共享密钥: [*****]

AC - AC

- AC-AC间控制隧道DTLS加密: 自动
- AC-AC间数据隧道DTLS加密: OFF
- *AC-AC间DTLS加密预共享密钥: [*****]
- AC-AC间敏感信息加密预共享密钥: [*****]

CAPWAP心跳检测时间间隔(秒): 25

CAPWAP心跳检测次数: 6

在弹出的“配置密钥”对话框中，配置 AP 账号的用户名/密码为：admin/Huawei@123，配置离线 VAP 密钥为 a1234567，然后点击“确定”按钮，如下所示。

配置密码

i 为提高系统安全性,请完成如下配置。

AP帐号

i 为提高访问AP的安全性,请配置AP的用户名和密码,同时该配置属于全局配置,对所有AP有效。

* 用户名: * 密码:

离线VAP

i AP离线时会发出管理SSID,便于管理员使用无线连接AP,为保证连接的安全性,配置连接管理SSID的密码。

* 离线VAP密码:

配置 WAC2 基本信息。(与 WAC1 配置相同,请大家自行配置,不再赘述)

注意:在 VRRP 双机热备组网方式中,主备 WAC 的 CAPWAP 源地址都需要配置为 VRRP 虚地址(即 10.23.100.33),否则双机热备无法正常工作。

步骤 8 配置无线配置同步功能

配置 WAC1 的无线配置同步功能。

选择“配置 > 可靠性配置 > 可靠性配置”,启用无线配置同步功能,然后按照如下参数配置,最后点击“应用”,使配置生效。其中 PSK 密钥统一配置为 Huawei@123。

无线配置同步

i 配置将从 VRRP 主设备同步到 VRRP 备设备,备设备相关的配置仅支持查看。配置同步复用热备份(HSR)通道配置。

启用无线配置同步: ON

定时同步开关: ON

定时同步间隔(分钟): 定时同步启动时间:

IP地址类型:

本端AC IP地址: 对端AC IP地址:

VRID: 接口名称:

PSK密钥:

配置 WAC2 的无线配置同步功能。

选择“配置 > 可靠性配置 > 可靠性配置”,启用无线配置同步功能,然后按照如下参数配置,最后点击“应用”,使配置生效。其中 PSK 密钥统一配置为 Huawei@123。

无线配置同步

i 配置将从 VRRP 主设备同步到 VRRP 备设备,备设备相关的配置仅支持查看。通道&VRID配置与可靠性配置不一致,点击应用后将把配置转换成可靠性的配置。

启用无线配置同步: ON

定时同步开关: ON

定时同步间隔(分钟): 定时同步启动时间:

IP地址类型:

本端AC IP地址: 对端AC IP地址:

VRID: 接口名称:

PSK密钥:

步骤 9 配置 AP 上线（WAC1）

配置过程请参考 1.2.2 步骤 6 相关内容，不再赘述。

注意：仅需要在主用 WAC1 上配置即可，备用 WAC2 无需配置。

步骤 10 配置无线业务（WAC1）

配置过程请参考 1.2.2 步骤 7 相关内容，不再赘述。

注意：仅需要在主用 WAC1 上配置即可，备用 WAC2 无需配置。

步骤 11 触发配置同步

选择“监控 > AC > 无线配置同步信息”，若发现配置未同步，可以在“操作”列进行手动同步，如下所示。（下图已经同步，不再显示手动同步字样）



对端IP地址	对端角色	对端型号	对端版本	链路状态	配置同步状态	最后同步时间	操作
10.23.100.2	Backup	AirEngine9700-M1	V200R021C00SPC100B171	● up	同步成功	16:22:24	--

3.3 结果验证

3.3.1 检查 AP 上线状态

在主用 WAC1 上选择“监控 > AP”，选择“AP 统计”选项卡，查看 AP 的状态为“normal”，如下所示。

SSID: **VAP**

自动刷新: OFF

AP型VAP列表

应用统计清零

AP ID ▲	AP名称 ▲	射频ID ▲	WLAN ID ▲	SSID ▲	BSSID ▲	认证方式 ▲	接入用户数 ▲	状态 ▲
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA/WPA2-PSK	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA/WPA2-PSK	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA/WPA2-PSK	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA/WPA2-PSK	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA/WPA2-PSK	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA/WPA2-PSK	0	on

10 共6条

注: 选择列表中的VAP,查看该VAP应用统计信息。

3.3.3 检查 HSB 通道状态

在 WAC1 上选择“配置 > 可靠性配置 > 可靠性配置”，查看 HSB 通道状态为“已连接”，说明 HSB 通道工作正常，如下所示。

Wireless LAN AirEngine9700-M1

设备名称: WAC1

监控 配置 诊断 维护

配置向导 可靠性配置 > 可靠性配置

备份方式: VRRP热备份 双链路热备份 双链路冷备份 N+1备份/无

热备份(HSB)通道配置

*备份业务: WLAN业务 NAC业务 DHCP

IP地址类型: IPv4

*本端AC IP地址: 10 . 23 . 100 . 1

*对端AC IP地址: 10 . 23 . 100 . 2

*关联VRID: 1

HSB通道状态: 已连接

注意,配置了VRRP热备份后,要求AC源地址必须要配置跟HSB关联VRID相同的虚地址。 [修改AC源地址](#)

高级

在 WAC2 上选择“配置 > 可靠性配置 > 可靠性配置”，查看 HSB 通道状态为“已连接”，说明 HSB 通道工作正常，如下所示。

设备名称: WAC2

配置向导

AC配置

AP配置

安全管理

QoS

扩展业务

可靠性配置

可靠性配置

VRRP/BFD

可靠性配置 > 可靠性配置

备份方式: VRRP热备份 双链路热备份 双链路冷备份 N+1备份/无

热备份(HSB)通道配置

*备份业务: WLAN业务 NAC业务 DHCP

IP地址类型: IPv4

*本端AC IP地址: 10 . 23 . 100 . 2

*对端AC IP地址: 10 . 23 . 100 . 1

*关联VRID: 1

HSB通道状态: 已连接

注意,配置了VRRP热备份后,要求AC源地址必须要配置跟HSB关联VRID相同的虚地址。 [修改AC源地址](#)

高级

3.3.4 检查无线配置同步状态信息

在 WAC1 上选择“监控 > AC > 无线配置同步信息”，可以查看无线配置同步的状态信息，其中链路状态为“up”，表示配置已同步成功。

AC概况 漫游用户数概况 接口流量统计 **无线配置同步信息** 业务逃生 Navi-AC

自动刷新: OFF

无线配置同步信息

对端IP地址	对端角色	对端型号	对端版本	链路状态	配置同步状态	最后同步时间	操作
10.23.100.2	Backup	AirEngine9700-M1	V200R021C00SPC100B171	up	同步成功	16:22:24	--

10 共1条

在 WAC2 上选择“监控 > AC > 无线配置同步信息”，可以查看无线配置同步的状态信息，其中链路状态为“up”，表示配置已同步成功。

AC概况 漫游用户数概况 接口流量统计 **无线配置同步信息** 业务逃生 Navi-AC

自动刷新: OFF

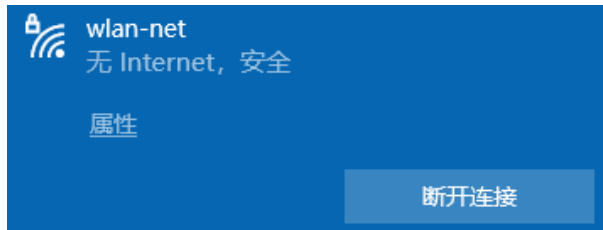
无线配置同步信息

对端IP地址	对端角色	对端型号	对端版本	链路状态	配置同步状态	最后同步时间	操作
10.23.100.1	Master	AirEngine9700-M1	V200R021C00SPC100B171	up	同步成功	16:23:57	--

10 共1条

3.3.5 STA 关联无线信号，测试网络连通性

STA 扫描接入无线网络“wlan-net”。



测试 STA 与业务网关的网络连通性。

```
C:\Windows\system32>ping 10.23.101.254

正在 Ping 10.23.101.254 具有 32 字节的数据:
来自 10.23.101.254 的回复: 字节=32 时间=4ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=8ms TTL=254

10.23.101.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 4ms, 最长 = 8ms, 平均 = 6ms
```

3.4 配置参考

3.4.1 WAC1 配置

```
Software Version V200R021C00SPC100
#
defence engine enable
sysname WAC1
#
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif100
http server enable
#
vrrp recover-delay 60
#
vlan batch 100 to 101
#
stp enable
#
interface Vlanif1
 ip address dhcp-alloc unicast
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.23.100.33
```

```
admin-vrrp vrid 1
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1800
management-interface
#
interface MEth0/0/1
 ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
 ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source ip-address 10.23.100.33
capwap dtls psk %^%#EjVsX!hYu4YZ2_G4#DzXA@:RKv34&REZ}|-y_]mY%^%#
capwap dtls inter-controller psk %^%#{9Wo7!%#BFZ<@EQ|JG>Rp<|47s,v>YPa.#^!]A9%^%#
capwap dtls no-auth enable
#
hsb-service 0
 service-ip-port local-ip 10.23.100.1 peer-ip 10.23.100.2 local-data-port 10241 peer-data-port 10241
 service-keep-alive detect retransmit 3 interval 6
#
hsb-group 0
 track vrrp vrid 1 interface Vlanif100
 bind-service 0
 hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
 temporary-management psk %^%#PwFE@vw_"@n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
 ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)!%^%#
 traffic-profile name default
 security-profile name default
 security-profile name wlan-net
 security wpa-wpa2 psk pass-phrase %^%#51sYLQj@,Ph}m2@A1j:Of3n/)t5j=+!"K+9yB{.%^%# aes
 ssid-profile name default
 ssid-profile name wlan-net
 ssid wlan-net
 vap-profile name default
```

```
vap-profile name wlan-net
  service-vlan vlan-id 101
  ssid-profile wlan-net
  security-profile wlan-net
ap-group name default
ap-group name ap-group1
  radio 0
    vap-profile wlan-net wlan 1
  radio 1
    vap-profile wlan-net wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0
  ap-name AP1
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410
  ap-name AP2
  ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110
  ap-name AP3
  ap-group ap-group1
provision-ap
master controller
  master-redundancy track-vrrp vrid 1 interface Vlanif100
  master-redundancy peer-ip ip-address 10.23.100.2 local-ip ip-address 10.23.100.1
psk %^%#W;HBAZCAY'c:L6*55/MVqK/#T~/{"O(fuW,7OFI'%^%#
#
return
```

3.4.2 WAC2 配置

```
Software Version V200R021C00SPC100
#
defence engine enable
sysname WAC2
#
vrrp recover-delay 60
#
vlan batch 100 to 101
#
stp enable
#
interface Vlanif1
  ip address dhcp-alloc unicast
#
interface Vlanif100
  ip address 10.23.100.2 255.255.255.0
  vrrp vrid 1 virtual-ip 10.23.100.33
  admin-vrrp vrid 1
#
```

```
interface MEth0/0/1
 ip address 172.21.39.5 255.255.255.0
#
interface Ethernet0/0/47
 ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source ip-address 10.23.100.33
capwap dtls psk %^%#EJVsX!hYu4YZ2_G4#DzXA@:RKv34&REZ]-y_]mY%^%#
capwap dtls inter-controller psk %^%#fn"&!O[*],H,)sO8]j:.7FT*XoFd\E%z`f<D]FcL%^%#
capwap dtls no-auth enable
#
hsb-service 0
 service-ip-port local-ip 10.23.100.2 peer-ip 10.23.100.1 local-data-port 10241 peer-data-port 10241
 service-keep-alive detect retransmit 3 interval 6
#
hsb-group 0
 track vrrp vrid 1 interface Vlanif100
 bind-service 0
 hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
 temporary-management psk %^%#PwFE@vw_"@n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
 ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)I%^%#
 traffic-profile name default
 security-profile name default
 security-profile name wlan-net
 security wpa-wpa2 psk pass-phrase %^%#51sYLQj@,Ph}m2@A1j:Of3n/)t5j=+!"K+9yB{.%^%# aes
 ssid-profile name default
 ssid-profile name wlan-net
 ssid wlan-net
 vap-profile name default
 vap-profile name wlan-net
 service-vlan vlan-id 101
 ssid-profile wlan-net
 security-profile wlan-net
 ap-group name default
```

```
ap-group name ap-group1
  radio 0
    vap-profile wlan-net wlan 1
  radio 1
    vap-profile wlan-net wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0
  ap-name AP1
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410
  ap-name AP2
  ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110
  ap-name AP3
  ap-group ap-group1
provision-ap
master controller
  master-redundancy track-vrrp vrid 1 interface Vlanif100
  master-redundancy peer-ip ip-address 10.23.100.1 local-ip ip-address 10.23.100.2
psk %^%#h$UW(fq2a2o7Gl/GL#JE}gig1:Fno*Z&]gVje!B>%^%#
#
return
```

3.4.3 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 100 to 101
#
dhcp enable
#
interface Vlanif1
#
interface Vlanif100
  ip address 10.23.100.254 255.255.255.0
  dhcp select interface
  dhcp server excluded-ip-address 10.23.100.1 10.23.100.3
  dhcp server excluded-ip-address 10.23.100.33
#
interface Vlanif101
  ip address 10.23.101.254 255.255.255.0
  dhcp select interface
#
interface MEth0/0/1
  ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
```

```
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

3.4.4 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
port link-type trunk
```

```
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

3.5 思考题

本实验中使用命令“hsb-service-type dhcp hsb-group 0”将 DHCP 业务绑定了 HSB 备份组，同时配置了无线配置同步功能。请思考，以上配置主要同步什么信息？

参考答案：

当两台主备 WAC 作为 DHCP 服务器时形成主备机制，当主用服务器出现故障，链路需要切换到备份 DHCP 服务器之前，用户地址分配状态信息将同步备份到备份服务器上。备份 DHCP 服务器可以继续为用户分配 IP 地址，并且不会存在地址重复分配现象。

4 云管理组网实验

4.1 实验介绍

4.1.1 关于本实验

本实验通过配置云管理，使得学员掌握云 WAC+FIT AP 组网配置和云 AP 组网配置。

4.1.2 实验目的

- 掌握 WLAN 的基本业务流程。
- 掌握云 WAC+FIT AP 组网架构以及 WAC 上云配置方式。
- 掌握云 AP 的组网架构以及 AP 上云配置方式。

4.1.3 实验组网介绍

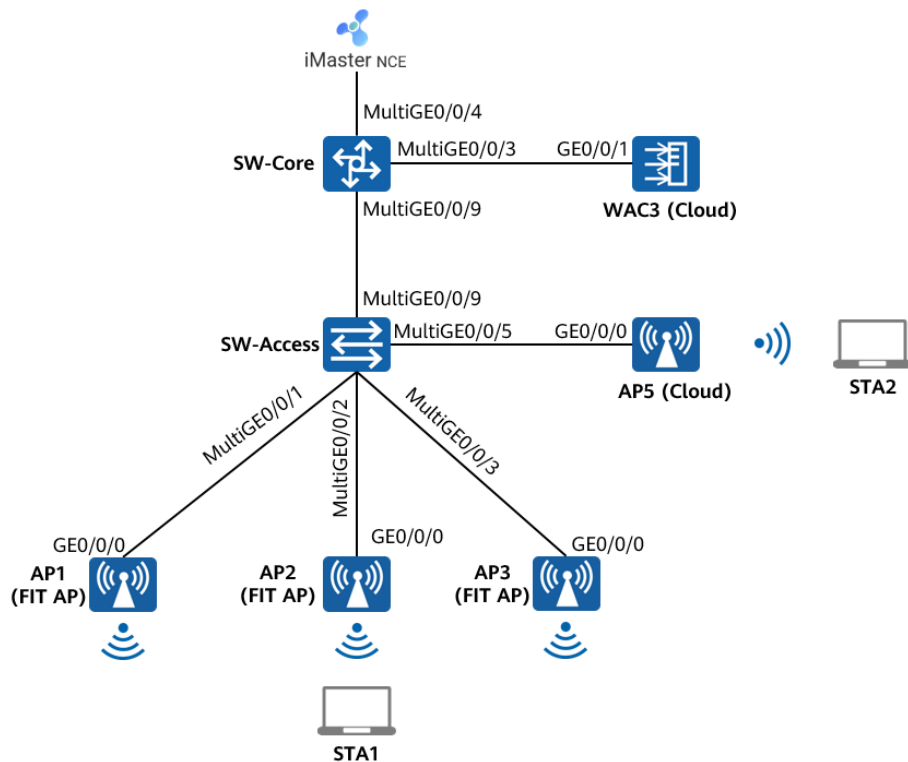


图4-1 云管理组网实验拓扑图

4.1.4 实验规划

表4-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/3	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/4	Access	PVID: 99
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101 200 201
SW-Access	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/5	Trunk	PVID:1 Allow-pass: VLAN 200 201
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101 200 201
WAC1	GE 0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表4-2 IP 地址规划

设备	端口	IP地址
SW-Core	Vlanif99	172.21.39.253/17
	Vlanif100	10.23.100.254/24
	Vlanif101	10.23.101.254/24
	Vlanif200	10.23.200.254/24
	Vlanif201	10.23.201.254/24
WAC3	Vlanif100	10.23.100.3/24
AP5	/	DHCP自动获取
iMaster NCE-Campus	/	172.21.39.88/17

(后文简称为NCE)		
--------------	--	--

表4-3 WAC3 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	100
业务VLAN	101
AP组	ap-group1
VAP模板	wlan-net
安全模板	wlan-net
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	wlan-net
SSID	wlan-net

表4-4 AP5 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	200
业务VLAN	201
AP组	default
VAP模板	ap5
安全模板	ap5
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	ap5
SSID	ap5

4.2 实验任务配置

4.2.1 配置思路

- 1.配置 SW-Core、SW-Access、WAC3 设备网络互通。
- 2.配置 WAC3 上云，配置 WAC3 与 NCE 网络互通。
- 3.配置 WAC3 上云，AP1、AP2、AP3 在 WAC3 中上线。
- 4.配置 WAC3 的 WLAN 业务。
- 5.配置 AP5 上云。
- 6.配置 AP5 的 WLAN 业务。
- 7.检查 WLAN 业务可用性。

4.2.2 配置步骤

步骤 1 配置交换机 VLAN 及 IP 地址

配置接入交换机 SW-Access 设备。

在 SW-Access 上创建 VLAN 100、101、200、201。

```
<Huawei> system-view
[Huawei] sysname SW-Access
[SW-Access] vlan batch 100 101 200 201
```

配置 SW-Access 下行端口类型及相应 VLAN。

```
[SW-Access] interface MultiGE 0/0/1
[SW-Access-MultiGE0/0/1] port link-type trunk
[SW-Access-MultiGE0/0/1] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/1] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/1] quit
[SW-Access] interface MultiGE 0/0/2
[SW-Access-MultiGE0/0/2] port link-type trunk
[SW-Access-MultiGE0/0/2] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/2] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/2] quit
[SW-Access] interface MultiGE 0/0/3
[SW-Access-MultiGE0/0/3] port link-type trunk
[SW-Access-MultiGE0/0/3] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/3] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/3] quit
[SW-Access] interface MultiGE 0/0/5
[SW-Access-MultiGE0/0/5] port link-type trunk
[SW-Access-MultiGE0/0/5] port trunk allow-pass vlan 200 201
[SW-Access-MultiGE0/0/5] port trunk pvid vlan 200
[SW-Access-MultiGE0/0/5] quit
```

配置 SW-Access 上行端口类型及允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/9
[SW-Access-MultiGE0/0/9] port link-type trunk
[SW-Access-MultiGE0/0/9] port trunk allow-pass vlan 100 101 200 201
[SW-Access-MultiGE0/0/9] quit
```

配置核心交换机 SW-Core 设备。

在 SW-Core 上创建 VLAN 100、101、200、201。

```
<Huawei> system-view
[Huawei] sysname SW-Core
[SW-Core] vlan batch 100 101 200 201
```

配置 SW-Core 下行端口类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/9
[SW-Core-MultiGE 0/0/9] port link-type trunk
[SW-Core-MultiGE 0/0/9] port trunk allow-pass vlan 100 101 200 201
[SW-Core-MultiGE 0/0/9] quit
```

配置 SW-Core 与 WAC3 互联端口的类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/3
[SW-Core-MultiGE0/0/3] port link-type trunk
[SW-Core-MultiGE0/0/3] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE0/0/3] quit
```

配置 SW-Core 的 IP 地址。

配置 SW-Core 的 IP 地址。其中 VLAN 100 是 WAC3 的管理 VLAN，VLAN 101 是 WAC3 的业务 VLAN，VLAN 200 是 AP5 的管理 VLAN，VLAN201 是 AP5 的业务 VLAN。

```
[SW-Core] interface vlan 100
[SW-Core-Vlanif100] ip address 10.23.100.254 24
[SW-Core-Vlanif100] quit
[SW-Core] interface vlan 101
[SW-Core-Vlanif101] ip address 10.23.101.254 24
[SW-Core-Vlanif101] quit
[SW-Core] interface vlan 200
[SW-Core-Vlanif200] ip address 10.23.200.254 24
[SW-Core-Vlanif200] quit
[SW-Core] interface vlan 201
[SW-Core-Vlanif201] ip address 10.23.201.254 24
[SW-Core-Vlanif201] quit
```

步骤 2 初始化 WAC3 设备

AirEngine 9700-M1 出厂时在接口 MEth0/0/1 上配置了 IP 地址 169.254.1.1/24，使用网线将 PC 网卡与此接口进行互联，并配置 PC 网卡地址为 169.254.1.100/24，使用浏览器访问 <https://169.254.1.1> 地址，即可打开 AirEngine 9700-M1 设备的 Web 管理页面。



Wireless LAN
Access Controller

用户名:

密码:

确认密码:

串口认证类型: AAA认证 密码认证

串口密码:

串口确认密码:

首次登录 Web 网管时，需要设置用户名和密码，用于 Web 网管和 STelnet 登录。还需要设置串口登录的认证方式和认证信息。

此处设置用户名/密码为：admin/Huawei@123，串口认证类型为密码认证，串口密码为 Huawei@123，然后点击“注册”，如下所示。



Wireless LAN
Access Controller

用户名:

密码:

确认密码:

串口认证类型: AAA认证 密码认证

串口密码:

串口确认密码:

注册成功后，注册用户将用于 STelnet 和 Web 网管登录。然后重新输入用户名和密码，点击“登录”，即可进行 Web 网管。

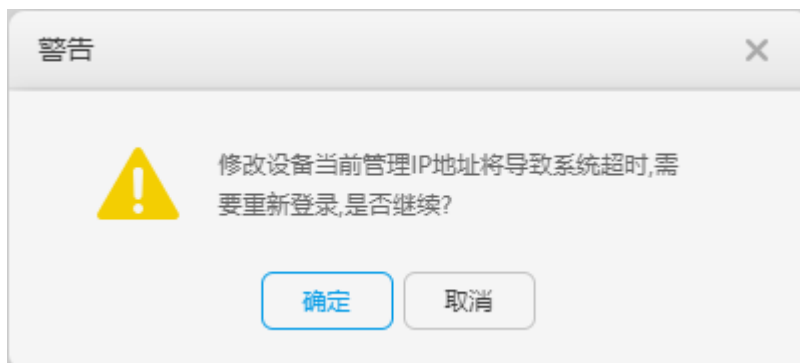


由于在实际的生产网络中，几乎不会使用缺省的管理地址（即 169.254.1.1/24）对设备进行 Web 网管，所以接下来需要对管理地址进行修改。

选择“配置 > AC 配置 > 接口管理”，选择“管理网口”选项卡，配置 WAC3 的 IP 地址为 172.21.39.6，掩码保持不变，最后点击“应用”，如下所示。



修改管理 IP，需要重新登录，点击“确定”。



WAC3 的管理 IP 修改后，需要同步修改 PC 网卡的 IP 地址，本实验中将 PC 网卡地址配置为 172.21.39.100/24，然后使用浏览器访问 <https://172.21.39.6>，重新进行登录。

登录成功后，发现 WAC3 的管理 IP 已经被成功修改为 172.21.39.6/24，如下所示。



为了实验方便，进一步修改 Web 网管的超时时间，本实验配置为 60 分钟（缺省为 10 分钟），注意，实际的生产网络中出于安全考虑，不建议将 Web 网管的超时时间配置过长。

选择“维护 > AC 维护 > 系统管理”，选择“服务管理”选项卡，将 Web 服务的超时时间修改为 60 分钟，然后点击“应用”，如下所示。



步骤 3 配置 WAC3 设备的 VLAN 和 IP 地址

配置 WAC3 设备。修改 WAC3 设备名称，并创建 VLAN 100、101，修改 GE0/0/1 端口类型为 Trunk，并允许通过 VLAN 100、101。

修改 WAC1 的设备名称。

选择“监控 > AC”，选择“AC 概况”，在“AC 基本信息”中，点击“设备名称”后面的“更改”字样，将设备名称修改为 WAC3。

AC基本信息

设备型号:	AirEngine9700-M1	
设备名称:	AirEngine9700-M1	[更改]
设备序列号:	102257532207	
MAC地址:	9cb2-e8b5-a294	
系统软件版本:	V200R021C00SPC100	[升级]
License资源已使用数/总数:	0/1024	[查看详情]
AP资源授权license状态:	演示	[查看详情]

重命名

*设备名称:

在 WAC3 上创建 VLAN 100、101。

选择“配置 > AC 配置 > VLAN”，选择“VLAN”选项卡，点击“批量新建”按钮，新建 VLAN 100、101，如下所示。

Wireless LAN AirEngine9700-M1

设备名称: WAC3

监控
配置
诊断
维护

- 配置向导
- AC配置
- 基本配置
- VLAN
- 接口管理
- IP

全局IPv6: OFF

VLAN
VLANIF
VLAN Pool

新建
删除
批量新建
批量删除
刷新

VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan

10 ▼ 共1条



Wireless LAN AirEngine9700-M1
设备名称: WAC3


配置向导 AC配置 > VLAN > VLAN > 批量新建VLAN

* VLAN ID: (1-4094,格式: 1,3-5,7)

基本配置

VLAN

接口管理



Wireless LAN AirEngine9700-M1
设备名称: WAC3

全局IPv6: OFF

配置向导 AC配置 VLANIF VLAN Pool

基本配置

VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan
<input type="checkbox"/> 100	VLAN 0100	commonVlan
<input type="checkbox"/> 101	VLAN 0101	commonVlan

10 共3条

AP配置

配置 WAC3 的 GE0/0/1 端口类型及允许通过的 VLAN。

选择“配置 > AC 配置 > 接口管理”，选择“物理接口”选项卡，点击 1 号接口（即 GE0/0/1 接口），配置链路类型为 Trunk，允许通过的 VLAN 为 100 和 101，然后点击“确定”，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC3

物理接口 | 逻辑接口 | 管理网口

接口属性 | LLDP

选择面板上的接口进行配置 (Eth-Trunk接口也可点击紫色圆圈进行选中,或 [点此](#) 进行新建。)

2 4 6 8 10 12 6
1 3 5 7 9 11 5

已选中 Up Down Shutdown

恢复默认配置

*接口名称: GigabitEthernet0/0/1

接口状态: ON

链路类型: 2 Trunk

允许通过VLAN(Tagged): 3 100,101

高级

4 确定 取消

创建 Vlanif100 接口，并配置接口 IP 地址。

选择“配置 > AC 配置 > VLAN”，选择“VLANIF”选项卡，点击“新建”。



Wireless LAN AirEngine9700-M1
设备名称: WAC3

全局IPv6: OFF

VLAN **VLANIF** VLAN Pool

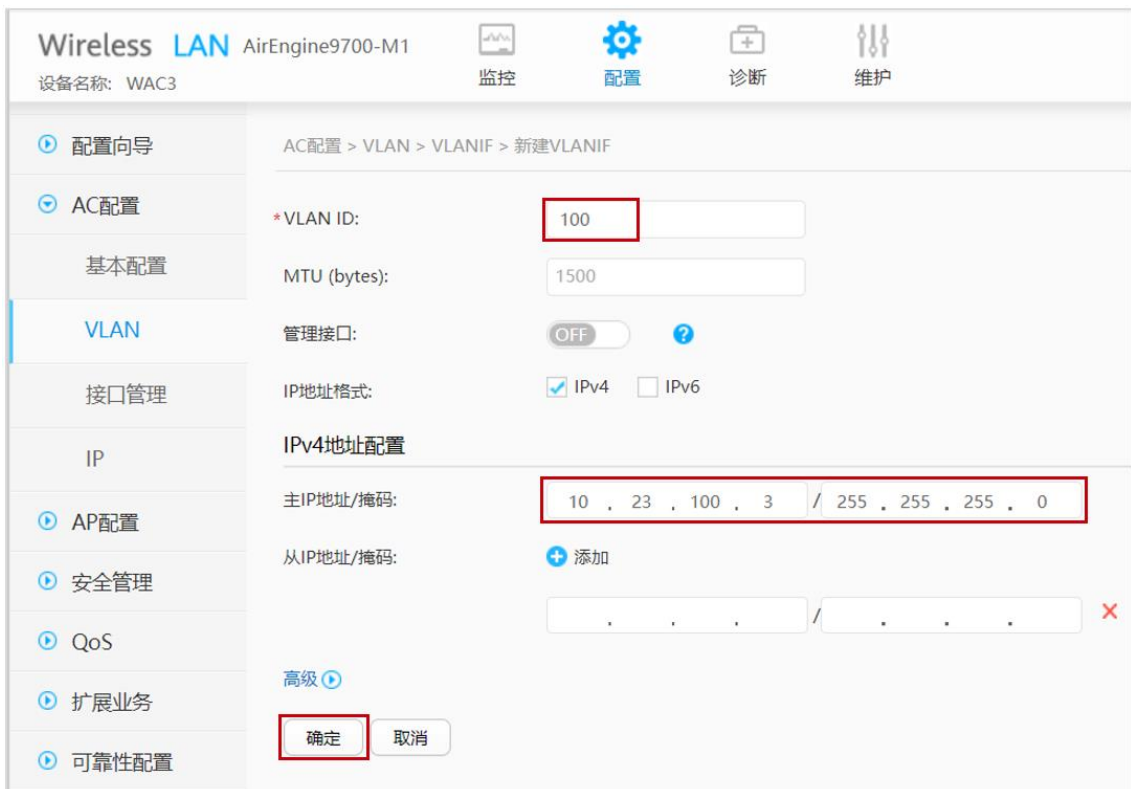
新建 删除 刷新

接口名称 ▲ 连接状态 ▲

Vlanif1 不可用

10 共1条

在“新建 VLANIF”页面中，配置 VLAN ID 为 100，IP 地址为 10.23.100.3，掩码为 255.255.255.0，然后点击“确定”，如下所示。



Wireless LAN AirEngine9700-M1
设备名称: WAC3

AC配置 > VLAN > VLANIF > 新建VLANIF

*VLAN ID: 100

MTU (bytes): 1500

管理接口: OFF

IP地址格式: IPv4 IPv6

IPv4地址配置

主IP地址/掩码: 10 . 23 . 100 . 3 / 255 . 255 . 255 . 0

从IP地址/掩码: + 添加

高级

确定 取消



Wireless LAN AirEngine9700-M1
设备名称: WAC3

全局IPv6: OFF

VLAN VLANIF VLAN Pool

新建 删除 刷新

接口名称 ▲	连接状态 ▲	IPv4地址/掩码 ▲
<input type="checkbox"/> Vlanif1	不可用	
<input type="checkbox"/> Vlanif100	可用	10.23.100.3/255.255.255.0

步骤 4 配置 NCE 与 WAC3 网络互通

iMaster NCE-Campus 的 IP 地址和网关在软件安装阶段已配置完成，本实验不再赘述。iMaster NCE-Campus 地址配置为 172.21.39.88/17，网关地址是 172.21.39.253（位于 SW-Core 上）。

配置 SW-Core 的 VLAN 信息及 IP 地址，确保 NCE 与 SW-Core 之间网络互通。

```
[SW-Core] vlan 99
[SW-Core-vlan99] name Manage
[SW-Core-vlan99] quit
[SW-Core] interface MultiGE 0/0/4
[SW-Core-MultiGE0/0/4] port link-type access
[SW-Core-MultiGE0/0/4] port default vlan 99
[SW-Core-MultiGE0/0/4] quit
[SW-Core] interface Vlanif 99
[SW-Core-Vlanif99] ip address 172.21.39.253 17
[SW-Core-Vlanif99] quit
```

配置 WAC3 的静态路由，确保 NCE 与 WAC3 之间网络互通。

选择“配置 > AC 配置 > IP”，选择“路由”选项卡，点击“静态路由配置表”，展开对应的配置界面，然后点击“新建”，新建静态路由。

在“新建静态路由”页面，依次分别配置如下两条静态路由，然后点击“确定”。其中静态路由 0.0.0.0/0 用于访问其他外部网络，静态路由 172.21.39.88/32 用于访问 NCE 服务器。

配置完成后，查看静态路由如下所示。



Wireless LAN AirEngine9700-M1
设备名称: WAC3

监控 配置 诊断 维护

配置向导 DHCP地址池 DHCP中继 NAT 路由 DNS

AC配置 → 路由表

基本配置 ↓ 静态路由配置表

VLAN 新建 删除 刷新

目的IP地址	子网掩码	下一跳	出接口	优先级
<input type="checkbox"/> 0.0.0.0	0.0.0.0	10.23.100.254	Vlanif100	60
<input type="checkbox"/> 172.21.39.88	255.255.255.255	10.23.100.254	Vlanif100	60

10 共2条

步骤 5 配置 WAC3 为云模式

配置 WAC3 为云模式，并指定 NCE 的 IP 地址及端口。

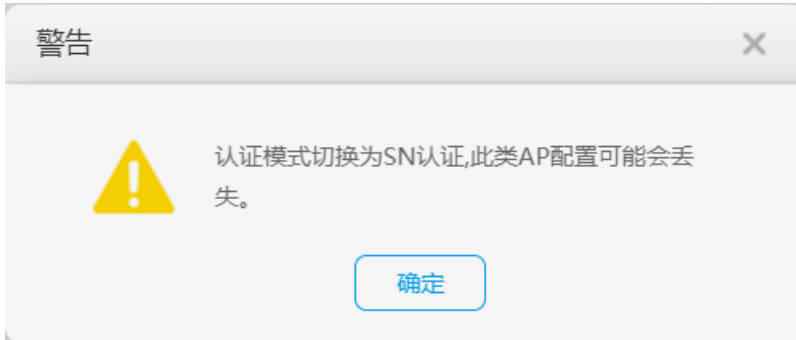
在整个 Web 管理页面的右上角区域，点击“传统模式”选项，对 WAC 的工作模式进行修改，在弹出的下拉列表中，选择“云模式”，如下所示。



在弹出的对话框中点击“确定”按钮，如下所示。



WAC 切换为“云模式”后，AP 的认证模式会自动切换为 SN 认证，点击“确定”即可，如下所示。



注意：切换 WAC 的工作模式后，系统会自动提示保存配置，保存成功后，需要重新登录 Web 管理页面才能进行后续的配置。

配置云化管理的相关参数。

选择“维护 > AC 维护 > 云化管理”，配置云管理控制器 IP 地址为 172.21.39.88，端口号为 10020，源接口为 Vlanif100，然后点击“应用”，如下所示。



测试 WAC3 与 NCE 的网络连通性。

选择“诊断 > Ping”，在 IPv4 地址栏输入 NCE 的地址 172.21.39.88，然后点击“开始”按钮，开始 Ping 测试，测试结果如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC3

1 诊断

智能诊断
 1 通过使用Ping工具,用户可以检查指定IP地址或主机名的设备是否可达,测试网络连接是否出现故障。
 一键信息采集
 * IP地址/主机名 3 IPv4 172.21.39.88 ?
 2 无线报文头捕获
 2 Ping
 4 开始
 5

```

PING 172.21.39.88: 56 data bytes,
Reply from 172.21.39.88: bytes=56 Sequence=1 ttl=62 time=1 ms
Reply from 172.21.39.88: bytes=56 Sequence=2 ttl=62 time=3 ms
Reply from 172.21.39.88: bytes=56 Sequence=3 ttl=62 time=1 ms
Reply from 172.21.39.88: bytes=56 Sequence=4 ttl=62 time=1 ms
Reply from 172.21.39.88: bytes=56 Sequence=5 ttl=62 time=1 ms

--- 172.21.39.88 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/1/3 ms
    
```

步骤 6 配置 NCE 中纳管 WAC3 设备

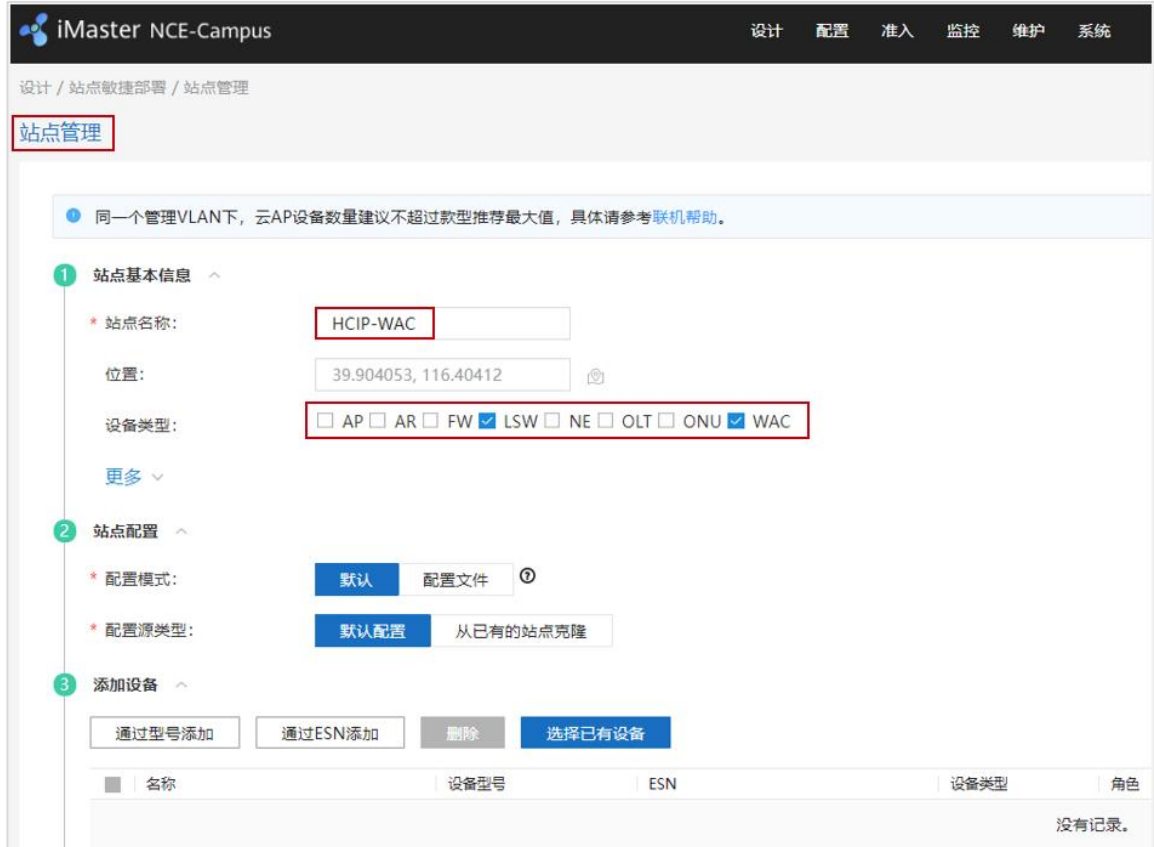
登录 NCE，在 NCE 主菜单中选择“设计 > 站点管理”，新建站点“HCIP-WAC”，设备类型勾选“LSW”和“WAC”，点击右下角的“确定”。

设计 配置 准入 监控 维护 系统

iMaster NCE-Campus
此页面的仪表盘功能，洞察全网数据状态与趋势哦。

系统概览

- 站点敏捷部署
 - 1 站点管理
 - 设备管理
- 基础网络设计
 - 物理拓扑
 - 链路管理
 - 网络规划导入
 - 网络设置
 - 模板管理

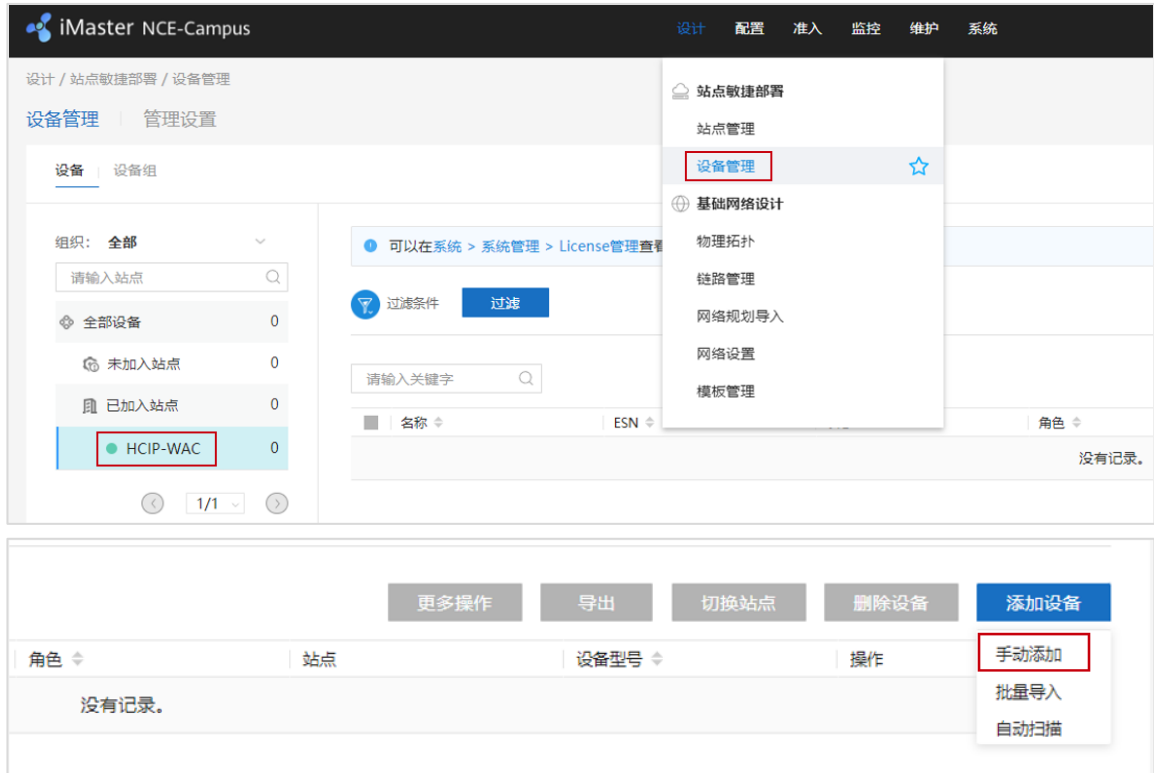


在 WAC3 上查询设备的 ESN 编号。

选择“维护 > AC 维护 > License 管理”，可以查询到 WAC3 的 ESN 信息为 102257532207。（实验中 ESN 编号以实际情况为准）



在 NCE 主菜单中选择“设计 > 设备管理”，选中站点“HCIP-WAC”，然后点击“添加设备 > 手动添加”，如下所示。



The screenshot shows the iMaster NCE-Campus web interface. The top navigation bar includes '设计', '配置', '准入', '监控', '维护', and '系统'. The main content area is titled '设计 / 站点敏捷部署 / 设备管理' and '设备管理 | 管理设置'. On the left, there is a sidebar with '组织: 全部' and a search box '请输入站点'. Below this is a list of device groups: '全部设备' (0), '未加入站点' (0), '已加入站点' (0), and 'HCIP-WAC' (0). The 'HCIP-WAC' group is highlighted with a red box. In the center, there is a search box '请输入关键字' and a '过滤' button. On the right, a dropdown menu is open, showing options: '站点敏捷部署', '站点管理', '设备管理' (highlighted with a red box), '基础网络设计', '物理拓扑', '链路管理', '网络规划导入', '网络设置', and '模板管理'. Below the main content area, there is a toolbar with buttons: '更多操作', '导出', '切换站点', '删除设备', and '添加设备'. The '添加设备' button is highlighted with a red box. Below the toolbar is a table with columns: '角色', '站点', '设备型号', and '操作'. The table is currently empty, showing '没有记录.'. A dropdown menu is open from the '操作' column, showing options: '手动添加' (highlighted with a red box), '批量导入', and '自动扫描'.

在弹出的手动添加界面，协议类型选择“NETCONF 协议”，站点选择“HCIP-WAC”，模式选择“设备型号”，然后点击“增加”按钮。

设计 / 站点敏捷部署 / 设备管理

设备管理 | 管理设置

设备 设备组

手动添加

* 协议类型:

设备通过NETCONF协议向控制器发出纳管请求

NETCONF协议

控制器利用SNMP协议向设备发出纳管请求

SNMP协议

① 当设备名称符合设备命名规则时，控制器将下发设备名称到设备并更新设备名称，否则不下发。(设备命名规则为英文、数字、_)

站点:

模式: ESN

* 设备信息:

名称	ESN	角色

在弹出的页面中，按照以下参数进行配置，点击“确定”。

* 设备信息:

类型: 型号:

数量: 角色:

然后修改设备名称为“WAC3”，填写 ESN 编号，描述信息为“HCIP”，点击“确定”。

HCIP-WAC

设备型号: ESN

名称	ESN	角色	描述	类型	设备型号	性能	操作
<input type="text" value="WAC3"/>	<input type="text" value="102257532207"/>	WAC	<input type="text" value="HCIP"/>	WAC	AirEngine9700-M1	--	<input type="button" value="删除"/>

在设备管理页面，发现 WAC3 的状态为“正常”，表明 NCE 已成功纳管设备。



步骤 7 配置 DHCP 服务器

SW-Core 作为 DHCP 服务器为 AP1、AP2、AP3 及 STA 分配 IP 地址。在 SW-Core 上启用 DHCP 服务，在 SW-Core 上配置 vlanif100 端口为 AP 提供 IP 地址。

```
[SW-Core] dhcp enable
[SW-Core] interface vlanif 100
[SW-Core-Vlanif100] dhcp select interface
[SW-Core-Vlanif100] quit
```

在 SW-Core 上配置 Vlanif101 端口为 STA 提供 IP 地址。

```
[SW-Core] interface vlanif 101
[SW-Core-Vlanif101] dhcp select interface
[SW-Core-Vlanif101] quit
```

步骤 8 配置 AP 在 WAC3 中上线

配置 AP1、AP2 和 AP3 在 WAC3 中上线，需要首先配置 WAC 基础信息。

选择“配置 > AC 配置 > 基本配置”，选择“AC 基本信息”选项卡，配置 WAC 源地址为 Vlanif100 接口，AP 认证方式为 SN 认证，如下所示。

展开“高级”选项，配置“CAPWAP 链路配置”，详细配置参数如下所示，此处配置的密码均为 a1234567，然后点击最下方的“应用”按钮。

在弹出的“配置密钥”对话框中，配置 AP 账号的用户名/密码为：admin/Huawei@123，配置离线 VAP 密钥为 a1234567，然后点击“确定”按钮，如下所示。

配置密钥 ✕

ⓘ 为提高系统安全性,请完成如下配置。

AP帐号

ⓘ 为提高访问AP的安全性,请配置AP的用户名和密码,同时该配置属于全局配置,对所有AP有效。

* 用户名: * 密码:

离线VAP

ⓘ AP离线时会发出管理SSID,便于管理员使用无线连接AP,为保证连接的安全性,配置连接管理SSID的密钥。

* 离线VAP密钥:

WAC 基础信息配置完毕后,在 NCE 主菜单中选择“设计 > 设备管理”,选中站点“HCIP-WAC”,然后点击“WAC3”,进入 WAC3 的管理界面,如下所示。

ⓘ 可以在系统 > 系统管理 > License管理查看设备对应License系列的使用量和状态。

🔍 过滤条件

请输入关键字

<input type="checkbox"/>	名称	ESN	状态	角色
<input type="checkbox"/>	WAC3	102257532207	● 告警	WAC

共1条

发现有三台未被纳管的设备,同时选中三台设备,点击“修复”。

基本信息
位置
工具
资源
故障告警

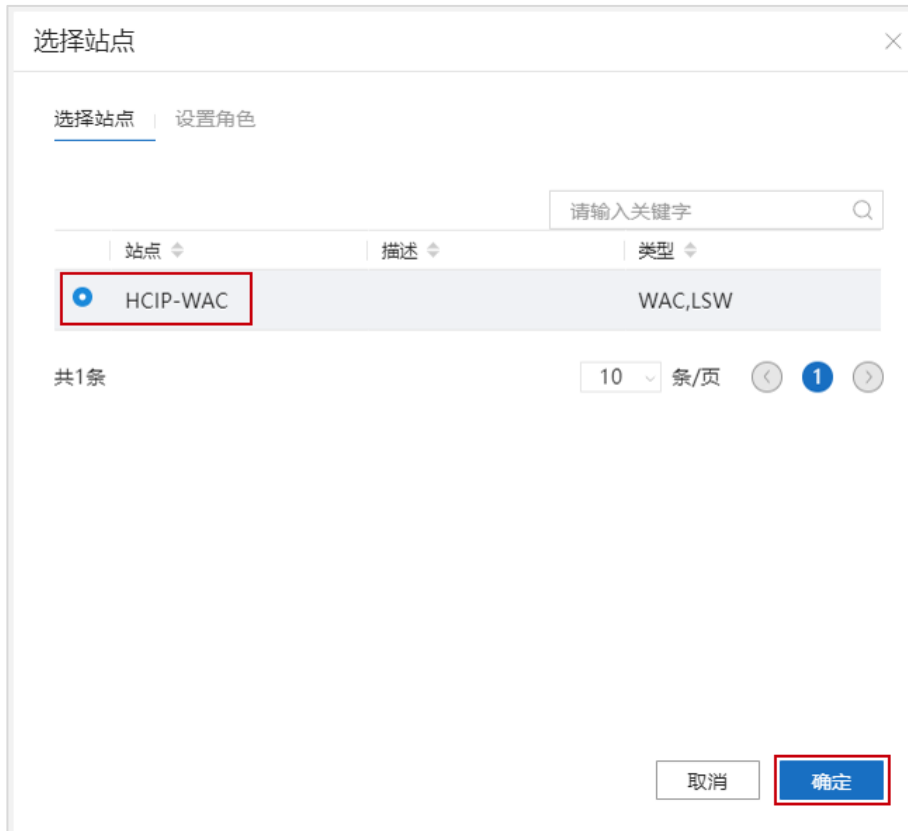
AP列表

🔍 筛选条件

<input checked="" type="checkbox"/>	名称	状态	异常原因	ESN	型号
<input checked="" type="checkbox"/>	2102353VUR10N5119363	●	未纳管	2102353VUR10N5119363	AirEngine5761-11
<input checked="" type="checkbox"/>	2102353VUR10N5119339	●	未纳管	2102353VUR10N5119339	AirEngine5761-11
<input checked="" type="checkbox"/>	2102353VUR10N5119370	●	未纳管	2102353VUR10N5119370	AirEngine5761-11

共3条

在弹出的对话框中,选择“HCIP-WAC”站点,点击“确定”。



提示三台设备均已修复成功，正常被 NCE 纳管。



在 WAC3 的管理界面中，发现三台 AP 的状态为“正常”，运行状态为“normal”。



依据 AP 的 SN 编号，识别并修改 AP 名称。以修改 AP1 的名称为例，在设备管理界面，点击 SN 编号为“2102353VUR10N5119370”对应的修改按钮进行修改，如下所示。

过滤条件 过滤

请输入关键字

更多操作 导出 切换站点 删除设备

名称	ESN	状态	角色	站点	设备型号	操作
2102353VUR10N511...	2102353VUR10N5119339	正常	AP	HCIP-WAC	AirEngine5761-11	编辑 删除
2102353VUR10N511...	2102353VUR10N5119363	正常	AP	HCIP-WAC	AirEngine5761-11	编辑 删除
2102353VUR10N511...	2102353VUR10N5119370	正常	AP	HCIP-WAC	AirEngine5761-11	编辑 删除
WAC3	102257532207	告警	WAC	HCIP-WAC	AirEngine9700-M1	编辑 删除

共4条 20 条/页

修改设备

名称: AP1

描述:

资产编号:

ESN: 2102353VUR10N5119370

角色: AP

设备型号: AirEngine5761-11

类型: AP

站点: HCIP-WAC

公网IP地址:

设备软件版本: V200R021C00SPC200

取消 确定

AP1、AP2、AP3 的名称修改完成后，如下所示。

过滤条件 过滤

请输入关键字

更多操作 导出 切换站点 删除设备

名称	ESN	状态	角色	站点	设备型号	操作
AP1	2102353VUR10N5119370	正常	AP	HCIP-WAC	AirEngine5761-11	编辑 删除
AP2	2102353VUR10N5119363	正常	AP	HCIP-WAC	AirEngine5761-11	编辑 删除
AP3	2102353VUR10N5119339	正常	AP	HCIP-WAC	AirEngine5761-11	编辑 删除
WAC3	102257532207	告警	WAC	HCIP-WAC	AirEngine9700-M1	编辑 删除

共4条 20 条/页

在 WAC3 上创建 AP 组。选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“新建”按钮，配置 AP 组名称为 ap-group1，然后点击“确定”，如下所示。



Wireless LAN AirEngine9700-M1
设备名称: WAC3

监控 配置 诊断 维护

配置向导 AP组 静态负载均衡组

AC配置 修改 新建 删除 刷新

AP配置 组名称 ▲ VAP模板 ▲

default

AP组配置

AP配置 20 共1条



Wireless LAN AirEngine9700-M1
设备名称: WAC3

监控 配置 诊断 维护

配置向导 AP配置 > AP组配置 > AP组 > 新建AP组

AC配置

AP配置 * AP组名称: ap-group1

确定 取消

AP组配置

AP配置

修改 AP 所属的 AP 组。缺省情况下，新添加的 AP 都位于 default 组，需要将 AP1、AP2 和 AP3 移动至 ap-group1 中。

选择“配置 > AP 配置 > AP 配置”，选择“AP 信息”选项卡，同时选中此三台 AP，点击“修改 AP 配置”按钮，将“AP 组”修改为 ap-group1，然后点击“确定”，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC3

监控 配置 诊断 维护

配置向导 AP信息 AP白名单 AP黑名单 AP邻居关系 AP设备类型

AC配置

AP配置

AP组配置

AP配置

射频规划/调优

分支AP组配置

模板管理

AP列表

1 点击AP ID列可进入AP的个性化配置页面。

修改AP配置 添加 替换 删除 加入黑名单 闪灯 清空所有AP

AP ID	AP MAC地址	AP名称	AP组	IP地址
0	9cb2-e82d-5410	AP2	default	10.23.100.45
1	9cb2-e82d-54f0	AP1	default	10.23.100.174
2	9cb2-e82d-5110	AP3	default	10.23.100.38

10 共3条

Wireless LAN AirEngine9700-M1
设备名称: WAC3

监控 配置 诊断 维护

配置向导 AP配置 > AP配置 > AP信息 > 修改AP

AC配置

AP配置

AP组配置

AP配置

射频规划/调优

分支AP组配置

模板管理

安全管理

QoS

扩展业务

AP组: ap-group1

AC地址列表: + 添加

已选AP列表

AP ID	AP MAC地址	AP名称	AP组	IP地址获取方式
0	9cb2-e82d-5410	AP2	default	- none -
1	9cb2-e82d-54f0	AP1	default	- none -
2	9cb2-e82d-5110	AP3	default	- none -

10 共3条

确定 取消

检查发现，三台 AP 均已属于 ap-group1 组，并且已经获取到 IP 地址，状态为“normal”，AP 上线成功。



Wireless LAN AirEngine9700-M1
设备名称: WAC3

配置向导 AC配置 AP配置 AP组配置 AP配置 射频规划/调优 分支AP组配置 模板管理

AP信息 AP白名单 AP黑名单 AP邻居关系 AP设备类型

AP列表

点击AP ID列可进入AP的个性化配置页面。

修改AP配置 添加 替换 删除 加入黑名单 闪灯 清空所有AP

AP ID	AP MAC地址	AP名称	AP组	IP地址
0	9cb2-e82d-5410	AP2	ap-group1	10.23.100.45
1	9cb2-e82d-54f0	AP1	ap-group1	10.23.100.174
2	9cb2-e82d-5110	AP3	ap-group1	10.23.100.38

10 共3条

步骤 9 配置无线业务（WAC3）

此步骤的具体配置与 1.2.2 步骤 7 类似，不再赘述。

步骤 10 配置 DHCP 服务器

SW-Core 作为 DHCP 服务器为 AP5 及 STA 分配 IP 地址，在 SW-Core 上配置 Vlanif200 端口为 AP5 提供 IP 地址，并通过 DHCP option 148 字段修改 AP5 的模式为云模式，同时携带 NCE 的 IP 地址及端口。（AP5 为出厂空配置）

```
[SW-Core] interface Vlanif 200
[SW-Core-Vlanif200] dhcp select interface
[SW-Core-Vlanif200] dhcp server option 148 ascii "agilemode=agile-cloud;agilemanage-
mode=ip;agilemanage-domain=172.21.39.88;agilemanage-port=10020;ap-agilemode=agile-cloud;"
[SW-Core-Vlanif200] quit
```

在 SW-Core 上配置 Vlanif201 端口为 AP5 的 STA 提供 IP 地址。

```
[SW-Core] interface Vlanif 201
[SW-Core-Vlanif201] dhcp select interface
[SW-Core-Vlanif201] quit
```

在 SW-Core 上查看 AP5 获取到的 IP 地址（依据实际情况），如下所示。

```
[SW-Core] display ip pool interface Vlanif200 used
Pool-name      : Vlanif200
Pool-No       : 2
Lease         : 1 Days 0 Hours 0 Minutes
Domain-name   : -
Option-code   : 148
Option-subcode : --
Option-type   : ascii
```

```

Option-value   : "agilemode=agile-cloud;agilemanage-mode=ip;agilemanage-
domain=172.21.39.88;agilemanage-port=10020;ap-agilemode=agile-cloud;"
DNS-server0    : -
NBNS-server0   : -
Netbios-type   : -
Position       : Interface
Status         : Unlocked
Gateway-0      : -
Network        : 10.23.200.0
Mask           : 255.255.255.0
VPN instance   : --
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total      :254      Used      :1
                  Idle       :253      Expired   :0
                  Conflict   :0        Disabled  :0

-----
Network section
      Start      End      Total      Used Idle(Expired) Conflict Disabled
-----
      10.23.200.1 10.23.200.254 254      1      253(0)      0      0
-----

Client-ID format as follows:
DHCP   : mac-address           PPPoE   : mac-address
IPSec  : user-id/portnumber/vrf  PPP     : interface index
L2TP   : cpu-slot/session-id    SSL-VPN : user-id/session-id

-----
Index      IP      Client-ID      Type      Left      Status
-----
221      10.23.200.222      9cb2-e82d-5230      DHCP      86400      Used
-----
    
```

步骤 11 配置 NCE 纳管 AP5

获取 AP5 的 ESN 编号。可以通过查看 AP5 背面的标签获取，也可以通过登录 AP5 的 Web 页面获取，如下所示。

Wireless LAN

AirEngine5761-11

设备名称: AP5

首页
诊断
维护

基本信息	设备名称:	AP5
告警&事件	设备型号:	AirEngine5761-11
日志	MAC地址:	9cb2-e82d-5230
管理员记录	序列号:	2102353VUR10N5119348
恢复出厂配置	当前版本:	V200R021C00SPC200
WMI	重启后软件版本:	flash:/AirEngineX761-V200R021C00SPC200.cc
	当前配置文件:	flash:/vrpcfg.zip

在 NCE 主菜单中选择“设计 > 站点管理”，新建站点“HCIP-AP”，设备类型勾选“AP”。添加设备选择“通过型号添加”，设备类型选择“AP”，设备型号选择“AirEngine5761-11”，数量为 1，角色选择“AP”，点击“确定”。

设计
配置
准入
监控
维护
系统

iMaster NCE-Campus

此页面的仪表盘功能，洞察全网数据状态与趋势哦。

站点敏捷部署

站点管理

设备管理

基础网络设计

物理拓扑

链路管理

网络规划导入

网络设置

模板管理

系统概览

设计 / 站点敏捷部署 / 站点管理

站点管理

1 同一个管理VLAN下，云AP设备数量建议不超过款型推荐最大值，具体请参考[联机帮助](#)。

1 站点基本信息

* 站点名称:

位置:

设备类型: AP AR FW LSW NE OLT ONU WAC

更多

2 站点配置

* 配置模式: ①

* 配置源类型:

3 添加设备

设备类型: 设备型号:

数量: 角色:

设备类型	角色
没有记录。	

然后修改设备名称为“AP5”，填写 ESN 编号，描述信息为“HCIP-AP5”，点击“确定”。

3 添加设备

名称	设备型号	ESN	设备类型	角色	描述	性能	操作
AP5	AirEngine5761-11	2102353VUR10N5119348	AP	AP	HCIP-AP5	1G	

选择“设计 > 设备管理”，可以看到 AP5 已经被正常纳管。

过滤条件

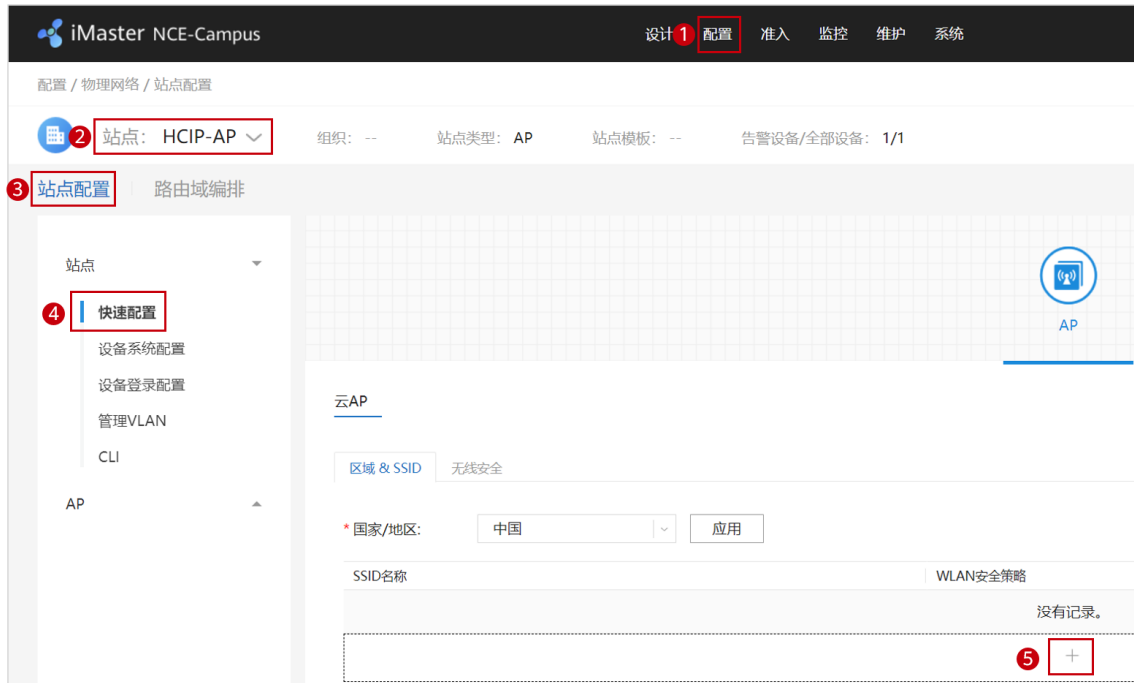
请输入关键字

名称	ESN	状态	角色	站点
AP1	2102353VUR10N5119370	正常	AP	HCIP-WAC
AP2	2102353VUR10N5119363	正常	AP	HCIP-WAC
AP3	2102353VUR10N5119339	正常	AP	HCIP-WAC
AP5	2102353VUR10N5119348	正常	AP	HCIP-AP
WAC3	102257532207	告警	WAC	HCIP-WAC

共5条

步骤 12 配置无线业务（AP5）

在 NCE 上选择“配置 > 物理网络 > 站点配置”，选择“HCIP-AP”站点，在“站点配置 > 快速配置”页面中，点击“+”符号，新建无线业务。



新建无线业务的参数配置如下：SSID 名称为 ap5，数据转发模式为直接转发，业务 VLAN 为 201，WLAN 安全策略为半开放网络，密钥类型为 PSK，加密方式为 WPA2，加密算法为 AES，密钥设置为 a12345678，最后点击右下角的“应用”按钮，使配置生效。

云AP

区域 & SSID 无线安全

* SSID名称:

数据转发模式:

全局DHCP获取地址:

去使能时，AP根据业务VLAN对终端流量进行转发，若AP上配置对应的VLANIP地址池；否则有上游设备网关为终端分配地址，需在[配置 > 物理网络 > 站点配置](#)

VLAN:

安全认证

WLAN安全策略:

- 开放网络
- 半开放网络
- 安全网络

密钥类型:

加密方式:

加密算法:

* 密钥:

开启MAC上报:

在 NCE 上选择“配置 > 物理网络 > 站点配置 > 站点配置 > AP > 高级 > 接口”，对云 AP 的接口进行设置，放行对应的业务 VLAN。

在“接口选择”区域，点击“+”符号，添加面板类型，其中设备型号选择“AirEngine5761-11”，然后点击“确定”。



全局DHCP | 子网 | **接口** | IPv6业务 | Mesh | IPsec VPN | AP安装位置 | LED灯

云AP接口 | 中心AP接口 | 分布式AP接口

接口选择

配置类型： 全局配置 个性化配置

ⓘ 在全局配置的面板中对各接口配置的参数将应用于站点中匹配此面板类型的所有设备。在同一

+

电口 光口 | 已选择 ↑ 上行口

添加面板

设备类型：AirEngine5761-11

预览：
0

电口 光口

取消 确定

在上一步骤中成功添加的面板类型中，选择“0”号接口（即 GigabitEthernet0/0/0 接口），对接口进行如下配置：场景选择“上行直连交换机”，允许通过的 VLAN 配置为 201，最后点击右下角的“应用”按钮。

云AP接口
中心AP接口
分布式AP接口

接口选择

配置类型: 全局配置 个性化配置

! 在全局配置的面板中对各接口配置的参数将应用于站点中匹配此面板类型的所有设备。在同一个面板中,

AP100EC, AP1050DN-S, AP163, AP300EC, AP3050DE, AP310, AP330, AP363, AP365...

0

+

电口
光口
已选择
↑ 上行口

接口配置

接口名称: GigabitEthernet0/0/0

接口属性: 电口

接口描述:

LLDP:

场景:

WAN

上行直连交换机

下行直连交换机

下行直连PC

* 缺省VLAN:

* 允许通过的VLAN: 每个设备最多可配置64个VLAN。

4.3 结果验证

4.3.1 在 WAC3 上检查云管理信息

选择“维护 > AC 维护 > 云化管理”，可以查看云管理控制器配置信息。

4.3.2 STA 接入无线网络，测试网络连通性

STA 接入 “wlan-net”，测试连通性如下。

```
C:\Users\admin>ipconfig
无线局域网适配器 WLAN:
    连接特定的 DNS 后缀 . . . . .:
    本地链接 IPv6 地址. . . . .: fe80::3ce1:b4f7:546e:45a1%14
    IPv4 地址 . . . . .: 10.23.101.40
    子网掩码 . . . . .: 255.255.255.0
    默认网关. . . . .: 10.23.101.254
```

```
C:\Users\admin>ping 10.23.101.254
正在 Ping 10.23.101.254 具有 32 字节的数据:
来自 10.23.101.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=8ms TTL=254
10.23.101.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

往返行程的估计时间(以毫秒为单位):

最短 = 5ms, 最长 = 9ms, 平均 = 7ms

STA 接入 “ap5”，测试连通性如下。

```
C:\Users\admin>ipconfig
无线局域网适配器 WLAN:
    连接特定的 DNS 后缀 . . . . .:
    本地链接 IPv6 地址 . . . . .: fe80::3ce1:b4f7:546e:45a1%14
    IPv4 地址 . . . . .: 10.23.201.133
    子网掩码 . . . . .: 255.255.255.0
    默认网关 . . . . .: 10.23.201.254

C:\Users\admin>ping 10.23.201.254
正在 Ping 10.23.201.254 具有 32 字节的数据:
来自 10.23.201.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.23.201.254 的回复: 字节=32 时间=8ms TTL=254
来自 10.23.201.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.23.201.254 的回复: 字节=32 时间=4ms TTL=254
10.23.201.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 4ms, 最长 = 8ms, 平均 = 5ms
```

4.3.3 在 NCE 上查看设备运行状态

选择 “设计 > 设备管理”，可以查看设备运行状态。

<input type="checkbox"/>	名称	ESN	状态	角色	站点	设备型号
<input type="checkbox"/>	AP1	2102353VUR10N5119370	● 正常	AP	HCIP-WAC	AirEngine5761-11
<input type="checkbox"/>	AP2	2102353VUR10N5119363	● 正常	AP	HCIP-WAC	AirEngine5761-11
<input type="checkbox"/>	AP3	2102353VUR10N5119339	● 正常	AP	HCIP-WAC	AirEngine5761-11
<input type="checkbox"/>	AP5	2102353VUR10N5119348	● 正常	AP	HCIP-AP	AirEngine5761-11
<input type="checkbox"/>	WAC3	102257532207	● 正常	WAC	HCIP-WAC	AirEngine9700-M1

共5条

4.3.4 在 NCE 上查看终端接入状况

选择 “监控 > 终端”，可以查看用户在线时长、用户列表等信息。

监控 维护 系统
☰ ☆ 🔥 0 ⚡

📄 概览

- LAN概览
- 站点间
- 站点
- 终端 ☆
- 设备360
- WAC组

🔔 告警

- 当前告警
- 历史告警
- 事件
- 屏蔽告警
- 告警通知
- 告警设置

设备终端监控

站点 / VN / 终端: HCIP-AP

📌 终端数据通过网络设备收集，默认展现10分钟内上报的用户记录，如需查看7天内历史用户，请点击 [历史用户](#)。

用户在线时长

📌 用户列表最多支持6万条数据展示，导出列表请到 [监控 > 报表 > 统计分析 > 报表定制](#) 创建对应的报表任务。

用户列表

📏 在线

用户名	终端M...	终端IP	终端IPv6	关联设...	接入设备MAC	SSID	接入类型
08****6f	08****6F	10****25	--	AP5	9C-B2-E8-2D-52-30	ap5	无线接入

4.4 配置参考

4.4.1 WAC3 配置

```

Software Version V200R021C00SPC100
#
sysname WAC3
#
    
```

```
http secure-server ssl-policy default_policy
http secure-server server-source -i MEth0/0/1
http server enable
#
vlan batch 100 to 101
#
stp enable
#
management-port isolate enable
management-plane isolate enable
#
interface Vlanif1
 ip address dhcp-alloc unicast
#
interface Vlanif100
 ip address 10.23.100.3 255.255.255.0
#
interface MEth0/0/1
 ip address 172.21.39.6 255.255.255.0
#
interface Ethernet0/0/47
 ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif100 10.23.100.254
ip route-static 172.21.39.88 255.255.255.255 Vlanif100 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#^UY*(/s.~&jK$VHVY-Y>0lRL!``@k7w#`Y~%R]>V%^%#
capwap dtls inter-controller psk %^%#Cl;<X"Hg5BWF8dX-b{;%~)l'W#{<.kZk2-%S%#7%^%#
capwap message-integrity psk %^%#*JU'.fC&0;Pvm8[+ur-Pfy:H(T)<)iqVr,9WWM;X%^%#
capwap sensitive-info psk %^%#\MPI4+"|NH|,>g0C6_GWT=p10ACVx9YiO.YHYg>*%^%#
capwap inter-controller sensitive-info psk %^%#jcaO([qQSUSvB;Z\PJ25DWDDr-qvP!O-J6z/4DSH!%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
cloud-mng controller ip-address 172.21.39.88 port 10020 source-interface Vlanif100
#
wlan
 temporary-management psk %^%#NA'y2_qi*04'/tE>zQU-X5ts#{6r}"q5eUJpf4GJ%^%#
 ap username admin password cipher %^%#5!1~(fh,-PMe.<BSbdHYA&Jq<GIQJLn'WB*LG#LO%^%#
 traffic-profile name default
 security-profile name default
```

```
security-profile name wlan-net
  security wpa-wpa2 psk pass-phrase %^%#Sf2V!Uqky*mZw&6RPu8VFQ:z'ukl'${BtT:Z&{@/%^%# aes
security-profile name default-wds
security-profile name default-mesh
ssid-profile name default
ssid-profile name wlan-net
  ssid wlan-net
vap-profile name default
vap-profile name wlan-net
  service-vlan vlan-id 101
  ssid-profile wlan-net
  security-profile wlan-net
wds-profile name default
mesh-handover-profile name default
mesh-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-whitelist-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
ap auth-mode sn-auth
ap-group name default
ap-group name ap-group1
  regulatory-domain-profile domain1
radio 0
  vap-profile wlan-net wlan 1
radio 1
  vap-profile wlan-net wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
  ap-name AP3
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
  ap-name AP1
  ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
  ap-name AP2
  ap-group ap-group1
provision-ap
#
return
```


4.4.2 AP5 配置

```
Software Version V200R021C00SPC200
#
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif1
http server enable
#
vlan batch 200 to 201 3911
#
dhcp enable
#
acl name nat 2000
rule 5 deny source 169.254.2.0 0.0.0.255
rule 10 permit
#
interface Vlanif1
nat outbound 2000
ip address dhcp-alloc unicast
#
interface Vlanif3911
ip address 10.1.1.1 255.255.255.0
arp-proxy enable
dhcp select global
#
interface Ethernet0/0/0
#
interface Ethernet0/0/46
ip address 169.254.4.1 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/0
port hybrid tagged vlan 2 to 3910 3912 to 4094
dhcp snooping trusted
#
interface GigabitEthernet0/0/1
port hybrid tagged vlan 2 to 3910 3912 to 4094
dhcp snooping trusted
#
interface NULL0
#
wmi-server
server ip-address 172.21.39.88 port 10032
collect-item device-data interval 300
collect-item radio-data interval 300
collect-item ssid-data interval 300
```

```
collect-item interface-data interval 300
collect-item terminal-data interval 300
collect-item log-data disable
collect-item location-data disable
collect-item security-data disable
collect-item application-statistics-data disable
collect-item neighbor-device-data interval 300
collect-item emdi-data disable
collect-item cpcar-data disable
collect-item dns-data enable
collect-item dns-data interval 300
collect-item non-wifi-data enable
collect-item non-wifi-data interval 300
#
wmi-server2
collect-item log-data disable
#
wlan
temporary-management psk %^%#NPjnC\Vs5V}Ov3Y^%kJS*rP[K4iix2Dn`+@0aSGB%^%#
traffic-profile name default
security-profile name ap5
security wpa-wpa2 psk pass-phrase %^%#FzDm;<bTwKdpY@!7Zs(;$]BnEt(sp&U3Z5&MZzjK%^%# aes
security-profile name default
security-profile name default-mesh
ssid-profile name ap5
ssid ap5
ssid-profile name default
vap-profile name ap5
service-vlan vlan-id 201
ssid-profile ap5
security-profile ap5
vap-profile name default
mesh-profile name default
regulatory-domain-profile name default
air-scan-profile name 5G
air-scan-profile name 2.4G
air-scan-profile name default
rrm-profile name 5G
calibrate min-tx-power 12
airtime-fair-schedule enable
smart-roam quick-kickoff-threshold disable
sta-load-balance dynamic disable
rrm-profile name 2.4G
calibrate min-tx-power radio-5g 9
airtime-fair-schedule enable
smart-roam quick-kickoff-threshold disable
sta-load-balance dynamic disable
rrm-profile name default
```

```
radio-2g-profile name 2.4G
  power auto-adjust enable
  rrm-profile 2.4G
  air-scan-profile 2.4G
radio-2g-profile name default
radio-5g-profile name 5G
  power auto-adjust enable
  rrm-profile 5G
  a-msdu disable
  air-scan-profile 5G
radio-5g-profile name default
wids-spoof-profile name default
wids-whitelist-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
  user-interface vty 0 idle-timeout 10 0
  user-interface vty 1 idle-timeout 10 0
  user-interface vty 2 idle-timeout 10 0
  user-interface vty 3 idle-timeout 10 0
  user-interface vty 4 idle-timeout 10 0
  traffic-optimize broadcast-suppression other-broadcast rate-threshold 64
  traffic-optimize broadcast-suppression other-multicast rate-threshold 64
ble-profile name default
port-link-profile name default
port-link-profile name default-GE-0
wired-port-profile name default
wired-port-profile name default-GE-0
  port-link-profile default-GE-0
ap-group name default
  ble-profile default
  wired-port-profile default-GE-0 gigabitethernet 0
radio 0
  radio-2g-profile 2.4G
  radio-5g-profile 5G
  antenna-gain 2
radio 1
  radio-5g-profile 5G
  antenna-gain 2
radio 2
  radio-2g-profile 2.4G
  radio-5g-profile 5G
ap-id 0 type-id 144 ap-mac 9cb2-e82d-5230 ap-sn 2102353VUR10N5119348
  ap-name AP5
radio 0
  vap-profile ap5 wlan 1
radio 1
  vap-profile ap5 wlan 1
```

```
provision-ap
#
return
```

4.4.3 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101 200 to 201
#
dhcp enable
#
vlan 99
 name Manage
#
interface Vlanif1
#
interface Vlanif99
 ip address 172.21.39.253 255.255.128.0
#
interface Vlanif100
 ip address 10.23.100.254 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.254 255.255.255.0
 dhcp select interface
#
interface Vlanif200
 ip address 10.23.200.254 255.255.255.0
 dhcp select interface
 dhcp server option 148 ascii "agilemode=agile-cloud;agilemanage-mode=ip;agilemanage-
domain=172.21.39.88;agilemanage-port=10020;ap-agilemode=agile-cloud;"
#
interface Vlanif201
 ip address 10.23.201.254 255.255.255.0
 dhcp select interface
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 shutdown
#
interface MultiGE0/0/2
 shutdown
```

```
#
interface MultiGE0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
 port link-type access
 port default vlan 99
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101 200 to 201
#
interface NULL0
#
return
```

4.4.4 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101 200 to 201
#
interface Vlanif1
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
```

```
interface MultiGE0/0/3
  port link-type trunk
  port trunk pvid vlan 100
  port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
  shutdown
#
interface MultiGE0/0/5
  port link-type trunk
  port trunk pvid vlan 200
  port trunk allow-pass vlan 200 to 201
#
interface MultiGE0/0/6
  shutdown
#
interface MultiGE0/0/7
  shutdown
#
interface MultiGE0/0/8
  shutdown
#
interface MultiGE0/0/9
  port link-type trunk
  port trunk allow-pass vlan 100 to 101 200 to 201
#
interface NULL0
#
return
```

4.5 思考题

上述实验中采用 DHCP 的方式将 AP5 切换到云模式，请思考，除了 DHCP 方式外还有什么方式可以将 FIT AP 切换为云模式？

参考答案：

云 AP 支持以下方式进行模式切换和 iMaster NCE-Campus 地址的获取：

通过 DHCP 服务器获取：优先级最高，如果设备同时满足多种方式的获取条件，优先采用 DHCP 方式获取的。

通过注册中心获取：优先级最低。

通过命令行/Web 手动配置：优先级介于通过 DHCP 服务器获取与通过注册中心获取两种方式之间。

5 802.1X 认证实验

5.1 实验介绍

5.1.1 关于本实验

通过 802.1X 认证实验，使学员掌握 802.1X 准入认证基本原理和配置方法。

5.1.2 实验目的

- 掌握 WLAN 的基本业务配置流程。
- 掌握 802.1X 准入认证基本原理及相关配置。

5.1.3 实验组网介绍

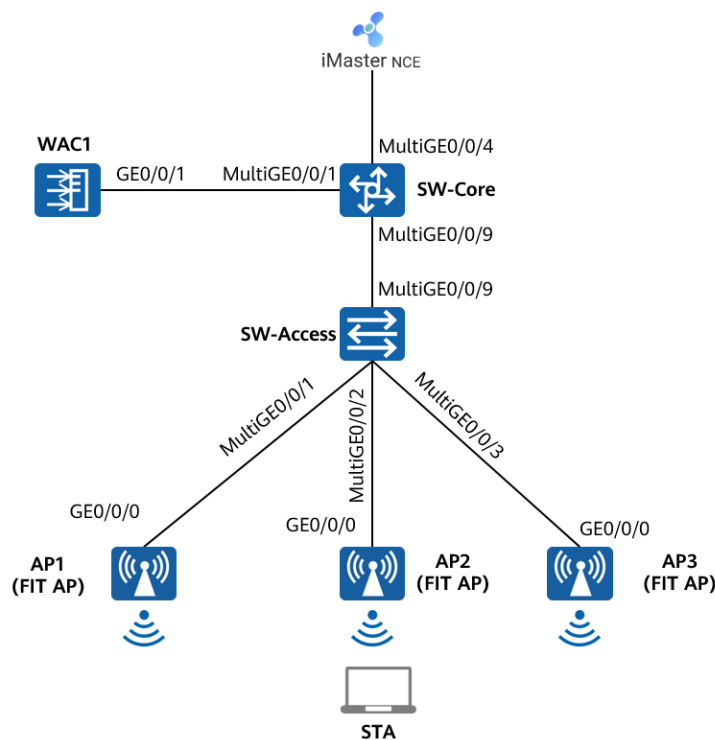


图5-1 802.1X 认证实验拓扑图

5.1.4 实验规划

表5-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/4	Access	PVID: 99
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表5-2 IP 地址规划

设备	端口	IP地址
SW-Core	Vlanif100	10.23.100.254/24
	Vlanif101	10.23.101.254/24
	Vlanif99	172.21.39.253/17
WAC1	Vlanif100	10.23.100.1/24
iMaster NCE-Campus	/	172.21.39.88/17

表5-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	隧道转发
管理VLAN	100
业务VLAN	101
AP组	ap-group1
VAP模板	wlan-net
安全模板	wlan-net
安全策略	WPA2+802.1X+AES
SSID模板	wlan-net
SSID	wlan-net
RADIUS认证参数	RADIUS认证方案名称: radius_huawei RADIUS计费方案名称: scheme1 RADIUS服务器模板名称: radius_huawei 其中RADIUS服务器信息如下: IP地址: 172.21.39.88 认证端口号: 1812 计费端口号: 1813 共享密钥: Huawei@123
802.1X接入模板	名称: d1 认证方式: EAP
认证模板	名称: p1 绑定的模板和方案如下: 802.1X接入模板: d1 RADIUS服务器模板: radius_huawei RADIUS认证方案: radius_huawei RADIUS计费方案: scheme1

5.2 实验任务配置

5.2.1 配置思路

- 1.配置基础网络，确保网络互通。
- 2.配置 AP 上线。
- 3.配置 NCE 与 WAC1 网络互通。
- 4.在 WAC1 上配置 802.1X 认证。
- 5.配置 WLAN 基本业务。
- 6.在 NCE 服务器上配置 802.1X 认证。
- 7.验证 802.1X 准入认证。

5.2.2 配置步骤

步骤 1 配置基础网络和 AP 上线

请参考 1.2.2 步骤 1~1.2.2 步骤 6，此处不再赘述。

步骤 2 配置 NCE 与 WAC1 之间网络互通

iMaster NCE-Campus 的 IP 地址和网关在软件安装阶段已配置完成，本实验不再赘述。
iMaster NCE-Campus 地址配置为 172.21.39.88/17，网关地址是 172.21.39.253（位于 SW-Core 上）。

配置 SW-Core 的 VLAN 信息及 IP 地址，确保 NCE 与 SW-Core 之间网络互通。

```
[SW-Core] vlan 99
[SW-Core-vlan99] name Manage
[SW-Core-vlan99] quit
[SW-Core] interface MultiGE 0/0/4
[SW-Core-MultiGE0/0/4] port link-type access
[SW-Core-MultiGE0/0/4] port default vlan 99
[SW-Core-MultiGE0/0/4] quit
[SW-Core] interface Vlanif 99
[SW-Core-Vlanif99] ip address 172.21.39.253 17
[SW-Core-Vlanif99] quit
```

配置 WAC1 的静态路由，确保 NCE 与 WAC1 之间网络互通。

选择“配置 > AC 配置 > IP”，选择“路由”选项卡，点击“静态路由配置表”，展开对应的配置界面，然后点击“新建”，新建静态路由。

在“新建静态路由”页面，依次分别配置如下两条静态路由，然后点击“确定”。其中静态路由 0.0.0.0/0 用于访问其他外部网络，静态路由 172.21.39.88/32 用于访问 NCE 服务器。

配置完成后，查看静态路由如下所示。

目的IP地址	子网掩码	下一跳	出接口	优先级
<input type="checkbox"/> 0.0.0.0	0.0.0.0	10.23.100.254	Vlanif100	60
<input type="checkbox"/> 172.21.39.88	255.255.255.255	10.23.100.254	Vlanif100	60

步骤 3 配置 802.1X 认证（WAC1）

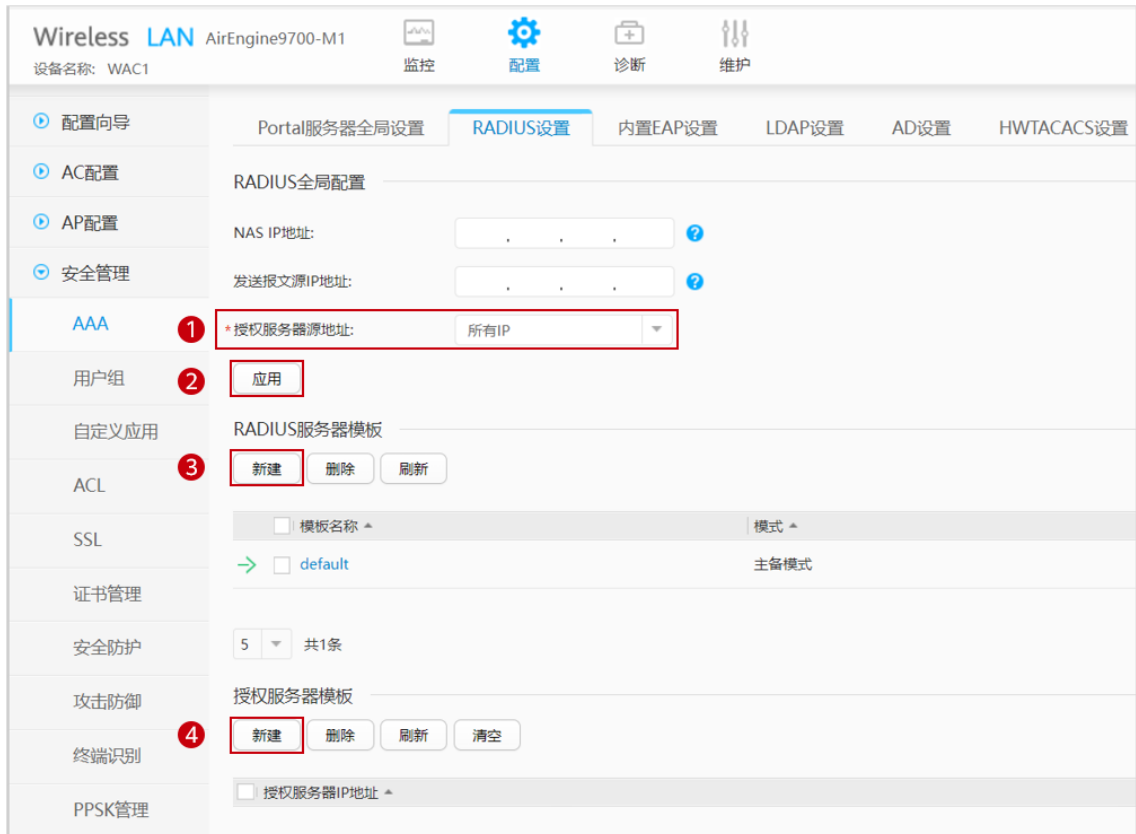
配置 RADIUS 协议的相关参数，主要包括如下三部分内容：RADIUS 全局配置、RADIUS 服务器模板和授权服务器模板。

选择“配置 > 安全管理 > AAA”，选择“RADIUS 设置”选项卡，依次设置如下。

RADIUS 全局配置：配置“授权服务器源地址”为“所有 IP”，然后点击“应用”。

RADIUS 服务器模板：点击“新建”，新建 RADIUS 服务器模板，具体细节参见下文。

授权服务器模板：点击“新建”，新建授权服务器模板，具体细节参见下文。



The screenshot shows the configuration page for RADIUS settings on a Huawei AirEngine9700-M1 device. The left sidebar has 'AAA' selected. The main content area is titled 'RADIUS 设置' and includes sections for 'RADIUS 全局配置', 'RADIUS 服务器模板', and '授权服务器模板'. Red boxes and circled numbers 1-4 highlight the '授权服务器源地址' dropdown (set to '所有 IP'), the '应用' button, the '新建' button for RADIUS server templates, and the '新建' button for authorization server templates respectively.

新建“RADIUS 服务器模板”的具体细节请参考如下配置。

新建RADIUS服务器模板

*模板名称: ① radius_huawei

模式: 主备模式 负载均衡模式

NAS IP地址: ② 指定IP地址
10 , 23 , 100 , 1

*模板默认共享密钥: ③ Huawei@123

④ 新建服务器 删除 IP地址

<input type="checkbox"/> IP地址 ▲	共享密钥 ▲	认证端口号 ▲	计费端口号 ▲
→ <input type="checkbox"/> 172.21.39.88	*****	1812	1813

5 共1条

高级 ⓘ

⑤ 确定 取消

新建服务器配置

* IP地址: IPv4 172 . 21 . 39 . 88

共享密钥: Huawei@123

服务器配置

认证

* 端口号: 1812

权重值: 80

发送报文源IP地址: LoopBack VLANIF IP地址

Vlanif100 ... X

Virtual-ip: OFF

计费

* 端口号: 1813

权重值: 80

发送报文源IP地址: LoopBack VLANIF IP地址

Vlanif100 ... X

Virtual-ip: OFF

新建“授权服务器模板”的具体细节请参考如下配置。

新建授权服务器

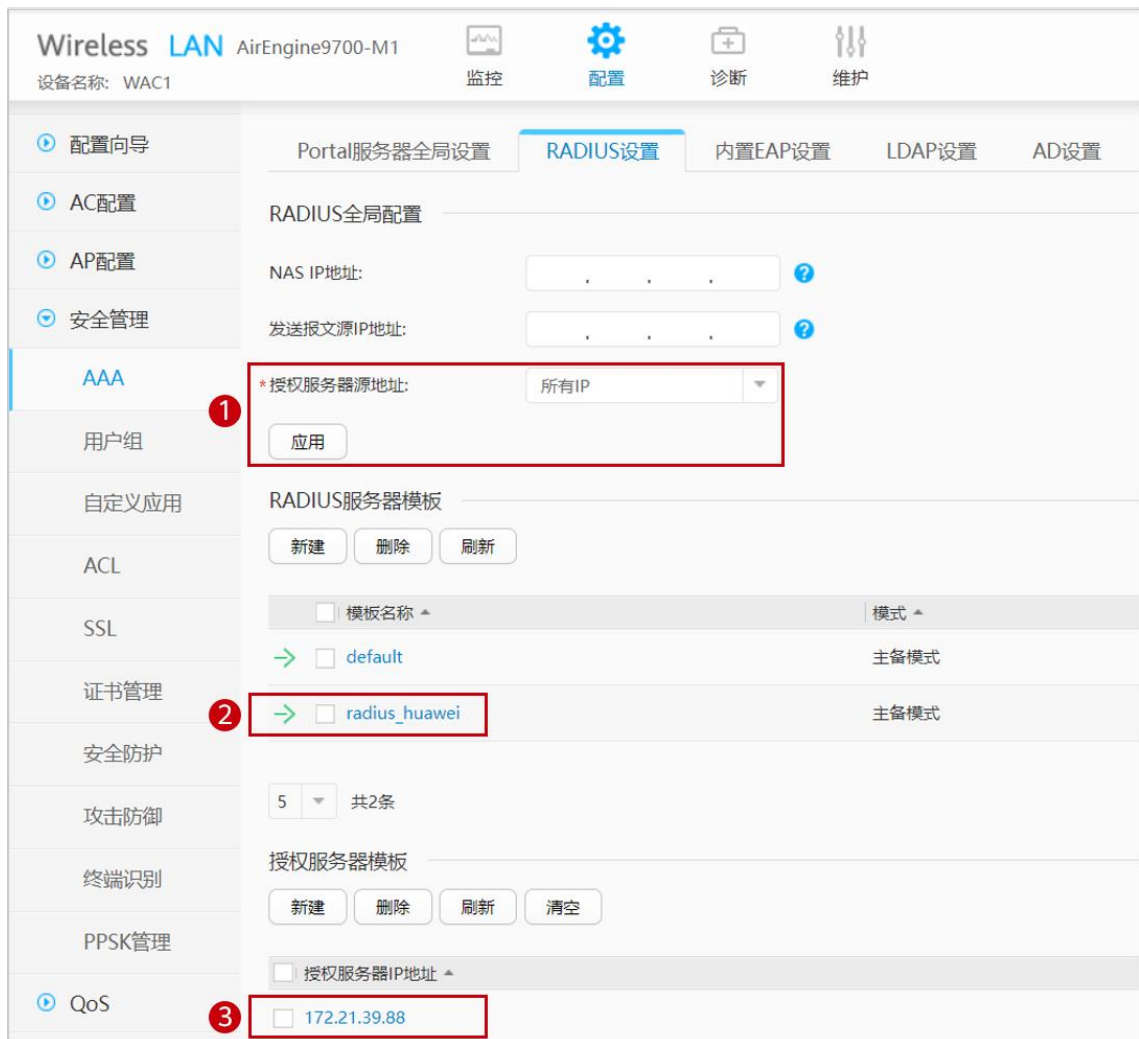
* 授权服务器IP地址: 172 . 21 . 39 . 88

模板名称: radius_huawei

* 密钥: Huawei@123



建议在“RADIUS 设置”全部配置完成后,进行全面检查,如下所示。



配置 AAA 认证方案模板。

选择“配置 > AP 配置 > 模板管理 > AAA > 认证方案模板”, 点击“新建”, 配置模板名称为“radius_huawei”, 然后点击“确定”。



选择“radius_huawei”认证方案模板，配置第一认证模式为“RADIUS 认证”，点击“应用”。



配置 AAA 计费方案模板。

选择“配置 > AP 配置 > 模板管理 > AAA > 计费方案模板”，点击“新建”，配置模板名称为“scheme1”，然后点击“确定”。



选择“scheme1”计费方案模板，配置计费模式为“RADIUS 计费”，计费形式为“实时计费”，实时计费时间间隔为 3 分钟，然后点击“应用”。



计费方案模板: 展示模板引用关系

计费模式:

计费形式: 按时长计费 实时计费

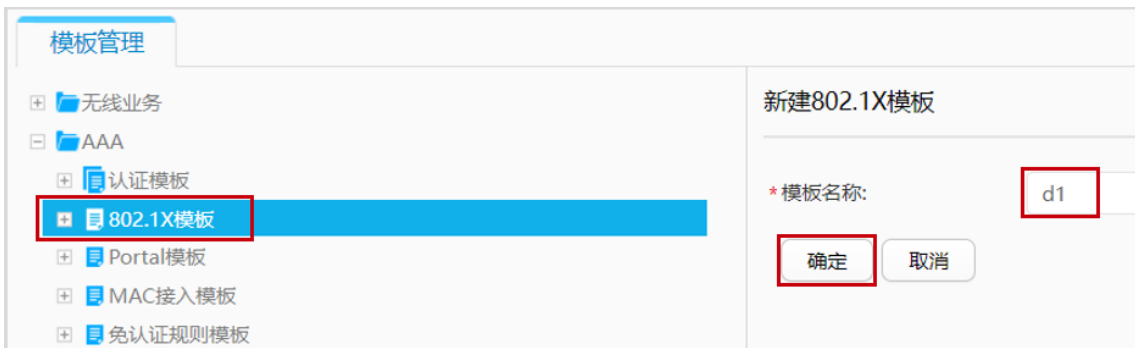
*实时计费时间间隔(分钟): 实时计费请求无响应最大次数:

实时计费失败后策略: 拒绝用户上线 允许用户上线

开始计费后失败策略: 拒绝用户上线 允许用户上线

配置 802.1X 模板。

选择“配置 > AP 配置 > 模板管理 > AAA > 802.1X 模板”，点击“新建”，配置模板名称为“d1”，然后点击“确定”。



模板管理

- 无线业务
- AAA
 - 认证模板
 - 802.1X模板**
 - Portal模板
 - MAC接入模板
 - 免认证规则模板

新建802.1X模板

*模板名称:

选择名称为“d1”的 802.1X 模板，配置用户认证方式为“EAP”，然后点击“应用”。



802.1X模板: 展示模板引用关系

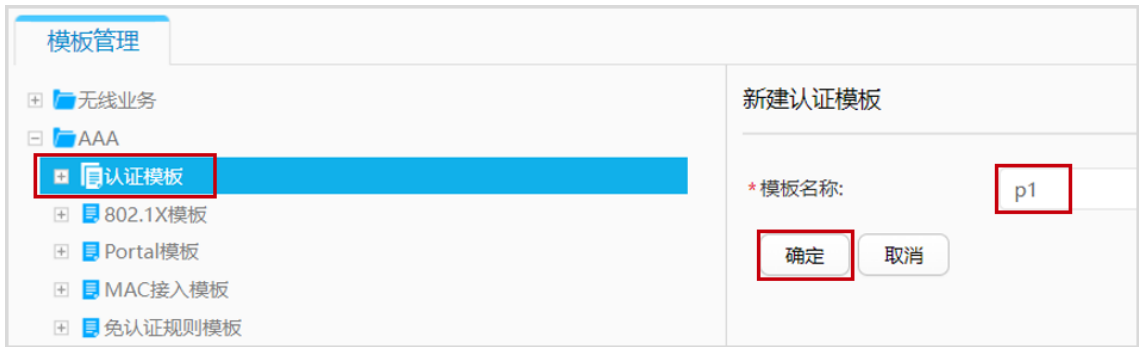
模板介绍信息: 通过802.1X接入模板统一管理802.1X接入相关的所有配置。包括802.1X用户的认证方式、

用户认证方式: EAP PAP CHAP

高级

配置认证模板。

选择“配置 > AP 配置 > 模板管理 > AAA > 认证模板”，点击“新建”，配置模板名称为“p1”，然后点击“确定”。



选择名称为“p1”的认证模板，在其中引用 802.1X 模板“d1”、RADIUS 服务器模板“radius_huawei”、认证方案“radius_huawei”、计费方案“scheme1”，如下所示。



The image contains two screenshots of the Huawei network management interface, specifically the 'Template Management' (模板管理) section.

Top Screenshot: Authentication Scheme Template Configuration

- Left Panel (Tree View):** Shows a hierarchy: 无线业务 > AAA > 认证模板 > p1. The '认证方案模板' (Authentication Scheme Template) item is highlighted with a red box and a circled '1'.
- Right Panel (Configuration):**
 - '认证方案模板:' (Authentication Scheme Template): dropdown menu with 'radius_huawei' selected, highlighted with a red box and a circled '2'.
 - '第一认证模式:' (First Authentication Mode): dropdown menu with 'RADIUS认证' (RADIUS Authentication) selected.
 - '第三认证模式:' (Third Authentication Mode): dropdown menu with '不配置' (Not Configured) selected.
 - '第五认证模式:' (Fifth Authentication Mode): dropdown menu with '不配置' (Not Configured) selected.
 - '第七认证模式:' (Seventh Authentication Mode): dropdown menu with '不配置' (Not Configured) selected.
 - '应用' (Apply) button: highlighted with a red box and a circled '3'.

Bottom Screenshot: Billing Scheme Template Configuration

- Left Panel (Tree View):** Shows a hierarchy: 无线业务 > AAA > 认证模板 > p1. The '计费方案模板' (Billing Scheme Template) item is highlighted with a red box and a circled '1'.
- Right Panel (Configuration):**
 - '计费方案模板:' (Billing Scheme Template): dropdown menu with 'scheme1' selected, highlighted with a red box and a circled '2'.
 - '计费模式:' (Billing Mode): dropdown menu with 'RADIUS计费' (RADIUS Billing) selected.
 - '计费形式:' (Billing Form): radio buttons for '按时长计费' (By Duration Billing) and '实时计费' (Real-time Billing). '实时计费' is selected.
 - '*实时计费时间间隔(分钟):' (Real-time Billing Time Interval in Minutes): input field with '3'.
 - '实时计费失败后策略:' (Real-time Billing Failure Strategy): radio buttons for '拒绝用户上线' (Reject User Online) and '允许用户上线' (Allow User Online). '允许用户上线' is selected.
 - '开始计费后失败策略:' (Start Billing Failure Strategy): radio buttons for '拒绝用户上线' (Reject User Online) and '允许用户上线' (Allow User Online). '拒绝用户上线' is selected.
 - '应用' (Apply) button: highlighted with a red box and a circled '3'.

步骤 4 配置无线业务

创建名为“wlan-net”的安全模板，并配置安全策略。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > 安全模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



选择“wlan-net”安全模板，配置如下参数，点击“应用”。



创建名为“wlan-net”的 SSID 模板，并配置 SSID 名称为“wlan-net”。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > SSID 模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



选择“wlan-net”SSID 模板，配置 SSID 名称为“wlan-net”，点击“应用”。



SSID模板: wlan-net 展示模板引用关系

模板介绍信息: SSID用来指定不同的无线网络。在STA上搜索可接入的无线网络时,显示出来的网络名称就是SSID。

基础配置 高级配置

* SSID名称: wlan-net

最大用户数: 64

应用

创建名为“wlan-net”的 VAP 模板，配置业务数据转发模式、业务 VLAN，并且引用 SSID 模板、安全模板和认证模板。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > VAP 模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



模板管理

无线业务

- VAP模板
 - default
- SSID模板
- 安全模板
- 流量模板

新建VAP模板

*模板名称: wlan-net

确定 取消

选择“wlan-net” VAP 模板，配置转发模式为隧道转发，业务 VLAN 为 VLAN 101，点击“应用”。



VAP模板: wlan-net 展示模板引用关系

模板介绍信息: 在VAP模板下配置各项参数,然后在AP组或AP中引用VAP模板,AP上就会生成VAP,VAP用来为STA提供无线接入服务。通过配置VAP模板下的参数,使AP实现为STA

基础配置 高级配置

使能状态: ON

转发模式: 隧道转发

指定报文直接转发: IPv4 ?

业务VLAN: 单个VLAN VLAN Pool 业务VLAN ID: 101

应用

配置“wlan-net” VAP 模板所关联的 SSID 模板为“wlan-net”，点击“应用”。



配置“wlan-net” VAP 模板所关联的安全模板为“wlan-net”，点击“应用”。



配置“wlan-net” VAP 模板所关联的认证模板为“p1”，点击“应用”。

模板管理

认证模板: ... × 展示模板引用关系

模板介绍信息: 通过配置认证模板下的参数 (例如: 配置认证模板下绑定的接入模板, 确定认证模板的认证方...

Portal选项: 基于Portal服务器的MAC快速认证

认证前授权VLAN: ?

认证失败授权: VLAN 用户组

认证失败授权VLAN: ?

认证失败重认证: OFF

认证服务器不可用时授权用户组权限: ... ×

认证成功授权用户组权限: ... ×

计费开始触发时机: 认证通过 认证通过后获取IP

计费更新触发时机: 漫游触发 会话更新: OFF

信息更新触发

IP地址更新触发

认证成功推送页面: ▾

流量统计: OFF

配置 AP 组引用 VAP 模板。

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组的配置界面。

Wireless LAN AirEngine9700-M1

设备名称: WAC1

监控 配置 诊断 维护

配置向导

AC配置

AP配置

AP组配置

AP配置

射频规划/调优

AP组 静态负载均衡组

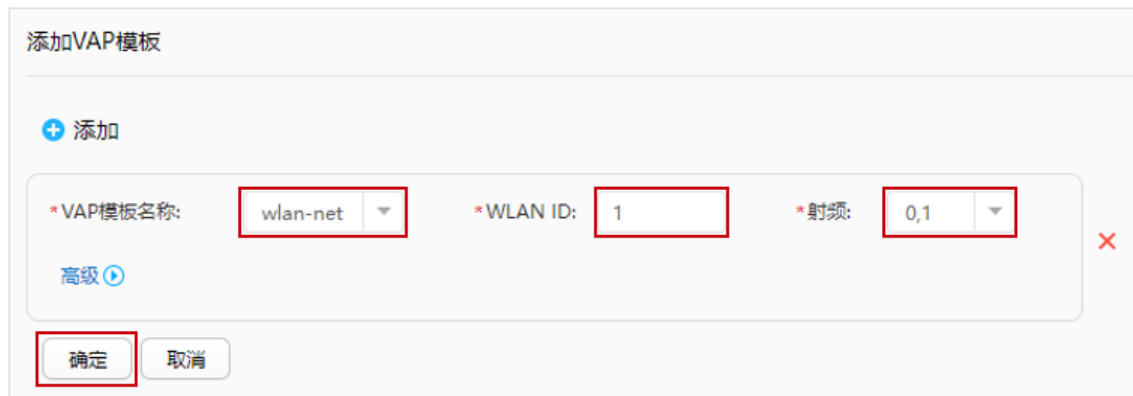
组名称 ^	VAP模板 ^	射频0模板 ^
<input type="checkbox"/> default		2.4G-default
<input checked="" type="checkbox"/> ap-group1		2.4G-default

20 ▾ 共2条

在 AP 组配置界面中，选择“VAP 配置”，在“VAP 模板列表”中，点击“添加”。



配置 VAP 模板名称为“wlan-net”，WLAN ID 为 1，射频为 0 和 1，点击“确定”。



最后查看“VAP 模板列表”如下。

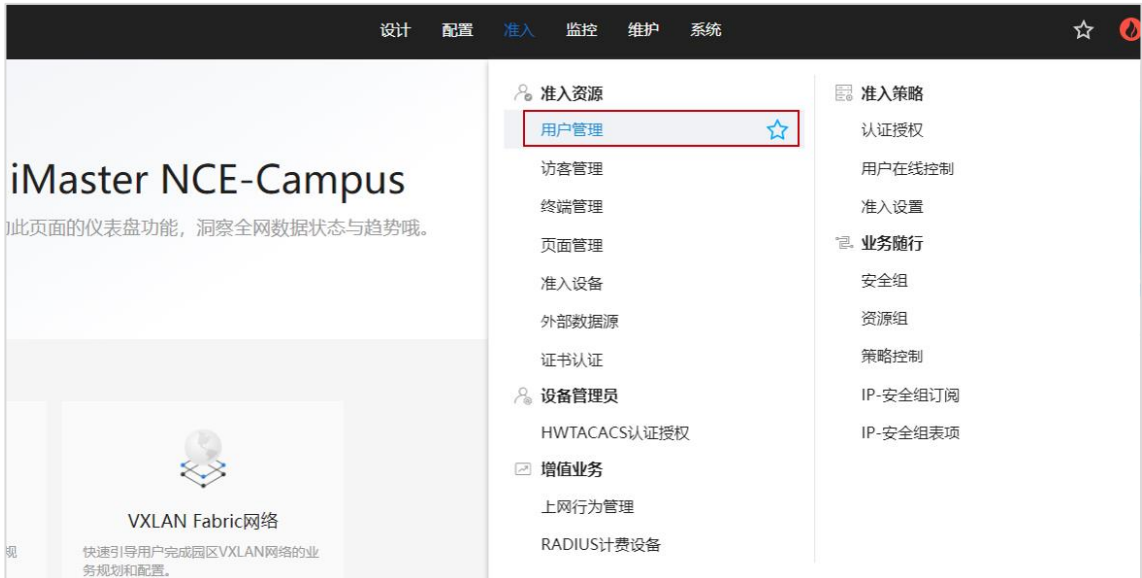


步骤 5 配置 802.1X 认证（NCE）

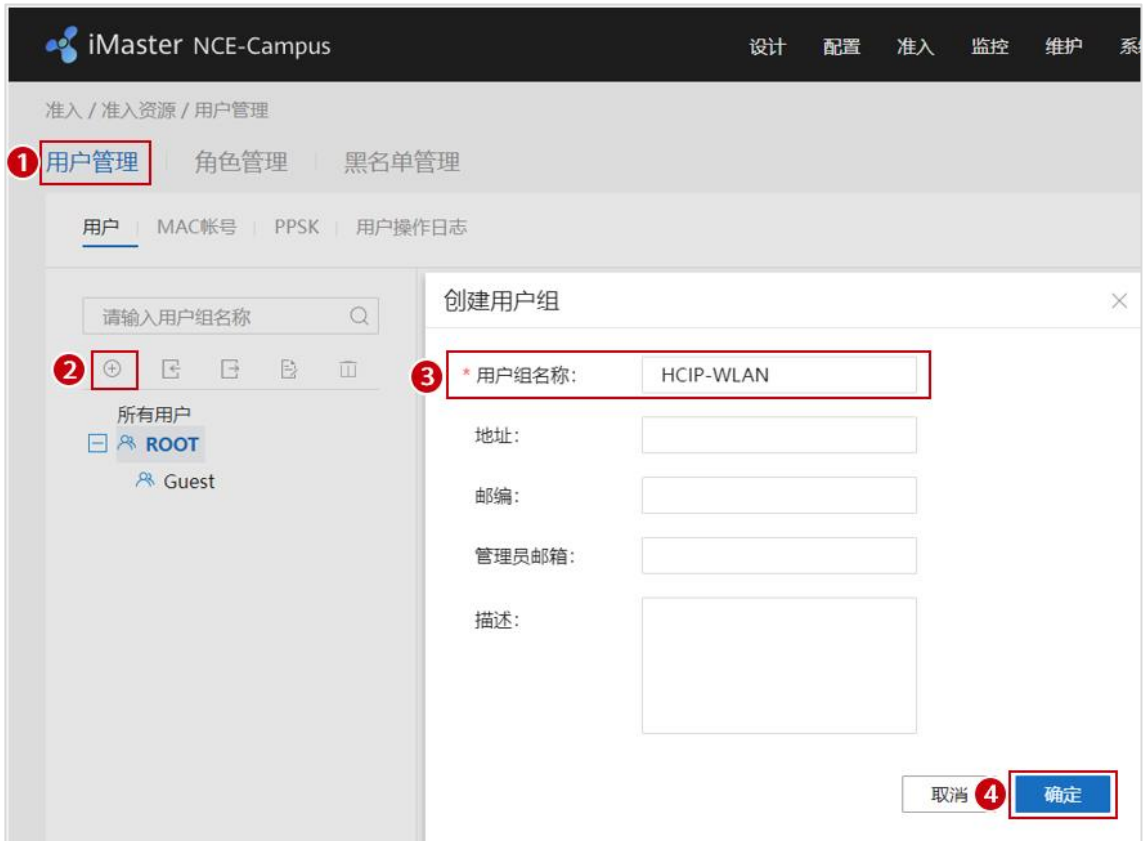
在 NCE 上配置准入认证，需要提前创建租户账号/密码，本文不再赘述。

在 NCE 上创建 802.1X 认证所用的用户名和密码。

在主菜单中选择“准入 > 准入资源 > 用户管理”。



选择“用户管理 > 用户”，点击“+”按钮，新建用户组“HCIP-WLAN”。

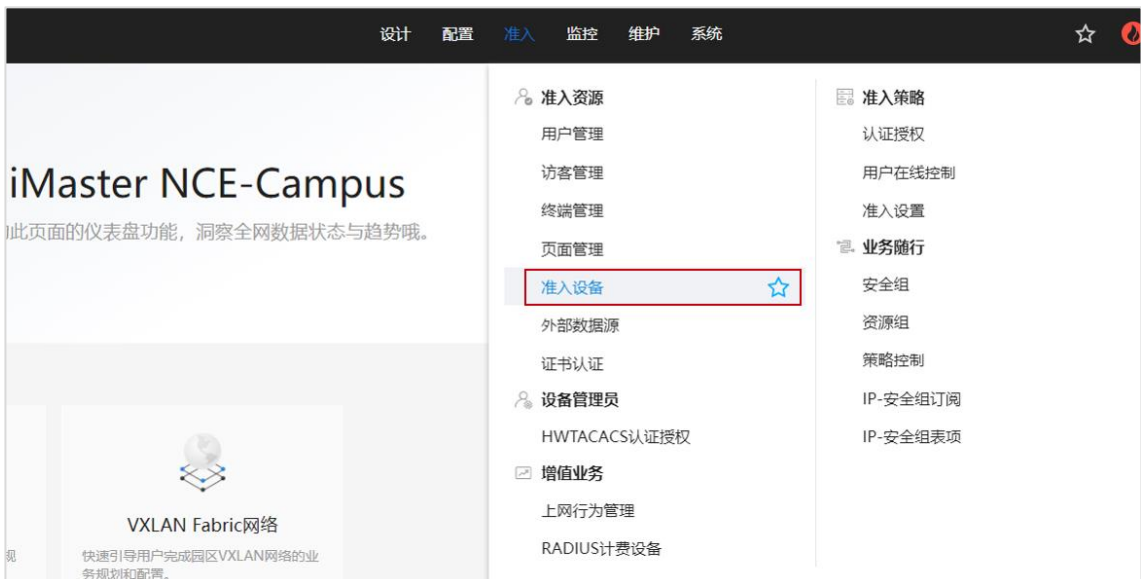


选中“HCIP-WLAN”用户组，单击“创建”，新增用于 802.1X 认证的用户名“dot1x-user”，密码设置为“Huawei@123”，允许登录方式选择“802.1X & Portal 2.0”，最后点击“确定”。



在 NCE 上添加准入设备（WAC1）。

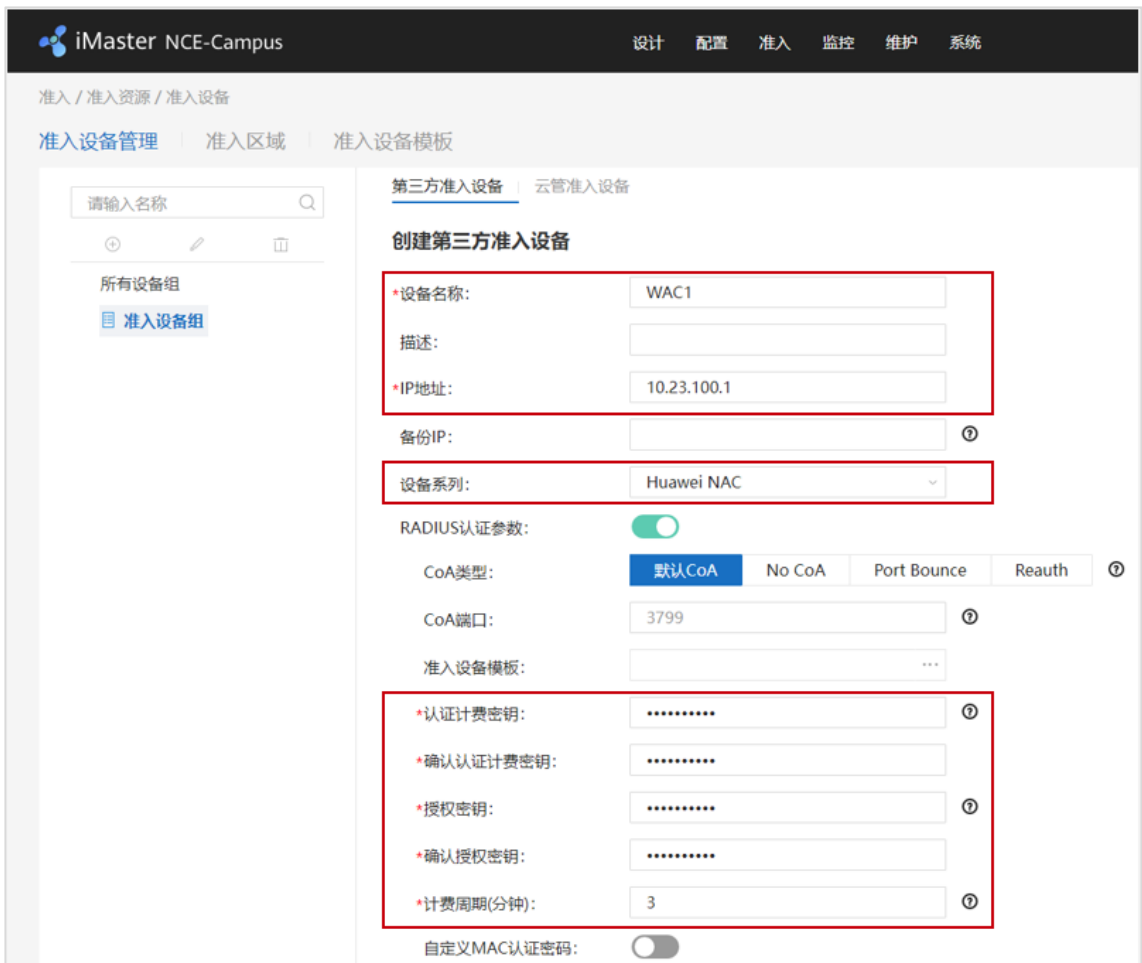
选择“准入 > 准入资源 > 准入设备”，配置准入设备。



选择“第三方准入设备”，点击“创建”，创建第三方准入设备。

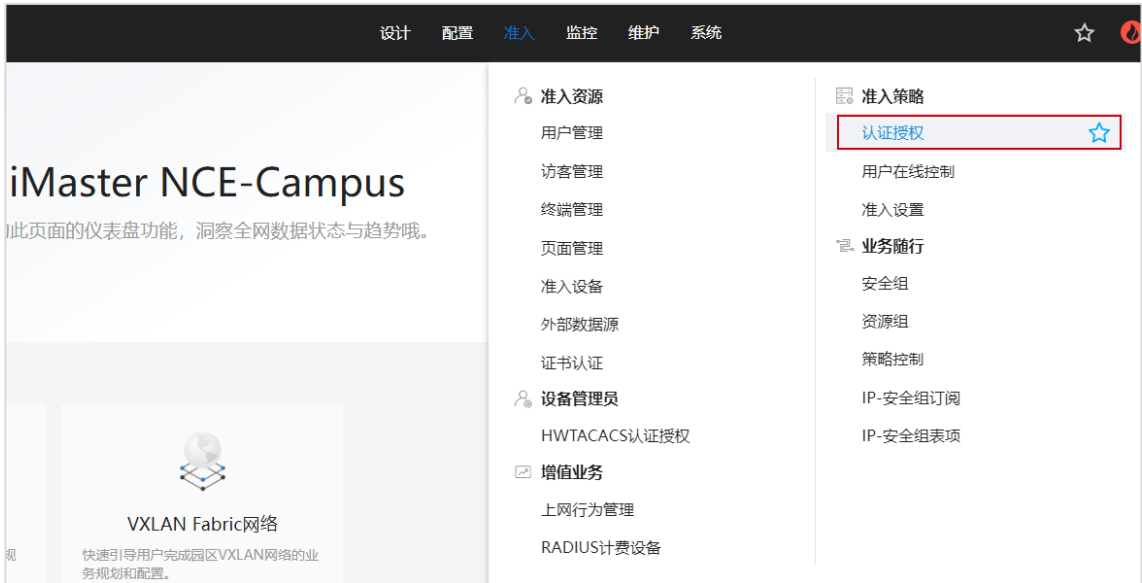


按照如下参数进行配置，其中“认证计费密钥”与“授权密钥”均为 Huawei@123，计费周期设置为 3 分钟，与 WAC1 中配置的参数保持一致。

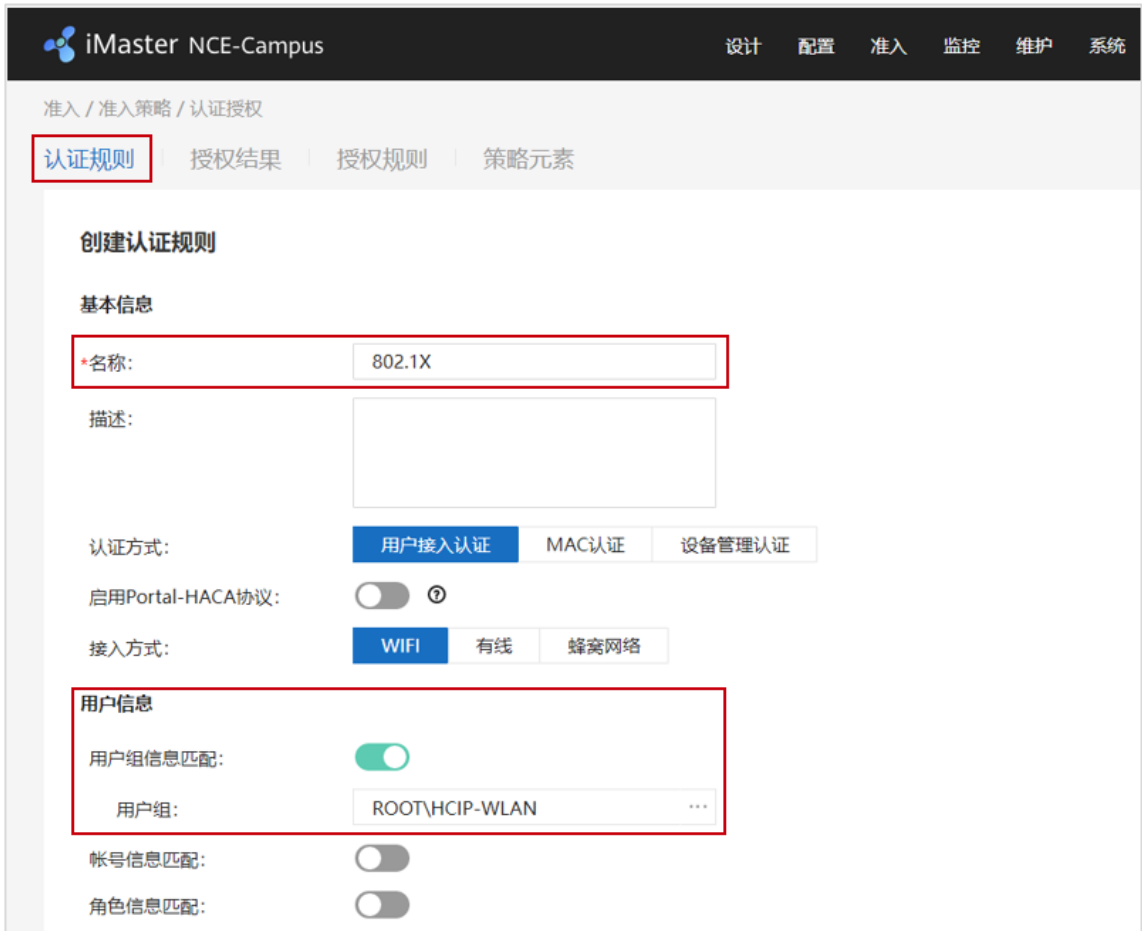


在 NCE 上创建认证规则、授权规则、授权结果。

选择“准入 > 准入策略 > 认证授权”。



选择“认证规则”，点击“创建”，按如下参数配置认证规则。



位置信息

站点信息匹配:

使能准入设备组匹配:

接入设备类型: ⓘ

设备信息匹配:

SSID匹配:

终端信息匹配: ⓘ

终端IP范围:

其他信息

时间信息:

定制条件:

认证信息

RADIUS中继:

接入参数:

*数据源:

<input type="checkbox"/>	优先级	名称
<input type="checkbox"/>	1	本地数据源

双因子认证:

优先识别协议:

优先识别协议:

*认证协议: 全选

PAP协议(本地帐号、AD、LDAP、RADIUS Token、第三方HTTP服务器)

CHAP协议(本地帐号)

EAP-MD5协议(本地帐号)

EAP-PEAP-MSCHAPv2协议(本地帐号、AD、LDAP)

EAP-TLS协议(本地帐号、AD、LDAP)

EAP-PEAP-GTC协议(本地帐号、AD、LDAP、RADIUS Token)

EAP-TTLS-PAP协议(本地帐号、AD、LDAP)

EAP-PEAP-TLS协议(本地帐号、AD、LDAP)

PAP协议, CHAP协议和EAP-MD5协议为不安全协议, 请谨慎选择。

高级选项

帐号不存在:

身份认证失败:

选择“授权规则”，点击“创建”，按如下参数配置授权规则。

iMaster NCE-Campus 设计 配置 准入 监控 维护 系统

准入 / 准入策略 / 认证授权

认证规则 | 授权结果 | **授权规则** | 策略元素

创建授权规则

基本信息

*名称: 802.1X

描述:

认证方式: 用户接入认证 | MAC认证 | 设备管理认证

启用Portal-HACA协议:

接入方式: WIFI | 有线 | 蜂窝网络

用户信息

用户组信息匹配:

*用户组: ROOT\HCIP-WLAN

外部组信息匹配:

帐号信息匹配:

角色信息匹配:

位置信息

站点信息匹配:

准入设备组匹配:

接入设备类型: ---请选择---

设备信息匹配:

SSID匹配:

SSID: 增加

wlan-net

终端信息匹配:

终端IP范围: 通过换行符分隔IP地址，请输入IP地址/掩码(如192.168.1.1/32或2001:0DB8:0:0:0:0:1428:57AB/64)或IP地址段(如192.168.1.1-

区域匹配:

SSID VAP

自动刷新: OFF

AP型VAP列表

应用统计清零

AP ID	AP名称	射频ID	WLAN ID	SSID	BSSID	认证方式	接入用户数	状态
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA2+802.1X	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA2+802.1X	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA2+802.1X	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA2+802.1X	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA2+802.1X	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA2+802.1X	0	on

10 共6条

注: 选择列表中的VAP,查看该VAP应用统计信息。

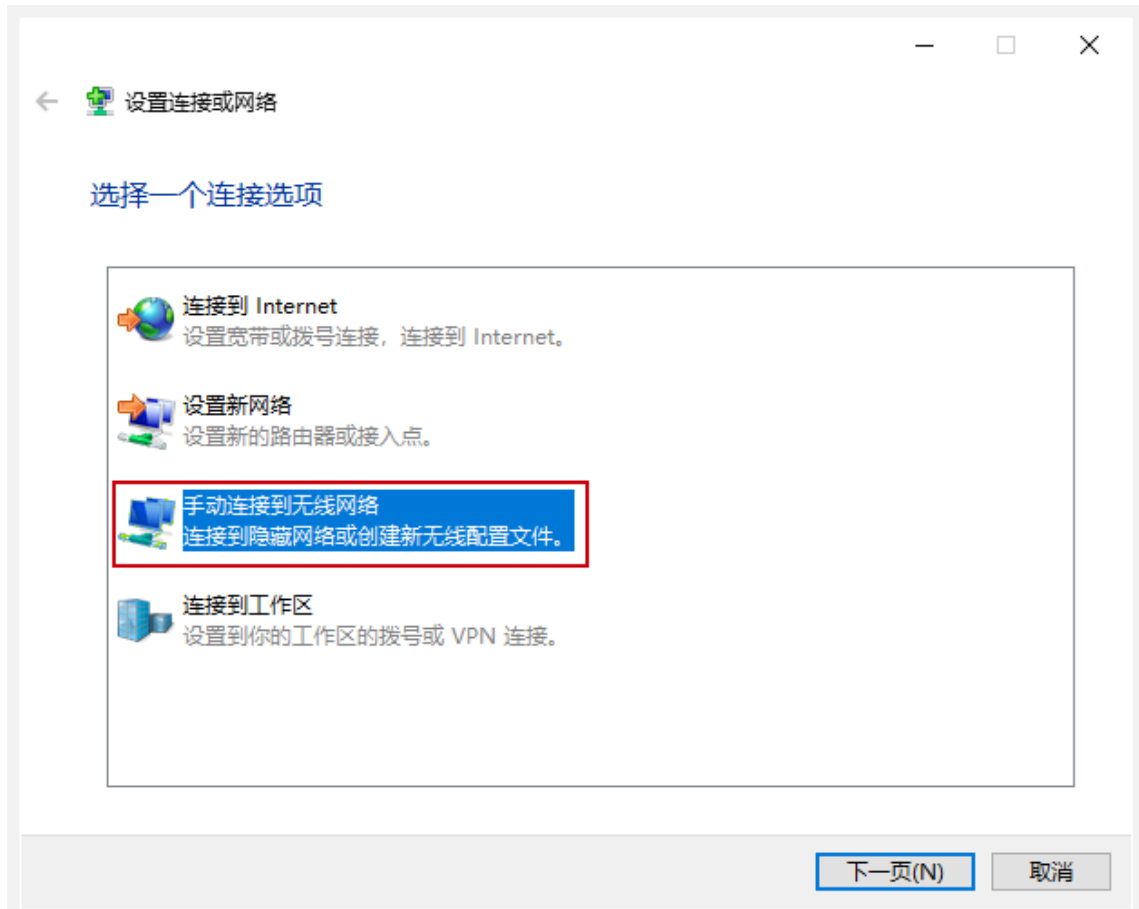
5.3.3 STA 通过 802.1X 方式接入无线网络

STA 接入无线网络时，需要提前设置 802.1X 参数，本实验仅介绍 Win10 的设置方法。

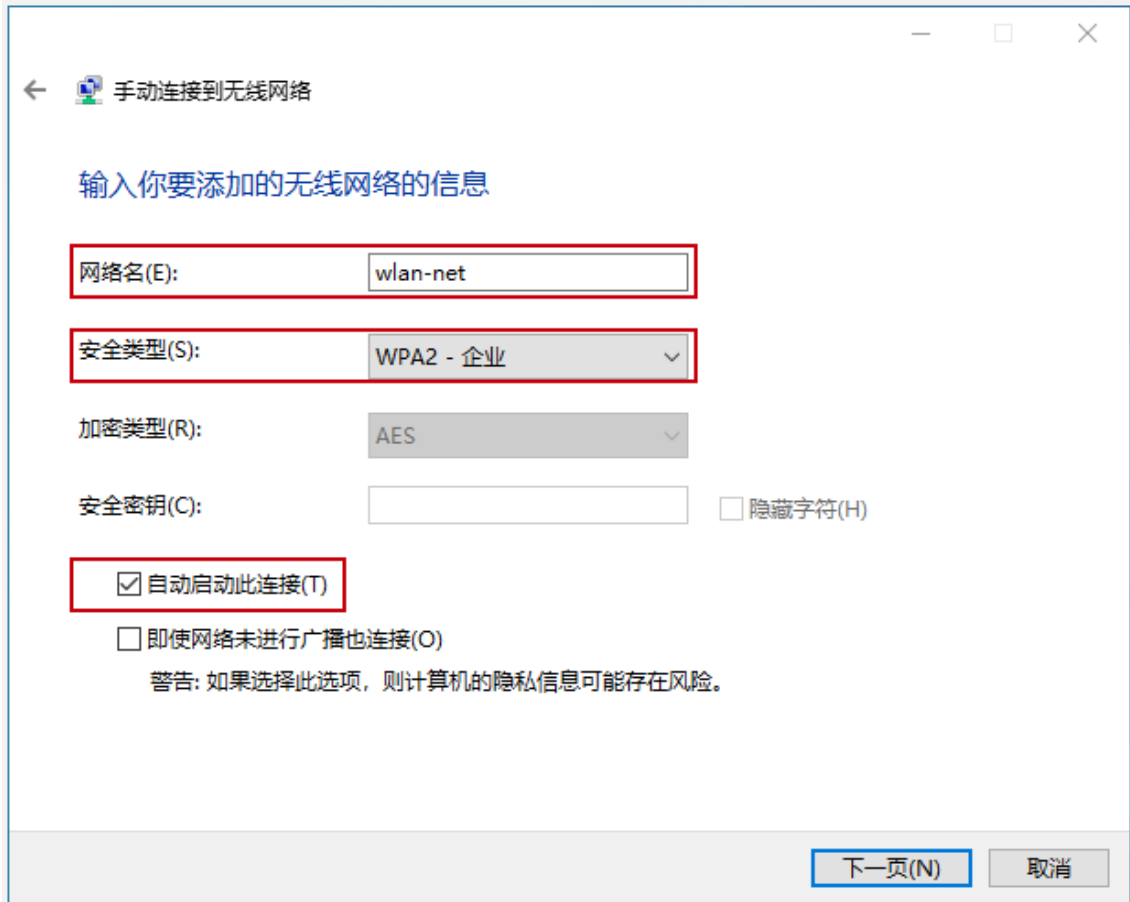
选择“控制面板 > 网络和 Internet > 网络和共享中心”（控制面板的“查看方式”选择“类别”时可显示“网络和 Internet”），单击“设置新的连接或网络”。



在弹出的对话框中选择“手动连接到无线网络”，然后点击“下一页”。



手动添加“网络名”，设置“安全类型”和“加密类型”，并选中“自动启动此连接”，单击“下一页”完成设置。



← 手动连接到无线网络

输入你要添加的无线网络的信息

网络名(E): wlan-net

安全类型(S): WPA2 - 企业

加密类型(R): AES

安全密钥(C): 隐藏字符(H)

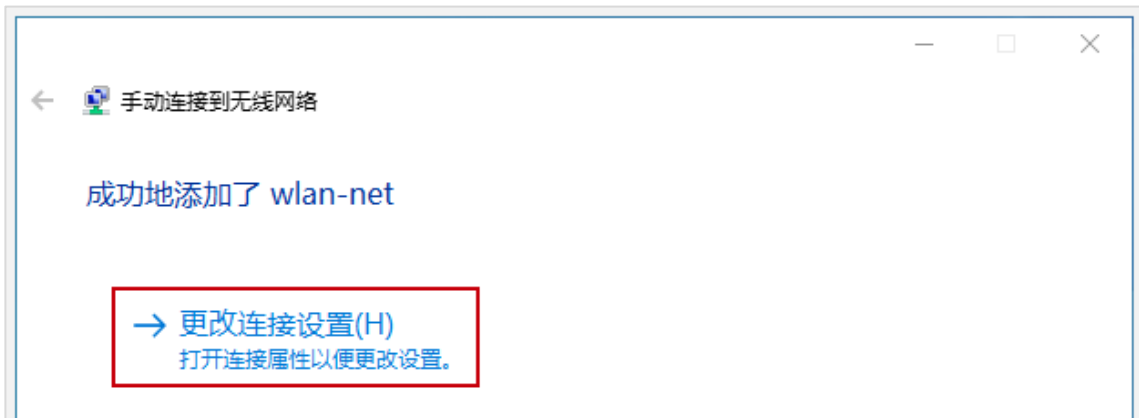
自动启动此连接(T)

即使网络未进行广播也连接(O)

警告: 如果选择此选项, 则计算机的隐私信息可能存在风险。

下一页(N) 取消

显示已成功添加了“wlan-net”无线网络，然后点击“更改连接设置”。

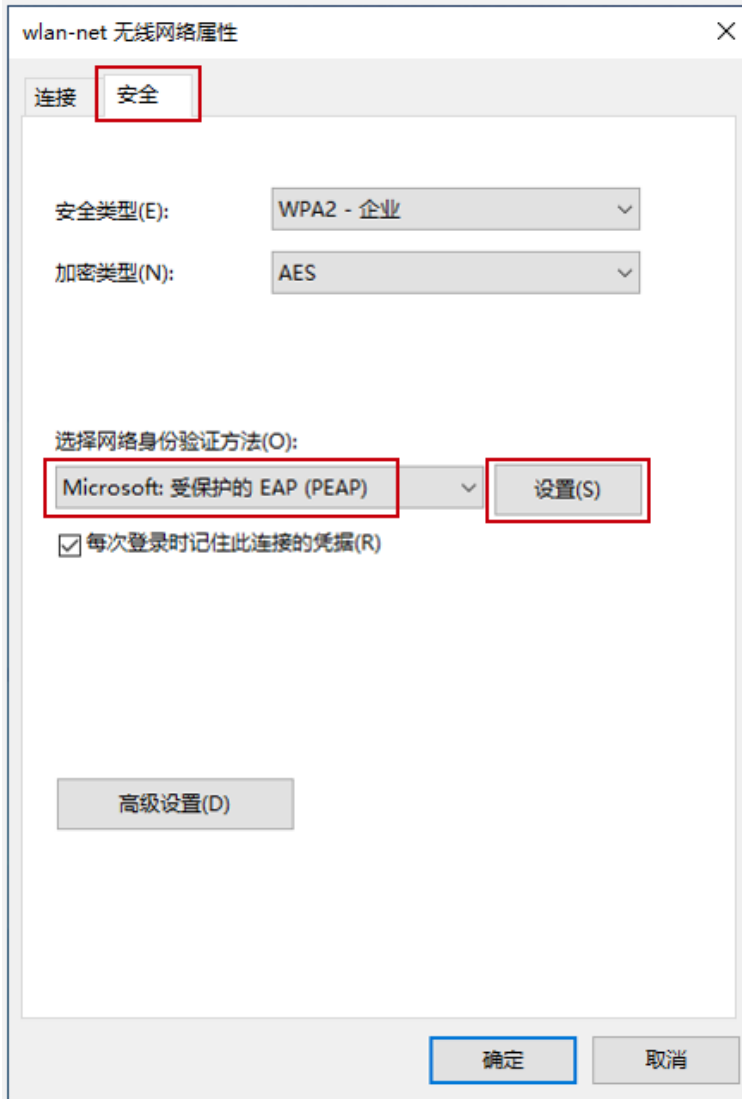


← 手动连接到无线网络

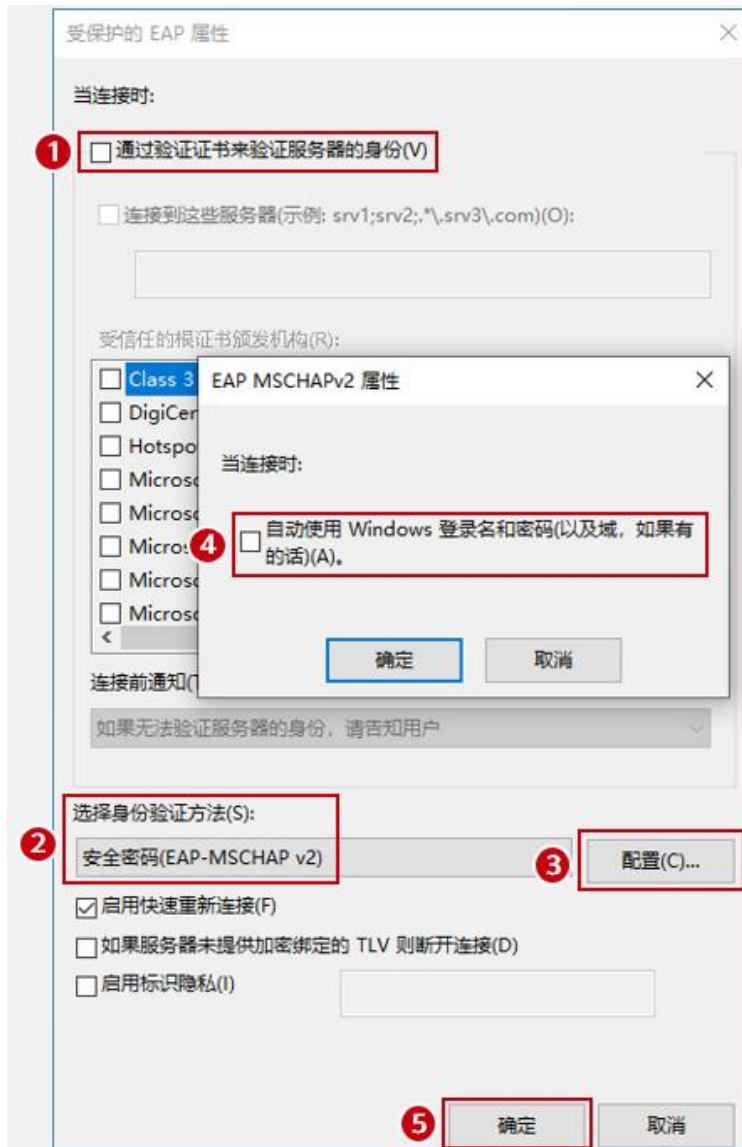
成功地添加了 wlan-net

→ 更改连接设置(H)
打开连接属性以便更改设置。

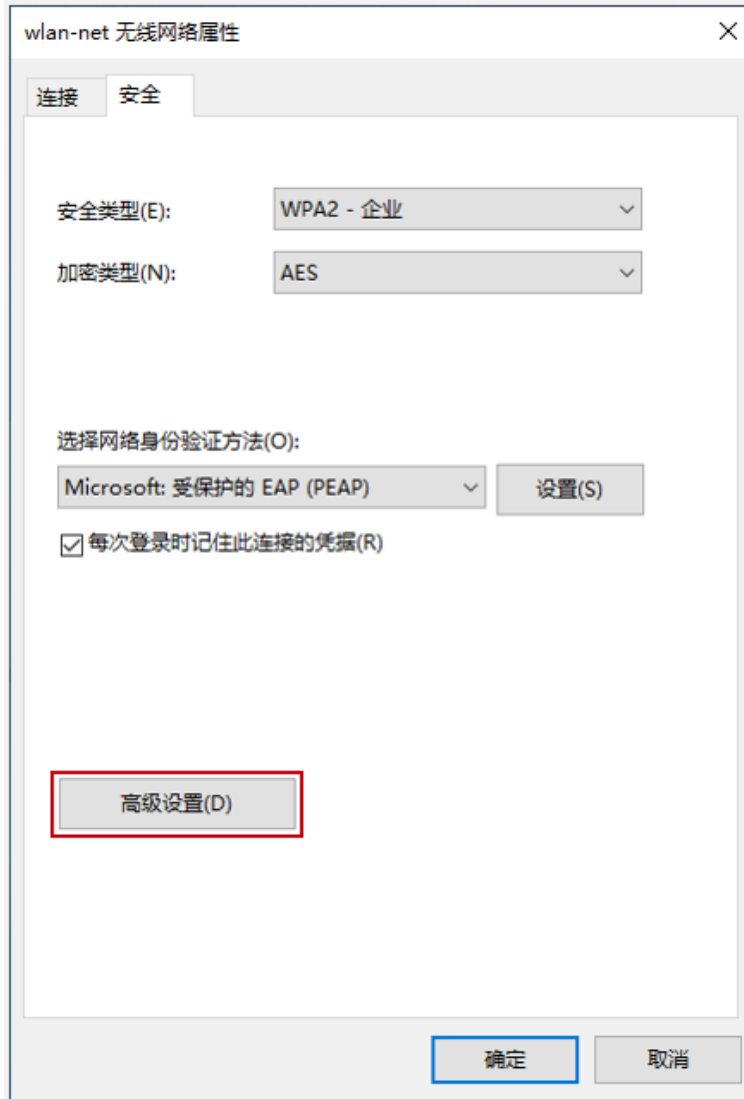
点击“安全”页签，“选择网络身份验证方法”设置为“Microsoft: 受保护的 EAP (PEAP)”，然后单击“设置”。



取消勾选“通过验证证书来验证服务器的身份”，“选择身份验证方法”选择“安全密码（EAP-MSCHAP v2）”，然后单击“配置”，在弹出的对话框中，取消勾选“自动使用Windows 登录名和密码”，最后点击“确定”。



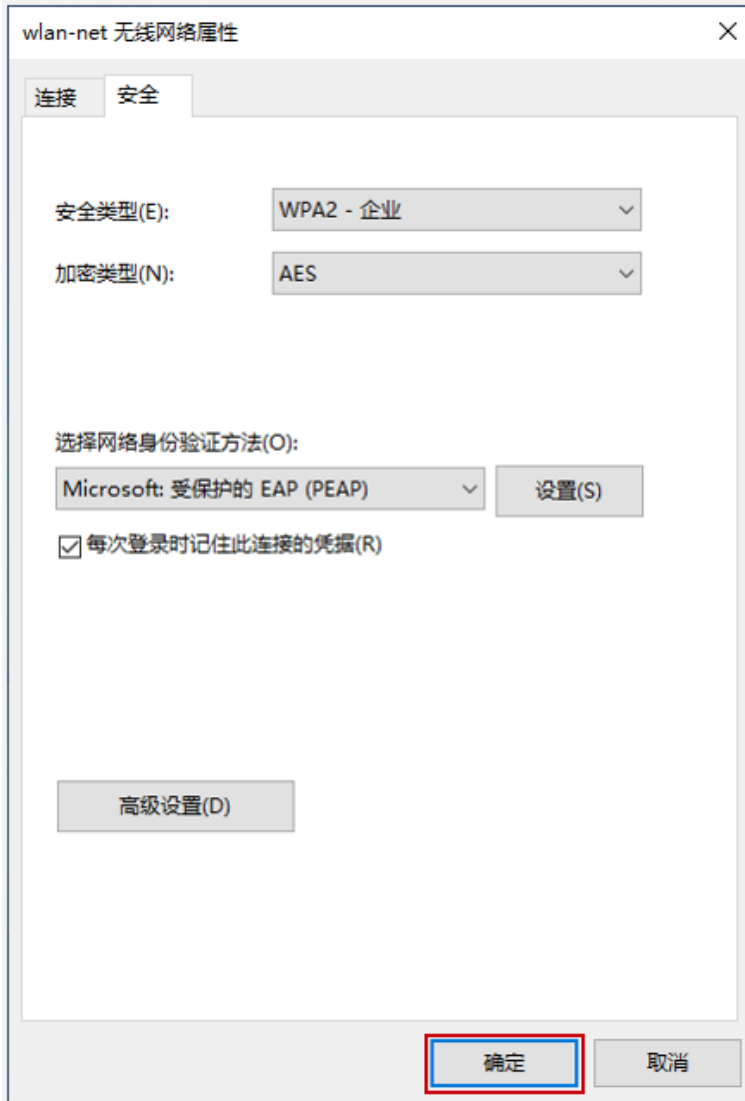
在“安全”页签，单击“高级设置”。



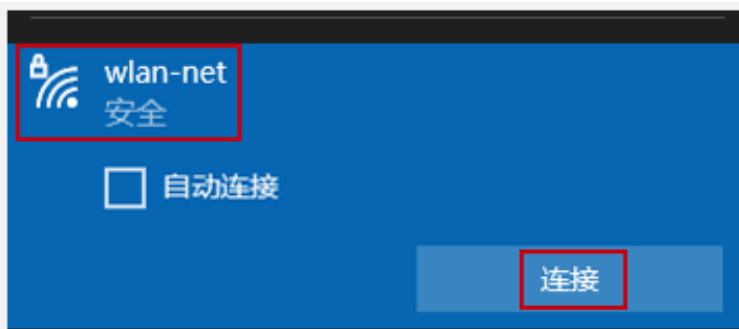
在弹出的对话框中点击“802.1X 设置”页签，设置“指定身份验证模式”为“用户身份验证”，单击“确定”。



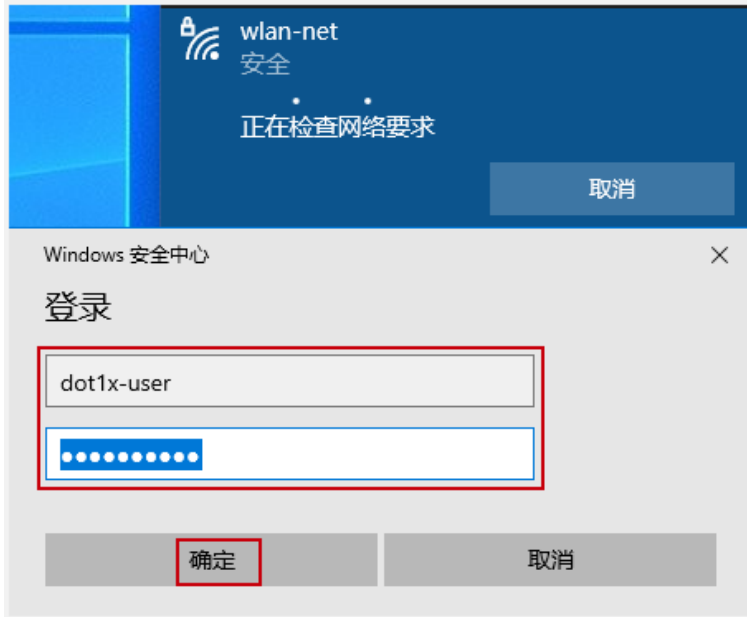
最后点击“确定”，完成 Windows 10 操作系统中的 802.1X 参数设置。



全部设置完成后，选择名称为“wlan-net”的 SSID，点击“连接”。



输入正确的用户名和密码（此处为 dot1x-user/Huawei@123）。



连接成功后，通过 ipconfig 命令查看无线网卡获取到的地址为 10.23.101.0/24 网段。并使用 ping 命令测试网络连通性，如下所示。

```

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::3ce1:b4f7:546e:45a1%12
    IPv4 地址 . . . . . : 10.23.101.196
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.23.101.254

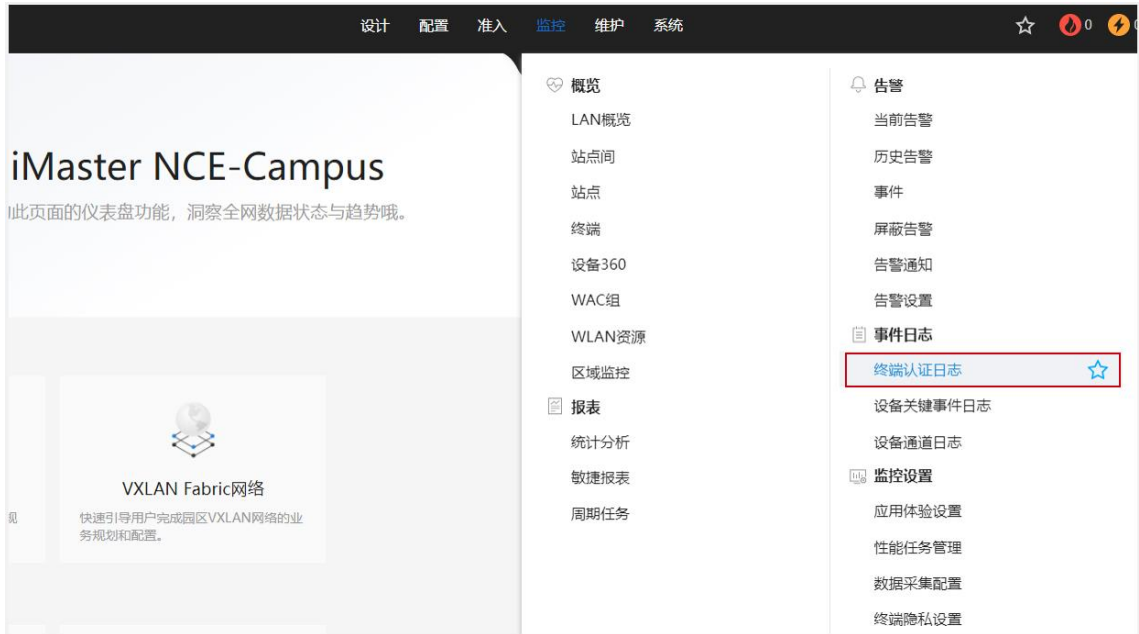
C:\Windows\system32>ping 10.23.101.254

正在 Ping 10.23.101.254 具有 32 字节的数据:
来自 10.23.101.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=12ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.23.101.254 的回复: 字节=32 时间=10ms TTL=254

10.23.101.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 6ms, 最长 = 12ms, 平均 = 9ms
    
```

5.3.4 查看 NCE 终端认证日志

在 NCE 上，选择“监控 > 事件日志 > 终端认证日志”，查看终端认证日志。



选择“RADIUS 上下线日志 > RADIUS 认证日志”，可以查看终端认证记录，其中使用的认证规则为“802.1X”，授权规则为“802.1X”，认证结果为“成功”。



5.3.5 在 WAC1 检查终端认证情况

在 WAC1 上查看 NAC 接入用户的详细信息，选择“监控 > 用户”，选择“上线用户统计”选项卡，在用户列表中可以查看当前接入用户的详细信息，如下所示。



5.4 配置参考

5.4.1 WAC1 配置

```
Software Version V200R021C00SPC100
#
defence engine enable
sysname WAC1
#
http timeout 10080
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif100
http server enable
#
vlan batch 100 to 101
#
authentication-profile name p1
dot1x-access-profile d1
authentication-scheme radius_huawei
accounting-scheme scheme1
radius-server radius_huawei
#
management-port isolate enable
management-plane isolate enable
#
radius-server template radius_huawei
radius-server shared-key cipher %^%#3:KT&'S!#Fg;Rz~2dA9R2hU/&4Z8L/T{VQ4Ry(sC%^%#
radius-server authentication 172.21.39.88 1812 source Vlanif 100 weight 80
radius-server accounting 172.21.39.88 1813 source Vlanif 100 weight 80
radius-attribute nas-ip 10.23.100.1
radius-server ip-address 172.21.39.88 shared-key cipher %^%#uz^0YJYF@Dub8K)ss9;/;2k=v87NT-
Wn(lBS6A0]Q%^%#
radius-server authorization 172.21.39.88 shared-key cipher %^%#</OAY!//D0%Mn>>GL,#SJt|>3-
nx>!g58f@09>jJ%^%# server-group radius_huawei
radius-server authorization server-source all-interface
#
aaa
authentication-scheme radius_huawei
authentication-mode radius
accounting-scheme scheme1
accounting-mode radius
accounting realtime 3
local-user admin password irreversible-cipher
$1a$Z#{";)Ik6$LUMXJS;VWR$p7mWZtx|EN3q#M`}27Bg+[8<)ELp.$
local-user admin privilege level 15
local-user admin service-type telnet ssh http
#
```

```
interface Vlanif1
 ip address dhcp-alloc unicast
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
#
interface MEth0/0/1
 ip address 172.21.39.4 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif100 10.23.100.254
ip route-static 172.21.39.88 255.255.255.255 Vlanif100 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%#
capwap dtls inter-controller psk %^%#tc.5LFZ\oJ^bM8*YYv#<te,1Oq8kAL.}J+v{puP%^%#
capwap message-integrity psk %^%#eJ&eRx$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x*%^%#
capwap sensitive-info psk %^%#;,L1<.L'e+li6MX,^QxH{6z#&#z[v4Oe"pCPrFJ'%^%#
capwap inter-controller sensitive-info psk %^%#ji6gT7>2y3dm)n~Bb"%8z$0]B62~|NkD,WJF[n2U%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
wlan
 calibrate enable manual
 temporary-management psk %^%#PwFE@vw_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
 ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)I%^%#
 traffic-profile name default
 security-profile name default
 security-profile name wlan-net
 security wpa2 dot1x aes
 ssid-profile name default
 ssid-profile name wlan-net
 ssid wlan-net
 vap-profile name default
 vap-profile name wlan-net
 forward-mode tunnel
 service-vlan vlan-id 101
 ssid-profile wlan-net
 security-profile wlan-net
 authentication-profile p1
 ap-group name default
 ap-group name ap-group1
 radio 0
 vap-profile wlan-net wlan 1
```

```
radio 1
  vap-profile wlan-net wlan 1
radio 2
  vap-profile wlan-net wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
  ap-name AP1
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
  ap-name AP2
  ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
  ap-name AP3
  ap-group ap-group1 provision-ap
#
dot1x-access-profile name d1
dot1x-access-profile name dot1x_access_profile
#
mac-access-profile name mac_access_profile
#
return
```

5.4.2 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101
#
dhcp enable
#
vlan 99
  name Manage
#
interface Vlanif1
#
interface Vlanif99
  ip address 172.21.39.253 255.255.128.0
#
interface Vlanif100
  ip address 10.23.100.254 255.255.255.0
  dhcp select interface
#
interface Vlanif101
  ip address 10.23.101.254 255.255.255.0
  dhcp select interface
#
interface MEth0/0/1
```

```
ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
port link-type access
port default vlan 99
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

5.4.3 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
```

```
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

5.5 思考题

在上述实验配置下，配置 802.1X 用户的认证方式为 EAP 方式。请思考，802.1X 用户的认证方式还可配置为哪些？

参考答案：

通过 **dot1x authentication-method** 命令配置 802.1X 用户的认证方式。802.1X 用户的认证方式可配置为：EAP、CHAP、PAP。

EAP：采用可扩展的认证协议 EAP（Extensible Authentication Protocol）中继认证方式。

CHAP：采用质询握手认证协议 CHAP（Challenge Handshake Authentication Protocol）的 EAP 终结认证方式。

PAP：采用密码认证协议 PAP（Password Authentication Protocol）的 EAP 终结认证方式。

6 Portal 认证实验

6.1 实验介绍

6.1.1 关于本实验

本实验通过配置 Portal 准入认证，使学员掌握 Portal 准入认证的组网和配置。

6.1.2 实验目的

- 描述 WLAN 的基本业务流程。
- 掌握 Portal 准入认证基本原理及相关配置。

6.1.3 实验组网介绍

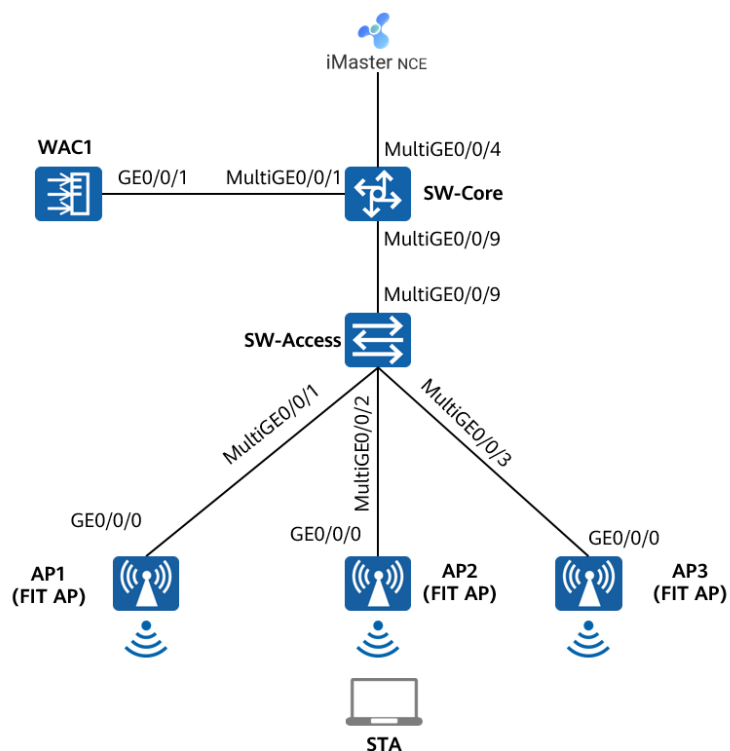


图6-1 Portal 认证实验拓扑图

6.1.4 实验规划

表6-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/4	Access	PVID: 99
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表6-2 IP 地址规划

设备	端口	IP地址
SW-Core	Vlanif100	10.23.100.254/24
	Vlanif101	10.23.101.254/24
	Vlanif99	172.21.39.253/17
WAC1	Vlanif100	10.23.100.1/24
iMaster NCE-Campus	/	172.21.39.88/17

表6-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	隧道转发
管理VLAN	100

业务VLAN	101
AP组	ap-group1
VAP模板	wlan-net
安全模板	wlan-net
安全策略	OPEN
SSID模板	wlan-net
SSID	wlan-net
RADIUS认证参数	RADIUS认证方案名称: radius_huawei RADIUS计费方案名称: scheme1 RADIUS服务器模板名称: radius_huawei, 其中: IP地址: 172.21.39.88 认证端口号: 1812 计费端口号: 1813 共享密钥: Huawei@123
Portal服务器模板	名称: abc IP地址: 172.21.39.88 URL地址: https:// 172.21.39.88:19008/portal WAC1向Portal服务器主动发送报文时使用的目的端口号: 50200 Portal认证共享密钥: Huawei@123
Portal接入模板	名称: portal1 绑定的模板: Portal服务器模板abc
免认证规则模板	名称: free1
认证模板	名称: p1 绑定的模板和认证方案: Portal接入模板portal1 RADIUS服务器模板radius_huawei RADIUS认证方案radius_huawei RADIUS计费方案scheme1 免认证规则模板free1

6.2 实验任务

6.2.1 配置思路配置

- 1.配置基础网络，确保网络互通。
- 2.配置 AP 上线。
- 3.配置 iMaster NCE-Campus 与 WAC1 网络互通。
- 4.在 WAC1 上配置 Portal 认证。
- 5.配置 WLAN 基本业务。
- 6.在 NCE 服务器上配置 Portal 认证。
- 7.验证 Portal 认证。

6.2.2 配置步骤

步骤 1 配置基础网络和 AP 上线

请参考 1.2.2 步骤 1~1.2.2 步骤 6，此处不再赘述。

步骤 2 配置 NCE 与 WAC1 之间网络互通

请参考 5.2.2 步骤 2，此处不再赘述。

步骤 3 配置 Portal 认证（WAC1）

配置 RADIUS 协议的相关参数，主要包括如下三部分内容：RADIUS 全局配置、RADIUS 服务器模板和授权服务器模板。

选择“配置 > 安全管理 > AAA”，选择“RADIUS 设置”选项卡，依次设置如下。

RADIUS 全局配置：配置“授权服务器源地址”为“所有 IP”，然后点击“应用”。

RADIUS 服务器模板：点击“新建”，新建 RADIUS 服务器模板，具体细节参见下文。

授权服务器模板：点击“新建”，新建授权服务器模板，具体细节参见下文。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

Portal服务器全局设置 **RADIUS设置** 内置EAP设置 LDAP设置 AD设置 HWTACACS设置

配置向导
AC配置
AP配置
安全管理
AAA
用户组
自定义应用
ACL
SSL
证书管理
安全防护
攻击防御
终端识别
PPSK管理

RADIUS全局配置
NAS IP地址: . . .
发送报文源IP地址: . . .
* 授权服务器源地址: 所有IP

RADIUS服务器模板
新建 删除 刷新

模板名称 default 模式 主备模式

5 共1条

授权服务器模板
新建 删除 刷新 清空

授权服务器IP地址

新建“RADIUS 服务器模板”的具体细节请参考如下配置。

新建RADIUS服务器模板

* 模板名称: radius_huawei

模式: 主备模式 负载均衡模式

NAS IP地址: 指定IP地址
10 , 23 , 100 , 1

* 模板默认共享密钥: Huawei@123

新建服务器 删除 IP地址

IP地址	共享密钥	认证端口号	计费端口号
172.21.39.88	*****	1812	1813

5 共1条

高级

确定 取消

新建服务器配置

* IP地址: IPv4 172 . 21 . 39 . 88

共享密钥: Huawei@123

服务器配置

认证

* 端口号: 1812

权重值: 80

发送报文源IP地址: LoopBack VLANIF IP地址

Vlanif100 ... X

Virtual-ip: OFF

计费

* 端口号: 1813

权重值: 80

发送报文源IP地址: LoopBack VLANIF IP地址

Vlanif100 ... X

Virtual-ip: OFF

新建“授权服务器模板”的具体细节请参考如下配置。

新建授权服务器

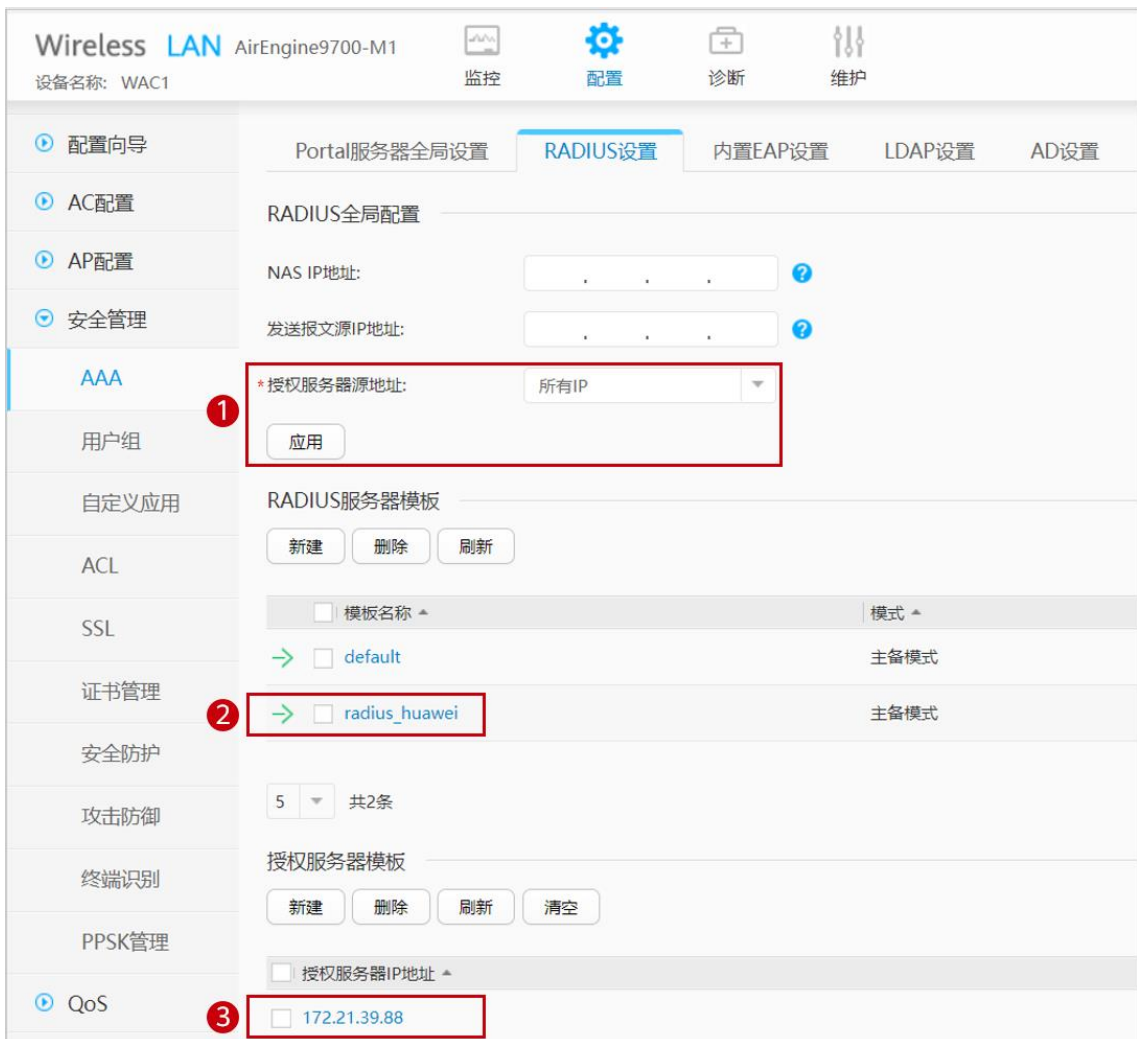
* 授权服务器IP地址: 172 . 21 . 39 . 88

模板名称: radius_huawei

* 密钥: Huawei@123



建议在“RADIUS 设置”全部配置完成后,进行全面检查,如下所示。



配置 AAA 认证方案模板。

选择“配置 > AP 配置 > 模板管理 > AAA > 认证方案模板”, 点击“新建”, 配置模板名称为“radius_huawei”, 然后点击“确定”。



选择“radius_huawei”认证方案模板，配置第一认证模式为“RADIUS 认证”，点击“应用”。



配置 AAA 计费方案模板。

选择“配置 > AP 配置 > 模板管理 > AAA > 计费方案模板”，点击“新建”，配置模板名称为“scheme1”，然后点击“确定”。



选择“scheme1”计费方案模板，配置计费模式为“RADIUS 计费”，计费形式为“实时计费”，实时计费时间间隔为 3 分钟，然后点击“应用”。



计费方案模板:

计费模式:

计费形式: 按时长计费 实时计费

*实时计费时间间隔(分钟): 实时计费请求无响应最大次数:

实时计费失败后策略: 拒绝用户上线 允许用户上线

开始计费后失败策略: 拒绝用户上线 允许用户上线

配置 Portal 服务器模板。

选择“配置 > 安全管理 > AAA”，选择“Portal 服务器全局设置”选项卡，配置如下参数。

注意：WAC1 设备端侦听 Portal 协议报文的端口号为 2000。



The screenshot shows the configuration page for Portal servers on a Huawei AirEngine9700-M1 device. The interface includes a sidebar with navigation options like '配置向导', 'AC配置', 'AP配置', '安全管理', 'AAA', '用户组', '自定义应用', 'ACL', 'SSL', '证书管理', '安全防护', '攻击防御', '终端识别', 'PPSK管理', 'QoS', '扩展业务', and '可靠性配置'. The main content area is titled 'Portal服务器全局设置' and contains several sections:

- Portal服务器全局设置:** Includes tabs for '内置Portal全局设置' (highlighted with a red box and '1') and '外置Portal全局设置'.
- 外置Portal对接协议:** A section for configuring external protocols, with a red box and '2' highlighting the '华为Portal协议' configuration. It includes:
 - Portal协议版本: V1 & V2, V2
 - 设备侦听Portal协议报文的端口号: 2000
 - 本机网关地址: 所有地址
 - AC间漫游错误码回复: ON
- HTTP协议:** A section for configuring HTTP protocols, including:
 - HTTP对接方式: 基于HTTPS的Portal对接, 基于HTTP的Portal对接
 - * SSL策略: [Empty field] [...]
 - 设备侦听HTTP协议报文的端口号: 8443
 - 本机网关地址: 所有地址, 指定地址, 无
 - Portal认证请求的目的IP地址: [Empty field] [...]
- Portal认证服务器列表:** A table for listing authentication servers, with a red box and '3' highlighting the '应用' (Apply) button. Below the table are buttons for '新建' (highlighted with a red box and '4'), '删除', and '刷新'.

新建 Portal 认证服务器的配置细节如下所示，配置完成后，点击“确认”。

注意：NCE 作为 Portal 服务器时，默认监听 50200 端口。所以新建 Portal 认证服务器的报文端口号需要配置为 50200。

安全管理 > AAA > 外置Portal全局设置 > 新建认证服务器

* 服务器名称: abc

* 服务器IP地址: IPv4
服务器IP地址: 172.21.39.88

协议类型: Portal HTTP HACA

* 共享密码: Huawei@123

报文端口号: 50200 发送报文源IP地址: 10.23.100.1

本机网关地址: . . .

URL: https://172.21.39.88:19008/f

URL配置结果: https://172.21.39.88:19008/portal

URL: https://172.21.39.88:19008/f

URL配置结果: https://172.21.39.88:19008/portal?ac-ip=&redirect-url=redirect-url&usermac=user-mac&userip=user-ipaddress&ssid=ssid

URL选项配置

重定向配置

AC-IP关键字/AC-IP: ac-ip / . . .

AC-MAC关键字/AC-MAC: / - -

系统名称关键字/系统名称: /

AP-IP关键字: /

AP-MAC关键字: /

用户访问URL关键字: redirect-url

用户IP地址关键字: userip

AP名称关键字: /

AP组名称关键字: /

登录URL关键字/登录URL: /

用户MAC关键字: usermac

SSID关键字: ssid

AP位置关键字: /

MAC地址选项

MAC地址格式: 无分隔符

URL加密

参数加密后名称: /

加密密码: /

加密向量名称: /

服务器探测配置

确定 取消

配置 Portal 模板。

选择“配置 > AP 配置 > 模板管理 > AAA > Portal 模板”，点击“新建”，配置模板名称为“portal1”，然后点击“确定”。

选择名称为“portal1”的 Portal 模板，配置 Portal 认证方式为“外置 Portal 服务器”，对接使用协议为“Portal 协议”，主 Portal 服务器组为“abc”，然后点击“应用”。

配置免认证规则模板。

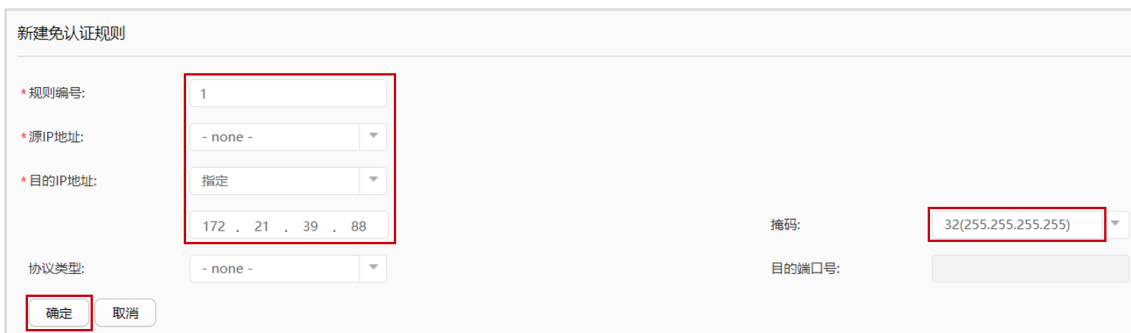
选择“配置 > AP 配置 > 模板管理 > AAA > 免认证规则模板”，点击“新建”，配置模板名称为“free1”，然后点击“确定”。



选择名称为“free1”的免认证规则模板，配置控制方式为“免认证规则”，然后点击“新建”，新建免认证规则，最后点击“应用”使配置生效。

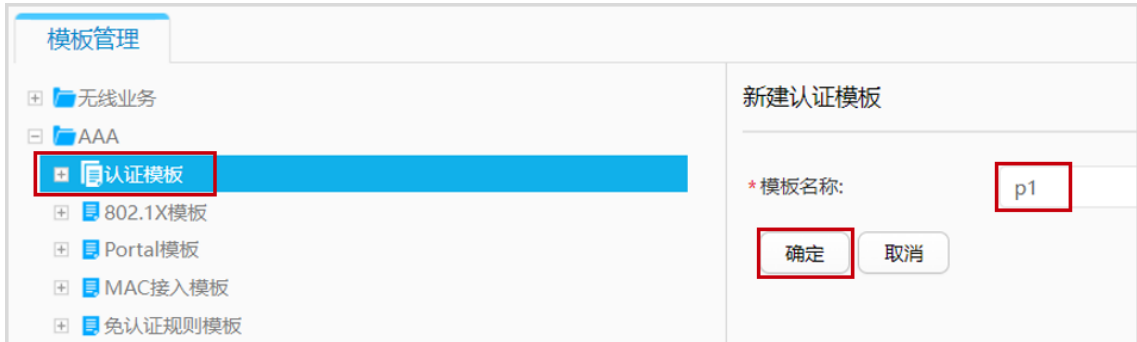


新建免认证规则的配置细节如下所示。免认证规则模板通常用于放行最基本的网络访问权限，例如访问 DNS 服务器、下载补丁、更新病毒库等。此处仅放行 NCE 服务器地址。



配置认证模板。

选择“配置 > AP 配置 > 模板管理 > AAA > 认证模板”，点击“新建”，配置模板名称为“p1”，然后点击“确定”。



选择名称为“p1”的认证模板，在其中引用 Portal 模板“portal1”、免认证规则模板“free1”、RADIUS 服务器模板“radius_huawei”、认证方案“radius_huawei”、计费方案“scheme1”，如下所示。



模板管理

- 无线业务
- AAA
 - 认证模板
 - p1
 - 802.1X模板
 - Portal模板
 - MAC接入模板
 - 1 免认证规则模板**
 - RADIUS模板
 - 二级计费RADIUS模板
 - HACA模板
 - LDAP模板
 - AD模板
 - HWTACACS模板
 - 认证方案模板
 - 授权方案模板
 - 计费方案模板
 - 业务方案模板
 - 内置EAP服务器配置
 - 本地用户配置

免认证规则模板: **2** free1

模板介绍信息: 用户认证成功之前,为满足用户基本的

控制方式: 免认证规则 ACL

免认证规则列表

新建 删除 刷新

规则编号 ▲ 源IP地址/掩码

1

10 ▼ 共1条

3 应用

模板管理

- 无线业务
- AAA
 - 认证模板
 - p1
 - 802.1X模板
 - Portal模板
 - MAC接入模板
 - 免认证规则模板
 - 1 RADIUS模板**
 - 二级计费RADIUS模板

RADIUS模板: **2** radius_huawei

服务器工作模式 ▲

主备模式

主备模式

3 应用 **i** 点击应用后,将使用页面配置覆盖指定模板



步骤 4 配置无线业务

创建名为“wlan-net”的安全模板，并配置安全策略。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > 安全模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



选择“wlan-net”安全模板，配置安全策略为“OPEN”，点击“应用”。



创建名为“wlan-net”的 SSID 模板，并配置 SSID 名称为“wlan-net”。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > SSID 模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



选择“wlan-net”SSID 模板，配置 SSID 名称为“wlan-net”，点击“应用”。



SSID模板: wlan-net 展示模板引用关系

模板介绍信息: SSID用来指定不同的无线网络。在STA上搜索可接入的无线网络时,显示出来的网络名称就是SSID。

基础配置 高级配置

* SSID名称: wlan-net

最大用户数: 64

应用

创建名为“wlan-net”的 VAP 模板，配置业务数据转发模式、业务 VLAN，并且引用 SSID 模板、安全模板和认证模板。

选择“配置 > AP 配置 > 模板管理 > 无线业务 > VAP 模板”，点击“新建”，配置模板名称为“wlan-net”，然后点击“确定”。



模板管理

无线业务

VAP模板

default

SSID模板

安全模板

流量模板

新建VAP模板

* 模板名称: wlan-net

确定 取消

选择“wlan-net” VAP 模板，配置转发模式为隧道转发，业务 VLAN 为 VLAN 101，点击“应用”。



VAP模板: wlan-net 展示模板引用关系

模板介绍信息: 在VAP模板下配置各项参数,然后在AP组或AP中引用VAP模板,AP上就会生成VAP,VAP用来为STA提供无线接入服务。通过配置VAP模板下的参数,使AP实现为STA

基础配置 高级配置

使能状态: ON

转发模式: 隧道转发

指定报文直接转发: IPv4 ?

业务VLAN: 单个VLAN VLAN Pool 业务VLAN ID: 101

应用

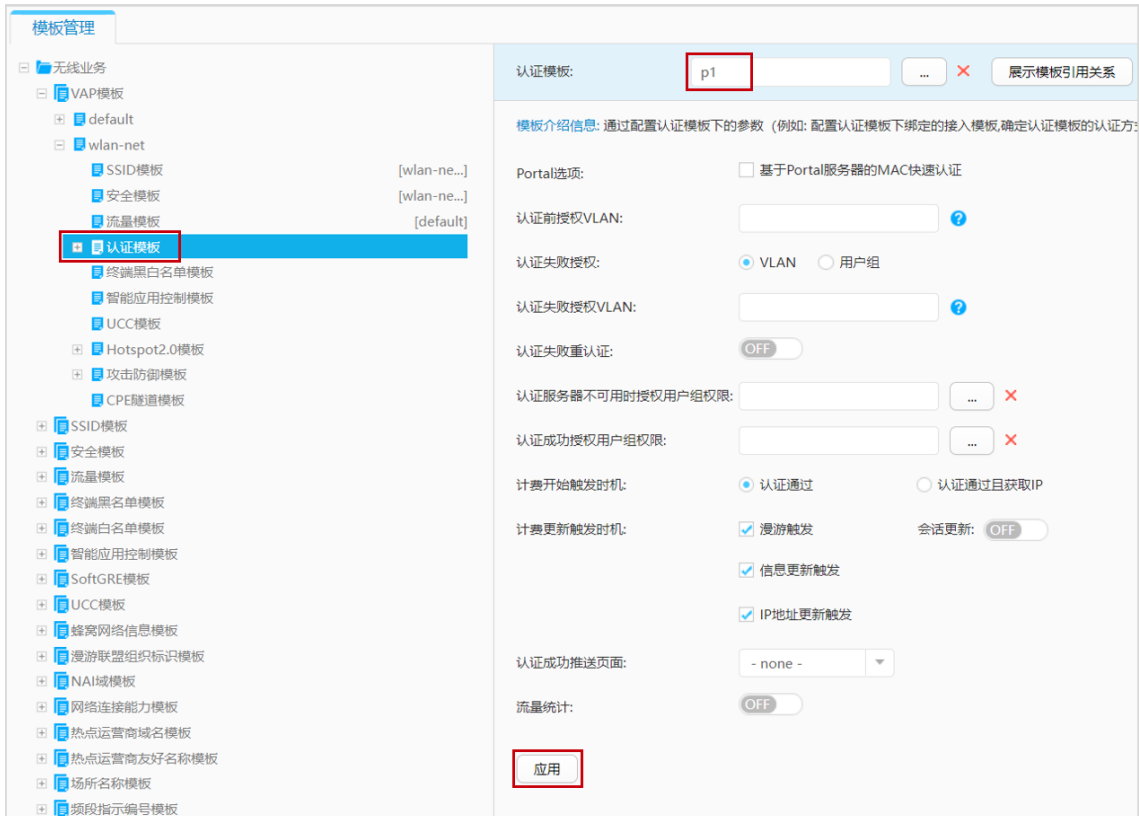
配置“wlan-net” VAP 模板所关联的 SSID 模板为“wlan-net”，点击“应用”。



配置“wlan-net”VAP模板所关联的安全模板为“wlan-net”，点击“应用”。



配置“wlan-net”VAP模板所关联的认证模板为“p1”，点击“应用”。



配置 AP 组引用 VAP 模板。

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组的配置界面。

在 AP 组配置界面中，选择“VAP 配置”，在“VAP 模板列表”中，点击“添加”。

配置 VAP 模板名称为“wlan-net”，WLAN ID 为 1，射频为 0 和 1，点击“确定”。

最后查看“VAP 模板列表”如下。

VAP 模板列表

相关配置

新建 添加 移除 展示模板引用关系

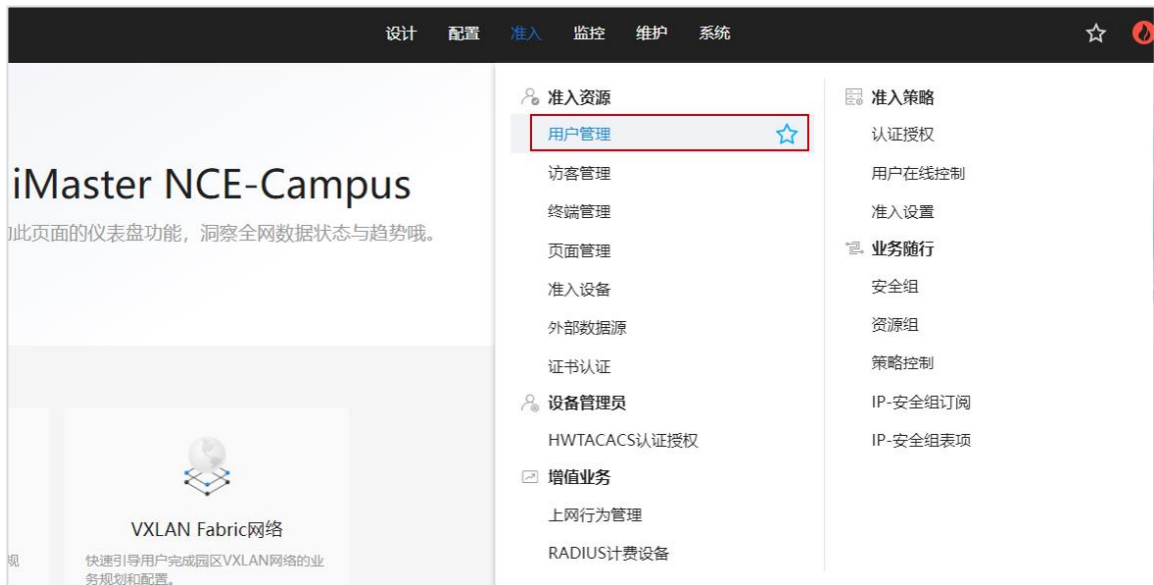
模板名称	SSID模板	认证模板	安全模板	WLAN ID	射频	转发模式	业务VLAN	使能状态
wlan-net	wlan-net	p1	wlan-net	1	0	隧道转发	101	● 开启
wlan-net	wlan-net	p1	wlan-net	1	1	隧道转发	101	● 开启

10 共2条

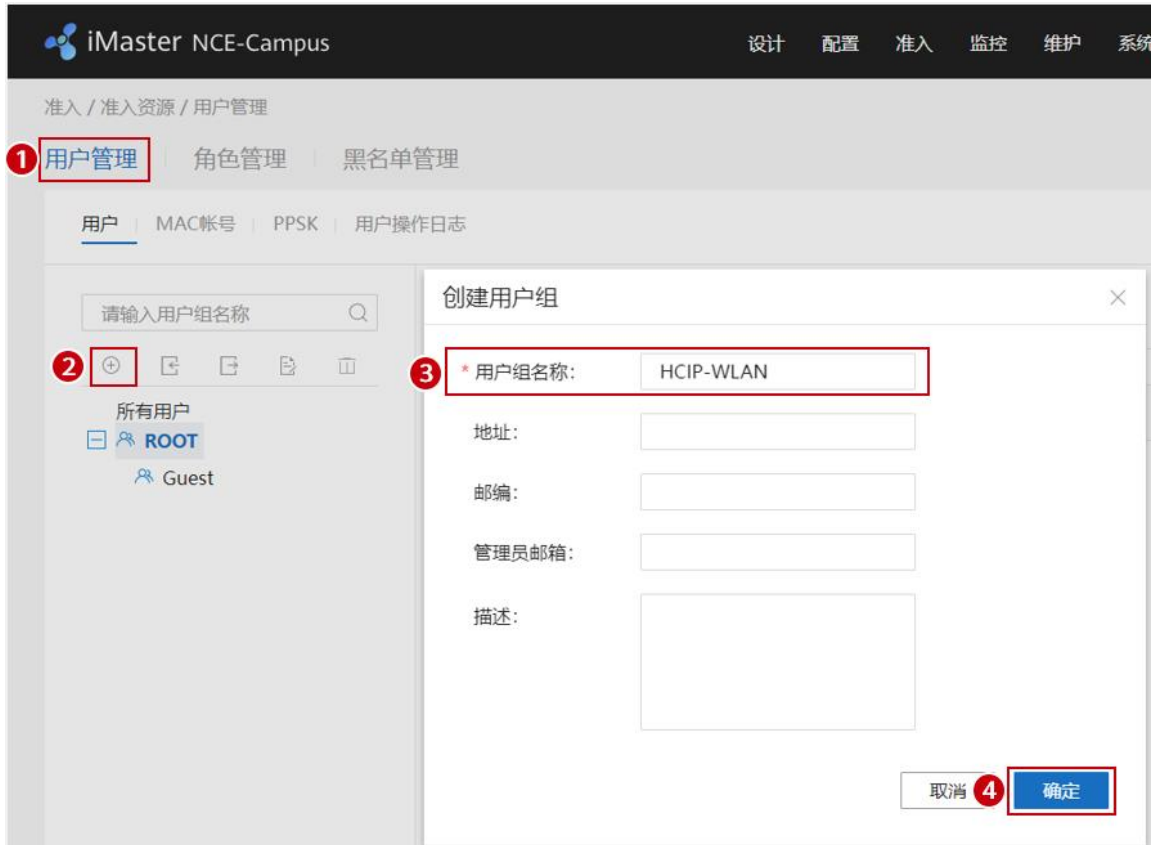
步骤 5 配置 Portal 认证（NCE）

在 NCE 上创建 Portal 认证所用的用户名和密码。

在主菜单中选择“准入 > 准入资源 > 用户管理”。



选择“用户管理 > 用户”，点击“+”按钮，新建用户组“HCIP-WLAN”。

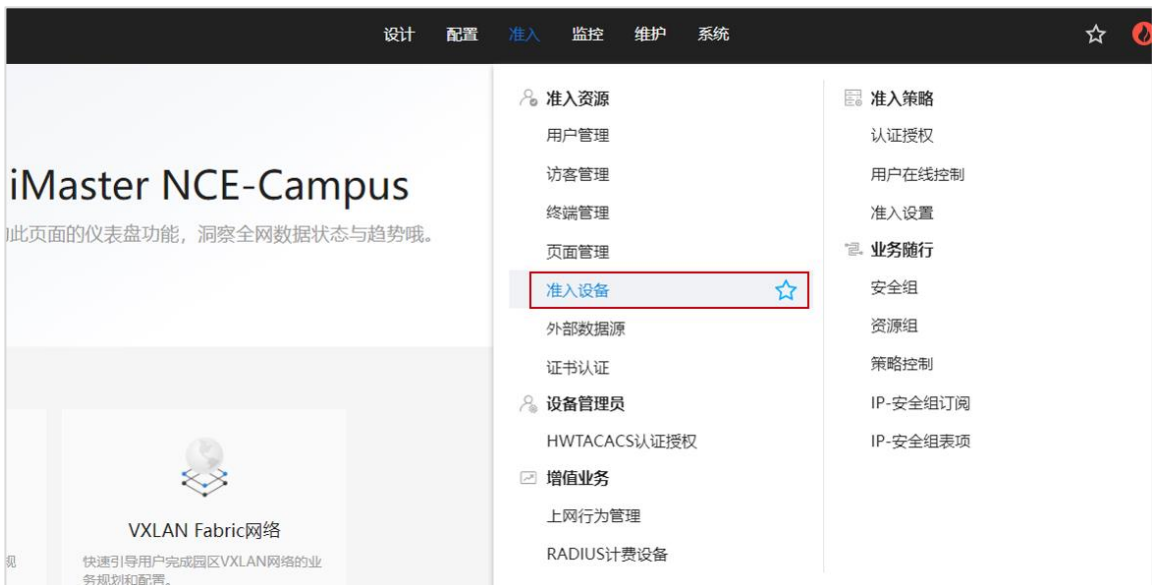


选中“HCIP-WLAN”用户组，单击“创建”，新增用于 Portal 认证的用户名“portal-user”，密码设置为“Huawei@123”，允许登录方式勾选“Portal”和“802.1X & Portal 2.0”，最后点击“确定”。

iMaster NCE-Campus 设计 配置 准入 监控 维护 系统
 准入 / 准入资源 / 用户管理
 用户管理 | 角色管理 | 黑名单管理
 用户 | MAC帐号 | PPSK | 用户操作日志
基本信息 ▾
 * 用户名: portal-user
 * 密码:
 * 确认密码:
 角色:
 最大接入终端数: 支持除HWTACACS认证之外的所有认证方式。
 过期时间:
 下次登录修改密码: 仅对控制器内置Portal认证和自助服务页面登录生效。
 * 允许登录方式: Portal 802.1X & Portal 2.0 HWTACACS
 进行Portal2.0认证需要同时勾选Portal及802.1X & Portal 2.0。进行HACA认证需要勾选Portal。
 仅允许使用移动证书认证: 即EAP-TLS协议的802.1X认证，Boarding场景请勿勾选该选项。
 其他信息 ^
 接入绑定信息 ^
 RADIUS属性 ⓘ ^

在 NCE 上添加准入设备（WAC1）。

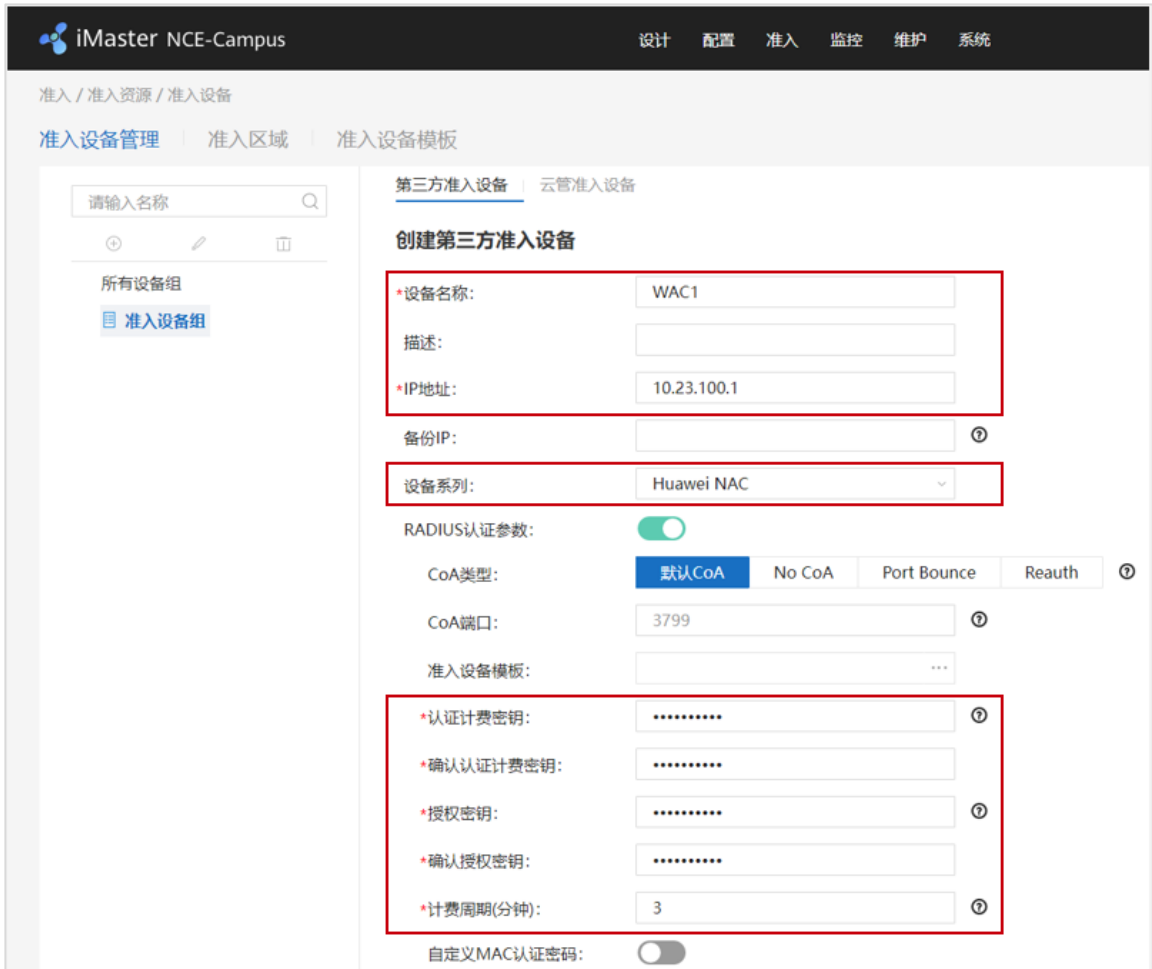
选择“准入 > 准入资源 > 准入设备”，配置准入设备。



选择“第三方准入设备”，点击“创建”，创建第三方准入设备。



按照如下参数进行配置，其中“认证计费密钥”与“授权密钥”均为 Huawei@123，计费周期设置为 3 分钟，与 WAC1 中配置的参数保持一致。



配置 Portal 认证参数。Portal 协议选择“Huawei Portal(Portal2.0)”，Portal 密钥为“Huawei@123”（与 WAC1 上配置的 shared-key 保持一致），Portal 认证端口保持默认值 2000，最后点击“确认”。此处的 Portal 认证端口为 WAC1 默认监听端口，用于监听 Portal 报文。

Portal认证参数:

Portal协议: Huawei Portal(Portal2.0)

Portal在线用户同步:

Portal心跳检验:

*Portal密钥:

*确认Portal密钥:

URL密钥:

确认URL密钥:

终端IP地址列表:

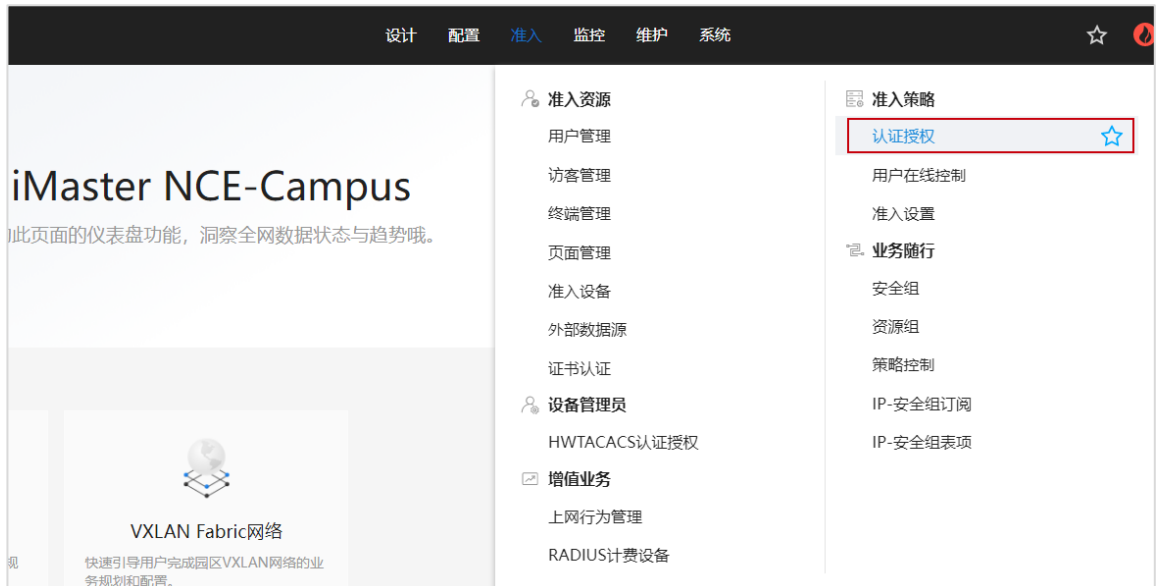
*Portal认证端口: 2000

Service-Type属性值设置:

HWTACACS认证参数:

在 NCE 上创建认证授权、授权规则、授权结果。

选择“准入 > 准入策略 > 认证授权”。



选择“认证规则”，点击“创建”，按如下参数配置认证规则。

iMaster NCE-Campus 设计 配置 准入 监控 维护 系统

准入 / 准入策略 / 认证授权

认证规则 | 授权结果 | 授权规则 | 策略元素

创建认证规则

基本信息

*名称: Portal

描述:

认证方式: 用户接入认证 | MAC认证 | 设备管理认证

启用Portal-HACA协议:

接入方式: WIFI | 有线 | 蜂窝网络

用户信息

用户组信息匹配:

用户组: ROOT\HCIP-WLAN

帐号信息匹配:

角色信息匹配:

位置信息

站点信息匹配:

使能准入设备组匹配:

接入设备类型: ---请选择---

设备信息匹配:

SSID匹配:

SSID: 增加

wlan-net

终端信息匹配:

终端IP范围: 通过换行符分隔IP地址, 请输入IP地址/掩码(如192.168.1.1/32或2001:0DB8:0:0:0:0:1428:57AB/64)或IP地址段(如192.168.1.1-

认证信息

RADIUS中继:

接入参数:

*数据源:

<input type="checkbox"/>	优先级	名称
<input type="checkbox"/>	1	本地数据源

共1条

双因子认证:

优先识别协议:

*认证协议:

- 全选
- PAP协议(本地帐号、AD、LDAP、RADIUS Token、第三方HTTP服务器)
- CHAP协议(本地帐号)
- EAP-MD5协议(本地帐号)
- EAP-PEAP-MSCHAPv2协议(本地帐号、AD、LDAP)
- EAP-TLS协议(本地帐号、AD、LDAP)
- EAP-PEAP-GTC协议(本地帐号、AD、LDAP、RADIUS Token)
- EAP-TTLS-PAP协议(本地帐号、AD、LDAP)
- EAP-PEAP-TLS协议(本地帐号、AD、LDAP)

PAP协议, CHAP协议和EAP-MD5协议为不安全协议, 请谨慎选择。

高级选项

帐号不存在:

身份认证失败:

选择“授权规则”，点击“创建”，按如下参数配置授权规则。

iMaster NCE-Campus 设计 配置 准入 监控 维护 系统

准入 / 准入策略 / 认证授权

认证规则 | 授权结果 | 授权规则 | 策略元素

创建授权规则

基本信息

*名称: Portal

描述:

认证方式: 用户接入认证 | MAC认证 | 设备管理认证

启用Portal-HACA协议:

接入方式: WIFI | 有线 | 蜂窝网络

用户信息

用户组信息匹配:

*用户组: ROOT\HCIP-WLAN

外部组信息匹配:

帐号信息匹配:

角色信息匹配:

位置信息

站点信息匹配:

准入设备组匹配:

接入设备类型: ---请选择---

设备信息匹配:

SSID匹配:

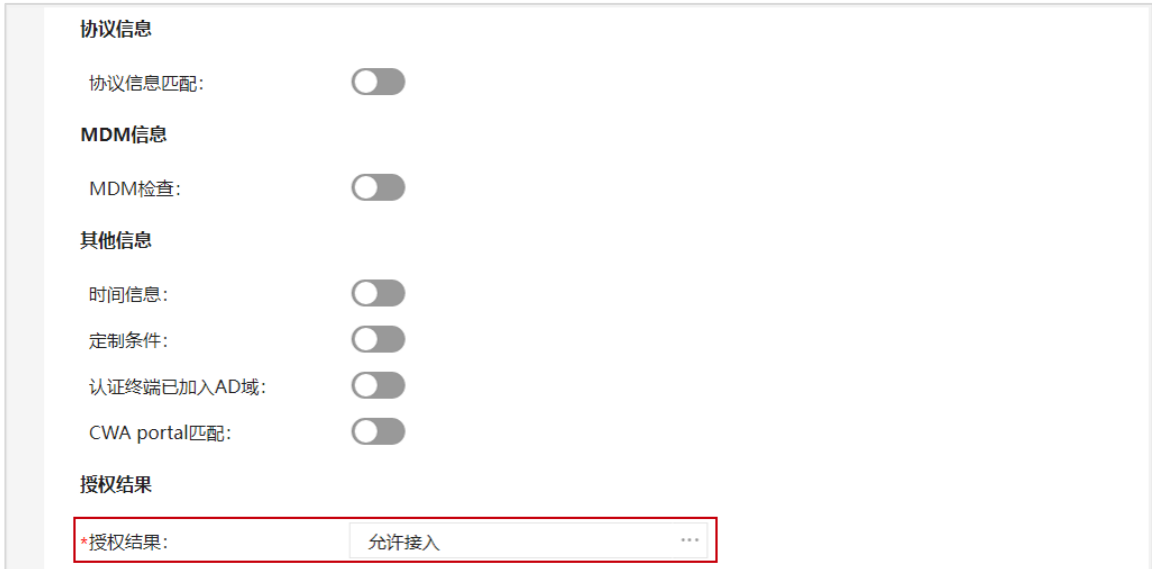
SSID: 增加

wlan-net

终端信息匹配:

终端IP范围: 通过换行符分隔IP地址, 请输入IP地址/掩码(如192.168.1.1/32或2001:0DB8:0:0:0:1428:57AB/64)或IP地址段(如192.168.1.1-

区域匹配:



在 NCE 上配置 Portal 页面推送策略（若无特殊需求可选择默认页面）。

选择“准入 > 准入资源 > 页面管理”，对 Portal 页面进行管理。



选择“Portal 页面推送策略”，点击“创建”，新建推送策略“Portal”，按照如下参数进行配置，最后点击“确定”。



The screenshot shows the configuration interface for the Portal Page Push Strategy in iMaster NCE-Campus. The page is titled "Portal 页面推送策略" and includes several sections:

- 名称 (Name):** Portal
- 描述 (Description):** (Empty text area)
- 接入方式 (Access Method):** 有线 (Wired) and 无线 (Wireless) buttons, with "无线" selected.
- 推送规则 (Push Rules):**
 - 站点信息匹配 (Site Information Matching): Disabled
 - 接入设备类型 (Access Device Type): 请选择... (Please select...)
 - SSID 匹配 (SSID Matching): Enabled
 - SSID (SSID): 增加 (Add) button, with "wlan-net" listed below.
 - 准入设备组 (Access Device Group): Disabled
 - 操作系统匹配 (OS Matching): Enabled
 - Windows PC, IOS, Android, Linux/Unix, Windows Phone, MAC OS, Other (all checked)
- 推送页面规则 (Push Page Rules):**
 - 认证方式 (Authentication Method): 用户名密码认证 (Username and Password Authentication)
 - 推送页面 (Push Page): 请输入推送页面名称 (Please enter the push page name). A preview of the login page is shown below, titled "默认用户名密码认证..." (Default Username and Password Authentication...).
 - 首推页面 (Default Page): 认证页面 (Authentication Page) selected, with options for 注册页面 (Registration Page) and 用户须知页面 (User Notice Page).
 - 认证成功后跳转 (Redirect after successful authentication): 不跳转 (Do not redirect)

查看 Portal 页面推送策略，如下所示。

请输入关键字

优先级	名称	认证方式	页面名称
1	Portal	用户名密码认证	默认用户名密码认证定制页面
N	Default	匿名认证	默认匿名认证定制页面

共2条

6.3 结果验证

6.3.1 检查 AP 上线状态

选择“监控 > AP”，选择“AP 统计”选项卡，可以查看 AP 的状态信息，其中“normal”代表 AP 已正常上线。

AP列表

智能诊断 上线失败记录 下线记录 SoftGRE隧道状态 导出信息 IoT插卡信息

AP ID	AP名称	AP组	状态名称
0	AP1	ap-group1	normal
1	AP2	ap-group1	normal
2	AP3	ap-group1	normal

10 共3条

总AP数：3 normal：3
AirEngine5761-11：3

6.3.2 检查 VAP 信息

选择“监控 > SSID”，选择“VAP”选项卡，可以查看 VAP 关联的 AP 名称、SSID 名称、BSSID 名称、认证方式、状态等信息。

SSID: VAP

自动刷新: OFF

AP型VAP列表

应用统计清零

AP ID ▲	AP名称 ▲	射频ID ▲	WLAN ID ▲	SSID ▲	BSSID ▲	认证方式 ▲	接入用户数 ▲	状态 ▲
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	Open+Portal	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	Open+Portal	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	Open+Portal	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	Open+Portal	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	Open+Portal	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	Open+Portal	0	on

10 共6条

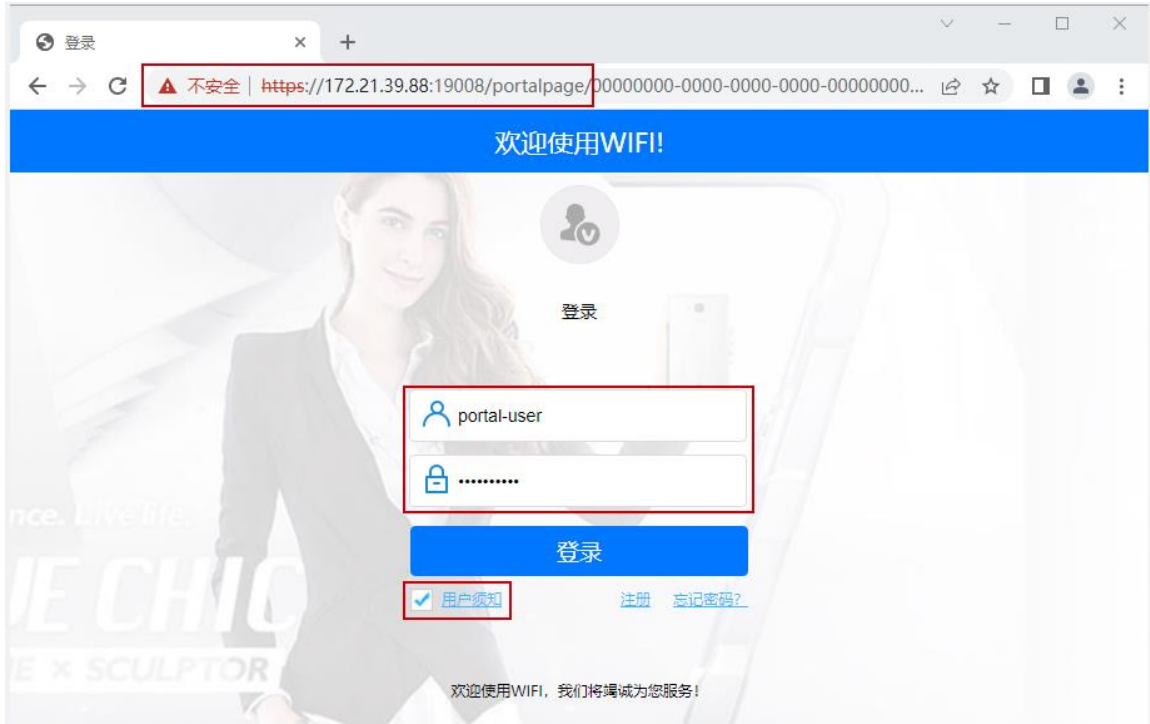
注: 选择列表中的VAP,查看该VAP应用统计信息。

6.3.3 STA 通过 Portal 认证方式接入无线网络

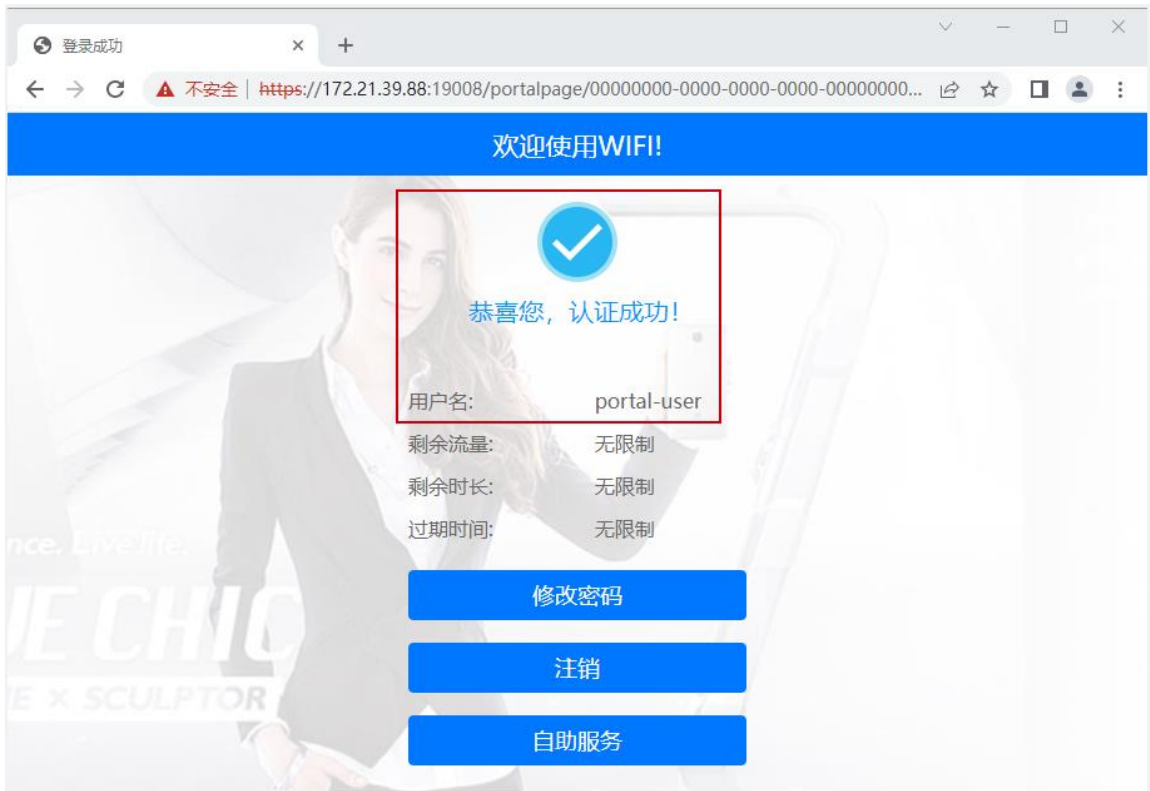
在 STA 上打开浏览器，输入任意 IP 地址，将会弹出 Portal 认证页面。



重定向至 Portal 认证页面，输入用户名“portal-user”，密码“Huawei@123”，勾选“用户须知”，进行登录。

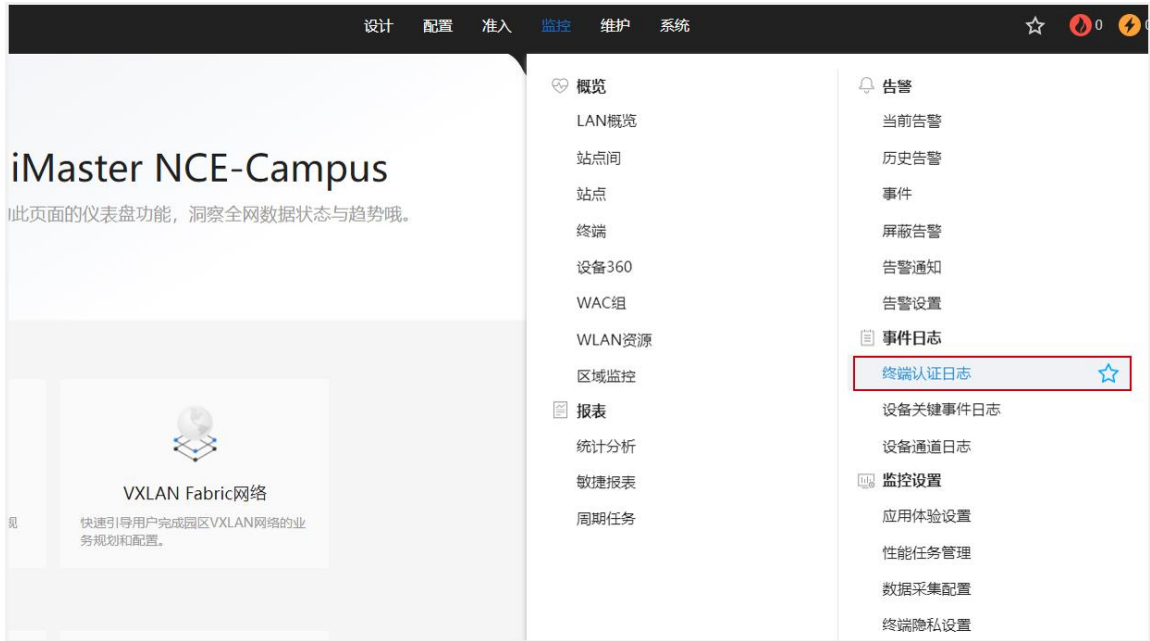


显示认证成功，后续即可正常访问网络资源。



6.3.4 查看 NCE 终端认证日志

在 NCE 上，选择“监控 > 事件日志 > 终端认证日志”，查看终端认证日志。



选择“Portal 上下线日志”，可以查看 Portal 终端认证记录，如下所示。



6.3.5 在 WAC1 上检查终端认证情况

在 WAC1 上查看 NAC 接入用户的详细信息，选择“监控 > 用户”，选择“上线用户统计”选项卡，在用户列表中可以查看当前接入用户的详细信息，如下所示。



6.4 配置参考

6.4.1 WAC1 配置

```
Software Version V200R021C00SPC100
#
defence engine enable
sysname WAC1
#
http timeout 10080
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif100
http server enable
#
vlan batch 100 to 101
#
authentication-profile name p1
portal-access-profile portal1
free-rule-template free1
authentication-scheme radius_huawei
accounting-scheme scheme1
radius-server radius_huawei
#
web-auth-server server-source all-interface
#
management-port isolate enable
management-plane isolate enable
#
radius-server template default
radius-server template radius_huawei
radius-server shared-key cipher %^%#]gR#5-y9p=z#}}Pk4-L;WGPdIm[,VBkhjz&Wf<G%%^%#
radius-server authentication 172.21.39.88 1812 source Vlanif 100 weight 80
radius-server accounting 172.21.39.88 1813 source Vlanif 100 weight 80
radius-server authorization 172.21.39.88 shared-key cipher %^%#5jF1YZq(*OsX-2U&P}A<]`!XH,|-r15kUd$G)=]"%^%# server-group radius_huawei
radius-server authorization server-source all-interface
#
free-rule-template name default_free_rule
#
free-rule-template name free1
free-rule 1 destination ip 172.21.39.88 mask 255.255.255.255
#
url-template name urlTemplate_0
url https://172.21.39.88:19008/portal
url-parameter device-ip ac-ip redirect-url redirect-url ssid ssid user-ipaddress userip user-mac usermac
#
web-auth-server abc
```

```
server-ip 172.21.39.88
port 50200
shared-key cipher %^%#/H+oJc*rtC_]{(WRUDt4un;&<1:g~NP{q(SD$ux#%^%#
url-template urlTemplate_0
source-ip 10.23.100.1
#
portal-access-profile name portal1
web-auth-server abc direct
#
portal-access-profile name portal_access_profile
#
aaa
authentication-scheme radius_huawei
authentication-mode radius
accounting-scheme scheme1
accounting-mode radius
accounting realtime 3
local-aaa-user password policy administrator
domain default
authentication-scheme default
accounting-scheme default
radius-server default
domain default_admin
authentication-scheme default
accounting-scheme default
#
interface Vlanif1
ip address dhcp-alloc unicast
#
interface Vlanif100
ip address 10.23.100.1 255.255.255.0
management-interface
#
interface MEth0/0/1
ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif100 10.23.100.254
ip route-static 172.21.39.88 255.255.255.255 Vlanif100 10.23.100.254
#
```

```
capwap source interface vlanif100
capwap dtls psk %^%#EJVsx!hYu4YZ2_G4#DzXA@:RKv34&REZ]}-y_]mY%^%#
capwap dtls inter-controller psk %^%#{9Wo7!%#BFZ<@EQ]:JG>Rp<|47s,v>YPa.#^!]A9%^%#
capwap dtls no-auth enable
#
wlan
  calibrate flexible-radio auto-switch
  temporary-management psk %^%#PwFE@vw_ "@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
  ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)!%^%#
  traffic-profile name default
  security-profile name default
  security-profile name wlan-net
    security open
  security-profile name default-wds
  security-profile name default-mesh
  ssid-profile name default
  ssid-profile name wlan-net
    ssid wlan-net
  vap-profile name default
  vap-profile name wlan-net
    forward-mode tunnel
    service-vlan vlan-id 101
    ssid-profile wlan-net
    security-profile wlan-net
    authentication-profile p1
  wds-profile name default
  mesh-handover-profile name default
  mesh-profile name default
  regulatory-domain-profile name default
  regulatory-domain-profile name domain1
  air-scan-profile name default
  rrm-profile name default
  radio-2g-profile name default
  radio-5g-profile name default
  wids-spoof-profile name default
  wids-whitelist-profile name default
  wids-profile name default
  wireless-access-specification
  ap-system-profile name default
  port-link-profile name default
  wired-port-profile name default
  ap-group name default
  ap-group name ap-group1
    regulatory-domain-profile domain1
  radio 0
    vap-profile wlan-net wlan 1
  radio 1
    vap-profile wlan-net wlan 1
```

```
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
  ap-name AP1
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
  ap-name AP2
  ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
  ap-name AP3
  ap-group ap-group1
provision-ap
#
return
```

6.4.2 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101
#
dhcp enable
#
vlan 99
  name Manage
#
interface Vlanif1
#
interface Vlanif99
  ip address 172.21.39.253 255.255.128.0
#
interface Vlanif100
  ip address 10.23.100.254 255.255.255.0
  dhcp select interface
#
interface Vlanif101
  ip address 10.23.101.254 255.255.255.0
  dhcp select interface
#
interface MEth0/0/1
  ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
  port link-type access
```

```
port default vlan 99
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

6.4.3 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
```

return

6.5 思考题

上述实验中未配置 DNS 服务器。请思考：DNS 服务器在 Portal 准入认证中有什么作用？

参考答案：

DNS 域名解析服务器，可以解析终端发出的域名探测，使得 AP 可以进行重定向到 Portal 认证页面，即终端访问任意域名即可重定向到 Portal 认证页面。

7 WLAN 漫游实验

7.1 实验介绍

7.1.1 关于本实验

本实验通过 WAC 内二层漫游及 WAC 间三层漫游的调试与配置，让学员掌握华为 WLAN 漫游的相关部署方法。

7.1.2 实验目的

- 掌握 WAC 内二层漫游组网配置。
- 掌握 WAC 间三层漫游组网配置。

7.1.3 实验组网介绍

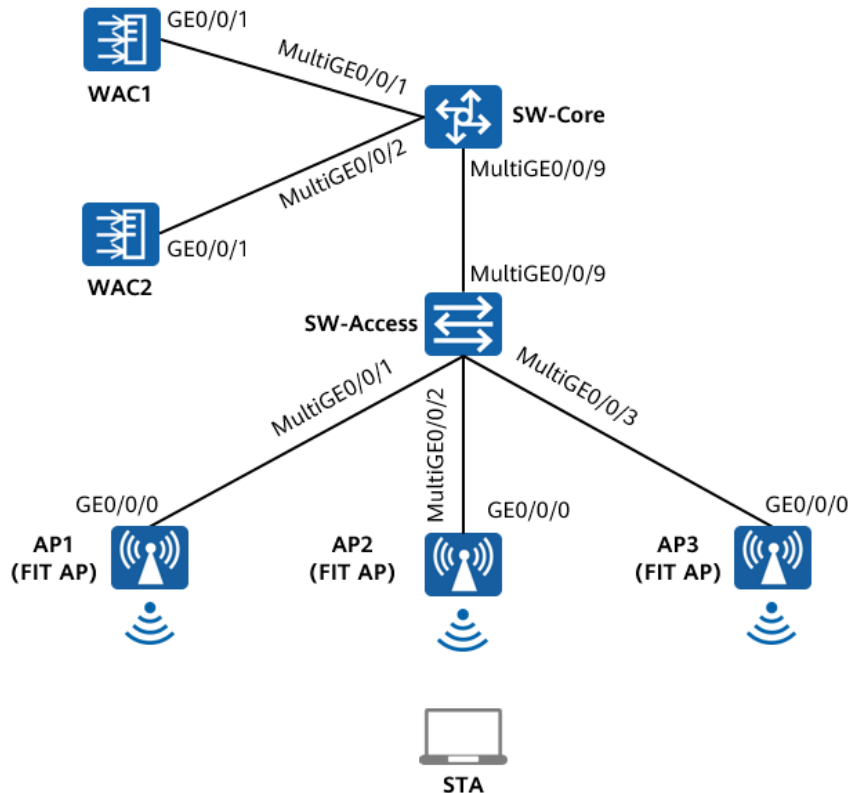


图7-1 WLAN 漫游实验拓扑图

7.1.4 实验规划

表7-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:1 Allow-pass: VLAN 200 201
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101 200 201
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101 200 201
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:200 Allow-pass: VLAN 200 201
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
WAC2	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 200 201

表7-2 IP 地址规划

设备	端口	IP地址
WAC1	VLANif 100	10.23.100.1/24
	VLANif 101	10.23.101.254/24
WAC2	VLANif 200	10.23.200.1/24
	VLANif 201	10.23.201.254/24
SW-Core	VLANif 100	10.23.100.254/24
	VLANif 200	10.23.200.254/24

表7-3 WAC1 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	100
业务VLAN	101
AP组	ap-group1
VAP模板	wlan-net1
安全模板	wlan-net
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	wlan-net
SSID	wlan-net

表7-4 WAC2 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	200
业务VLAN	201
AP组	ap-group2
VAP模板	wlan-net2
安全模板	wlan-net
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	wlan-net
SSID	wlan-net

7.2 实验任务配置

7.2.1 配置思路

- 1.配置 WAC1、WAC2、SW-Access、SW-Core 之间的网络互通。
- 2.配置 WAC1、WAC2 为 DHCP 服务器，给 AP 及 STA 分配 IP 地址。
- 3.配置 AP1、AP2 在 WAC1 上线。
- 4.配置 AP3 在 WAC2 上线。
- 5.配置 WLAN 业务参数，实现 STA 访问 WLAN 网络功能。
- 6.配置 WAC 间漫游功能。
- 7.验证漫游结果。

7.2.2 配置步骤

步骤 1 配置交换机 VLAN 信息

配置接入交换机 SW-Access 设备。

在 SW-Access 上创建 VLAN 100、101、200、201。

```
<Huawei> system-view
[Huawei] sysname SW-Access
[SW-Access] vlan batch 100 101 200 201
```

配置 SW-Access 下行端口类型、PVID 和允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/1
[SW-Access-MultiGE0/0/1] port link-type trunk
[SW-Access-MultiGE0/0/1] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/1] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/1] quit
[SW-Access] interface MultiGE 0/0/2
[SW-Access-MultiGE0/0/2] port link-type trunk
[SW-Access-MultiGE0/0/2] port trunk allow-pass vlan 100 101
[SW-Access-MultiGE0/0/2] port trunk pvid vlan 100
[SW-Access-MultiGE0/0/2] quit
[SW-Access] interface MultiGE 0/0/3
[SW-Access-MultiGE0/0/3] port link-type trunk
[SW-Access-MultiGE0/0/3] port trunk allow-pass vlan 200 201
[SW-Access-MultiGE0/0/3] port trunk pvid vlan 200
[SW-Access-MultiGE0/0/3] quit
```

配置 SW-Access 上行端口类型及允许通过的 VLAN。

```
[SW-Access] interface MultiGE 0/0/9
[SW-Access-MultiGE0/0/9] port link-type trunk
[SW-Access-MultiGE0/0/9] port trunk allow-pass vlan 100 101 200 201
[SW-Access-MultiGE0/0/9] quit
```

配置核心交换机 SW-Core 设备。

在 SW-Core 上创建 VLAN 100、101、200、201。

```
<Huawei> system-view
[Huawei] sysname SW-Core
[SW-Core] vlan batch 100 101 200 201
```

配置 SW-Core 下行端口类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/9
[SW-Core-MultiGE 0/0/9] port link-type trunk
[SW-Core-MultiGE 0/0/9] port trunk allow-pass vlan 100 101 200 201
[SW-Core-MultiGE 0/0/9] quit
```

配置 SW-Core 与 WAC1 互联端口的类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/1
[SW-Core-MultiGE 0/0/1] port link-type trunk
[SW-Core-MultiGE 0/0/1] port trunk allow-pass vlan 100 101
[SW-Core-MultiGE 0/0/1] quit
```

配置 SW-Core 与 WAC2 互联端口的类型及允许通过的 VLAN。

```
[SW-Core] interface MultiGE 0/0/2
[SW-Core-MultiGE 0/0/2] port link-type trunk
[SW-Core-MultiGE 0/0/2] port trunk allow-pass vlan 200 201
[SW-Core-MultiGE 0/0/2] quit
```

步骤 2 初始化 WAC1、WAC2 设备

配置过程请参考 1.2.2 步骤 3，不再赘述。

WAC1 的管理地址配置为 172.21.39.4/24，WAC2 的管理地址配置为 172.21.39.5/24。

步骤 3 配置 WAC1、WAC2 的 VLAN 信息

配置 WAC1 设备。修改 WAC1 设备名称，并创建 VLAN 100、101，修改 GE0/0/1 端口类型为 Trunk，并允许通过 VLAN 100、101。

修改 WAC1 的设备名称。

选择“监控 > AC”，选择“AC 概况”，在“AC 基本信息”中，点击“设备名称”后面的“更改”字样，将设备名称修改为 WAC1。

AC基本信息

设备型号:	AirEngine9700-M1	
设备名称:	AirEngine9700-M1	[更改]
设备序列号:	102257532103	
MAC地址:	9cb2-e8b5-a224	
系统软件版本:	V200R021C00SPC100	[升级]
License资源已使用数/总数:	0/1024	[查看详情]
AP资源授权license状态:	演示	[查看详情]

重命名

* 设备名称:

在 WAC1 上创建 VLAN 100、101。

选择“配置 > AC 配置 > VLAN”，选择“VLAN”选项卡，点击“批量新建”按钮，新建 VLAN 100、101，如下所示。

Wireless LAN AirEngine9700-M1

设备名称: WAC1

监控
配置
诊断
维护

- 配置向导
- AC配置
- 基本配置
- VLAN
- 接口管理
- IP

全局IPv6: OFF

VLAN
VLANIF
VLAN Pool

批量新建

VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan

10 共1条



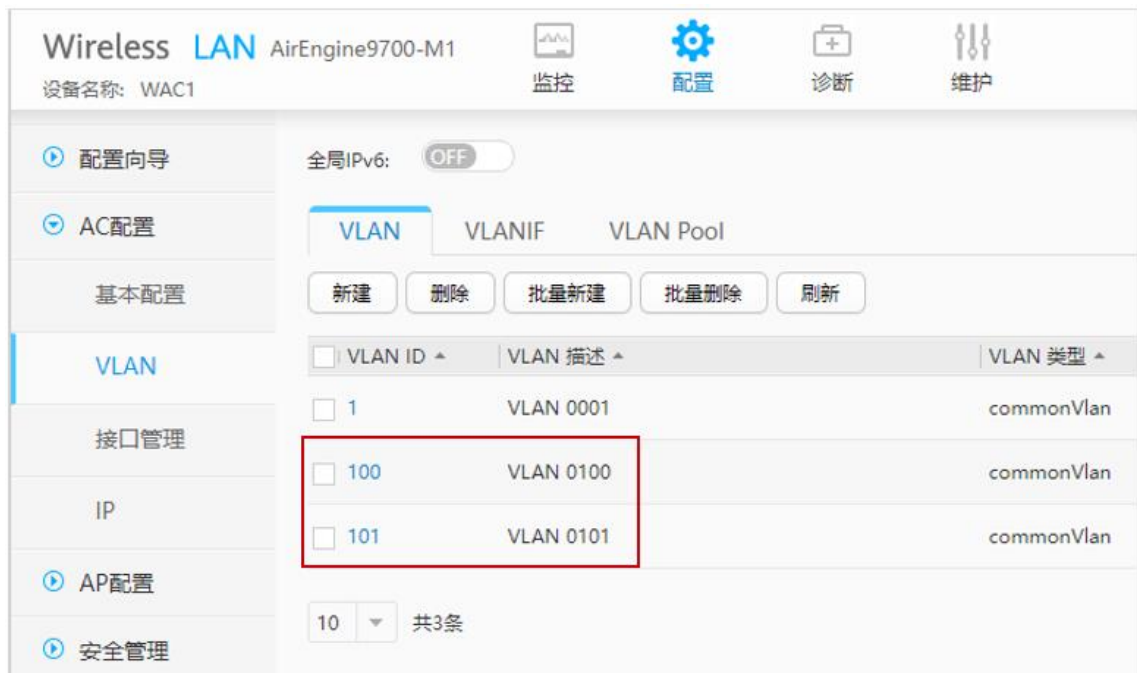
Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 AC配置 > VLAN > VLAN > 批量新建VLAN

*VLAN ID: (1-4094,格式: 1,3-5,7)

基本配置

VLAN



Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 全局IPv6: OFF

AC配置 **VLAN** VLANIF VLAN Pool

基本配置

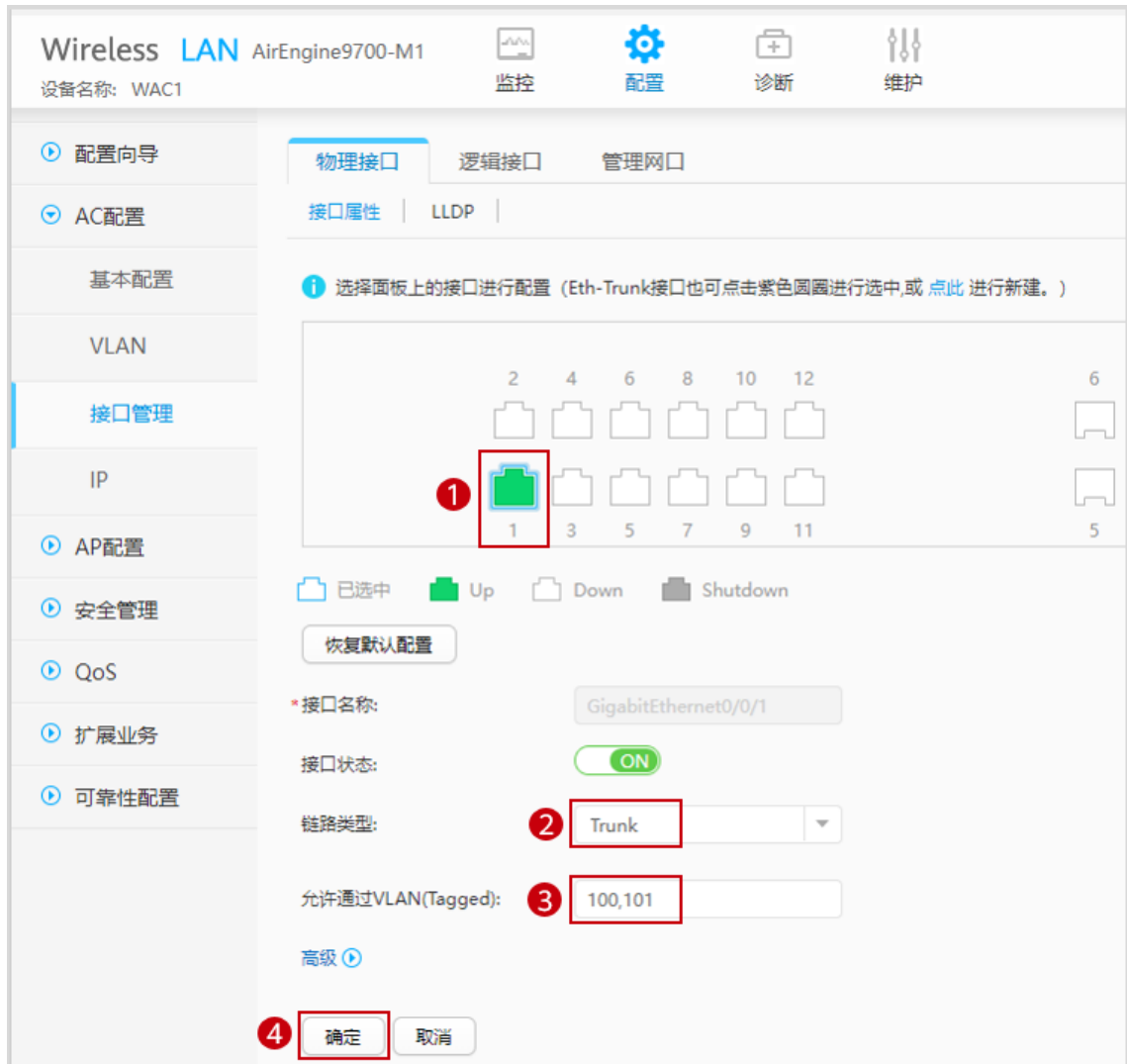
<input type="checkbox"/> VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan
<input type="checkbox"/> 100	VLAN 0100	commonVlan
<input type="checkbox"/> 101	VLAN 0101	commonVlan

10 共3条

接口管理 IP AP配置 安全管理

配置 WAC1 的 GE0/0/1 端口类型及允许通过的 VLAN。

选择“配置 > AC 配置 > 接口管理”，选择“物理接口”选项卡，点击 1 号接口（即 GE0/0/1 接口），配置链路类型为 Trunk，允许通过的 VLAN 为 100 和 101，然后点击“确定”，如下所示。



配置 WAC2 设备。修改 WAC2 设备名称，并创建 VLAN 200、201，修改 GE0/0/1 端口类型为 Trunk，并允许通过 VLAN 200、201。

修改 WAC2 的设备名称为 WAC2（请参考 WAC1 的修改方法，不再赘述）。

在 WAC2 上创建 VLAN 200、201。

选择“配置 > AC 配置 > VLAN”，选择“VLAN”选项卡，点击“批量新建”按钮，新建 VLAN 200、201，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC2

监控 配置 诊断 维护

配置向导 AC配置 基本配置 VLAN 接口管理 IP

全局IPv6: OFF

VLAN VLANIF VLAN Pool

新建 删除 批量新建 批量删除 刷新

VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan

10 共1条

Wireless LAN AirEngine9700-M1
设备名称: WAC2

监控 配置 诊断 维护

配置向导 AC配置 基本配置 VLAN

AC配置 > VLAN > VLAN > 批量新建VLAN

*VLAN ID: (1-4094,格式: 1,3-5,7)

确定 取消

Wireless LAN AirEngine9700-M1
设备名称: WAC2

监控 配置 诊断 维护

配置向导 AC配置 基本配置 VLAN 接口管理 IP AP配置 安全管理

全局IPv6: OFF

VLAN VLANIF VLAN Pool

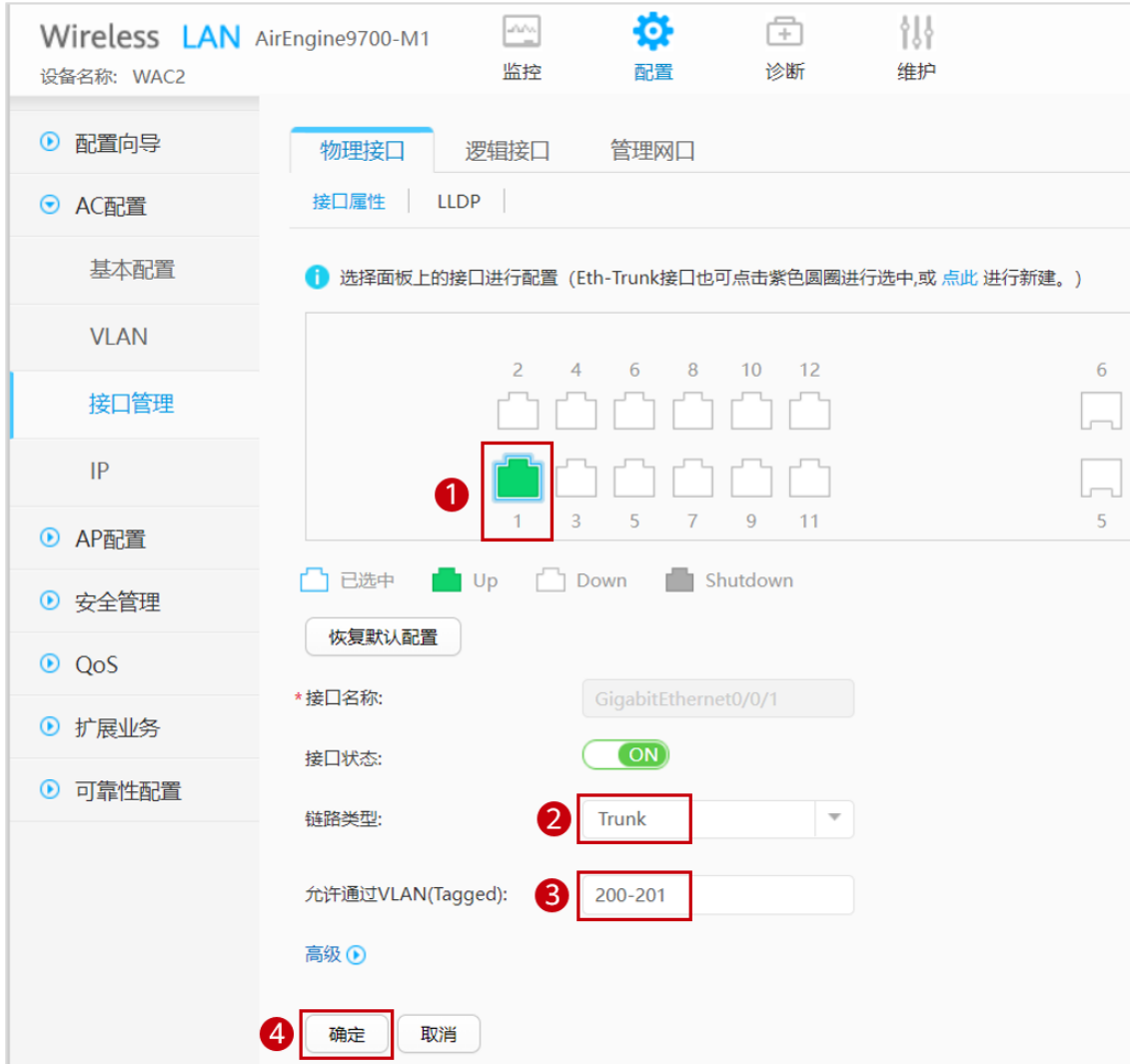
新建 删除 批量新建 批量删除 刷新

VLAN ID	VLAN 描述	VLAN 类型
<input type="checkbox"/> 1	VLAN 0001	commonVlan
<input type="checkbox"/> 200	VLAN 0200	commonVlan
<input type="checkbox"/> 201	VLAN 0201	commonVlan

10 共3条

配置 WAC2 的 GE0/0/1 端口类型及允许通过的 VLAN。

选择“配置 > AC 配置 > 接口管理”，选择“物理接口”选项卡，点击 1 号接口（即 GE0/0/1 接口），配置链路类型为 Trunk，允许通过的 VLAN 为 200 和 201，然后点击“确定”，如下所示。



步骤 4 配置 IP 地址信息

配置 SW-Core 的 IP 地址。

```
[SW-Core] interface vlanif 100
[SW-Core-Vlanif100] ip address 10.23.100.254 24
[SW-Core-Vlanif100] quit
[SW-Core] interface vlanif 200
[SW-Core-Vlanif200] ip address 10.23.200.254 24
[SW-Core-Vlanif200] quit
```

配置 WAC1 的 IP 地址。

分别创建 Vlanif100、Vlanif101 接口，并配置接口 IP 地址。

选择“配置 > AC 配置 > VLAN”，选择“VLANIF”选项卡，点击“新建”，按照如下参数分别配置 Vlanif100、Vlanif101 的 IP 地址。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 | 全局IPv6: OFF | 监控 | 配置 | 诊断 | 维护

AC配置 | VLAN | **VLANIF** | VLAN Pool

基本配置 | **新建** | 删除 | 刷新

VLAN

接口名称	连接状态	IPv4地址/掩码
<input type="checkbox"/> Vlanif1	不可用	

接口管理

IP | 10 | 共1条

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 | 监控 | 配置 | 诊断 | 维护

配置向导 | AC配置 > VLAN > VLANIF > 新建VLANIF

AC配置 | *VLAN ID: 100

基本配置 | MTU (bytes): 1500

VLAN | 管理接口: OFF

接口管理 | IP地址格式: IPv4 IPv6

IP | IPv4地址配置

主IP地址/掩码: 10 . 23 . 100 . 1 / 255 . 255 . 255 . 0

从IP地址/掩码: + 添加

高级

确定 | 取消

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 > AC配置 > VLAN > VLANIF > 新建VLANIF

*VLAN ID: 101

MTU (bytes): 1500

管理接口: OFF

IP地址格式: IPv4 IPv6

IPv4地址配置

主IP地址/掩码: 10 . 23 . 101 . 254 / 255 . 255 . 255 . 0

从IP地址/掩码: + 添加

高级

确定 取消

Wireless LAN AirEngine9700-M1
设备名称: WAC1

全局IPv6: OFF

VLAN VLANIF VLAN Pool

新建 删除 刷新

接口名称	连接状态	IPv4地址/掩码
<input type="checkbox"/> Vlanif1	不可用	
<input type="checkbox"/> Vlanif100	可用	10.23.100.1/255.255.255.0
<input type="checkbox"/> Vlanif101	可用	10.23.101.254/255.255.255.0

10 共3条

配置 WAC2 的 IP 地址。

分别创建 Vlanif200、Vlanif201 接口，并配置接口 IP 地址。

选择“配置 > AC 配置 > VLAN”，选择“VLANIF”选项卡，点击“新建”，按照如下参数分别配置 Vlanif200、Vlanif201 的 IP 地址。

Wireless LAN AirEngine9700-M1
设备名称: WAC2

监控 配置 诊断 维护

配置向导 全局IPv6: OFF

AC配置 VLAN **VLANIF** VLAN Pool

基本配置 **新建** 删除 刷新

VLAN

接口名称	连接状态	IPv4地址/掩码
<input type="checkbox"/> Vlanif1	● 不可用	

接口管理

IP 10 共1条

Wireless LAN AirEngine9700-M1
设备名称: WAC2

监控 配置 诊断 维护

配置向导 AC配置 > VLAN > VLANIF > 新建VLANIF

AC配置 *VLAN ID: 200

基本配置 MTU (bytes): 1500

VLAN 管理接口: OFF

接口管理 IP地址格式: IPv4 IPv6

IP IPv4地址配置

主IP地址/掩码: 10 . 23 . 200 . 1 / 255 . 255 . 255 . 0

从IP地址/掩码: + 添加

高级

确定 取消

Wireless LAN AirEngine9700-M1
设备名称: WAC2

配置向导 > AC配置 > VLAN > VLANIF > 新建VLANIF

*VLAN ID: 201

MTU (bytes): 1500

管理接口: OFF

IP地址格式: IPv4 IPv6

IPv4地址配置

主IP地址/掩码: 10 . 23 . 201 . 254 / 255 . 255 . 255 . 0

从IP地址/掩码: + 添加

高级

确定 取消

Wireless LAN AirEngine9700-M1
设备名称: WAC2

全局IPv6: OFF

VLAN VLANIF VLAN Pool

新建 删除 刷新

接口名称	连接状态	IPv4地址/掩码
<input type="checkbox"/> Vlanif1	不可用	
<input type="checkbox"/> Vlanif200	可用	10.23.200.1/255.255.255.0
<input type="checkbox"/> Vlanif201	可用	10.23.201.254/255.255.255.0

10 共3条

步骤 5 配置路由信息

在 SW-Core 上配置 WLAN 业务相关路由。

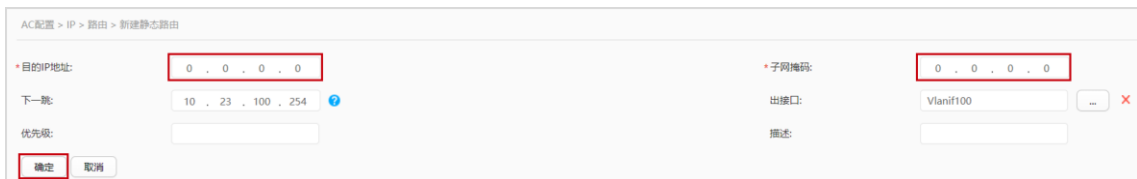
```
[SW-Core] ip route-static 10.23.101.0 255.255.255.0 10.23.100.1
[SW-Core] ip route-static 10.23.201.0 255.255.255.0 10.23.200.1
```

在 WAC1 上配置缺省路由。

选择“配置 > AC 配置 > IP”，选择“路由”选项卡，点击“静态路由配置表”，展开对应的配置界面，然后点击“新建”，新建静态路由。



在“新建静态路由”页面，配置缺省路由如下所示，然后点击“确定”。



在 WAC2 上配置缺省路由。

选择“配置 > AC 配置 > IP”，选择“路由”选项卡，点击“静态路由配置表”，展开对应的配置界面，然后点击“新建”，新建静态路由。



在“新建静态路由”页面，配置缺省路由如下所示，然后点击“确定”。

AC配置 > IP > 路由 > 新建静态路由

*目的IP地址: *子网掩码:

下一跳: 出接口: ... X

优先级: 描述:

步骤 6 配置 DHCP 服务器

配置 WAC1 作为 DHCP 服务器，为 AP1、AP2、STA 分配 IP 地址。

选择“配置 > AC 配置 > IP > DHCP 地址池”，将 DHCP 状态设置为“ON”，然后在 DHCPv4 地址池列表中点击“新建”，按照如下参数分别新建两个接口地址池。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 DHCP地址池 DHCP中继 NAT 路由 DNS

AC配置 DHCP状态: ON

基本配置 DHCPv4地址池列表

VLAN

接口管理 地址池名称 ▲ | IP地址池子网地址 ▲

IP

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 AC配置 > IP > DHCP地址池 > 新建DHCPv4地址池

AC配置 *地址池类型: 全局地址池 接口地址池

基本配置 *接口选择: ... ?

VLAN *接口IP地址:

接口管理 厂商自定义:

IP 高级 ?

AP配置

Wireless LAN AirEngine9700-M1
设备名称: WAC1

配置向导 > AC配置 > IP > DHCP地址池 > 新建DHCPv4地址池

*地址池类型: 全局地址池 接口地址池

*接口选择: Vlanif101

*接口IP地址: 10 . 23 . 101 . 254

厂商自定义: - none -

高级

确定 取消

检查 WAC1 的 DHCPv4 地址池列表，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

DHCP地址池 DHCP中继 NAT 路由 DNS

DHCP状态: ON

DHCPv4地址池列表

新建 删除 显示地址池信息 刷新

地址池名称 ▲	IP地址池子网地址 ▲	子网掩码 ▲
<input type="checkbox"/> Vlanif100	10.23.100.0	255.255.255.0
<input type="checkbox"/> Vlanif101	10.23.101.0	255.255.255.0

5 共2条

配置 WAC2 作为 DHCP 服务器，为 AP3、STA 分配 IP 地址。

选择“配置 > AC 配置 > IP > DHCP 地址池”，将 DHCP 状态设置为“ON”，然后在 DHCPv4 地址池列表中点击“新建”，按照如下参数分别新建两个接口地址池。

Wireless LAN AirEngine9700-M1
设备名称: WAC2

监控 配置 诊断 维护

配置向导 DHCP地址池 DHCP中继 NAT 路由 DNS

AC配置 DHCP状态: ON

基本配置 DHCPv4地址池列表

VLAN 新建 删除 显示地址池信息 刷新

接口管理 地址池名称 IP地址池子网地址

IP

Wireless LAN AirEngine9700-M1
设备名称: WAC2

监控 配置 诊断 维护

配置向导 AC配置 > IP > DHCP地址池 > 新建DHCPv4地址池

AC配置 *地址池类型: 全局地址池 接口地址池

基本配置 *接口选择: Vlanif200

VLAN *接口IP地址: 10 . 23 . 200 . 1

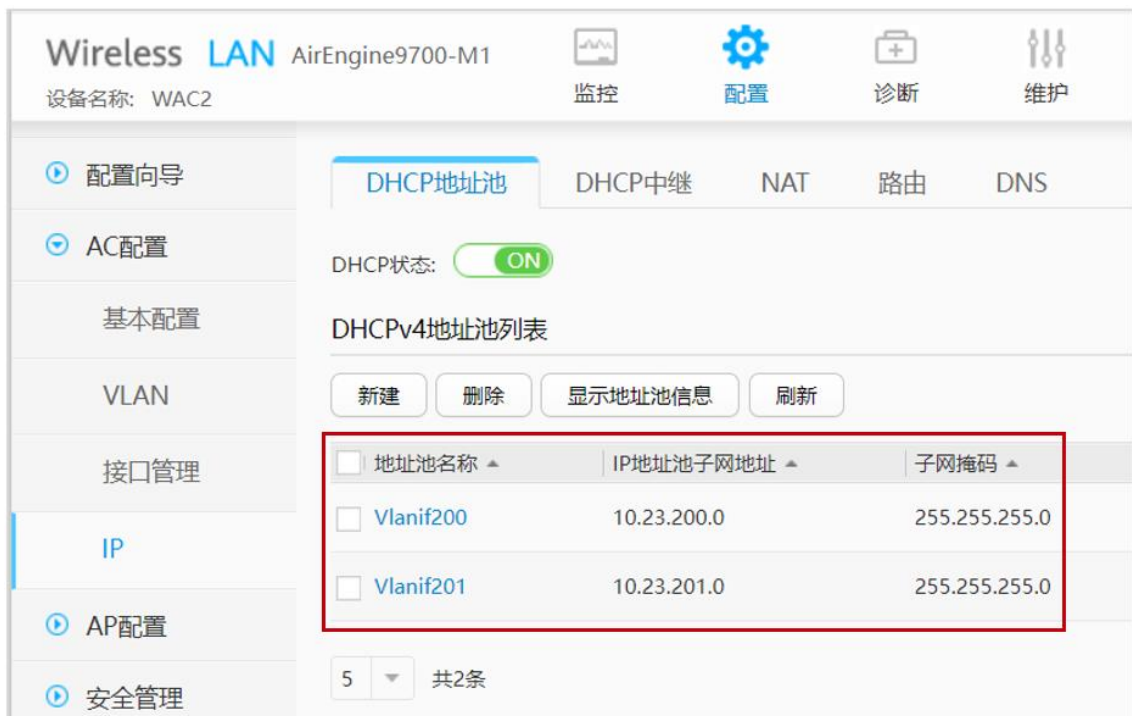
接口管理 厂商自定义: - none -

IP 高级

AP配置 确定 取消



检查 WAC2 的 DHCPv4 地址池列表，如下所示。



地址池名称 ▲	IP地址池子网地址 ▲	子网掩码 ▲
<input type="checkbox"/> Vlanif200	10.23.200.0	255.255.255.0
<input type="checkbox"/> Vlanif201	10.23.201.0	255.255.255.0

步骤 7 配置 AP1、AP2 上线

配置 AP1、AP2 在 WAC1 中上线，其配置步骤与 1.2.2 步骤 6 类似，不再赘述。

注意：WAC1 的 CAPWAP 源端口是 Vlanif 100，AP1 和 AP2 规划在 ap-group1 中。

步骤 8 配置 AP3 上线

配置 AP3 在 WAC2 中上线，其配置步骤与 1.2.2 步骤 6 类似，不再赘述。

注意：WAC2 的 CAPWAP 源端口是 Vlanif 200，AP3 规划在 ap-group2 中。

步骤 9 配置无线业务 (WAC1)

在 WAC1 上配置无线业务，其配置步骤与 1.2.2 步骤 7 类似，不再赘述。

注意：WAC1 的无线业务参数请按照表 7-3 WAC1 业务参数规划进行配置。

步骤 10 配置无线业务 (WAC2)

在 WAC2 上配置无线业务，其配置步骤与 1.2.2 步骤 7 类似，不再赘述。

注意：WAC2 的无线业务参数请按照表 7-4 WAC2 业务参数规划进行配置。

注意：WAC1 和 WAC2 无线业务的 SSID 及安全策略必须相同，这是实现 WLAN 漫游功能的必要条件。

步骤 11 配置 WAC 间漫游功能

在 WAC1 上创建漫游组，并配置 WAC1 和 WAC2 为漫游组成员。

选择“配置 > AC 配置 > 基本配置”，选择“AC 间漫游”选项卡，然后点击“新建”，创建一个名称为“mob1”的漫游组，最后点击“应用”，具体配置如下所示。



在 WAC2 上创建漫游组，并配置 WAC1 和 WAC2 为漫游组成员。

选择“配置 > AC 配置 > 基本配置”，选择“AC 间漫游”选项卡，然后点击“新建”，创建一个名称为“mob1”的漫游组，最后点击“应用”，具体配置如下所示。

步骤 12 配置 WAC 间数据隧道 DTLS 加密

SSID		VAP						
自动刷新: <input type="checkbox"/> OFF								
AP型VAP列表								
应用统计清零								
AP ID	AP名称	射频ID	WLAN ID	SSID	BSSID	认证方式	接入用户数	状态
0	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA/WPA2-PSK	0	on
0	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA/WPA2-PSK	0	on
5 共2条								
注: 选择列表中的VAP,查看该VAP应用统计信息。								

7.3.3 检查漫游组状态

在 WAC1/WAC2 上查看漫游组的状态，以 WAC1 为例进行说明。

在 WAC1 上选择“监控 > AC > 漫游用户数概况”，可以查看漫游组的状态，其中状态为“normal”，表示漫游组工作正常。

Wireless LAN AirEngine9700-M1		监控	配置	诊断	维护						
设备名称: WAC1											
概览	AC概况	漫游用户数概况	接口流量统计	无线配置同步信息							
网络KPI	自动刷新: <input type="checkbox"/> OFF										
AC	基于AC的AC间漫游用户总数统计 ?										
用户	导出										
射频	<table border="1"> <thead> <tr> <th>对端AC IP地址</th> <th>状态</th> </tr> </thead> <tbody> <tr> <td>10.23.100.1</td> <td>normal</td> </tr> <tr> <td>10.23.200.1</td> <td>normal</td> </tr> </tbody> </table>					对端AC IP地址	状态	10.23.100.1	normal	10.23.200.1	normal
对端AC IP地址	状态										
10.23.100.1	normal										
10.23.200.1	normal										
AP	10 共2条										
SSID											
CPE隧道											

7.3.4 观察 STA 漫游轨迹

STA 接入无线网络“wlan-net”后，在 AP1、AP2、AP3 的覆盖范围内进行移动，会触发漫游，在 WAC 上可以查看用户的漫游轨迹，以 WAC1 为例说明如下。

选择“监控 > 用户 > 上线用户统计”，在用户列表中可以查看当前的在线用户。

用户列表 (总用户数: 1, 2.4G: 0, 5G: 1)

智能诊断 应用统计 漫游轨迹 上线失败记录 下线记录 强制下线 导出信息

<input type="checkbox"/> 用户名 ▲ ▼	MAC地址 ▲ ▼	协商速率(Mbps) ↓ ▲ ▼	AP名称 ▲ ▼	IPv4地址 ▲ ▼	频段 ▲ ▼	认证方式 ▲ ▼
→ <input type="checkbox"/> 081f715390b4	081f-7153-90b4	57/156	AP1	10.23.101.128	5G	WPA2-PSK

10 共1条

每秒关联的用户数 : 0
 Dot1x每秒认证用户数 : 0 Portal每秒认证用户数 : 0 MAC每秒认证用户数 : 0

点击对应的用户名，即可查看用户明细信息，如：运行指标、漫游轨迹、下线记录等。

运行指标 应用统计 漫游轨迹 上线失败记录 下线记录 AP参数明细

刷新 导出

时间 ▲	AP-AC IP地... ▲	AP-AC IPv6... ▲	AC-AC IP地... ▲	AC-AC IPv6... ▲	当前AP名称 ▲	射频ID ▲	BSSID ▲	离开速率(M... ▲	接入RSS... ▲	离开RSS... ▲	二层/三层漫游 ▲
09:55:39	10.23.100.1	--	--	--	AP1	1	9cb2-e82d-5500	--/--	-21	--	--

10 共1条

7.4 配置参考

7.4.1 WAC1 配置

```

Software Version V200R021C00SPC100
#
sysname WAC1
#
http timeout 2880
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif100
http server enable
#
vlan batch 100 to 101
#
stp enable
#
dhcp enable
#
management-port isolate enable
management-plane isolate enable
#
pki realm default
certificate-check none
#
aaa
local-user admin password irreversible-cipher $1a$a9AWCs-
q5.$n|ec5XhLvJw,(]KNf[B%K[011J[:\T2~Fl/&R&(T$
    
```

```
local-user admin privilege level 15
local-user admin service-type ssh http
#
interface Vlanif1
 ip address dhcp-alloc unicast
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 dhcp select interface
 management-interface
#
interface Vlanif101
 ip address 10.23.101.254 255.255.255.0
 dhcp select interface
#
interface MEth0/0/1
 ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
 ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source interface vlanif100
capwap dtls inter-controller control-link encrypt on
capwap dtls psk %^%#GE$'=NySIMd>$B62GoO'Mkw:TmVsCChcg,Ni(--%^^%#
capwap dtls inter-controller psk %^%#ntHh31}TQ:k#NH4i%We/,E>xRRRT}{Dnduu,AM,^E%^^%#
capwap dtls no-auth enable
#
wlan
 temporary-management psk %^%#peYt1<1l-Bs8Jm-DJ)}*/_jF1LDN!+ILS/'\s"wL%^^%#
 ap username admin password cipher %^%#O/dj$>]yQ$1V=ZTXMsa'FHcAAV!ApO5S$-;RB8D$%^^%#
 traffic-profile name default
 security-profile name default
 security-profile name wlan-net
   security wpa-wpa2 psk pass-phrase %^%#N.vo7TDv>20UvyQiZvqNw<IMUJnR!0%4#{JPK;sG%^^%# aes
 security-profile name default-wds
 security-profile name default-mesh
 ssid-profile name default
 ssid-profile name wlan-net
   ssid wlan-net
 vap-profile name default
```



```
vap-profile name wlan-net1
  service-vlan vlan-id 101
  ssid-profile wlan-net
  security-profile wlan-net
wds-profile name default
mesh-handover-profile name default
mesh-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-whitelist-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
mobility-group name mob1
  member ip-address 10.23.100.1
  member ip-address 10.23.200.1
ap-group name default
ap-group name ap-group1
  regulatory-domain-profile domain1
radio 0
  vap-profile wlan-net1 wlan 1
radio 1
  vap-profile wlan-net1 wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
  ap-name AP1
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
  ap-name AP2
  ap-group ap-group1
provision-ap
#
return
```

7.4.2 WAC2 配置

```
Software Version V200R021C00SPC100
#
sysname WAC2
#
http timeout 2880
http secure-server ssl-policy default_policy
```

```
http secure-server server-source -i Vlanif200
http server enable
#
vlan batch 200 to 201
#
stp enable
#
dhcp enable
#
management-port isolate enable
management-plane isolate enable
#
aaa
 local-user admin password irreversible-cipher
$1a$6]9"ZyZND7$<a0>2`*V(laTNN+gWg:01O1Q)ewt6V[@y>HXMJP@$
 local-user admin privilege level 15
 local-user admin service-type ssh http
#
interface Vlanif1
 ip address dhcp-alloc unicast
#
interface Vlanif200
 ip address 10.23.200.1 255.255.255.0
 dhcp select interface
 management-interface
#
interface Vlanif201
 ip address 10.23.201.254 255.255.255.0
 dhcp select interface
#
interface MEth0/0/1
 ip address 172.21.39.5 255.255.255.0
#
interface Ethernet0/0/47
 ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 200 to 201
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.200.254
#
capwap source interface vlanif200
capwap dtls inter-controller control-link encrypt on
capwap dtls psk %^%#vn\1=HRVL@N"+C-7e:b#11%`PR@S60sh\SOH2r69%^%#
capwap dtls inter-controller psk %^%#ia.O&Gj|XF|RqJut_t)$l05E-|%MH!}Y-(c.3@D%^%#
```

```
capwap dtls no-auth enable
#
wlan
temporary-management psk %^%#6E3B'v&///<O[IYOiY(x#RGRYEhAB|SdwLO",AIZT%^%#
ap username admin password cipher %^%#:Te88XR+1A]0tUUB1R6(lnY3=wqkm>_jFW9Oq;BV%^%#
traffic-profile name default
security-profile name default
security-profile name wlan-net
    security wpa-wpa2 psk pass-phrase %^%#Xf(jQiRAq>Y4|lB`xG<W6-FyP(p'Z'iw_+W8"6zQ%^%# aes
security-profile name default-wds
security-profile name default-mesh
ssid-profile name default
ssid-profile name wlan-net
    ssid wlan-net
vap-profile name default
vap-profile name wlan-net2
    service-vlan vlan-id 201
    ssid-profile wlan-net
    security-profile wlan-net
wds-profile name default
mesh-handover-profile name default
mesh-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-whitelist-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
mobility-group name mob1
    member ip-address 10.23.100.1
    member ip-address 10.23.200.1
ap-group name default
ap-group name ap-group2
    regulatory-domain-profile domain1
radio 0
    vap-profile wlan-net2 wlan 1
radio 1
    vap-profile wlan-net2 wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
ap-name AP3
ap-group ap-group2
```

```
provision-ap
#
return
```

7.4.3 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 100 to 101 200 to 201
#
http server-source -i MEth0/0/1
#
interface Vlanif1
#
interface Vlanif100
 ip address 10.23.100.254 255.255.255.0
#
interface Vlanif200
 ip address 10.23.200.254 255.255.255.0
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200 to 201
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101 200 to 201
#
interface NULL0
#
ip route-static 10.23.101.0 255.255.255.0 10.23.100.1
ip route-static 10.23.201.0 255.255.255.0 10.23.200.1
#
return
```

7.4.4 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
```

```
sysname SW-Access
#
vlan batch 100 to 101 200 to 201
#
interface Vlanif1
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
 port link-type trunk
 port trunk pvid vlan 200
 port trunk allow-pass vlan 200 to 201
#
interface MultiGE0/0/4
 shutdown
#
interface MultiGE0/0/5
 shutdown
#
interface MultiGE0/0/6
 shutdown
#
interface MultiGE0/0/7
 shutdown
#
interface MultiGE0/0/8
 shutdown
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101 200 to 201
#
interface NULL0
#
return
```

7.5 思考题

我们在验证漫游的时候会配置相同的安全策略，请思考，在安全策略不同的时候终端会进行漫游吗？

参考答案：

如果漫游的两台 AP 配置不同的安全策略，终端不会触发漫游行为。

8

射频资源管理实验

8.1 实验介绍

8.1.1 关于本实验

本实验通过对射频资源管理相关技术的配置，让学员掌握射频资源管理技术的部署和配置。

8.1.2 实验目的

- 掌握 WLAN 射频调优的相关配置。
- 掌握 WLAN 频谱导航的相关配置。
- 掌握 WLAN 负载均衡的相关配置。
- 掌握 WLAN 用户 CAC 功能的相关配置。

8.1.3 实验组网介绍

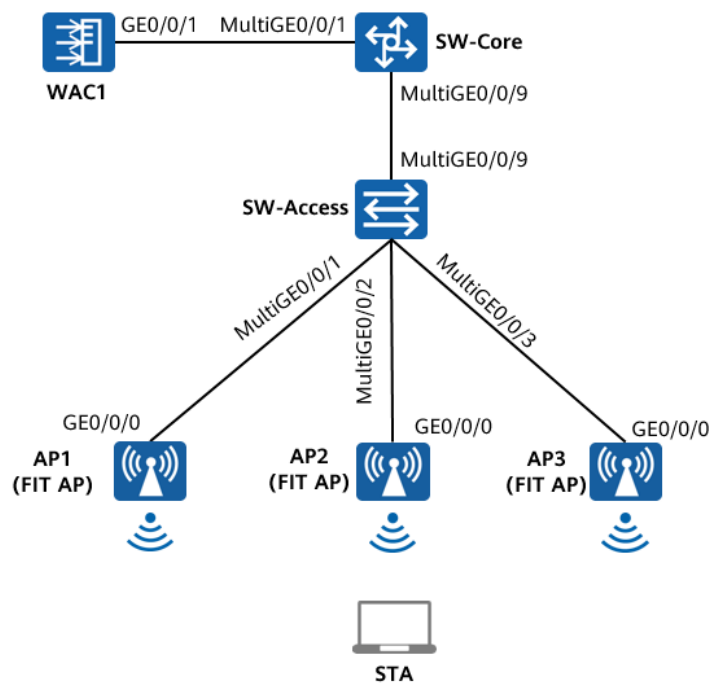


图8-1 射频资源管理实验拓扑图

8.1.4 实验规划

表8-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表8-2 IP 地址规划

设备	端口	IP地址
SW-Core	Vlanif100	10.23.100.254/24
	Vlanif101	10.23.101.254/24
WAC1	Vlanif100	10.23.100.1/24
	MEth0/0/1	172.21.39.4/24

表8-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	100
业务VLAN	101
AP组	ap-group1

VAP模板	wlan-net
安全模板	wlan-net
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	wlan-net
SSID	wlan-net

8.2 实验任务配置

8.2.1 配置思路

- 1.配置基础网络互通，保证设备间的二层、三层互通。
- 2.配置 AP 上线。
- 3.配置 WLAN 业务。
- 4.配置射频调优。
- 5.配置频谱导航。
- 6.配置负载均衡。
- 7.配置用户 CAC 功能。

8.2.2 配置步骤

步骤 1 配置基础网络、AP 上线、无线业务

请参考 1.2.2 步骤 1 ~ 1.2.2 步骤 7，此处不再赘述。

步骤 2 配置射频调优

配置射频调优模式为自动调优（默认已配置），并开启 DFA 功能。

选择“配置 > AP 配置 > 射频规划/调优”，选择“调优配置”选项卡，按照如下参数进行配置，然后点击“应用”。

射频规划
调优配置

① WLAN网络中,AP的工作状态会受到周围环境的影响。例如,当相邻AP的工作信道存在重叠频段时,某个AP的功率过大会对相邻AP造成干扰。

注意事项:

- 对于配置WDS网桥或Mesh链路的射频,射频调优功能不生效。
- 射频调优功能不适用于AP相互无法感知的场景,例如: AP使用定向天线、AP相隔较远或者AP间被阻隔等导致无法相互感知的情况。
- 射频调优功能不适用于高密场景、WDS/Mesh回传场景、轨交场景和室外定向天线的覆盖场景。
- 射频的工作模式为监控模式时,此射频不参与调优。
- 配置射频调优、智能漫游、WIDS等依赖于信道扫描的功能后,在扫描过程中如果触发了射频的信道切换,在信道切换的瞬间会导致用户业务中断。

调优开关: ON

*** 触发条件:** 自动 ? * 优化开始时间: 03:00:00 调优间隔(分钟): 1440

定时

手动 ?

高级 ▾

冗余射频切换: ON 切换为5G/Monitor 自动关闭

高级调优策略(可选): 入侵模式 ? 非Wi-Fi ? 底噪调优(noise-floor) ?

调优灵敏度: 中 ▾

非法邻居干扰: ON

干扰信道恶化黑名单阈值: 16

高密抗干扰: ON

应用

在 2.4G 频段开启信道、功率动态调整功能。在 5G 频段开启信道、功率、带宽动态调整功能。(带宽动态调整仅对 5G 射频生效)

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组配置界面。



The screenshot shows the 'AP组' (AP Group) configuration page in the Huawei Wireless LAN management interface. The page title is 'Wireless LAN AirEngine9700-M1' and the device name is 'WAC1'. The left sidebar contains navigation options: '配置向导', 'AC配置', 'AP配置', 'AP组配置', 'AP配置', and '射频规划/调优'. The main content area is titled '静态负载均衡组' and includes buttons for '修改', '新建', '删除', and '刷新'. A table lists AP groups with columns for '组名称', 'VAP模板', and '射频0模板'. The 'ap-group1' row is highlighted with a red box. Below the table, there is a dropdown menu set to '20' and the text '共2条'.

组名称	VAP模板	射频0模板
default		2.4G-default
ap-group1	wlan-net	2.4G-default

在 AP 组配置界面中，选择“射频管理 > 射频 0”，配置如下参数，然后点击“应用”。



The screenshot shows the '射频管理' (Radio Management) configuration page in the Huawei Wireless LAN management interface. The page title is 'Wireless LAN AirEngine9700-M1' and the device name is 'WAC1'. The left sidebar contains navigation options: '配置向导', 'AC配置', 'AP配置', 'AP组配置', 'AP配置', '射频规划/调优', '分支AP组配置', and '模板管理'. The main content area is titled 'AP配置 > AP组配置 > AP组' and includes a dropdown menu for 'AP组配置' set to 'ap-group1' and a '查看成员' button. Below this, there is a '显示所有模板' checkbox and a '配置模型介绍' link. A tree view shows the configuration structure: 'VAP配置', '射频管理', '域管理模板 [domain...]', '射频0', '射频1', '射频2', 'AP', and 'WIDS'. The '射频0' folder is highlighted with a red box.

射频0配置(2.4G)

基础配置 高级配置

工作状态: ON

工作模式: 正常模式 监控模式

功率自动调优: 跟随(全局: 开) 关

信道自动调优: 跟随(全局: 开) 关

大数据调优: ON ?

天线增益(dB):

频谱分析: OFF

全信道检测: OFF

切换为5G: OFF

发送功率(dBm): ?

信道: ?

WDS/Mesh桥接距离(0.1km):

冗余射频切换: 跟随(全局: 开) 关

→ WIDS

应用

在 AP 组配置界面中，选择“射频管理 > 射频 1”，配置如下参数，然后点击“应用”。

射频1配置(5G)

基础配置 高级配置

工作状态: ON

工作模式: 正常模式 监控模式

功率自动调优: 跟随(全局: 开) 关

信道自动调优: 跟随(全局: 开) 关

大数据调优: ON ?

天线增益(dB):

频谱分析: OFF

全信道检测: OFF

发送功率(dBm): ?

信道: ?

WDS/Mesh桥接距离(0.1km):

频宽自动调整: ON

→ WIDS

应用

手动触发射频调优。

选择“配置 > AP 配置 > 射频规划/调优”，选择“射频规划”选项卡，点击“立即调优”，调优范围选择“全部 AP”，然后点击“确定”，启动调优程序。

射频列表

AP ID	AP名称	射频ID	AP组名称	频段	工作模式	射频状态	频宽 / 信道
2	AP3	0	ap-group1	2.4G	正常模式	on	自动 20M/6
2	AP3	1	ap-group1	5G	正常模式	on	自动 20M/40
1	AP2	0	ap-group1	2.4G	正常模式	on	自动 20M/11
1	AP2	1	ap-group1	5G	正常模式	on	自动 20M/64
0	AP1	0	ap-group1	2.4G	正常模式	on	自动 20M/6
0	AP1	1	ap-group1	5G	正常模式	on	自动 20M/161

立即调优

立即调优一次,预计需要大约15min到达稳定状态。

调优范围:

全部AP
 指定AP组
 指定AP

查看调优进度，等待调优完成。

射频列表

正在调优... 33%

步骤 3 配置频谱导航

使能 VAP 的频谱导航功能。（缺省情况下已经使能）

选择“配置 > AP 配置 > 模板管理 > 无线业务 > VAP 模板”，选择“wlan-net”模板，点击“高级配置”，开启频谱导航功能，然后点击“应用”。

↓ 射频

频谱导航: ON

创建 RRM 模板，配置频谱导航参数。配置接入用户数起始门限为 90 个，5G 用户占比门限为 80%，5G 优先的 SNR 起始门限为 18 dB。

选择“配置 > AP 配置 > 模板管理 > 射频管理 > RRM 模板”，点击“新建”，配置模板名称为“wlan-rrm”，点击“确定”。



选择“wlan-rrm”模板，点击“高级配置”，配置频谱导航参数如下所示，然后点击“应用”。



创建射频模板，并引用 RRM 模板。

创建 2G 射频模板。选择“配置 > AP 配置 > 模板管理 > 射频管理 > 2G 射频模板”，点击“新建”，配置模板名称为“wlan-2g”，点击“确定”。



在 2G 射频模板中引用 RRM 模板，配置如下。



创建 5G 射频模板。选择“配置 > AP 配置 > 模板管理 > 射频管理 > 5G 射频模板”，点击“新建”，配置模板名称为“wlan-5g”，点击“确定”。



在 5G 射频模板中引用 RRM 模板，配置如下。



在 AP 组“ap-group1”中分别引用 2G 射频模板“wlan-2g”和 5G 射频模板“wlan-5g”。

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组配置界面。

在 AP 组配置界面中，选择“射频管理 > 射频 0 > 2G 射频模板”，配置如下。

在 AP 组配置界面中，选择“射频管理 > 射频 1 > 5G 射频模板”，配置如下。



最后，再次全面检查各种模板之间的相互引用关系，如下所示。



步骤 4 配置负载均衡

配置基于用户数的动态负载均衡功能。配置 STA 起始门限为 12 个，差值门限为 5 个；动态负载均衡组成员的 RSSI 阈值为 -63 dBm。

选择“配置 > AP 配置 > 模板管理 > 射频管理 > RRM 模板”，选择“wlan-rrm”模板，分别配置“基础配置”和“高级配置”。

“基础配置”的参数配置如下所示。



RRM模板: wlan-rrm 展示模板引用关系

模板介绍信息: RRM模板主要用于保持最优的射频资源状态,通过自动检查周边无线环境、动态调整信道和发射功率等射频资源、

基础配置 高级配置

空口时间公平调度: OFF

→ 强制用户下线

↓ 动态负载均衡

负载均衡: ON

→ 智能漫游

应用

“高级配置”的参数配置如下所示（下图仅展示负载均衡相关参数）。



↓ 动态负载均衡

负载均衡: ON

负载均衡起始阈值(终端数): 12

负载均衡负载差值阈值: 基于用户百分比 基于用户实际个数

5

RSSI阈值(dBm): -63

高级 ⓘ

→ 智能漫游

→ SFN

应用

“wlan-rrm”模板在步骤3中已经被引用，本步骤中无需重复引用。

步骤 5 配置用户 CAC 功能

配置用户 CAC 功能。打开基于用户数的 CAC 功能，配置接入和漫游阈值均为 40；打开弱信号终端禁止接入功能，配置 SNR 阈值为 13 dB。同时启用当接入终端达到阈值时自动隐藏 SSID 的功能。

选择“配置 > AP 配置 > 模板管理 > 射频管理 > RRM 模板”，选择“wlan-rrm”模板，点击“高级配置”选项卡，配置用户 CAC 参数如下。



“wlan-rrm”模板在步骤 3 中已经被引用，本步骤中无需重复引用。

8.3 结果验证

8.3.1 查看射频模板和 RRM 模板信息

在 WAC1 上查看 2G 射频模板、5G 射频模板以及 RRM 模板的配置信息。

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组配置界面。

在 AP 组配置界面中，分别查看“射频管理 > 射频 0 > 2G 射频模板 > RRM 模板”以及“射频管理 > 射频 1 > 5G 射频模板 > RRM 模板”，发现射频 0 和射频 1 中均引用了名称为“wlan-rrm”的 RRM 模板，如下所示。



Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导
AC配置
AP配置
AP组配置
AP配置
射频规划/调优
分支AP组配置
模板管理
安全管理
QoS
扩展业务
可靠性配置

AP配置 > AP组配置 > AP组

AP组配置: ap-group1 查看成员

显示所有模板 配置模型介绍

射频管理

- 域管理模板 [domain...]
- 射频0
 - 2G射频模板 [wlan-2g...]
 - RRM模板 [wlan-rr...]
 - 空口扫描模板 [default]
 - 射频1
 - 5G射频模板 [wlan-5g...]
 - RRM模板 [wlan-rr...]
 - 空口扫描模板 [default]
 - 射频2

AP
WIDS

点击“RRM”模板，即可查看详细的配置参数，如下所示。

↓ **用户CAC**

UAC策略: 关闭 基于用户

新增用户用户数阈值: 漫游用户用户数阈值:

达到接入阈值: SNR阈值(dB):

禁止弱信号终端接入: ON

↓ **频谱导航**

1 通过频谱导航功能,AP可以控制STA优先接入5G,减少2.4G频段上的负载和干扰,提升用户体验。

双频间负载均衡负载起始阈值(终端数): 双频间负载均衡负载差值阈值(%):

双频间负载均衡SNR阈值(dB): 终端支持频段信息老化probe次数:

拒绝终端关联最大次数:

↓ **动态负载均衡**

负载均衡: ON

负载均衡起始阈值(终端数):

负载均衡负载差值阈值: 基于用户百分比 基于用户实际个数

RSSI阈值(dBm):

[高级](#)

8.3.2 查看当前射频状态信息

在 WAC1 上查看 AP 当前的射频状态信息。

选择“监控 > 射频”，在“射频列表”中可以查看 AP 的频段、频宽、信道、功率、信道利用率等射频状态信息，如下所示。

AP ID	AP名称	射频ID	状态	频段	射频类型	频宽	信道	功率	实际功率/信道功率	接入用户	噪声强度	信道利用率	下行重传率	下行丢包率
2	AP3	0	on	2.4G	802.11ax	20M	1	9/29	0	-78	99%	0%	0%	
2	AP3	1	on	5G	802.11ax	20M	161	12/30	0	-94	4%	0%	0%	
1	AP2	0	on	2.4G	802.11ax	20M	6	9/29	0	-92	88%	0%	0%	
1	AP2	1	on	5G	802.11ax	20M	40	12/30	0	-94	4%	<1%(89/13923)	0%	
0	AP1	0	on	2.4G	802.11ax	20M	11	9/29	0	-94	57%	0%	0%	
0	AP1	1	on	5G	802.11ax	20M	64	12/30	0	-92	2%	+1%(9/6248)	0%	

8.4 配置参考

8.4.1 WAC1 配置

```
Software Version V200R021C00SPC100
#
sysname WAC1
#
```

```
http secure-server ssl-policy default_policy
http server enable
#
vlan batch 100 to 101
#
stp enable
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name macportal_authen_profile
authentication-profile name portal_authen_profile
#
ssl policy default_policy type server
  pki-realm default
  version tls1.2
  ciphersuite ecdhe_rsa_aes128_gcm_sha256 ecdhe_rsa_aes256_gcm_sha384
#
aaa
  authentication-scheme default
    authentication-mode local
  authentication-scheme radius
    authentication-mode radius
  authorization-scheme default
    authorization-mode local
  accounting-scheme default
    accounting-mode none
  local-aaa-user password policy administrator
  domain default
    authentication-scheme default
    accounting-scheme default
    radius-server default
  domain default_admin
    authentication-scheme default
    accounting-scheme default
  local-user admin password irreversible-cipher
  $1a$Z#*{";)lk6$LUMXJS;VWR$p7mWZtx|EN3q#M`}27Bg+[8<)ELp.$
  local-user admin privilege level 15
  local-user admin service-type telnet ssh http
#
interface Vlanif100
  ip address 10.23.100.1 255.255.255.0
#
interface MEth0/0/1
  ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
  ip address 169.254.3.1 255.255.255.0
```

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%#
capwap dtls inter-controller psk %^%#tc.5LFZ\oJ^bM8'YYv#<te,1Oq8kAl.}J+v{puP%^%#
capwap message-integrity psk %^%#eJ&eRx\$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x*%^%#
capwap sensitive-info psk %^%#;,L1<.L'e+li6MX,^QxH{6z#&#z[v4Oe"pCPrF}'%^%#
capwap inter-controller sensitive-info psk %^%#ji6gT7>2y3dm}n~Bb"%8z$0]B62~|NkD,WJF[n2U%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
wlan
 calibrate flexible-radio auto-switch
 temporary-management psk %^%#PwFE@vw_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
 ap username admin password cipher %^%#PBMhAQQ{@}1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)l%^%#
 traffic-profile name default
 security-profile name default
 security-profile name wlan-net
 security wpa-wpa2 psk pass-phrase %^%#+POS/J(&<Mm==dL=vxXYhhlfU|YWjQH})Q<WoUTU%^%#
 aes
 security-profile name default-wds
 security-profile name default-mesh
 ssid-profile name default
 ssid-profile name wlan-net
 ssid wlan-net
 vap-profile name default
 vap-profile name wlan-net
 service-vlan vlan-id 101
 ssid-profile wlan-net
 security-profile wlan-net
 wds-profile name default
 mesh-handover-profile name default
 mesh-profile name default
 regulatory-domain-profile name default
 regulatory-domain-profile name domain1
 air-scan-profile name default
 rrm-profile name default
 rrm-profile name wlan-rrm
 uac reach-access-threshold hide-ssid
 band-steer balance gap-threshold 80
 uac client-snr enable
 uac client-snr threshold 13
 uac client-number enable
```

```
uac client-number threshold access 40 roam 40
band-steer balance start-threshold 90
sta-load-balance dynamic rssi-threshold -63
sta-load-balance dynamic sta-number start-threshold 12
sta-load-balance dynamic sta-number gap-threshold number 5
band-steer snr-threshold 18
radio-2g-profile name default
radio-2g-profile name wlan-2g
interference detect-enable
interference co-channel threshold 60
interference adjacent-channel threshold 60
rrm-profile wlan-rrm
interference station threshold 25
radio-5g-profile name default
radio-5g-profile name wlan-5g
interference detect-enable
interference co-channel threshold 60
interference adjacent-channel threshold 60
rrm-profile wlan-rrm
interference station threshold 25
wids-spoof-profile name default
wids-whitelist-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
ap-group name default
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
  radio-2g-profile wlan-2g
  vap-profile wlan-net wlan 1
radio 1
  radio-5g-profile wlan-5g
  vap-profile wlan-net wlan 1
  calibrate auto-bandwidth-select enable
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0
  ap-name AP1
  ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410
  ap-name AP2
  ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110
  ap-name AP3
  ap-group ap-group1
provision-ap
#
```



```
dot1x-access-profile name dot1x_access_profile
#
mac-access-profile name mac_access_profile
#
return
```

8.4.2 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 100 to 101
#
dhcp enable
#
interface Vlanif1
#
interface Vlanif100
 ip address 10.23.100.254 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.254 255.255.255.0
 dhcp select interface
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
return
```

8.4.3 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
return
```

8.5 思考题

射频调优方案中 2.4G 调优信道集默认为 1、6、11 信道。请思考：为什么选择 1、6、11 信道进作为 2.4G 调优信道集。

参考答案：

1、6、11 信道属于 2.4G 频段非重叠信道，可以避免信号干扰。

9 室内网络规划实验

9.1 实验介绍

9.1.1 关于本实验

本实验通过使用 WLAN Planner 对室内场景进行规划设计，满足客户的无线需求。

9.1.2 实验目的

- 掌握 WLAN 室内网络规划流程。
- 掌握 WLAN Planner 工具的基本操作。

9.1.3 实验场景介绍

某公司室内办公区拟建 WLAN 网络，该项目的建筑图纸如图 9-1 所示。为满足公司员工移动办公及访客上网需求，现对该公司进行（室内）网络设计规划，确保 WLAN 网络覆盖客户要求的所有区域，并满足业务需求。

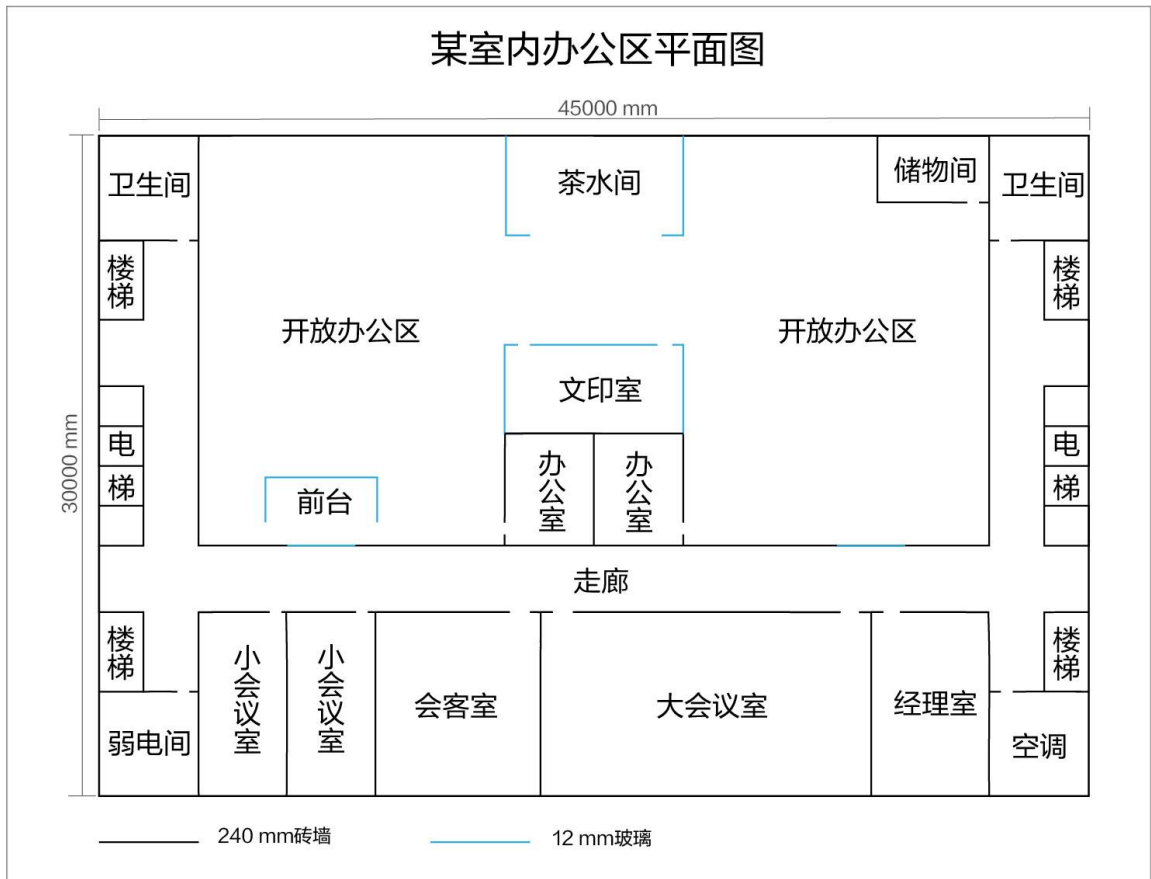


图9-1 WLAN 室内网规建筑图纸

9.1.4 前期准备工作

WLAN 网络前期规划主要分为需求收集和现场工勘两部分组成。

9.1.4.1 需求收集

需求收集阶段在 WLAN 网络规划是第一步，即在网络规划前与客户充分沟通，收集完整全面的项目和需求信息，减少因为前期了解的信息太少而出现重新设计的情况。

需求收集阶段所需获取的信息主要有基本需求、业务需求以及安装需求三大类，信息收集结果如下：

表9-1 基本需求收集 checklist

需求类型	收集结果
法律法规限制	国家码：CN
平面图纸	JPG比例图纸，建筑长度为45米
覆盖方式	室内放装

表9-2 业务需求收集 checklist

需求类型	收集结果
覆盖区域	重点覆盖区域：开放办公区、办公室、会议室、经理室 普通覆盖区域：走廊 无需覆盖区域：楼梯、卫生间、弱电间、储物间
场强要求	重点区域：≥ -65 dBm 普通区域：> -70 dBm
接入终端数	开放办公区：左右各40个工位，按照每个工位2终端考虑 大会议室：满座30人，每人1终端 小会议室：满座8人，每人1终端 会客室：满座12人，每人2终端 办公室、经理室：单人，最多不超过5终端
终端类型	笔记本、手机、Pad
带宽需求	开放办公区：4 Mbps；并发率：100% 会议室：8 Mbps；并发率：100% 会客室：16 Mbps；并发率：80% 办公室、经理室：16 Mbps；并发率：100%

表9-3 安装需求收集 checklist

需求类型	收集结果
配电方式	PoE交换机供电
交换机位置	左下角弱电间
特殊需求	无特殊需求

9.1.4.2 现场工勘

现场工勘的主要目的是获取现场的实际环境信息，如干扰源、障碍物衰减、楼层高度、新增障碍物和弱电井等信息，配合建筑图纸来确定 AP 选型、安装位置和方式、供电走线等设计。

表9-4 勘测结果

现场工勘采集项	勘测结果
确认图纸信息	客户提供的图纸与现场一致 楼层高度为2.6 m

	内部建筑中：桌、椅等高度正常，对信号干扰不大，可忽略
建筑材质及损耗	外层墙体为240 mm混凝土 会议室、办公室、会客室等墙体为240 mm加厚砖墙 茶水间、文印室、前台为12 mm加厚玻璃
确认干扰源	WLAN网络覆盖区域无干扰源
走线规则	交换机与AP之间网线均走天花板吊顶内部穿透，隐蔽走线，可打孔
交换机安装位置	弱电间与储物间均可放置
安装准入	已获取物业许可

9.2 实验任务配置

9.2.1 配置思路

- 1.根据现有信息，进行需求分析。
- 2.根据需求进行设备选型，并计算 AP 数量。
- 3.登录 WLAN Planner 平台，导入建筑图纸。
- 4.绘制环境、障碍物。
- 5.进行 AP 布放。
- 6.调整 AP 参数、天线角度。
- 7.进行交换机布放、线缆布放。
- 8.进行信号仿真。
- 9.调整 AP 位置，反复进行信号仿真，直到信号全面覆盖。
- 10.导出网规报告。

9.2.2 配置步骤

步骤 1 需求分析

根据前期的需求收集和现场工勘，分析出以下参数：

表9-5 网规需求分析表

参数类型	分析结果
国家码	CN

平面图纸	JPG比例图纸, 建筑长度为45米
覆盖方式	室内放装
带宽需求	开放办公区: 终端数160台; 单终端带宽需求4 Mbps; 并发率: 100% 大会议室: 终端数30台; 单终端带宽需求8 Mbps; 并发率: 100% 小会议室: 终端数8台; 单终端带宽需求8 Mbps; 并发率: 100% 会客室: 终端数24台; 单终端带宽需求16 Mbps; 并发率: 80% 办公室、经理室: 终端数5台; 16 Mbps; 并发率: 100%
覆盖区域	仅需覆盖一个楼层 重点覆盖区域: 一个会客室、两个开放办公区、三个会议室, 三个单人办公室 普通覆盖区域: 走廊
场强需求	重点覆盖区域: ≥ -65 dBm 普通覆盖区域: > -70 dBm 外泄场强: 无要求
终端类型	笔记本、手机、Pad, 支持2*2 MIMO, 5 GHz频宽支持40 MHz
供电方式	PoE交换机供电
安装方式	吸顶安装
交换机安装位置	放置左下角弱电间, PoE供电距离符合要求
客户验收项及标准	无特殊要求

步骤 2 设备选型、计算 AP 数量

结合室内场景业务占比统计表和单 AP 并发口径表, 计算出各个区域所需 AP 数量。

表9-6 室内场景业务占比统计表

业务类型	单业务基线速率 (Mbps)		室内场景下各业务占比			
	优秀	良好	开放办公区	会议室	单人办公室	会客室
4K视频	50	30	0%	2%	15%	10%
1080P视频	16	12	0%	8%	15%	10%
720P视频	8	4	0%	7%	15%	10%
电子白板无线投屏	32	16	0%	0%	0%	10%

电子邮件	32	16	6%	8%	10%	10%
网页浏览	8	4	21%	30%	20%	30%
游戏	2	1	8%	5%	10%	0%
即时通讯	0.512	0.256	35%	20%	10%	10%
VoIP (Voice)	0.256	0.128	30%	30%	5%	10%
单用户平均带宽 (Mbps) - 优秀			4	8	16	16

表9-7 单 AP 并发口径表

Wi-Fi 6 AP在满足不同用户接入带宽下的最大并发终端数 (2.4G@20 MHz 5G@40 MHz, 终端都支持Wi-Fi 6, 双空间流)				
序号	用户接入带宽	单射频 (5G) 最大并发终端数	双射频 (5G) 最大并发终端数	三射频 (2.4G+5G1+5G2) 最大并发终端数
1	2 Mbps	56	85	141
2	4 Mbps	39	56	95
3	6 Mbps	27	38	65
4	8 Mbps	21	30	51
5	16 Mbps	12	18	30

根据需求收集的信息, 计算出每个覆盖区域的最大并发终端数, 计算过程如下:

开放办公区左右各 40 个工位, 每个工位 2 个终端, 并发率为 100%, 则开放办公区总终端数量 = $40 * 2 * 2 * 100\% = 160$ 个终端。

大会议室满座 30 人, 每人 1 个终端, 并发率 100%, 则大会议室最大并发终端数量 = $30 * 1 * 100\% = 30$ 个终端。

小会议室满座 8 人, 每人 1 个终端, 并发率 100%, 则小会议室最大并发终端数量 = $8 * 1 * 100\% = 8$ 个终端。

会客室满座 12 人, 每人 2 个终端, 并发率 80%, 则会客室最大并发终端数量 = $12 * 2 * 80\% \approx 19$ 个终端。

单人办公室, 每人 5 个终端数, 并发率 100%, 则单人办公室最大并发终端数量 = $1 * 5 * 100\% = 5$ 个终端。

根据单 AP 并发口径表, 计算出每个覆盖区域所需 AP 数量, 计算公式为最大并发终端数量除以满足用户接入带宽下的单 AP 射频最大并发终端数, 计算过程如下:

开放办公区, 带宽需求为 4 Mbps, 对应双射频 AP 最大并发数为 56 台: $160/56 \approx 2$ (台)

大会议室，带宽需求为 8 Mbps，对应双射频 AP 最大并发数为 30 台： $30/30 = 1$ (台)

小会议室，带宽需求为 8 Mbps，对应双射频 AP 最大并发数为 30 台： $8/30 \approx 1$ (台)

会客室，带宽需求为 16 Mbps，对应双射频 AP 最大并发数为 18 台： $19/18 \approx 1$ (台)

单人办公室，带宽需求为 16 Mbps，对应双射频 AP 最大并发数为 18 台： $5/18 \approx 1$ (台)

步骤 3 登录 WLAN Planner 平台，新建项目

WLAN Planner 工具在企业服务工具云平台上，所有用户均可申请使用，链接如下：

<https://serviceturbo-cloud-cn.huawei.com/serviceturbocloud/#/toolsummary?entityId=d59de9ac-e4ef-409e-bbdc-eff3d0346b42>

#点击“运行”。



阅读客户网络数据安全管理规定后，点击确认。

客户网络数据安全规范V1.0 ×

一、目的

确保用户在ServiceTurbo Cloud上的相关操作遵从适用法律法规的要求，在客户数据提供者授权范围内使用客户数据并做好数据保护，基于《企业交付与服务网络安全与用户隐私保护管理规范》、《客户网络数据安全操作指导书》，在业务活动中遵从网络安全及隐私保护的相关规定。

二、适用范围

适用于使用ServiceTurbo Cloud（包括但不限于作业中心、工具/服务应用、知识中心、互动社区等）的用户，包括华为投资控股有限公司及其控股的所有关联公司（以下简称“华为”）的企业交付与服务业务领域的华为员工、租赁人员、外包人员，上述用户在业务操作过程中需遵循客户网络数据授权管理规定。

企业服务伙伴（以下简称“伙伴”）在使用ServiceTurbo Cloud时，如涉及获取、存储、使用和销毁客户网络数据的，伙伴及其员工需提前向数据所有者获取相关授权，并在授权的期限、范围内进行上述操作。华为作为平台方仅提供相关工具供伙伴对客户网络数据进行处理。伙伴需对平台上载、使用的客户网络数据的合法性与有效性负责，华为不承担因客户网络数据的合法性与有效性问题导致的任何责任。若因伙伴未获取合法授权、超出授权范围或伙伴其他原因导致华为损失的，伙伴需采取一切措施使华为免除责任，并赔偿华为因此遭受的所有损失。

三、法律声明

* 我已阅读并同意《客户网络数据安全规范》

确认

填写根据实际情况填写项目信息，之后勾选“我已阅读同意《法律声明》”，并点击确认。

项目信息 地区部、代表处/办事处、国家选项已屏蔽36个网络安全敏感国家的相关信息。 ×

项目类型：新建项目 已有项目

* 是否涉及客户网络数据： 是 否

* 作业凭证：项目编码 TD000000323701 ERP-PM

* 项目名称：Huawei

交付工程师：请输入完整的账号或邮箱

* 客户名称：HCIP-WLAN Q

* 项目经理：请输入完整的账号或邮箱

* 国家/地区：中国

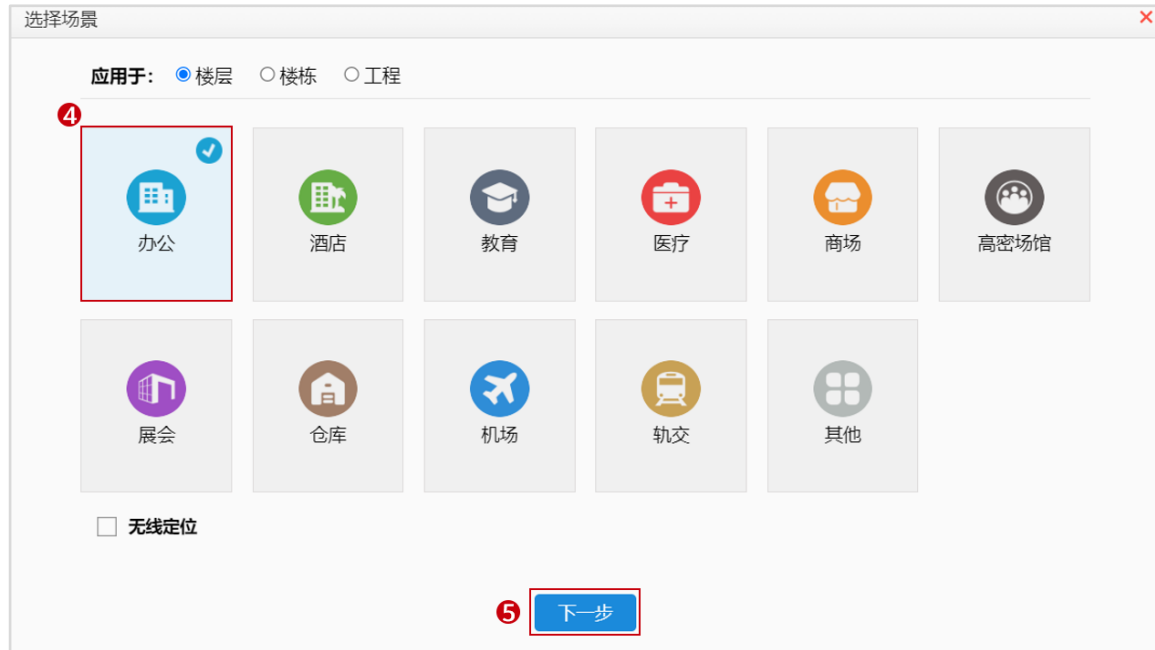
* 我已阅读并同意《法律声明》

步骤 4 创建楼层，导入图纸

创建楼层，导入图纸，选择室内场景，并输入楼栋名称；点击“选择文件”导入对应图纸。



选择 WLAN 场景，本项目为办公场景，点击下一步。



可基于内置好的建网标准来设定，本项目自行决定标准，选择“其他”，然后点击“确定”。

选择场景

应用于: 楼层 楼栋 工程

选择子场景

办公区-精品 (100Mbps@Everywh... 办公区-常规 (50Mbps@Everywher... 会议室-精品 (100Mbps@Everywh...

会议室-常规 (50Mbps@Everywher... 咖啡厅-精品 (50Mbps@Everywher... 咖啡厅-常规 (32Mbps@Everywher...

展厅-精品 (50Mbps@Everywhere) 展厅-常规 (50Mbps@Everywhere) 食堂-精品 (50Mbps@Everywhere)

食堂-常规 (16Mbps@Everywhere) 其他

上一步 确定

选择需要导入的图纸文件，点击确定。

新建

* 类型: 室内 室外

* 楼栋名称: HCIP-WLAN室内

批量导入: 选择文件

详细信息: HCIP-WLAN室内图纸

1.选择文件时，推荐导入图纸的大小在200MB以内。
2.图纸名称目前仅支持中英文、数字和部分特殊字符。

8 确定 取消

步骤 5 环境设置

根据客户需求收集 checklist 表和工勘信息进行环境及区域设置。

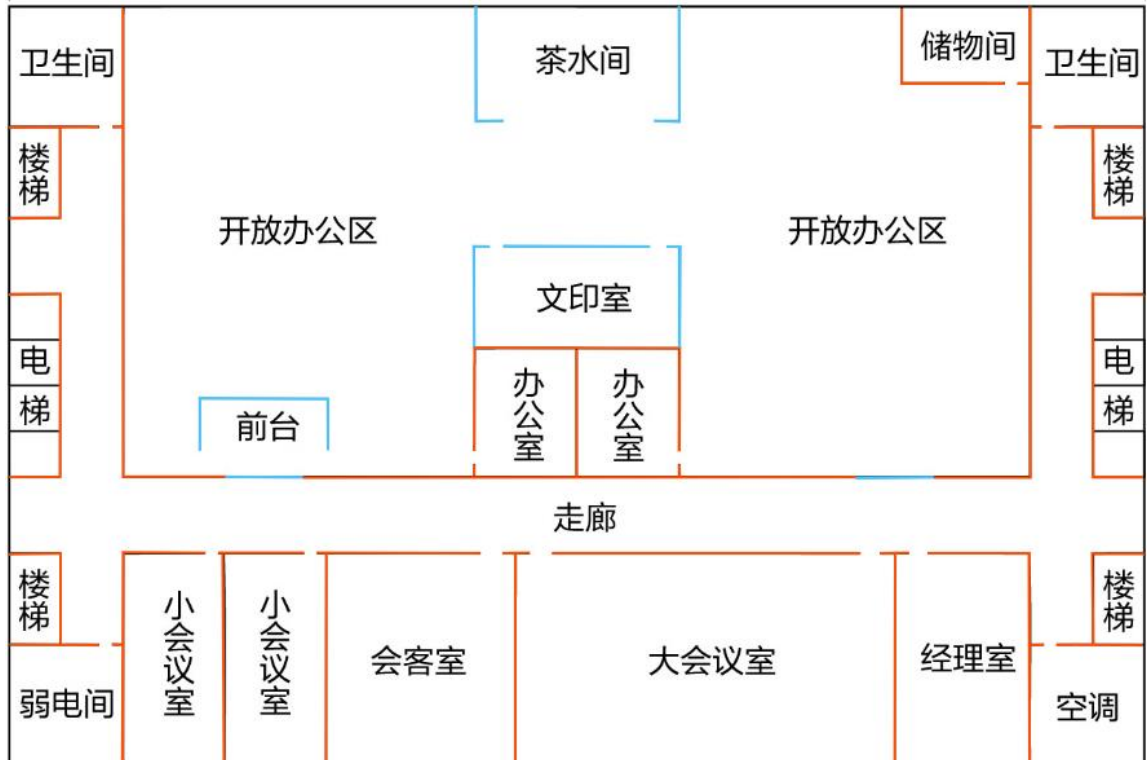
#设置比例尺。



图纸宽度为 45 米，在图纸上选择任意位置，水平从左到右拉直设置比例尺长度为 45 米。

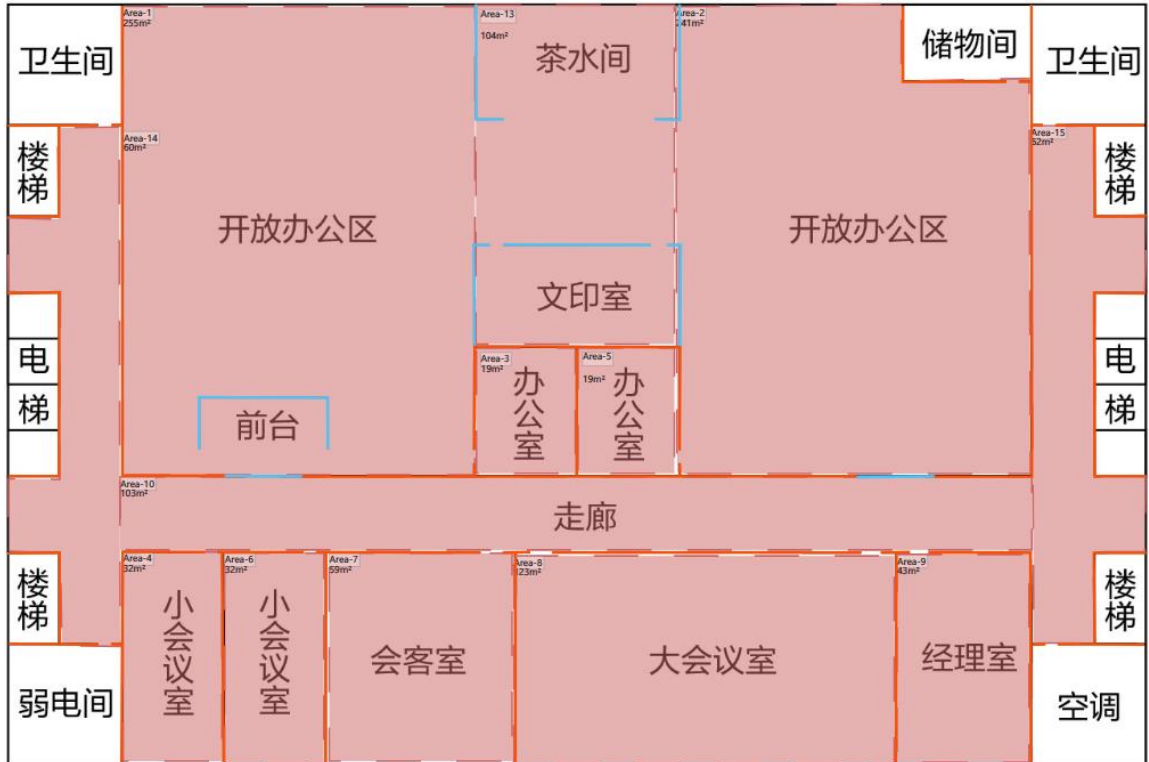


绘制障碍物，图纸边框使用绝缘边界绘制，室内墙体用 240 mm 加厚砖墙绘制，茶水间、前台和文印室使用 12 mm 加厚玻璃绘制，最终效果如下所示。



步骤 6 区域设置

根据客户要求框选出重要覆盖区域和普通覆盖区域，效果如下所示。



设置重点覆盖区域。

设置开放办公室，两个开放办公室参数一致。

基本属性

区域:

区域类型选择:

覆盖类型:

并发率(%):

终端情况

总带宽需求 320Mbps * 100%

<input type="text" value="40"/>	<input type="text" value="笔记本 (2*2)"/>	<input type="button" value="删除"/>
<input type="text" value="40"/>	<input type="text" value="智能手机 (2*2)"/>	<input type="button" value="删除"/>

设置小会议室（8 终端）和大会议室（30 终端）。

基本属性

区域:
Area-4

区域类型选择:
覆盖区域

覆盖类型:
普通覆盖($\geq -65\text{dBm}$)

并发率(%):
100

终端情况

总带宽需求 64Mbps * 100%

8 笔记本 (2*2) 删除

720P视频 (8Mbps) 删除

+

删除区域

基本属性

区域:
Area-8

区域类型选择:
覆盖区域

覆盖类型:
普通覆盖($\geq -65\text{dBm}$)

并发率(%):
100

终端情况

总带宽需求 240Mbps * 100%

30 笔记本 (2*2) 删除

720P视频 (8Mbps) 删除

+

删除区域

设置会客室。

基本属性

区域:

区域类型选择:

覆盖类型:

并发率(%):

终端情况

总带宽需求 384Mbps * 80%

<input type="text" value="12"/>	<input type="text" value="笔记本 (2*2)"/>	<input type="button" value="删除"/>
<input type="text" value="12"/>	<input type="text" value="智能手机 (2*2)"/>	<input type="button" value="删除"/>

+

设置单人办公室。

基本属性

区域:

区域类型选择:

覆盖类型:

并发率(%):

终端情况

总带宽需求 80Mbps * 100%

<input type="text" value="2"/>	<input type="text" value="笔记本 (2*2)"/>	<input type="text" value="删除"/>
<input type="text" value="1080P视频 (16Mbps)"/>		<input type="text" value="删除"/>
<input type="text" value="3"/>	<input type="text" value="智能手机 (2*2)"/>	<input type="text" value="删除"/>
<input type="text" value="1080P视频 (16Mbps)"/>		<input type="text" value="删除"/>

设置普通覆盖区域。

设置走廊。

基本属性

区域:

区域类型选择:

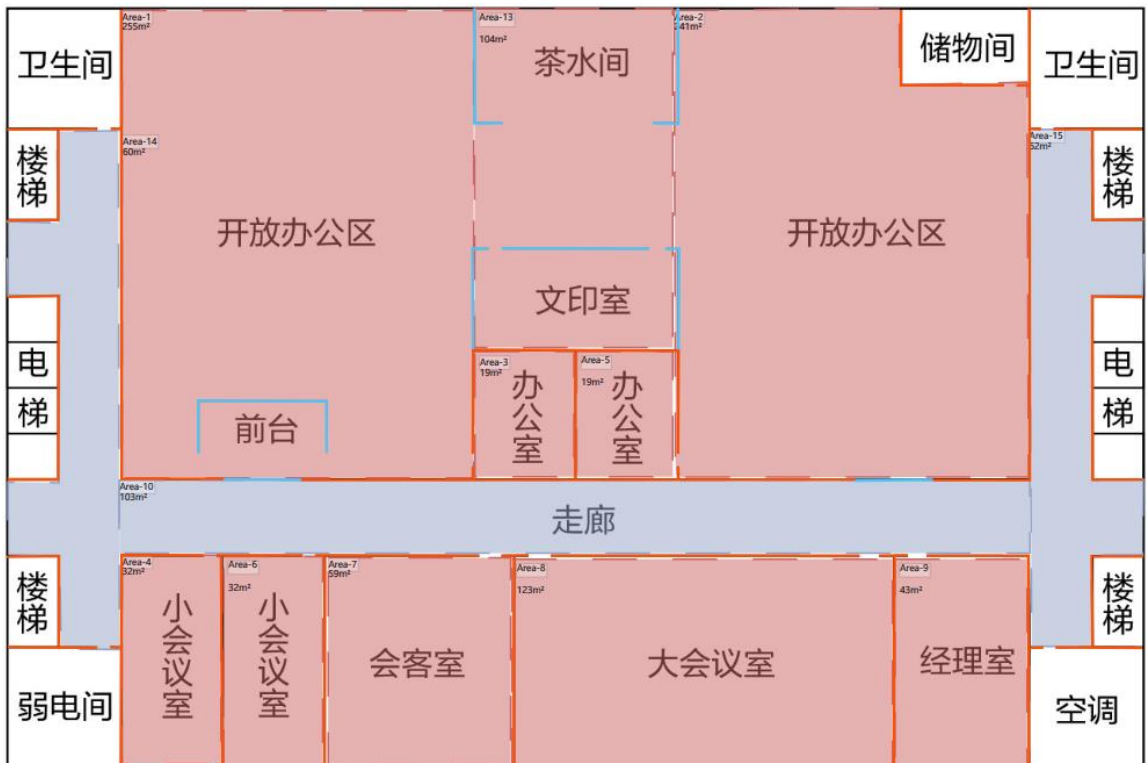
覆盖类型:

并发率(%):

终端情况

总带宽需求 40Mbps * 30%

查看完成基本属性设置后的区域。



步骤 7 AP 布放, 调整 AP 参数

#AP 布放可以手动逐一布放, 也可自动布放后手动调整 AP 数量和位置。



由于该项目仅有一层建筑, 选择“当前层”, 点击下一步。



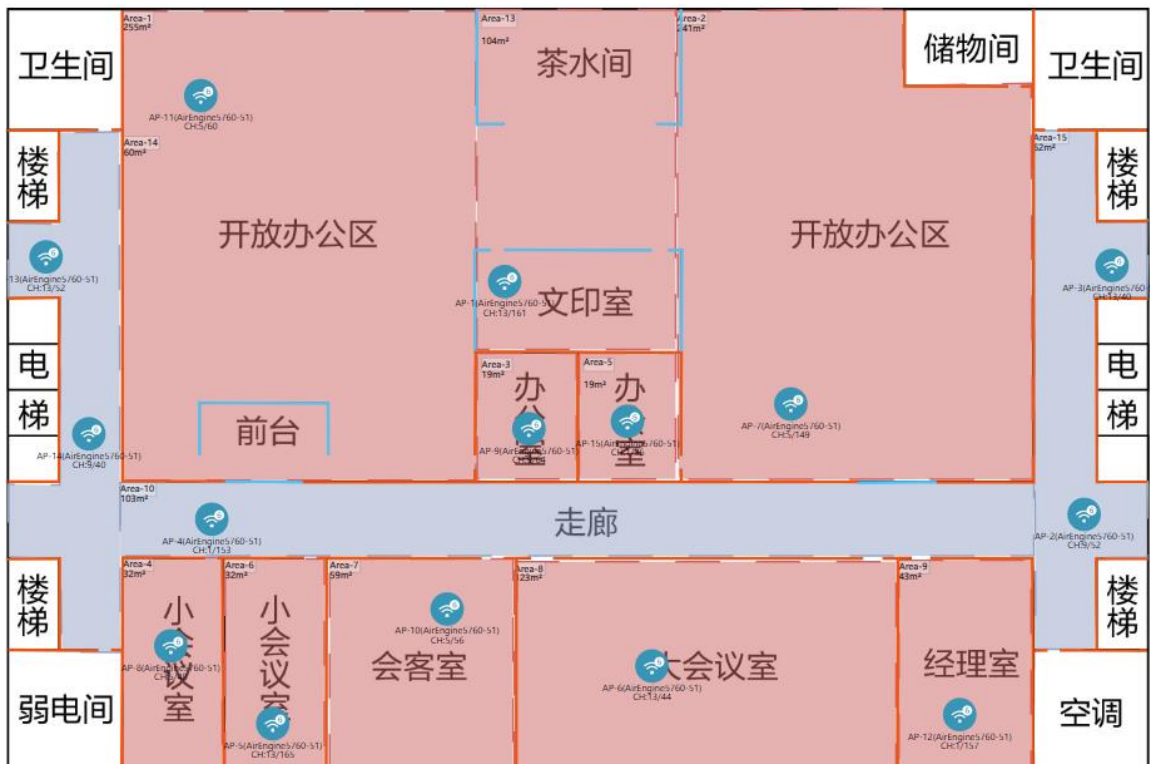
选择需要的 AP 型号，本项目使用 AirEngine5760-51。

设置信道参数。

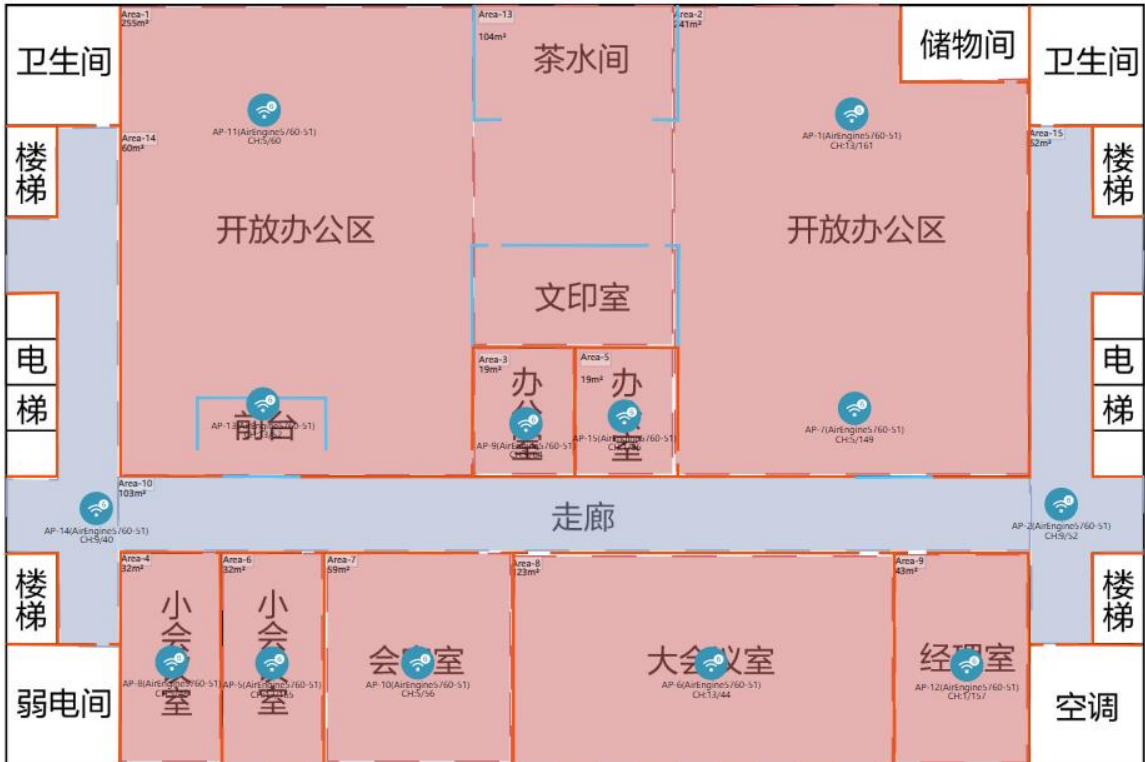
设置功率。



自动布放后，效果如下所示。

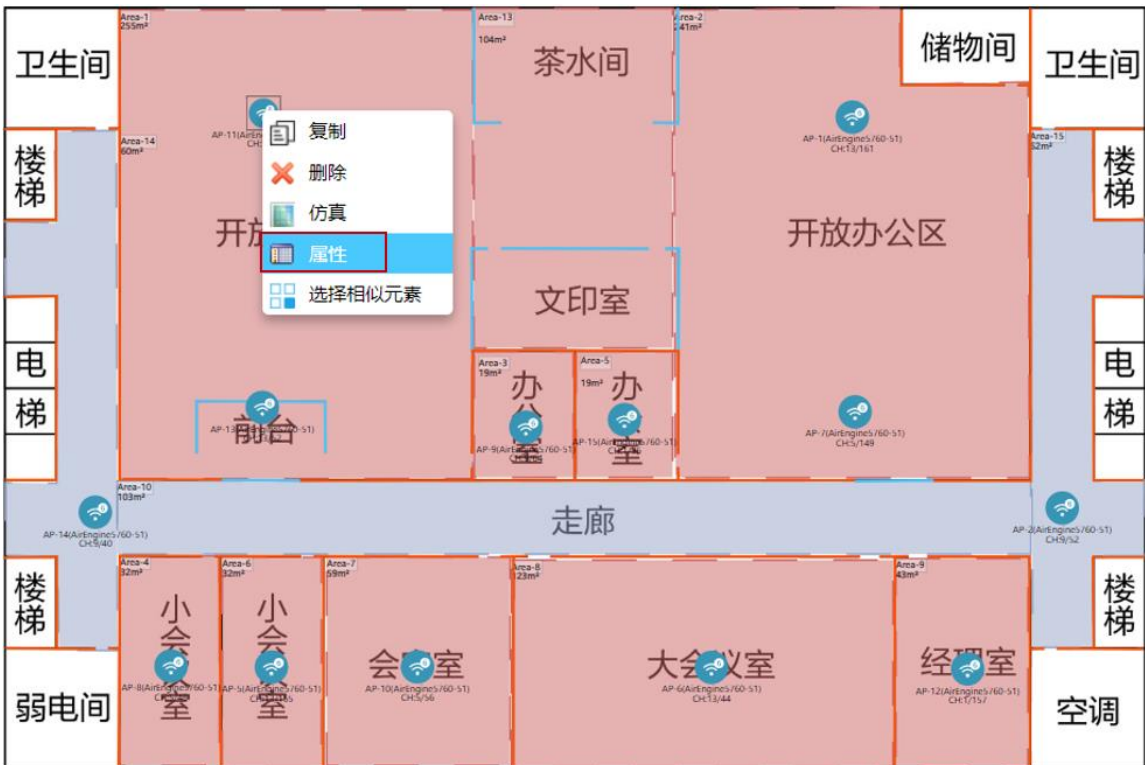


手动调整 AP 数量和位置后，最终效果如下所示。

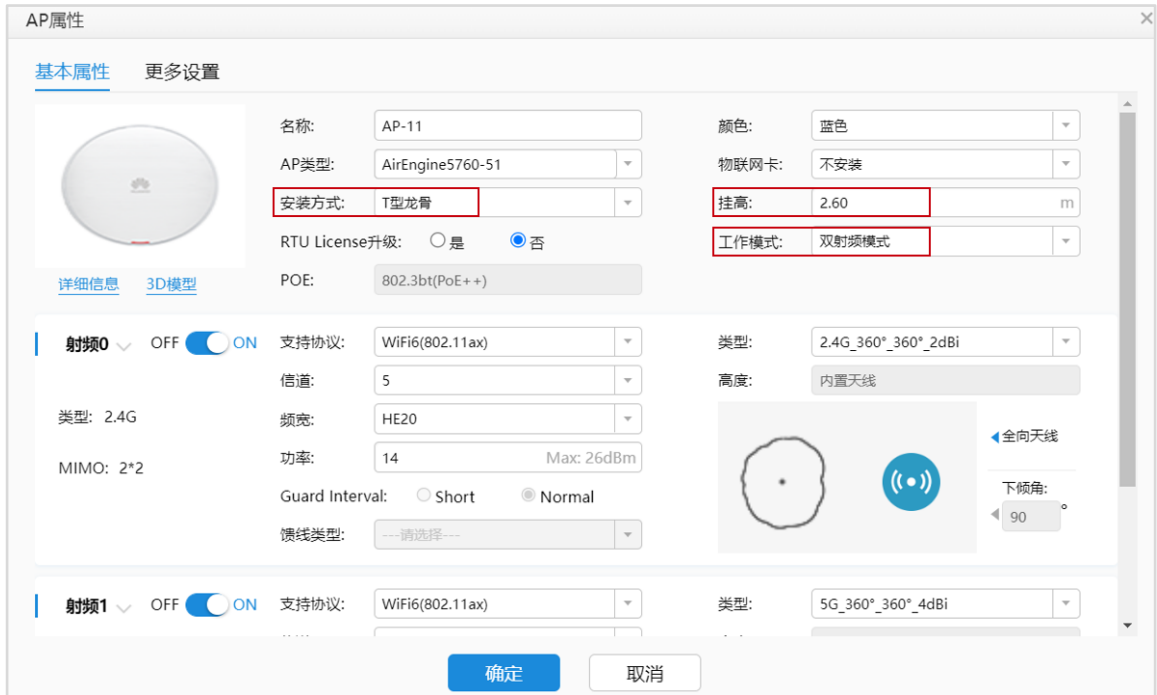


AP 参数调整。

选择活动区域 AP，右击选择“属性”（可以框选全部 AP，再右击设置），打开 AP 属性页面。



因客户要求 AP 吸顶部部署，则安装方式保持默认“T 型龙骨”即可，挂高为“2.6 m”，工作模式为“双射频模式”，其他参数保持默认，其他区域 AP 的属性配置一致，不再赘述。

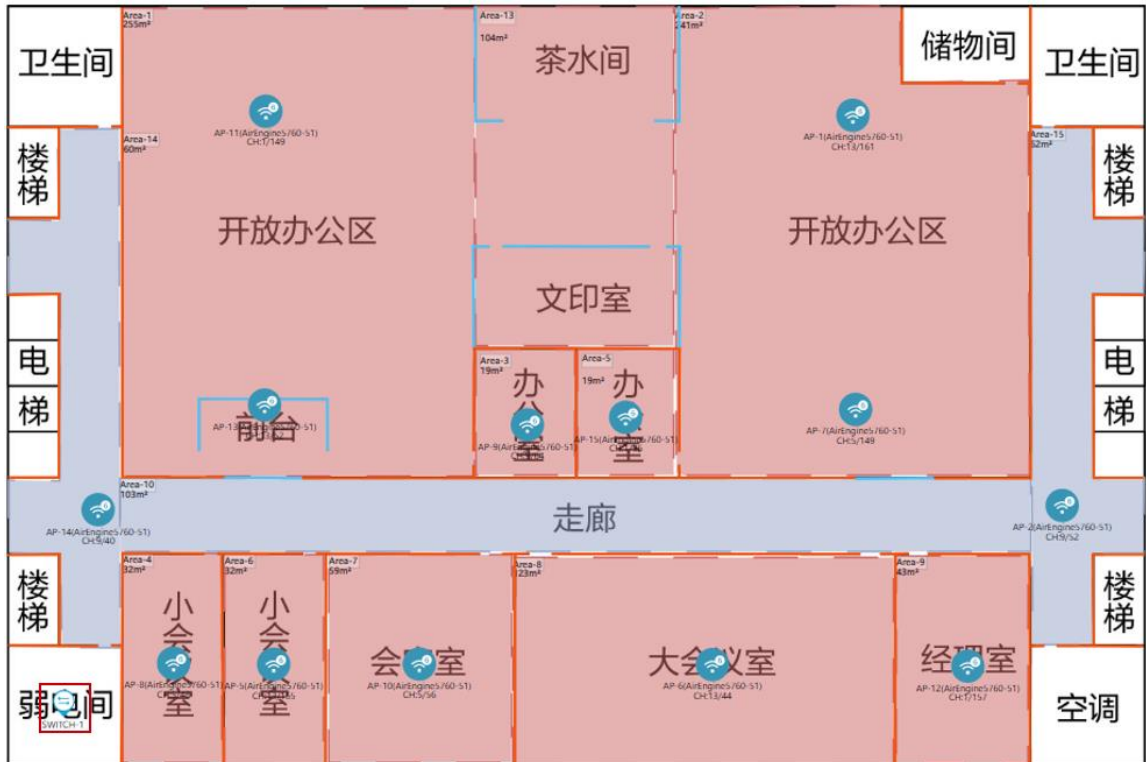


步骤 8 交换机摆放

选择交换机型号，本项目使用 S5731-S24P4X 交换机。

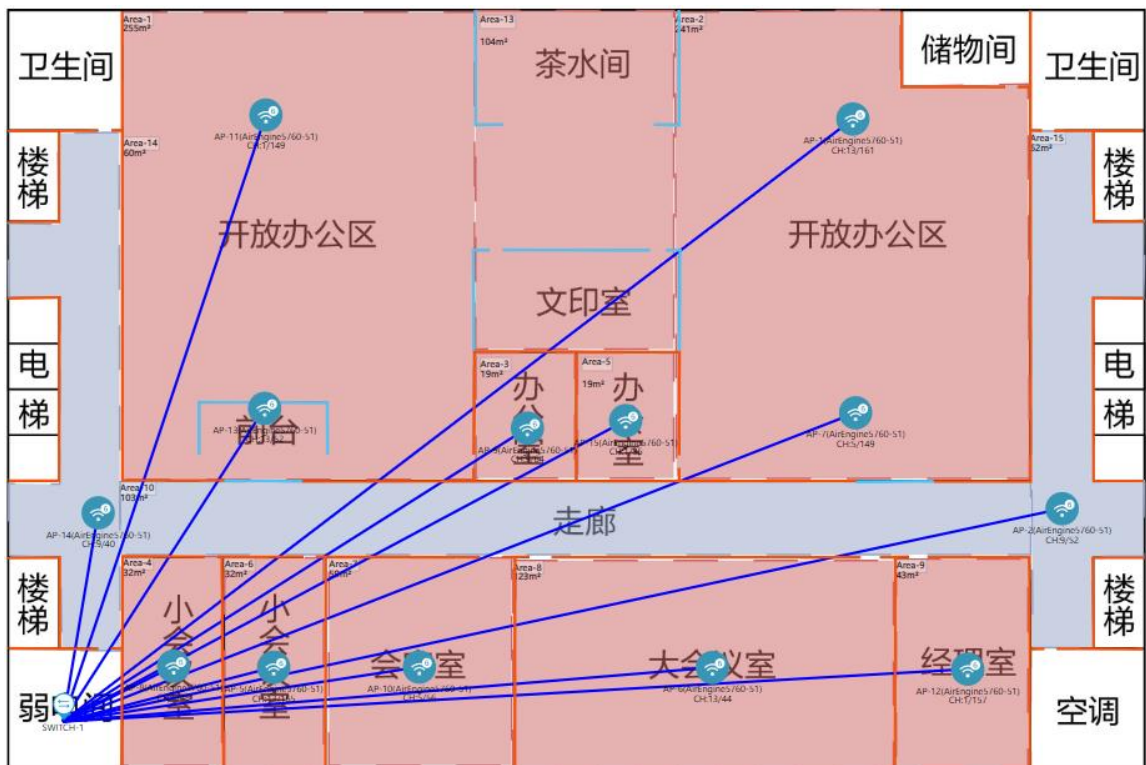


直接在左下角弱电间部署交换机即可。



步骤 9 线缆布放

由于现场可以使用吊顶来部署线缆，AP 与交换机之间的线缆可以直连。



步骤 10 信号仿真

查看重点覆盖区域，即信号强度大于-65 dBm 区域的覆盖情况，如果出现没有颜色的区域，则表示信号强度低于-65 dBm。

将仿真图示意中的信号强度调整为-65 dBm，随后点击“打开仿真图”。



本项目只需关注开放办公区、办公室、会议室以及会客室的信号覆盖情况。



查看普通覆盖区域，及信号强度小于 70 dBm 区域的覆盖情况，如果出现没有颜色的区域，则表示信号强度低于-70 dBm。

将仿真图示意中的信号强度调整为-70 dBm 即可。

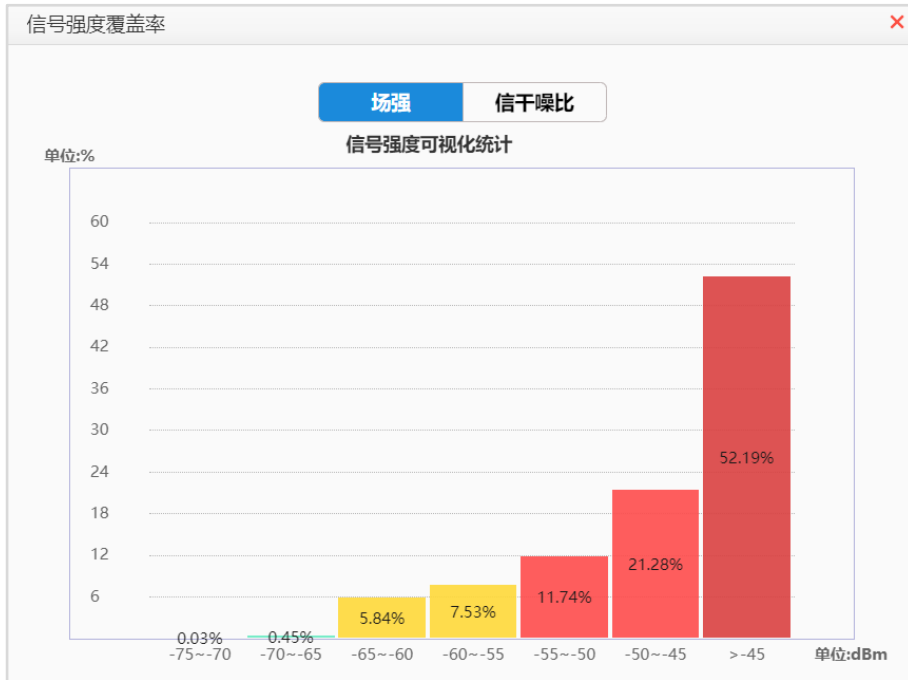


本项目只需关注走廊的信号覆盖情况。



如果发现信号覆盖不良，可以反复调整 AP 位置和数量，确保信号仿真没有问题。

查看覆盖满足度，可以查看是否有信号覆盖不良区域。



可以看到大部分区域的信号覆盖情况良好。

步骤 11 导出网规报告

在导出网规报告前，可以先进行网规检视。

1.环境设置 2.区域设置 3.设备布放 4.信号仿真 5.导出报告

网规报告 物料清单 漫游报告

报告内容

语言 中文 英文 楼层排序方式 升序 降序

方案设计满足度: 自定义Logo: 上传Logo 公司名称:

热图设置

统一配色: 是否包含障碍物: 是 否

频段: 2.4G 5G 6G

热图: 场强仿真图 信干噪比仿真图 物理层吞吐率仿真图 应用层吞吐率仿真图
 弱场强仿真图 建网标准达成度 终端定位热图 覆盖满足度

热图清晰度: 标清(不超过0.97M) 高清(原图分辨率不足) 超清(原图分辨率不足)

网规检视 导出

网规自动检视

环境设置	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> 障碍物设置: 检查是否有图纸（所有场景，室内室外GIS等）没有绘制障碍物。 <input checked="" type="checkbox"/> 障碍物类型: 检查是否有图纸（所有场景，室内室外GIS等）只绘制了一种障碍物。
设备布放	<input checked="" type="checkbox"/> AP布放过近: 检查AP间距，如果有小于8m（26.25英尺），并且AP间没有障碍物。
AP设置	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> 功率调优: 以楼层/室外区域维度查询AP功率是否均为默认功率。 <input checked="" type="checkbox"/> 信道设置: 以楼层/室外区域维度查询AP信道是否均为默认信道。
天线设置	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> 天线款式: 查询室外外接天线的AP是否连接了非推荐的室外覆盖天线款式。 <input checked="" type="checkbox"/> 角度设置: 查询单个AP维度下倾角&方位角是否是默认角度。
交付效果	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> 覆盖满足度: 覆盖满足度是否大于95%。 <input checked="" type="checkbox"/> 容量满足度: 容量满足度是否大于90%。 <input checked="" type="checkbox"/> 建网标准达成度: 建网标准达成度是否大于95%。 <input checked="" type="checkbox"/> 精品网AP选型策略: AP是否满足至少4T4R要求。
场景化	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> 定位场景: 1.定位AP间距是否满足小于等于15米。 2.定位AP之间是否构成等三角形形状。 3.定位AP与障碍物间距是否满足大于等于2米。 4.定位区域是否满足任意一点都有三个定位AP覆盖信号大于-65dB...

2 开始检视 导出报告

查看是否没有问题，若出现警告项，需自行确认，没有问题后可导出网规报告。

网规自动检视

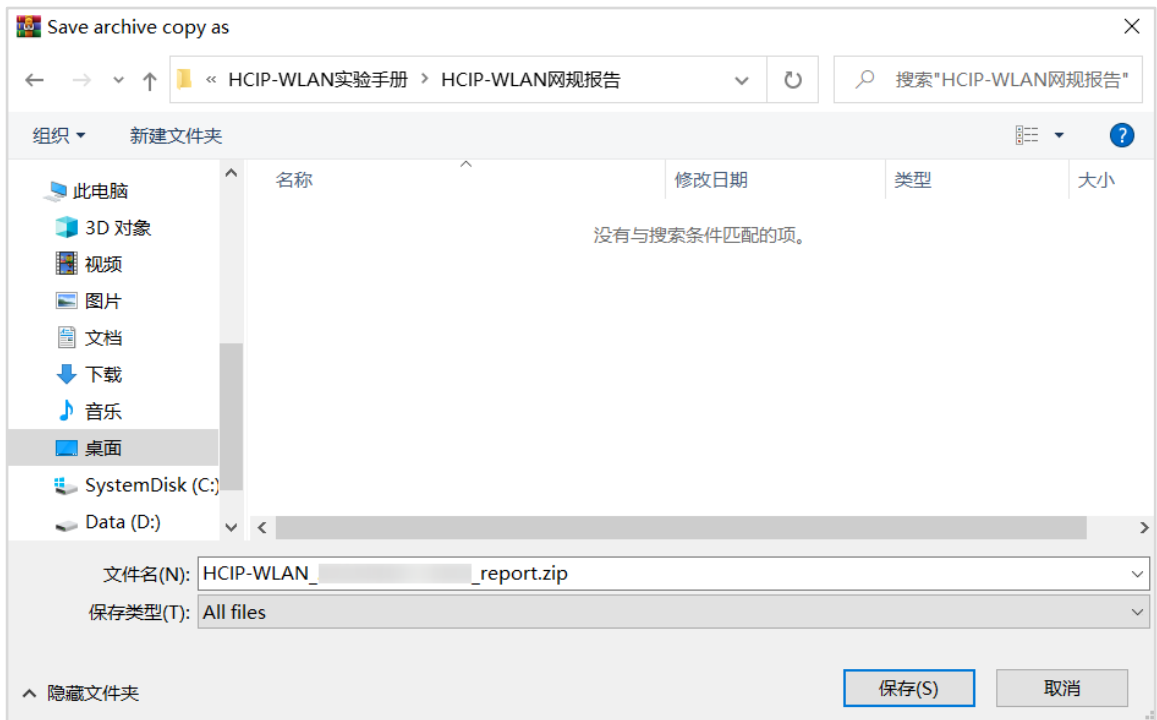
环境设置	<ul style="list-style-type: none"> ● 障碍物设置: 检查是否有图纸（所有场景，室内室外GIS等）没有绘制障碍物。 ✓ ● 障碍物类型: 检查是否有图纸（所有场景，室内室外GIS等）只绘制了一种障碍物。 ✓
设备布放	● AP布放过近: 检查AP间距，如果有小于8m（26.25英尺），并且AP间没有障碍物。 ✓
AP设置	<ul style="list-style-type: none"> ● 功率调优: 以楼层/室外区域维度查询AP功率是否均为默认功率。 ✓ ● 信道设置: 以楼层/室外区域维度查询AP信道是否均为默认信道。 ✓
天线设置	<ul style="list-style-type: none"> ● 天线款式: 查询室外外接天线的AP是否连接了非推荐的室外覆盖天线款式。 ✓ ● 角度设置: 查询单个AP维度下倾角&方位角是否是默认角度。 ✓
交付效果	<ul style="list-style-type: none"> ● 覆盖满足度: 覆盖满足度是否大于95%。 ✓ ● 容量满足度: 容量满足度是否大于90%。 ✓ ● 建网标准达成度: 建网标准达成度是否大于95%。 ✓ ● 精品网AP选型策略: AP是否满足至少4T4R要求。 ✓
场景化	<ul style="list-style-type: none"> ● 定位场景: 1.定位AP间距是否满足小于等于15米。 2.定位AP之间是否构成等三角形形状。 ✓ 3.定位AP与障碍物间距是否满足大于等于2米。 4.定位区域是否满足任意一点都有三个定位AP覆盖信号大于-65dB...

重新检视
3 导出报告

导出报告。



保存至本地。



#查看保存的网规报告。



9.3 思考题

1.网规设计一开始的需求收集需要确认哪些信息？

参考答案：

- (1) 法规限制：EIRP 限制和可用信道；
- (2) 图纸信息：图纸完整性；
- (3) 覆盖区域：重点区域、普通区域、无需覆盖区域；
- (4) 场强要求：对信号的强度要求；
- (5) 接入终端数：覆盖区域内的接入终端总数；

- (6) 终端类型;
- (7) 带宽要求;
- (8) 墙体类型: 预估墙体的信号衰减, 判断是否适合做穿透覆盖;
- (9) 配电方式;
- (10) 交换机位置;
- (11) 有无定位、物联网等特殊需求。

2. 某开放办公区有 120 个工位, 如果每个工位有 2 个终端, 现在要求按照 70%的并发满足每个终端 4 Mbps 带宽上网需求, 总共需要布放多少 AP?

参考答案:

接入终端数: $120 * 2 = 240$ (个)

并发终端数: $240 * 70\% = 168$ (个)

参考本实验中的单 AP 并发口径表, 计算得出: 所需 AP 数量为: $168 / 56 = 3$ (台)

10 室外网络规划实验

10.1 实验介绍

10.1.1 关于本实验

本实验通过使用 WLAN Planner 对室外场景进行规划设计，满足客户的无线需求。

10.1.2 实验目的

- 掌握 WLAN 室外网络规划流程。
- 掌握 WLAN Planner 工具的基本操作。

10.1.3 实验场景介绍

某步行街有一广场因人流量较高，现打算在广场周边部署室外无线网络，为在该区域驻足的行人提供免费的 Wi-Fi，从而增加客流量。

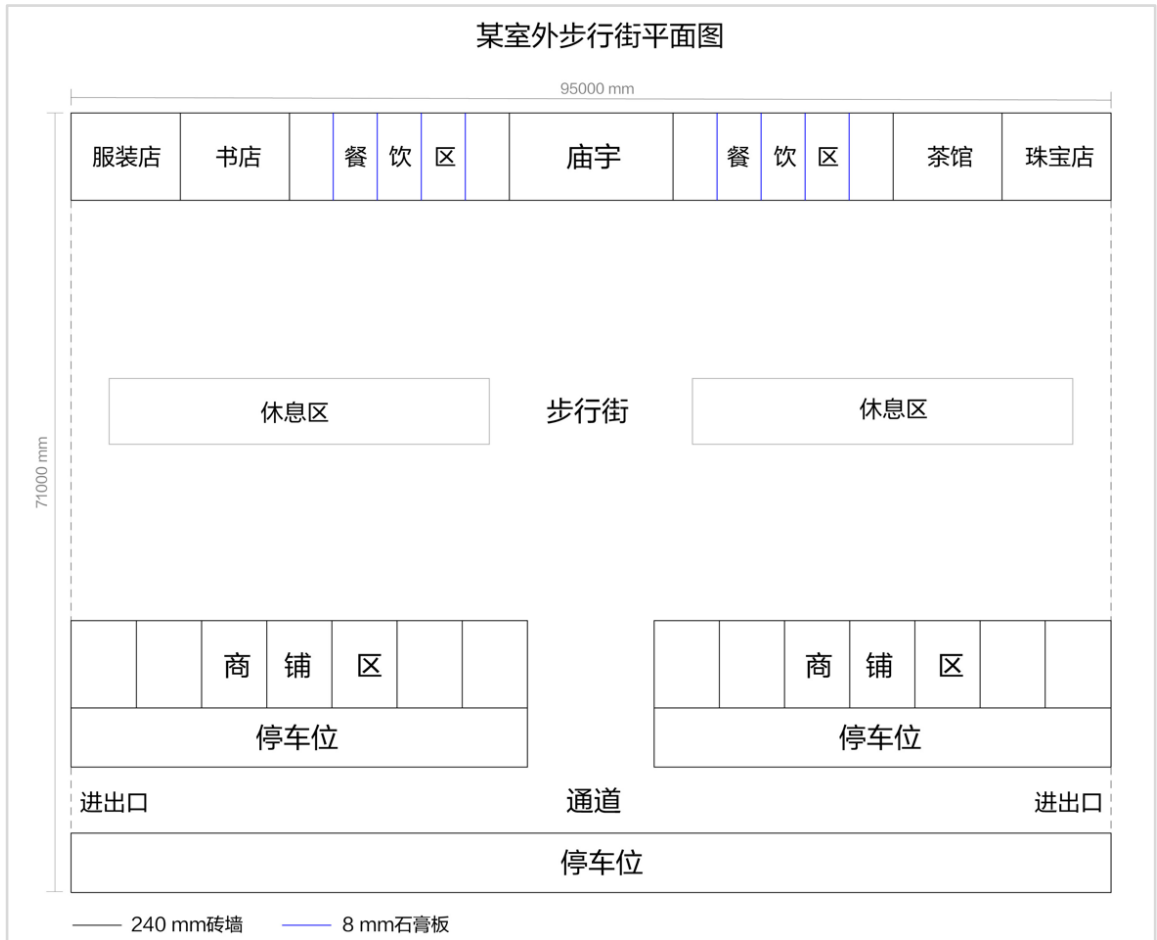


图10-1 WLAN 室外（步行街）网规建筑图纸

10.1.4 前期准备工作

WLAN 网络前期规划主要分为需求收集和现场工勘两部分组成。

10.1.4.1 需求收集

需求收集阶段在 WLAN 网络规划是第一步，即在网络规划前与客户充分沟通，收集完整全面的项目和需求信息，减少因为前期了解的信息太少而出现重新设计的情况。

需求收集阶段所需获取的信息主要有基本需求、业务需求以及安装需求三大类，信息收集结果如下：

表10-1 基本需求收集 checklist

需求类型	收集结果
法律法规限制	国家码：CN
平面图纸	JPG比例图纸，建筑长度为95米
覆盖方式	室外安装

表10-2 业务需求收集 checklist

需求类型	收集结果
覆盖区域	重点覆盖区域：商铺中间街道、休息区 普通覆盖区域：停车场 无需覆盖区域：商铺
场强要求	重点区域：≥ -65 dBm 普通区域：> -70 dBm
接入终端数	高峰期300人，每人1终端
终端类型	手机、Pad
带宽需求	每用户带宽需求：4 Mbps；并发率：60%

表10-3 安装需求收集 checklist

需求类型	收集结果
配电方式	PoE交换机供电
交换机位置	左边商铺区内部机房
特殊需求	无特殊需求

10.1.4.2 现场工勘

现场工勘的主要目的是获取现场的实际环境信息，如干扰源、障碍物衰减、楼层高度、新增障碍物和弱电井等信息，配合建筑图纸来确定 AP 选型、安装位置和方式、供电走线等设计

表10-4 勘测结果

现场工勘采集项	勘测结果
确认图纸信息	客户提供的图纸与现场一致 商铺高度为5 m
建筑材质及损耗	商铺外墙为240 mm加厚砖墙 餐饮区隔墙为8 mm石膏板 现场绿植均为半人高的绿化带，对信号干扰不大，可忽略
确认干扰源	WLAN网络覆盖区域无干扰源
AP安装方式	靠近商铺安装的AP可采用壁挂方式，安装在停车位的AP可采用抱杆安装

安装准入	已获取物业许可
------	---------

10.2 实验任务配置

10.2.1 配置思路

- 1.根据现有信息，进行需求分析。
- 2.根据需求进行设备选型，并计算 AP 数量。
- 3.登录 WLAN Planner 平台，导入建筑图纸。
- 4.绘制环境、障碍物。
- 5.AP 布放。
- 6.调整 AP 参数、天线角度。
- 7.信号仿真。
- 8.调整 AP 位置，反复进行信号仿真，直到信号全面覆盖。
- 9.导出网规报告。

10.2.2 配置步骤

步骤 1 需求分析

根据前期的需求收集和现场工勘，分析出以下参数：

表10-5 网规需求分析表

参数类型	分析结果
国家码	CN
平面图纸	JPG比例图纸，建筑长度为95米
覆盖方式	室外安装
带宽需求	商铺中间街道、休息区高峰期：终端数300台；4 Mbps；并发率：60%
覆盖区域	重点覆盖区域：商铺中间街道、休息区 普通覆盖区域：停车场 无需覆盖区域：商铺
场强需求	重点覆盖区域：≥ -65 dBm 普通覆盖区域：> -70 dBm

	外泄场强：无要求
终端类型	手机、Pad，支持2*2 MIMO，5 GHz频宽支持40 MHz
供电方式	壁挂AP可采用PoE交换机供电，抱杆AP可采用PoE适配器供电
安装方式	壁挂安装、抱杆安装
交换机安装位置	结合现场实际情况，与物业确定安装位置
客户验收项及标准	无特殊要求

步骤 2 设备选型、计算 AP 数量

结合室外场景业务占比统计表和单 AP 并发口径表，计算出各个区域所需 AP 数量。

表10-6 室外场景业务占比统计表

业务类型	单业务基线速率 (Mbps)		室外场景下各业务占比		
	优秀	良好	广场	街道	室外停车场
网页浏览	8	4	50%	60%	35%
流媒体 (1080P)	16	12	10%	10%	20%
VoIP	0.25	0.125	10%	10%	0%
游戏	2	1	10%	0%	30%
即时通讯	0.5	0.25	20%	20%	15%
单用户平均带宽 (Mbps) - 优秀			6	8	8

表10-7 单 AP 并发口径表

Wi-Fi 6 AP在满足不同用户接入带宽下的最大并发终端数 (2.4G@20 MHz 5G@40 MHz，终端都支持Wi-Fi 6，双空间流)				
序号	用户接入带宽	单射频 (5G) 最大并发终端数	双射频 (5G) 最大并发终端数	三射频 (2.4G+5G1+5G2) 最大并发终端数
1	2 Mbps	56	85	141
2	4 Mbps	39	56	95
3	6 Mbps	27	38	65
4	8 Mbps	21	30	51

5	16 Mbps	12	18	30
---	---------	----	----	----

根据需求收集的信息，计算出覆盖区域的最大并发终端数，计算过程如下：

步行街高峰期 300 人，每人 1 个终端，并发率为 60%，则步行街场景总终端数量 = $300 * 1 * 60\% = 180$ 个终端。

根据单 AP 并发口径表，计算出覆盖区域所需 AP 数量，计算公式为最大并发终端数量除以满足用户接入带宽下的单 AP 射频最大并发终端数，计算过程如下：

步行街场景，带宽需求为 4 Mbps，对应双射频 AP 最大并发数为 56 台： $300/18 \approx 5$ (台)

步骤 3 登录 WLAN Planner 平台，新建项目

WLAN Planner 工具在企业服务工具云平台上，任意用户均可申请使用，链接如下：

<https://serviceturbo-cloud-cn.huawei.com/serviceturbocloud/#/toolssummary?entityId=d59de9ac-e4ef-409e-bbdc-eff3d0346b42>

点击“运行”。



阅读客户网络数据安全规定后，点击确认。

客户网络数据安全规范V1.0 ×

一、目的

确保用户在ServiceTurbo Cloud上的相关操作遵从适用法律法规的要求，在客户数据提供者授权范围内使用客户数据并做好数据保护，基于《企业交付与服务网络安全与用户隐私保护管理规范》、《客户网络数据安全操作指导书》，在业务活动中遵从网络安全及隐私保护的相关规定。

二、适用范围

适用于使用ServiceTurbo Cloud（包括但不限于作业中心、工具/服务应用、知识中心、互动社区等）的用户，包括华为投资控股有限公司及其控股的所有关联公司（以下简称“华为”）的企业交付与服务业务领域的华为员工、租赁人员、外包人员，上述用户在业务操作过程中需遵循客户网络数据授权管理规定。

企业服务伙伴（以下简称“伙伴”）在使用ServiceTurbo Cloud时，如涉及获取、存储、使用和销毁客户网络数据的，伙伴及其员工需提前向数据所有者获取相关授权，并在授权的期限、范围内进行上述操作。华为作为平台方仅提供相关工具供伙伴对客户网络数据进行处理。伙伴需对平台上载、使用的客户网络数据的合法性与有效性负责，华为不承担因客户网络数据的合法性与有效性问题导致的任何责任。若因伙伴未获取合法授权、超出授权范围或伙伴其他原因导致华为损失的，伙伴需采取一切措施使华为免除责任，并赔偿华为因此遭受的所有损失。

三、法律声明

* 我已阅读并同意《客户网络数据安全规范》

确认

填写根据实际情况填写项目信息，之后勾选“我已阅读同意《法律声明》”，并点击确认。

项目信息 地区部、代表处/办事处、国家选项已屏蔽36个网络安全敏感国家的相关信息。 ×

项目类型：新建项目 已有项目

* 是否涉及客户网络数据： 是 否

* 作业凭证：项目编码 TD000000323701 ERP-PM

* 项目名称：Huawei

交付工程师：请输入完整的账号或邮箱

* 客户名称：HCIP-WLAN Q

* 项目经理：请输入完整的账号或邮箱

* 国家/地区：中国

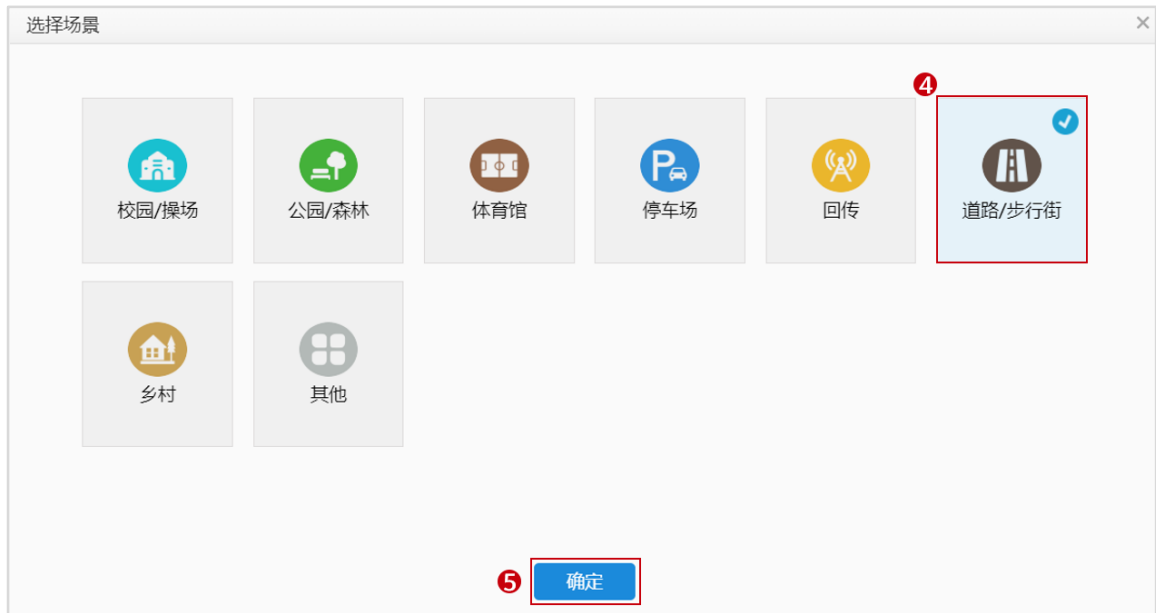
* 我已阅读并同意《法律声明》

步骤 4 新增区域，导入图纸

新增区域，导入图纸，选择室外场景，并输入区域名称；然后点击“选择场景”。



选择 WLAN 场景，本项目为“道路/步行街”场景，点击下一步。



选择需要导入的图纸文件，点击确定。

新建 ×

* 类型: 室内 室外

* 区域名称:

* 选择场景: 道路/步行街

室外类型:

楼层地图: ⑥ HCL...jpg

预览:



1.选择文件时，推荐导入图纸的大小在200MB以内。
2.图纸名称目前仅支持中英文、数字和部分特殊字符。

⑦

步骤 5 环境设置

根据客户需求收集 checklist 表和工勘信息进行环境及区域设置。

设置比例尺。



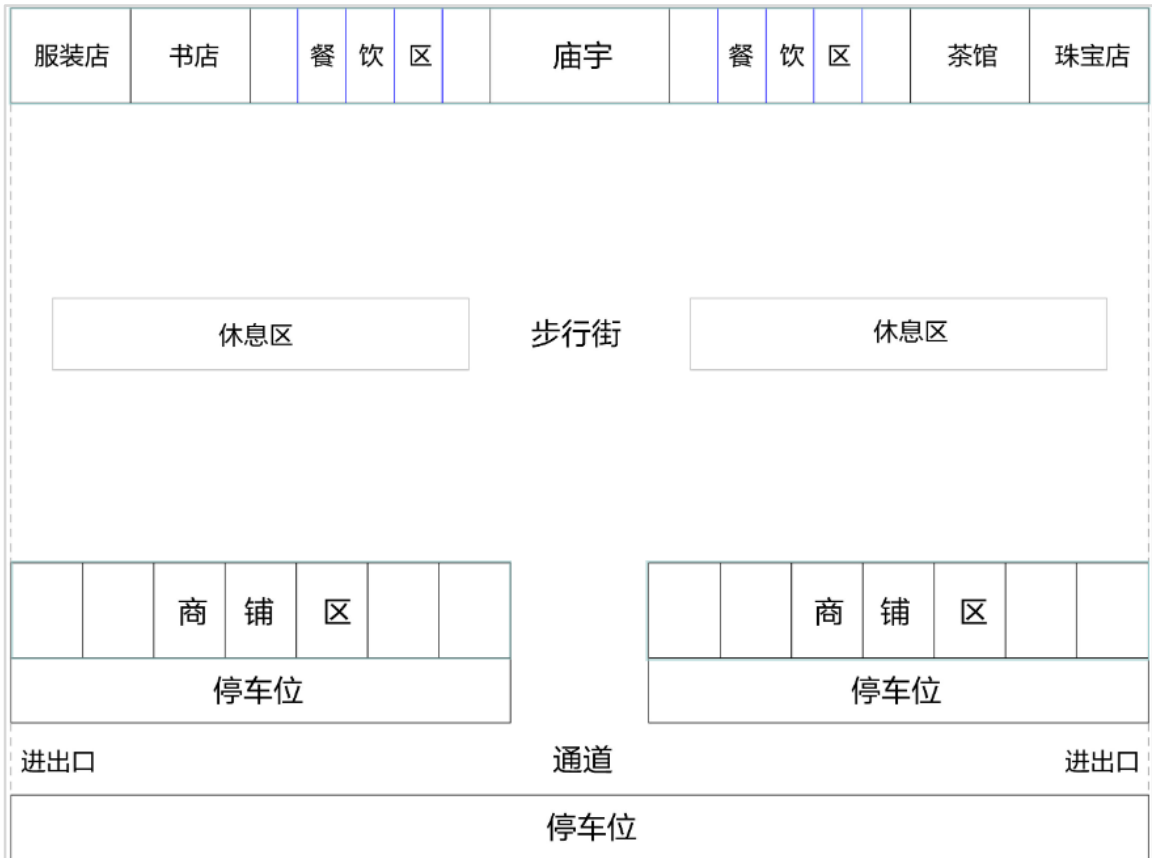
图纸宽度为 95 米，在图纸上选择任意位置，水平从左到右拉直设置比例尺长度为 95 米。



框选楼栋区域，设置障碍物高度。



环境设置后，效果如下所示。



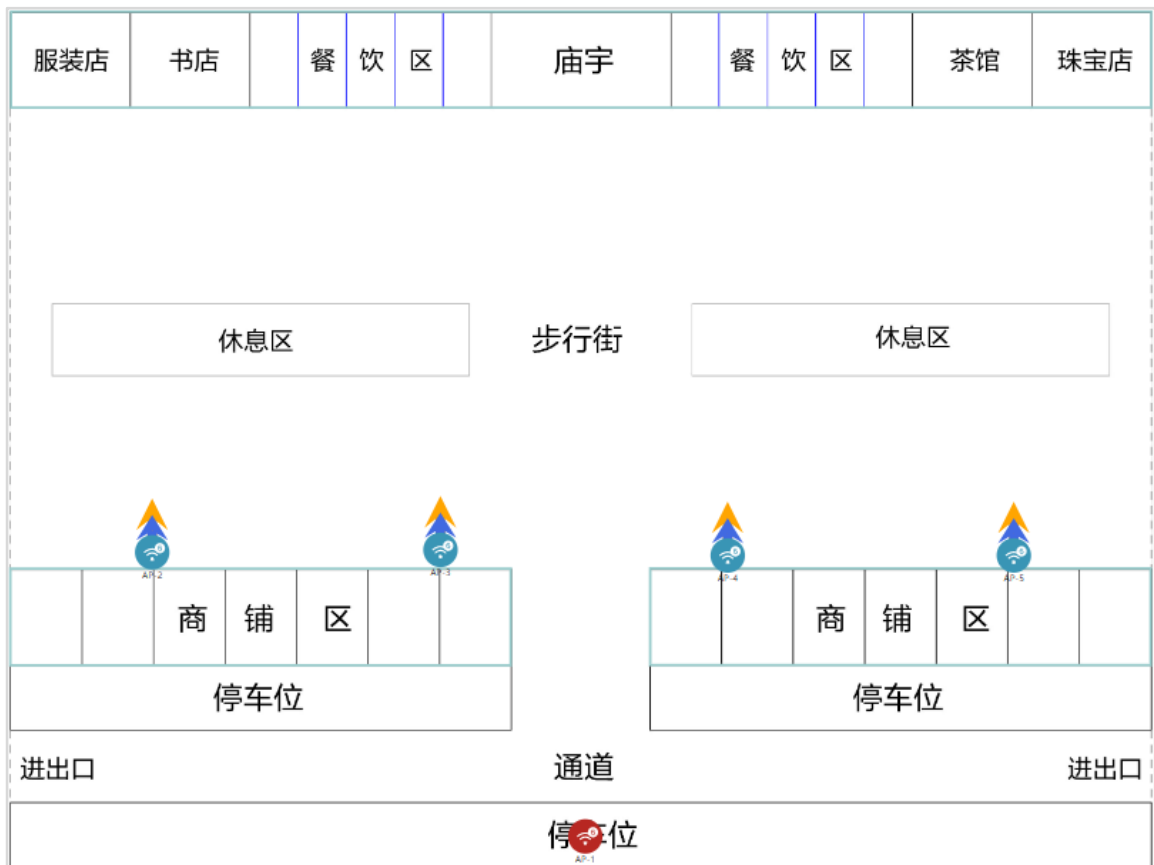
步骤 6 AP 布放, 调整 AP 参数

室外场景忽略区域设置步骤, 直接进入设备布放步骤, 且室外场景仅支持 AP 手动布放。

在工具栏中选择合适的 AP 款型, 进行手工布放。

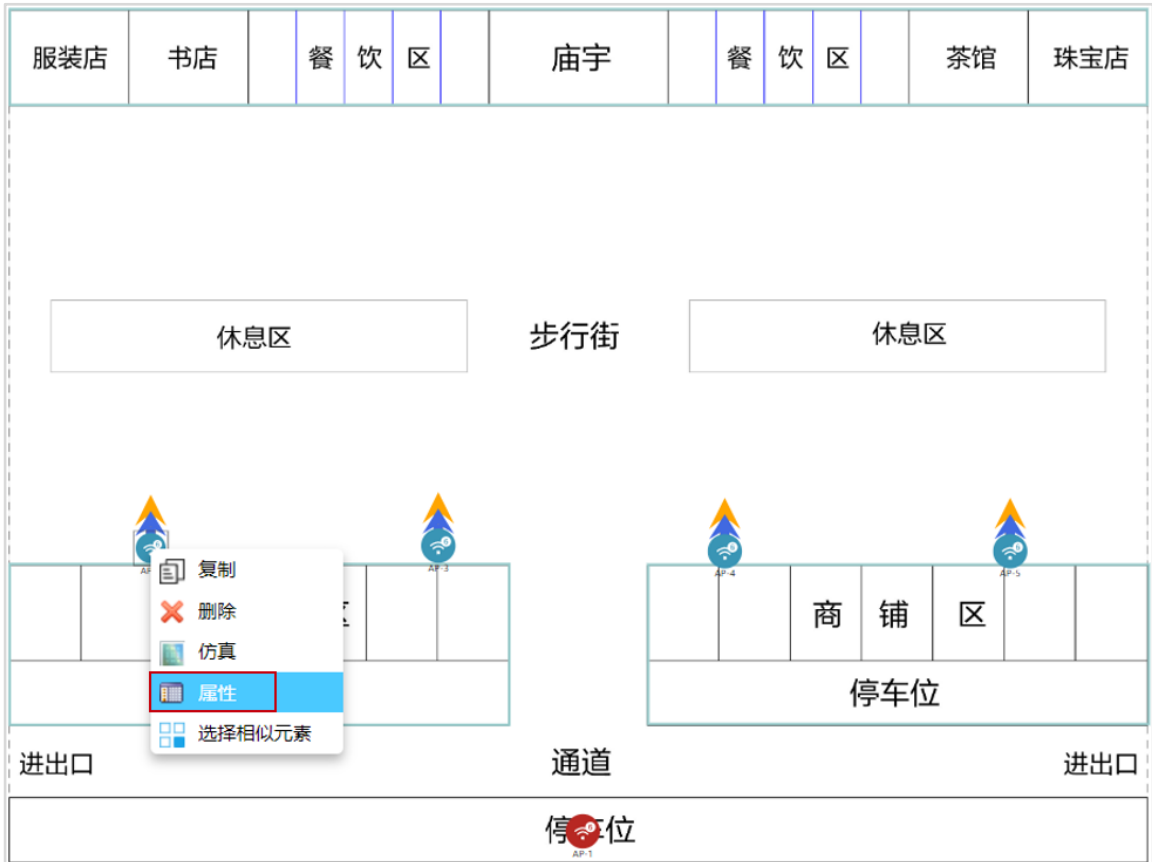


本项目壁挂 AP 使用 AirEngine5761R-11，抱杆 AP 使用 AirEngine5761R-11E，手动布放后效果如下。



AP 参数调整。

选择商铺区壁挂 AP，右击选择“属性”（可以框选全部 AP，再右击设置），打开 AP 属性页面。



因客户要求 AP 壁挂部署，则安装方式选择“挂墙”，挂高为“3 m”，其他参数保持默认，2.4G 和 5G 射频的下倾角均设置为 15 度，其他区域 AP 的属性配置一致，不再赘述。

AP属性

基本属性 更多设置

 名称: AP-3 颜色: 蓝色

AP类型: AirEngine5761R-11 物联网卡: 不支持

安装方式: 挂墙 挂高: 3.00 m

RTU License升级: 是 否 工作模式: 基础模式

POE: 802.3af(PoE)

射频0 OFF ON 支持协议: WiFi6(802.11ax) 类型: 2.4G_2*2_65*_40*_10dBi

信道: 1 高度: 3.00 m

类型: 2.4G 频宽: HE20 方位角: 0°

MIMO: 2*2 功率: 17 Max: 17dBm 下倾角: 15°

Guard Interval: Short Normal

馈线类型: ---请选择---

射频1 OFF ON 支持协议: WiFi6(802.11ax) 类型: 5G_2*2_65*_20*_11dBi

信道: 157 高度: 3.00 m

类型: 5G 频宽: HE40+ 方位角: 0°

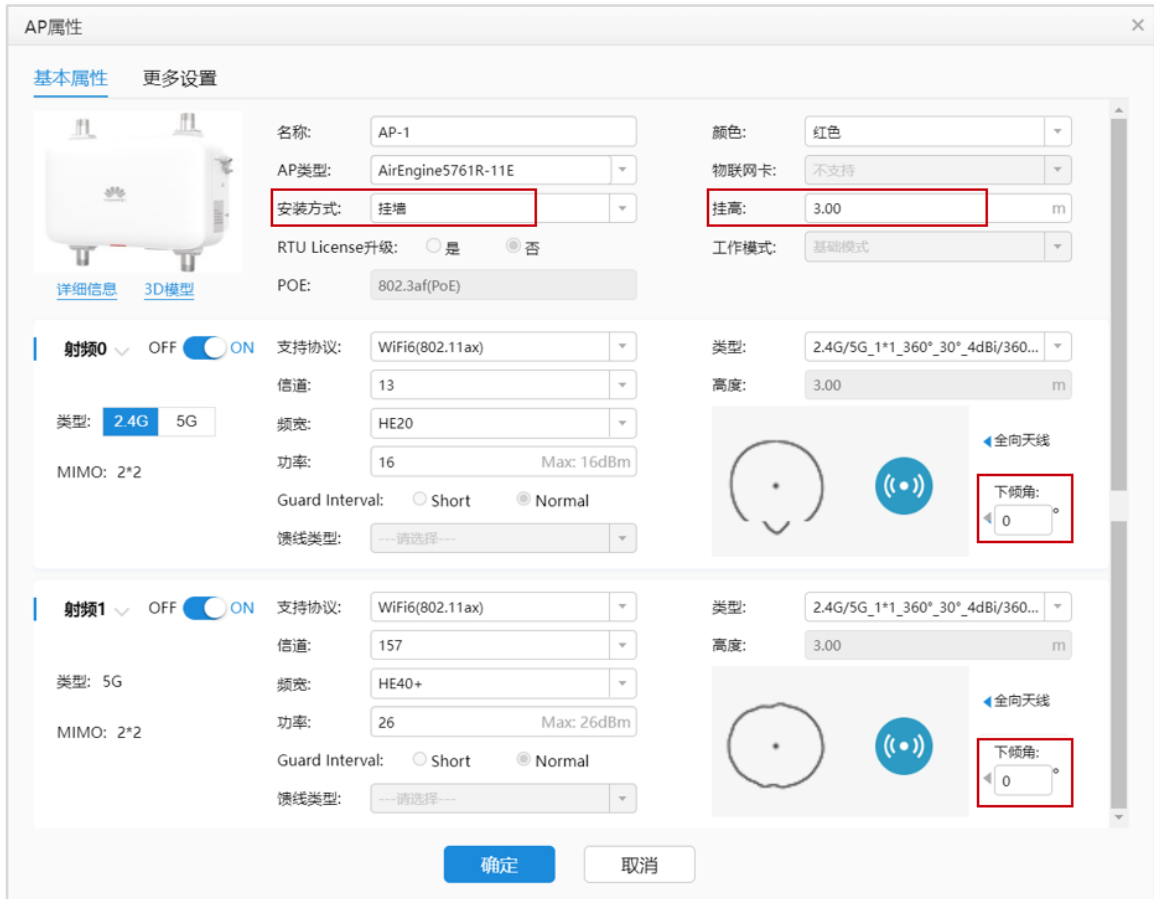
MIMO: 2*2 功率: 23 Max: 23dBm 下倾角: 15°

Guard Interval: Short Normal

馈线类型: ---请选择---

确定 取消

停车位处的 AP 为抱杆安装，选用 AirEngine5761R-11E 款型，参数设置如下所示。



步骤 7 信号仿真

查看重点覆盖区域，即信号强度大于-65 dBm 区域的覆盖情况，如果出现没有颜色的区域，则表示信号强度低于-65 dBm。

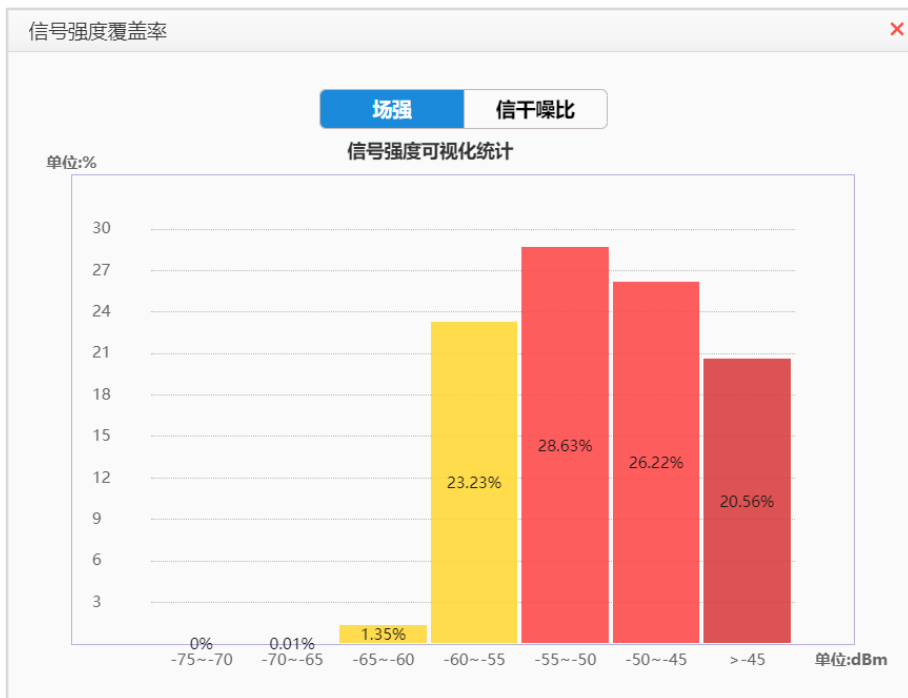
将仿真图示意中的信号强度调整为-65 dBm，随后点击“打开仿真图”。



本项目只需关注商铺之间街道和休息区的信号覆盖情况。



如果发现信号覆盖不良，可以反复调整 AP 位置和数量，确保信号仿真没有问题。
查看覆盖满足度，可以查看是否有信号覆盖不良区域。



可以看到大部分区域的信号覆盖情况良好。

步骤 8 导出网规报告

在导出网规报告前，可以先进行网规检视。

The screenshot shows the 'Export Report' (5. 导出报告) step in the software. The 'Report Content' (报告内容) section includes options for language (Chinese/English), floor sorting (Ascending/Descending), and a 'Export' (导出) button. The 'Heatmap Settings' (热图设置) section includes options for color scheme, frequency bands (2.4G, 5G, 6G), and various simulation and visualization options. Below this is the 'Automatic Inspection' (网规自动检视) section, which lists several check items:

- 环境设置**
 - 障碍物设置: 检查是否有图纸 (所有场景, 室内室外GIS等) 没有绘制障碍物。
 - 障碍物类型: 检查是否有图纸 (所有场景, 室内室外GIS等) 只绘制了一种障碍物。
- 设备布放**
 - AP布放过近: 检查AP间距, 如果有小于8m (26.25英尺), 并且AP间没有障碍物。
- AP设置**
 - 功率调优: 以楼层/室外区域维度查询AP功率是否均为默认功率。
 - 信道设置: 以楼层/室外区域维度查询AP信道是否均为默认信道。
- 天线设置**
 - 天线款型: 查询室外外接天线的AP是否连接了非推荐的室外覆盖天线款型。
 - 角度设置: 查询单个AP维度下倾角&方位角是否是默认角度。
- 交付效果**
 - 覆盖满足度: 覆盖满足度是否大于95%。
 - 容量满足度: 容量满足度是否大于90%。
 - 建网标准达成度: 建网标准达成度是否大于95%。
 - 精品网AP选型策略: AP是否满足至少4T4R要求。
- 场景化**
 - 定位场景: 1.定位AP间距是否满足小于等于15米。 2.定位AP之间是否构成等三角形形状。
3.定位AP与障碍物间距是否满足大于等于2米。 4.定位区域是否满足任意一点都有三个定位AP覆盖信号大于-65dB...

At the bottom of the inspection section, there is a 'Start Inspection' (开始检视) button and an 'Export Report' (导出报告) button. A red circle with the number '2' is placed over the 'Start Inspection' button.

查看是否没有问题，若出现警告项，需自行确认，没有问题后可导出网规报告。

网规自动检视

环境设置	<ul style="list-style-type: none">● 障碍物设置: 检查是否有图纸（所有场景，室内室外GIS等）没有绘制障碍物。 ✓● 障碍物类型: 检查是否有图纸（所有场景，室内室外GIS等）只绘制了一种障碍物。 ✓
设备布放	<ul style="list-style-type: none">● AP布放过近: 检查AP间距，如果有小于8m（26.25英尺），并且AP间没有障碍物。 ✓
AP设置	<ul style="list-style-type: none">● 功率调优: 以楼层/室外区域维度查询AP功率是否均为默认功率。 ✓● 信道设置: 以楼层/室外区域维度查询AP信道是否均为默认信道。 ✓
天线设置	<ul style="list-style-type: none">● 天线款型: 查询室外外接天线的AP是否连接了非推荐的室外覆盖天线款型。 ✓● 角度设置: 查询单个AP维度下倾角&方位角是否是默认角度。 ✓
交付效果	<ul style="list-style-type: none">● 覆盖满足度: 覆盖满足度是否大于95%。 ✓● 容量满足度: 容量满足度是否大于90%。 ✓● 建网标准达成度: 建网标准达成度是否大于95%。 ✓● 精品网AP选型策略: AP是否满足至少4T4R要求。 ✓
场景化	<ul style="list-style-type: none">● 定位场景: 1.定位AP间距是否满足小于等于15米。 2.定位AP之间是否构成等三角形状。 ✓3.定位AP与障碍物间距是否满足大于等于2米。 4.定位区域是否满足任意一点都有三个定位AP覆盖信号大于-65dB...

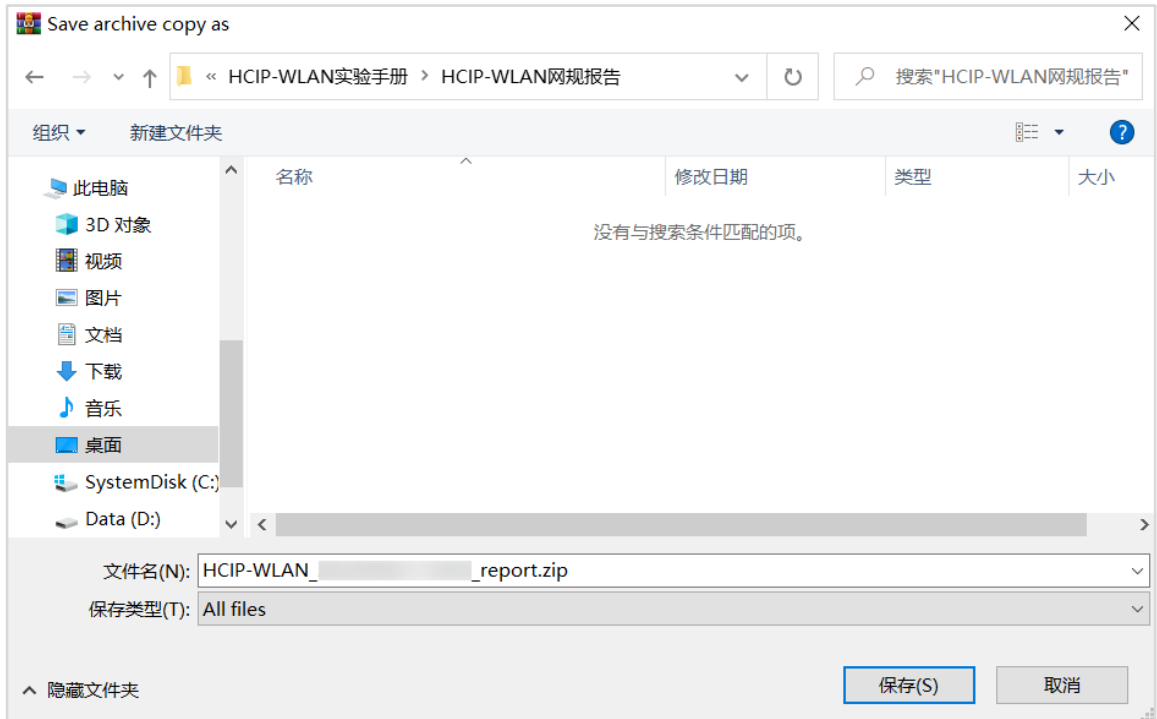
🔄 重新检视 📄 导出报告 3

导出报告。

导出报告/导出报告计算中... 35%

00:00:02 预计总耗时1分钟

保存至本地。



查看保存的网规报告。



10.3 思考题

1.在室外网规设计中，需求收集需要确认哪些信息？

参考答案：

- (1) 法规限制：EIRP 限制和可用信道；
- (2) 图纸信息：平面图纸或地图；
- (3) 覆盖区域：重点区域、普通区域、无需覆盖区域；
- (4) 场强要求：对信号的强度要求；
- (5) 接入终端数：覆盖区域内的接入终端总数；
- (6) 终端类型；
- (7) 带宽要求；
- (8) 周围环境：选址周围是否有建筑和树木遮挡；
- (9) AP 安装位置和配电方式：AP 一般会尽量利用灯杆、建筑外墙面安装，必要时可能要另
外立杆；
- (10) 交换机位置；
- (11) 干扰源：是否有基于无线回传的城市监控、微波站等干扰源。

2.室外 AP 全向天线和定向天线的使用场景有什么区别? 国内环境下, 它们的覆盖范围大概是多少?

参考答案:

全向天线推荐在室外开阔区域场景使用, 覆盖半径 60-80 米。

定向天线推荐在室外街道场景使用, 覆盖长度 120-150 米, 覆盖宽度 20-35 米。

11 CampusInsight 智能运维实验

11.1 实验介绍

11.1.1 关于本实验

本实验通过部署 CampusInsight 智能运维平台，使学员具备采用智能运维平台巡检无线网络的能力。

11.1.2 实验目的

- 掌握 WAC 与 CampusInsight 对接配置方法。
- 了解基本的 CampusInsight 运维功能。

11.1.3 实验组网介绍

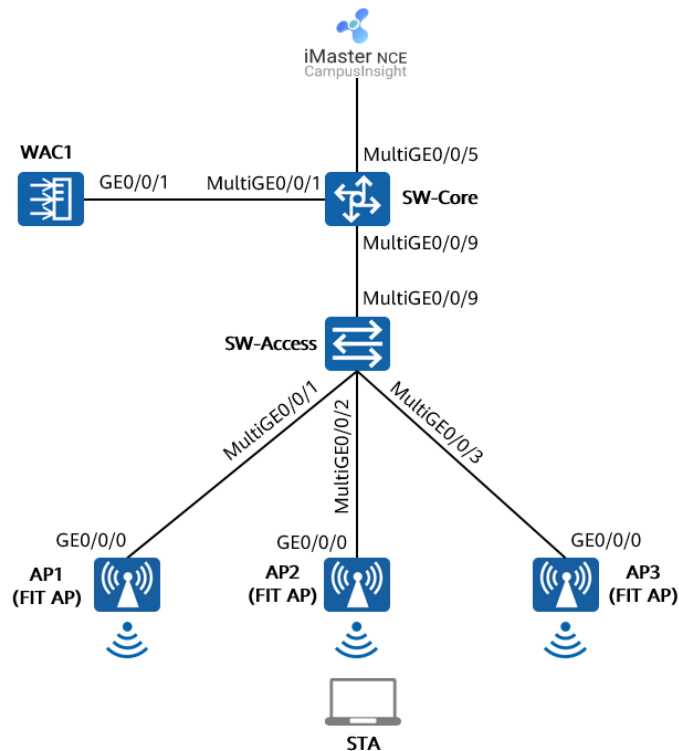


图11-1 CampusInsight 智能运维实验拓扑图

本实验中，AP1、AP2、AP3 由 WAC1 统一管理和配置，CampusInsight 服务器与核心交换机 SW-Core 互联，所属网段为 172.21.0.0/17。WAC1 与 CampusInsight 服务器对接联动，将业务运行日志和数据上报至 CampusInsight 服务器，管理员可以通过 CampusInsight 对 WLAN 网络进行统一智能运维。

11.1.4 实验规划

表11-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/5	Access	PVID: 99
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表11-2 IP 地址规划

设备	端口	IP地址
SW-Core	Vlanif100	10.23.100.254/24
	Vlanif101	10.23.101.254/24
	Vlanif99	172.21.39.253/17
WAC1	Vlanif100	10.23.100.1/24
CampusInsight服务器	/	172.21.39.99/17

表11-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	直接转发
管理VLAN	100
业务VLAN	101
AP组	ap-group1
VAP模板	wlan-net
安全模板	wlan-net
安全策略	WPA/WPA2+PSK+AES
密码	a12345678
SSID模板	wlan-net
SSID	wlan-net

11.2 实验任务配置

11.2.1 配置思路

- 1.配置 SW-Core、SW-Access、WAC1 设备的 VLAN 信息。
- 2.配置各网络设备的 IP 地址信息，确保网络互通。
- 3.在核心交换机 SW-Core 上配置 DHCP 服务器，确保 AP 可以获取 IP 地址。
- 4.配置 WLAN 业务参数，实现 STA 接入。
- 5.配置 CampusInsight 相关网络，确保网络互通。
- 6.配置 WAC1 与 CampusInsight 服务器联动。
- 7.通过 Web 登录 CampusInsight 服务器实现智能运维。

11.2.2 配置步骤

步骤 1 配置基础网络、AP 上线、无线业务

请参考 1.2.2 步骤 1 ~ 1.2.2 步骤 7，此处不再赘述。

步骤 2 配置 CampusInsight 与 WAC1 之间网络互通

CampusInsight 服务器的 IP 地址和网关在软件安装阶段已配置完成，本实验不再赘述。
CampusInsight 地址为 172.21.39.99/17，网关地址是 172.21.39.253（位于 SW-Core 上）。

配置 SW-Core 的 VLAN 信息及 IP 地址。

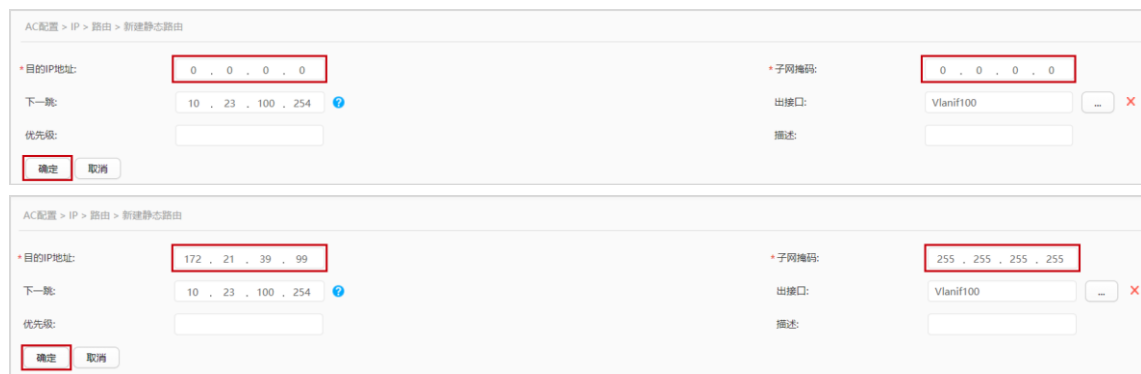
```
[SW-Core] vlan 99
[SW-Core-vlan99] name Manage
[SW-Core-vlan99] quit
[SW-Core] interface MultiGE 0/0/5
[SW-Core-MultiGE0/0/5] port link-type access
[SW-Core-MultiGE0/0/5] port default vlan 99
[SW-Core-MultiGE0/0/5] quit
[SW-Core] interface Vlanif 99
[SW-Core-Vlanif99] ip address 172.21.39.253 17
[SW-Core-Vlanif99] quit
```

在 WAC1 上配置静态路由，确保 CampusInsight 与 WAC1 之间网络互通。

选择“配置 > AC 配置 > IP”，选择“路由”选项卡，点击“静态路由配置表”，展开对应的配置界面，然后点击“新建”，新建静态路由。



在“新建静态路由”页面，依次分别配置如下两条静态路由，然后点击“确定”。其中静态路由 0.0.0.0/0 用于访问其他外部网络，静态路由 172.21.39.99/32 用于访问 CampusInsight 服务器。



配置完成后，查看静态路由如下所示。



The screenshot shows the configuration page for a Huawei AirEngine9700-M1 device, specifically the '路由' (Routing) section under 'IP' configuration. The page title is 'Wireless LAN AirEngine9700-M1' and the device name is 'WAC1'. The navigation menu on the left includes '配置向导', 'AC配置', '基本配置', 'VLAN', '接口管理', 'IP', 'AP配置', and '安全管理'. The main content area shows tabs for 'DHCP地址池', 'DHCP中继', 'NAT', '路由', and 'DNS'. Under the '路由' tab, there are sections for '路由表' and '静态路由配置表'. The '静态路由配置表' section contains a table with columns for '目的IP地址', '子网掩码', '下一跳', '出接口', and '优先级'. Two static routes are listed, both with a priority of 60. The second route is highlighted with a red box.

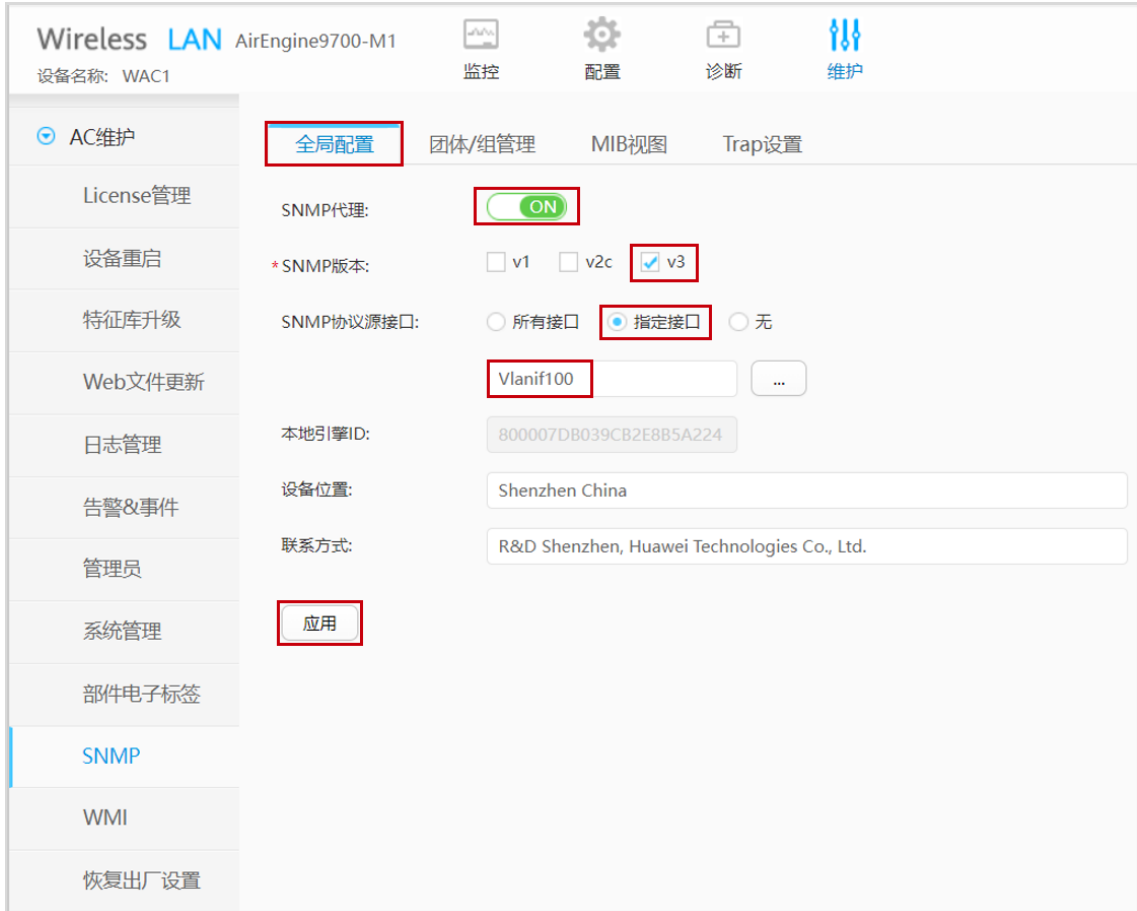
目的IP地址	子网掩码	下一跳	出接口	优先级
<input type="checkbox"/> 0.0.0.0	0.0.0.0	10.23.100.254	Vlanif100	60
<input type="checkbox"/> 172.21.39.99	255.255.255.255	10.23.100.254	Vlanif100	60

At the bottom of the table, it shows '10' items and '共2条' (Total 2 items).

步骤 3 配置 SNMP 协议

配置 SNMP 协议的目的是将 WAC1 添加至 CampusInsight 中进行管理。SNMPv2c 是不安全协议，建议配置更加安全的 SNMPv3 协议。

选择“维护 > AC 维护 > SNMP”，选择“全局配置”选项卡，开启 SNMP 代理功能，并按照如下参数进行配置，然后点击“应用”。



Wireless LAN AirEngine9700-M1
设备名称: WAC1

全局配置 团体/组管理 MIB视图 Trap设置

License管理 SNMP代理: ON

设备重启 * SNMP版本: v1 v2c v3

特征库升级 SNMP协议源接口: 所有接口 指定接口 无

Web文件更新 Vlanif100

日志管理 本地引擎ID: 800007DB039CB2E885A224

告警&事件 设备位置: Shenzhen China

管理员 联系方式: R&D Shenzhen, Huawei Technologies Co., Ltd.

系统管理 应用

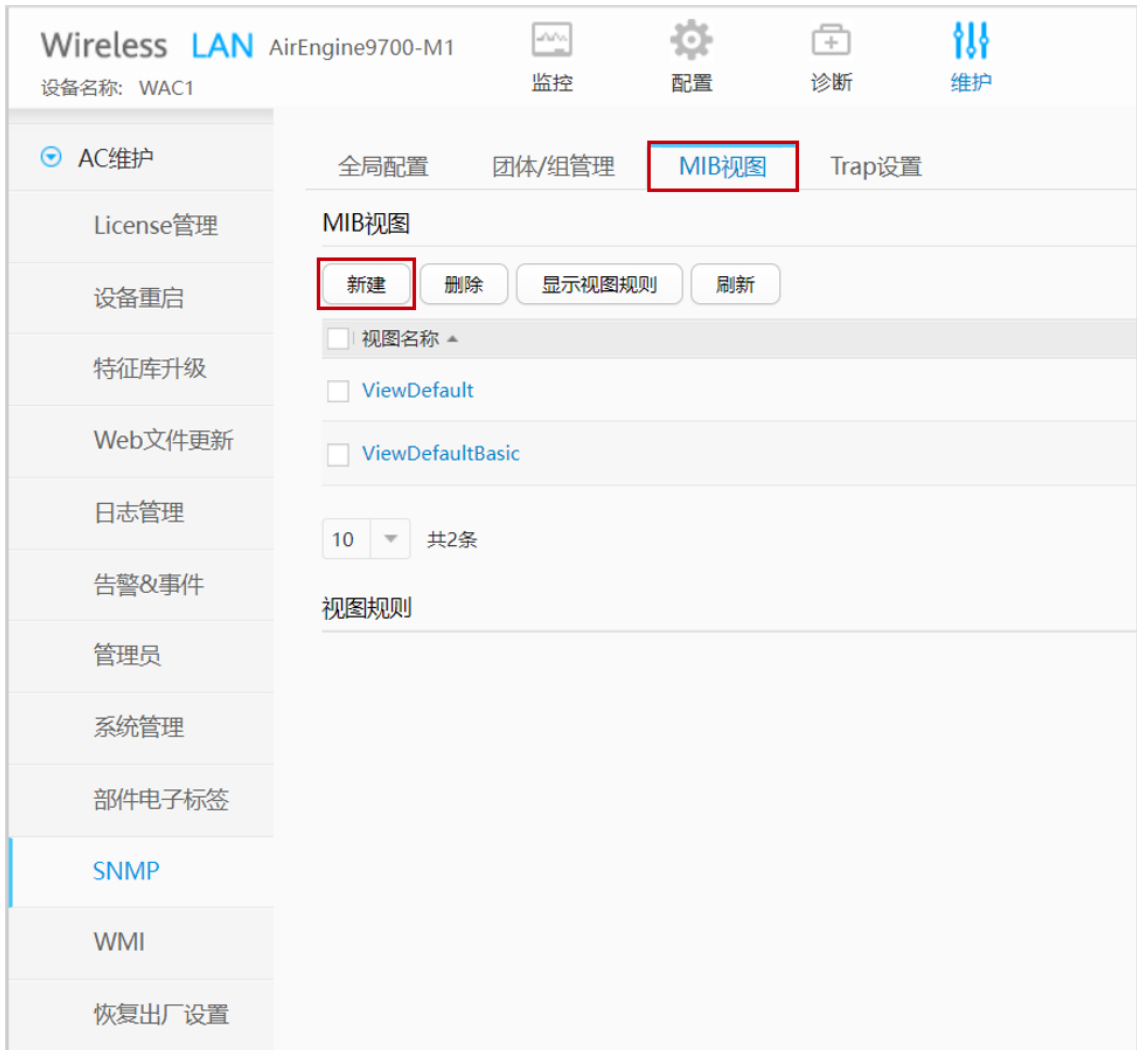
部件电子标签

SNMP

WMI

恢复出厂设置

选择“维护 > AC 维护 > SNMP”，选择“MIB 视图”选项卡，点击“新建”，新建 MIB 视图。



The screenshot shows the 'MIB View' configuration page in the Huawei Wireless LAN management interface. The page title is 'Wireless LAN AirEngine9700-M1' with the device name 'WAC1'. The navigation menu on the left includes 'AC维护', 'License管理', '设备重启', '特征库升级', 'Web文件更新', '日志管理', '告警&事件', '管理员', '系统管理', '部件电子标签', 'SNMP', 'WMI', and '恢复出厂设置'. The main content area has tabs for '全局配置', '团体/组管理', 'MIB视图', and 'Trap设置'. Under the 'MIB视图' tab, there are buttons for '新建', '删除', '显示视图规则', and '刷新'. Below these buttons, there is a list of MIB views: 'ViewDefault' and 'ViewDefaultBasic', each with a checkbox. A dropdown menu shows '10' items, with a total of '共2条'. At the bottom, there is a section for '视图规则' (View Rules).

在“MIB 视图 > 新建视图规则”界面，配置如下参数，然后点击“确定”。其中视图名称为 HCIP-test，规则包含 iso 子树。



The screenshot shows the 'New View Rule' configuration form. The breadcrumb is 'AC维护 > SNMP > MIB视图 > 新建视图规则'. The form fields are:

- *视图名称: HCIP-test (marked with 1)
- *规则: 包含 (marked with 2)
- *MIB子树名称: iso (marked with 3)
- MIB子树掩码: (marked with 3)

 Below the form is a table for rules:

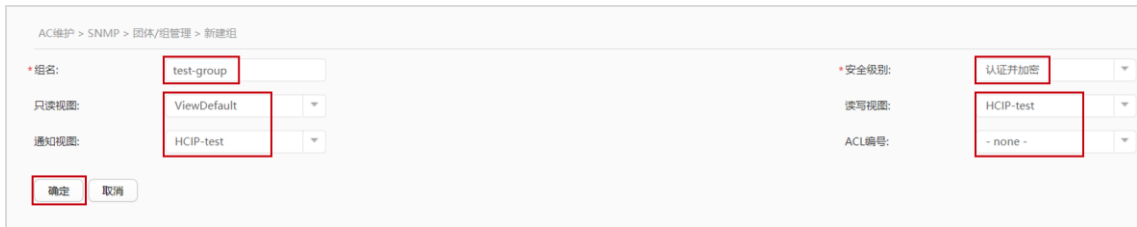
规则	MIB子树名称/OID	MIB子树掩码
暂无数据		

 At the bottom, there are '确定' (marked with 4) and '取消' buttons.

选择“维护 > AC 维护 > SNMP”，选择“团体/组管理”选项卡，在“组（适用于 SNMPv3）”中点击“新建”，新建组。



在“团体/组管理 > 新建组”界面，配置如下参数，然后点击“确定”。其中组名为 test-group，安全级别为认证并加密，读写视图和通知视图为 HCIP-test。



选择“维护 > AC 维护 > SNMP”，选择“团体/组管理”选项卡，在“用户（适用于 SNMPv3）”中点击“新建”，新建用户。



在“团体/组管理 > 新建用户”界面，配置如下参数，然后点击“确定”。其中用户名为 test-user，认证密码为 Huawei@123，加密密码为 Huawei@456，需与 CampusInsight 侧配置一致。

AC维护 > SNMP > 团体/组管理 > 新建用户

* 用户名:

组名称:

安全级别: (推荐使用认证并加密,其他级别存在安全风险)

认证方式: SHA2-256

* 认证密码:

加密方式: AES128 AES192 AES256

* 加密密码:

最后，选择“维护 > AC 维护 > 系统管理”，选择“管理面隔离”选项卡，按照如下步骤添加逻辑管理口 Vlanif 100，然后点击“应用”。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

AC维护 服务管理 1 **管理面隔离** 文件管理 系统时间

License管理 管理面隔离: ON

设备重启 逻辑管理口: 请选择 2 (最多添加4条数据)

特征库升级

Web文件更新

日志管理

告警&事件

管理员

3 接口名称

Vlanif100

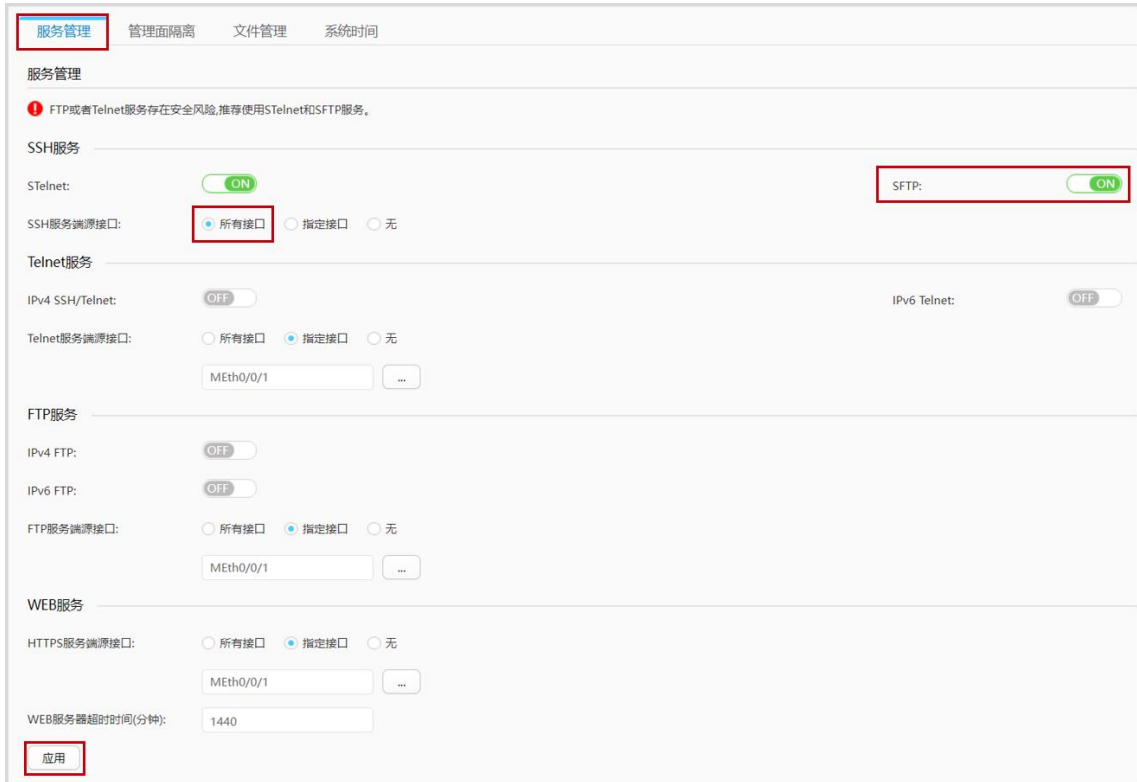
4

系统管理 部件电子标签

步骤 4 配置 SFTP 协议

配置 SFTP 协议的目的是使 CampusInsight 能使用 SFTP 协议从设备侧同步 AP 基本信息、端口信息、链路信息等。

选择“维护 > AC 维护 > 系统管理”，选择“服务管理”选项卡，开启 SFTP 服务，并配置 SSH 服务端源接口为“所有接口”，然后点击“应用”。



步骤 5 配置 LLDP 链路发现协议

配置 LLDP 链路发现协议的目的是使 CampusInsight 能够发现设备的 LLDP 链路。

在 WAC1 上启用全局 LLDP，确保状态为“ON”，如下所示。



开启 AP 的 LLDP 邻居上报功能。

选择“配置 > AP 配置 > AP 组配置”，选择“AP 组”选项卡，点击“ap-group1”，进入此 AP 组的配置界面。

The screenshot shows the configuration page for 'Wireless LAN' on an 'AirEngine9700-M1' device. The left sidebar has 'AP配置' selected, with 'AP组配置' highlighted. The main area shows a table of AP groups:

组名称	VAP模板	射频0模板
<input type="checkbox"/> default		2.4G-default
<input type="checkbox"/> ap-group1		2.4G-default

Buttons for '修改', '新建', '删除', and '刷新' are visible. A '20' dropdown and '共2条' are at the bottom.

在 AP 组配置界面中，选择“AP > AP 系统模板”，对缺省的 AP 系统模板（名称为 default）进行配置，点击“高级配置”，开启 LLDP 协议的邻居上报功能，然后点击最下方的“应用”，使配置生效。

The screenshot shows the configuration page for 'AP组配置' on the 'ap-group1' group. The left sidebar has 'AP配置' selected, with 'AP组配置' highlighted. The main area shows a tree view of templates:

- 显示所有模板 [配置模型介绍](#)
- VAP配置
- 射频管理
- AP
 - AP系统模板 [default]
 - AP有线口配置
 - ETH-TRUNK0 [default]
 - WIDS

The 'AP系统模板 [default]' entry is highlighted with a red box. A '查看成员' button is also visible.

* AP系统模板: default [展示模板引用关系] [新建]

模板介绍信息: AP系统模板提供对AP系统参数的配置、引用终端黑白名单模板以及频谱分析。

基础配置 [高级配置]

断链业务保持策略: 不保持

MTU (bytes): 1500

管理VLAN:

AC-AP间数据隧道DTLS加密: 遵循全局 开 关

广播组播抑制

Mesh

双链路/N+1备份

LLDP

LLDP使能延迟时间(秒): 2

报文发送延迟时间(秒): 2

报文存活时间(发送时间倍数): 4

邻居上报: ON

工作模式: 接收和发送

报文发送间隔(秒): 30

邻居上报抑制时间(秒): 30

步骤 6 配置日志数据、WLAN 业务数据上报功能

数据上报功能默认支持 HTTP/2 和 UDP 两种协议通道，推荐使用 HTTP/2 协议。

配置 WAC1 设备的 HTTP/2 协议通道。选择“维护 > AC 维护 > WMI”，选择“通道 1”选项卡，配置如下参数，然后点击“应用”。其中服务器地址为 172.21.39.99，端口号为 27371。

通道1 通道2

* 服务器地址: 172 . 21 . 39 . 99

* 端口: 27371

上报周期(s): 60

心跳时间(min): 3

重连次数: 0

监控数据上报: 设备 接口 CPCAR 应用 日志 安全 iPCA2.0

设备监控数据上报间隔(s): 10

CPCAR监控数据上报间隔(s): 300

日志监控数据上报间隔(s): 300

上报的日志模块: 终端上下线 设备操作 接口 硬件故障 云盒上下线 无线射频 自定义

应用 清空

单次数据上报最大量(KB): 5

服务器重连间隔(min): 5

接口监控数据上报间隔(s): 60

应用统计监控数据上报间隔(s): 300

安全监控数据上报间隔(s): 300

配置 AP 设备的 HTTP/2 协议通道。选择“配置 > AP 配置 > AP 组配置”，进入“ap-group1”的配置界面中，选择“AP > AP 系统模板 > WMI 模板（通道 2）”，点击“新建”，新建一个 WMI 模板，配置模板名称为 test，然后点击“确定”，如下所示。

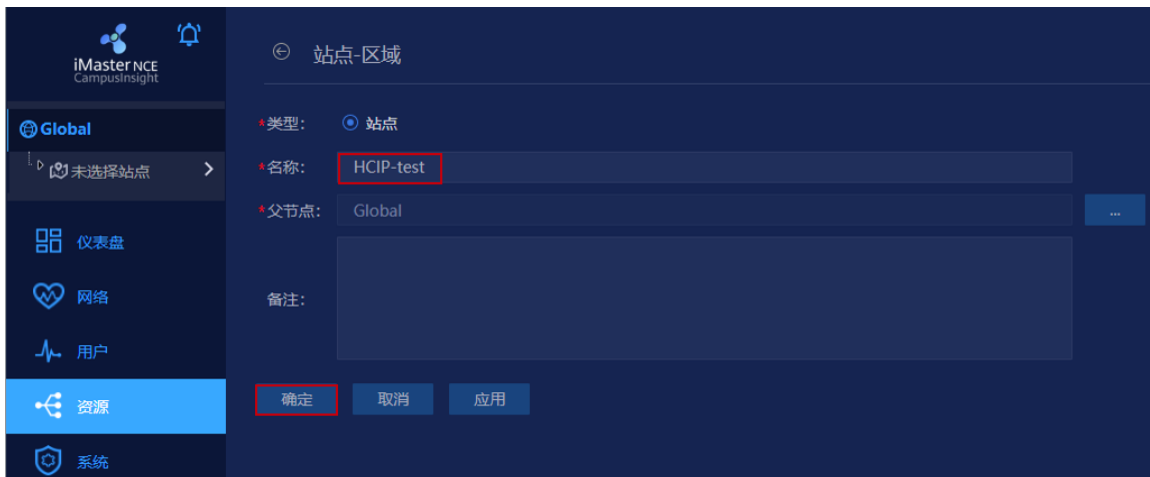
按照如下参数配置名称为 test 的 WMI 模板，然后点击“应用”，使配置生效。

步骤 7 配置 CampusInsight 服务器

登录 CampusInsight，在主菜单中选择“资源”，然后选择“站点-区域”页签，点击“添加”按钮。



添加站点，名称为“HCIP-test”，父节点为“Global”，然后点击“确定”。



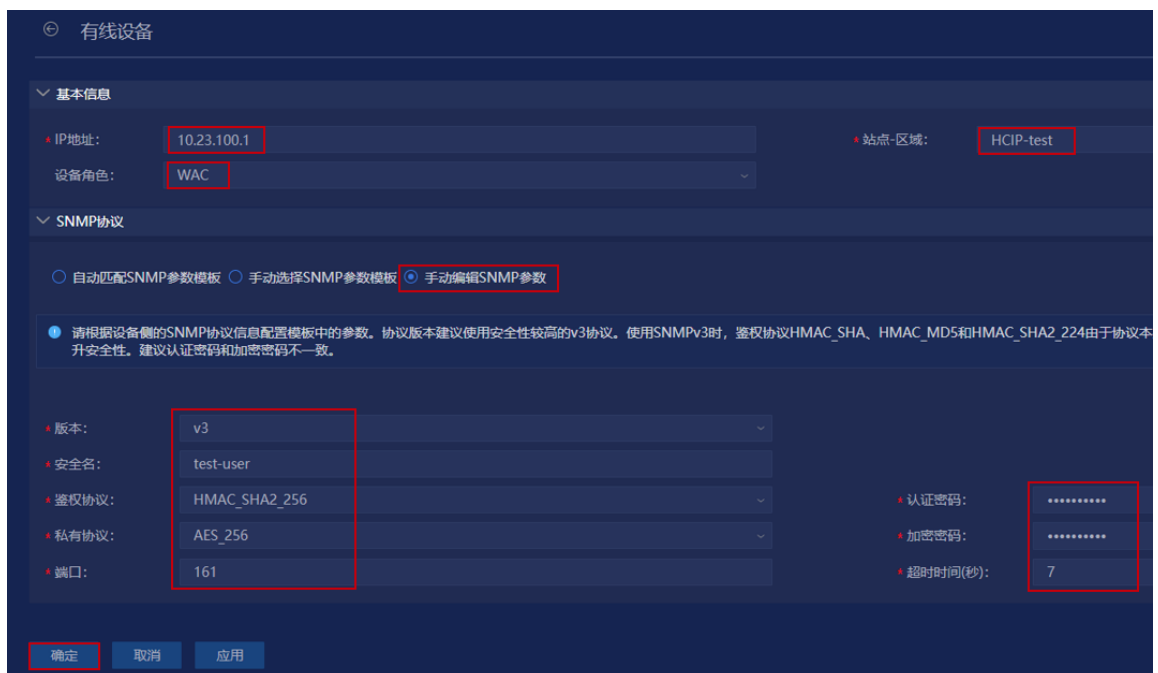
选择“资源 > 有线设备”，点击“增加设备”，选择“单个添加”。



按照如下参数进行配置：IP 地址为 WAC1 的地址“10.23.100.1”，站点-区域选择“HCIP-test”，设备角色选择“WAC”。

SNMP 协议选择“手动编辑 SNMP 参数”，版本选择“v3”，安全名配置为“test-user”，鉴权协议选择“HMAC_SHA2_256”，私有协议选择“AES_256”，端口为 161，认证密码为“Huawei@123”，加密密码为“Huawei@456”。最后点击“确定”。

此处的安全名需要与 WAC1 上配置的 SNMP 用户名一致，其他参数也需要一致。



检查有线设备上线状态，发现 WAC1 已经在线。

状态	名称	IP地址	MAC	设备型号	设备分类	厂商	站点-区域
● 在线	WAC1	10.23.100.1	9C-B2-E8-B5-A2-24	AirEngine9700-M1	AC	Huawei	/HCIP-test

共1条

WAC1 添加到 CampusInsight 后，其管理的 AP 将会自动添加到 CampusInsight 的 AP 列表当中，点击“无线设备”，发现三台 AP 均已在线。

状态	名称	AP分类	AP型号	IP地址	ESN	MAC	接入AC名称	站点-区域
● 在线	AP2	FIT AP	AirEngine5761-11	10.23.100.214	2102353VU...	9c-b2-e8-2d-54-10	WAC1	Unplanned
● 在线	AP3	FIT AP	AirEngine5761-11	10.23.100.117	2102353VU...	9c-b2-e8-2d-51-10	WAC1	Unplanned
● 在线	AP1	FIT AP	AirEngine5761-11	10.23.100.225	2102353VU...	9c-b2-e8-2d-54-f0	WAC1	Unplanned

共3条

在“HCIP-test”站点中添加楼宇。选择“资源 > 站点-区域”，选中“HCIP-test”，然后点击“添加”。

1 站点-区域

输入名称进行搜索... 3 添加 删除

名称	类型
HCIP-test	

类型选择“楼宇”，名称配置为“Building_01”，点击“确定”。



在“Building_01”楼宇中添加楼层。选择“资源 > 站点-区域”，选中“Building_01”，然后点击“添加”。



类型选择“楼层”，名称配置为“First floor”，点击“确定”。



选择“资源 > 无线设备”，同时选中三台 AP，然后点击“移动”，将三台 AP 移动至“First floor”楼层中。



发现三台 AP 的“站点-区域”已经变更为“/HCIP-test/Building_01/First floor”。

无线设备

站点-区域 有线设备 **无线设备** 链路

+ 移动 设置License 区域规划导入 区域规划导出

筛选

状态	名称	AP分类	AP型号	IP地址	ESN	MAC	接入...	站点-区域
● 在线	AP2	FIT AP	AirEngin...	10.23.100.214	21023...	9c-b2-e8...	WAC1	/HCIP-test/Building_01/First floor
● 在线	AP3	FIT AP	AirEngin...	10.23.100.117	21023...	9c-b2-e8...	WAC1	/HCIP-test/Building_01/First floor
● 在线	AP1	FIT AP	AirEngin...	10.23.100.225	21023...	9c-b2-e8...	WAC1	/HCIP-test/Building_01/First floor

共3条

步骤 8 配置 CampusInsight 运维功能

查看整网状态。

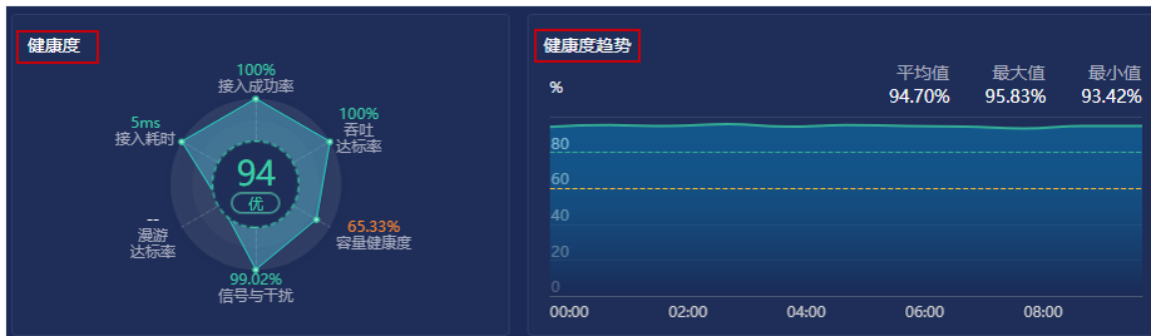
选择“仪表盘 > 概览”，可以查看“HCIP-test”站点的资源状态、健康度、用户数、流量、AP 速率/流量等关键信息，使管理员可以了解网络的整体运行情况。





查看无线健康度。

选择“网络 > 无线健康度”，可以查看无线网络的运行状况。



详细指标主要包括：接入成功率、接入耗时、漫游达标率、信号与干扰、容量健康度、吞吐达标率等。





查看用户旅程。

选择“用户 > 用户旅程”，在“常规视图”页签中可以查看接入用户的基本信息。

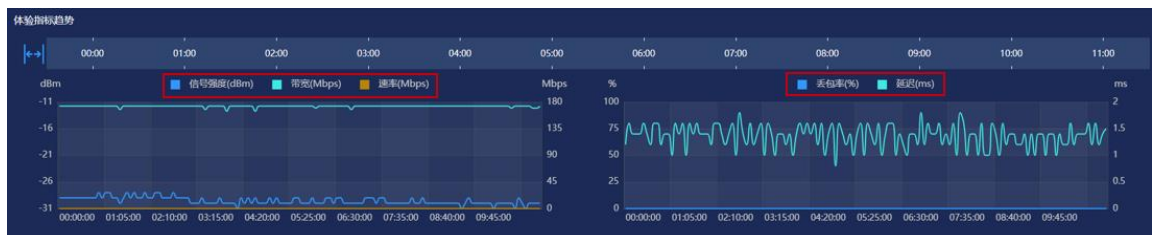
2个结果, 耗时: 260ms

常规视图 | VIP视图 | 当前用户

筛选

用户MAC	用户名	质差时长	VIP 用户	接入类型	总体验时长	平均RSSI(dBm)	平均下行速率	总流量	时延(毫秒)	丢包率(%)
08-1f-71-53-90-6f	081f7153906f	0		无线	9小时14分钟	-20	<1bps	12.37KB	0.23	0
08-1f-71-53-90-b4	081f715390b4	0		无线	9小时14分钟	-30	1.2Kbps	77.66MB	1.37	0

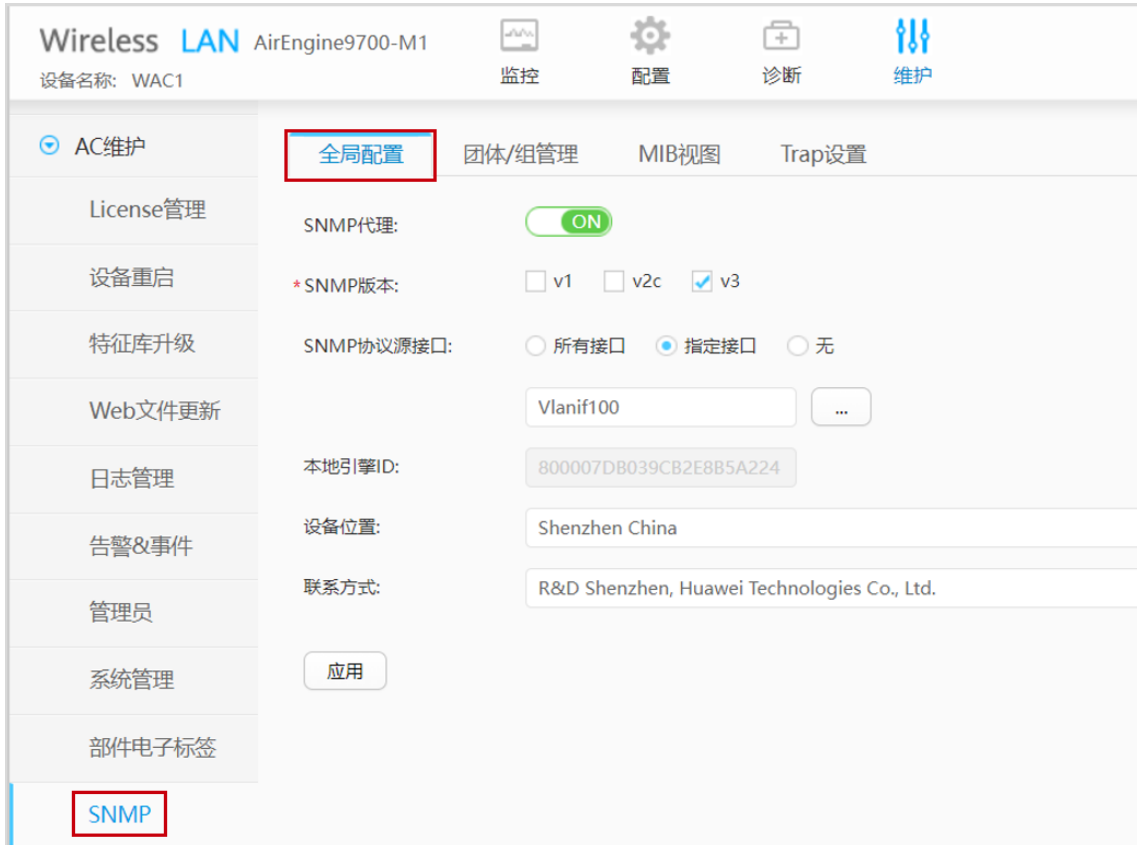
点击具体的用户 MAC (以 08-1f-71-53-90-b4 为例)，可以查看更加详细的指标。



11.3 结果验证

11.3.1 查看 WAC1 的 SNMP 协议

查看 SNMP 协议的全局配置。选择“维护 > AC 维护 > SNMP”，选择“全局配置”选项卡即可查看，如下所示。



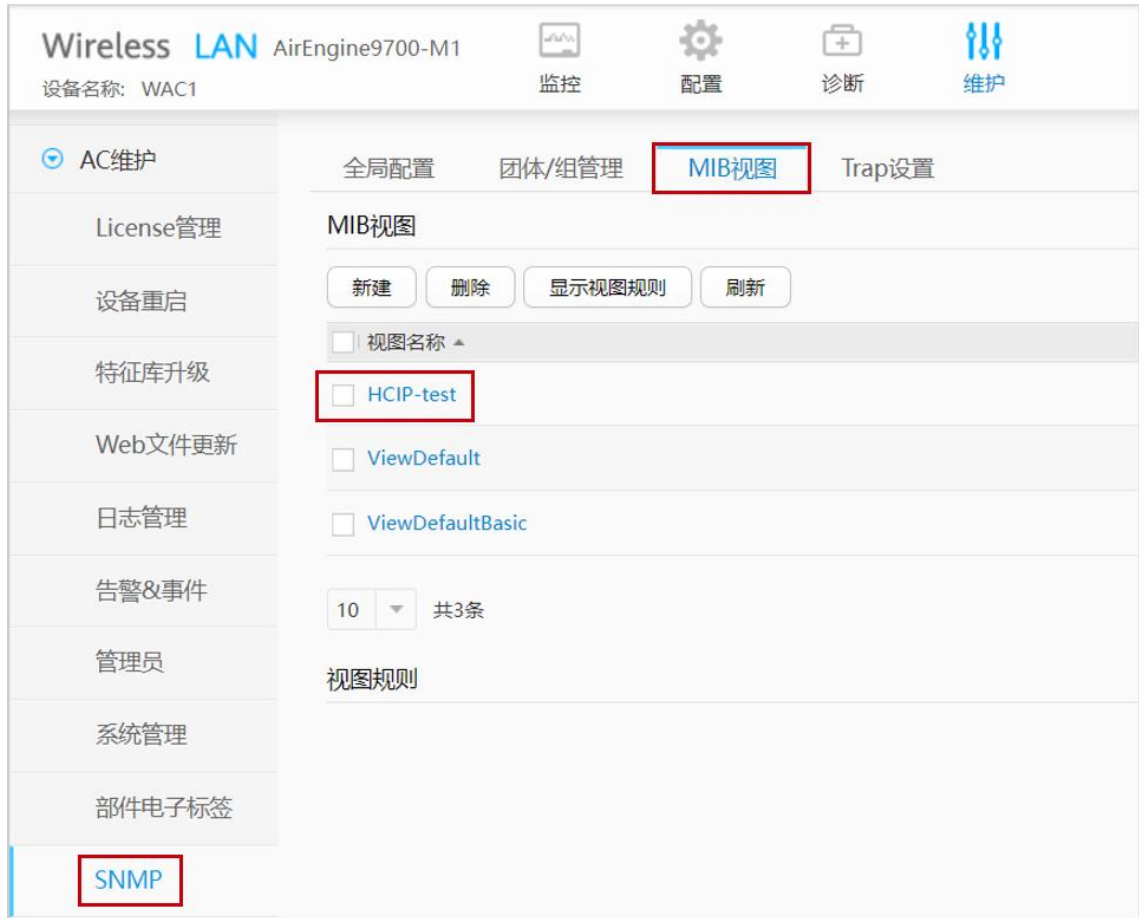
The screenshot displays the configuration page for WAC1 in the Huawei WLAN management system. The page title is "Wireless LAN AirEngine9700-M1" with the device name "WAC1". Navigation tabs include "监控" (Monitoring), "配置" (Configuration), "诊断" (Diagnosis), and "维护" (Maintenance). The left sidebar shows "AC维护" (AC Maintenance) selected, with sub-items like "License管理", "设备重启", "特征库升级", "Web文件更新", "日志管理", "告警&事件", "管理员", "系统管理", and "部件电子标签". The "SNMP" sub-item is highlighted with a red box. The main content area shows the "全局配置" (Global Configuration) tab selected, with sub-tabs for "团体/组管理", "MIB视图", and "Trap设置". The configuration includes: "SNMP代理" (SNMP Agent) set to "ON"; "SNMP版本" (SNMP Version) with "v3" selected; "SNMP协议源接口" (SNMP Protocol Source Interface) set to "指定接口" (Specify Interface) with "Vlanif100" entered; "本地引擎ID" (Local Engine ID) as "800007DB039CB2E8B5A224"; "设备位置" (Device Location) as "Shenzhen China"; and "联系方式" (Contact Information) as "R&D Shenzhen, Huawei Technologies Co., Ltd.". An "应用" (Apply) button is at the bottom.

查看 SNMP 协议的组信息和用户信息。选择“维护 > AC 维护 > SNMP”，选择“团体/组管理”选项卡即可查看，如下所示。



The screenshot shows the configuration page for SNMP on a Huawei AirEngine9700-M1 device. The left sidebar contains navigation options: AC维护, License管理, 设备重启, 特征库升级, Web文件更新, 日志管理, 告警&事件, 管理员, 系统管理, 部件电子标签, **SNMP**, and WMI. The main content area is titled "Wireless LAN AirEngine9700-M1" and includes tabs for 全局配置, **团体/组管理**, MIB视图, and Trap设置. Under "团体/组管理", there are sections for "团体(适用于SNMPv1或SNMPv2c)" and "组(适用于SNMPv3)". The "组" section includes a table with columns for 组名, 安全级别, 只读视图, 读写视图, and 通知视图. A single entry "test-group" is shown. Below this is a section for "用户(适用于SNMPv3)" with a table for 用户名, 认证算法, 加密算法, and 组名称. A single entry "test-user" is shown with SHA2-256 authentication and AES256 encryption. The "SNMP" option in the sidebar is highlighted with a red box.

查看 SNMP 协议的 MIB 视图。选择“维护 > AC 维护 > SNMP”，选择“MIB 视图”选项卡即可查看，如下所示。



The screenshot displays the configuration page for the MIB View of a Wireless LAN device (AirEngine9700-M1, device name WAC1). The interface includes a top navigation bar with icons for Monitoring, Configuration, Diagnosis, and Maintenance. A left sidebar lists various maintenance tasks, with 'SNMP' highlighted at the bottom. The main content area shows the 'MIB View' configuration options, including buttons for 'New', 'Delete', 'Show View Rules', and 'Refresh'. A list of MIB views is shown, with 'HCIP-test' selected and highlighted by a red box. Other views include 'ViewDefault' and 'ViewDefaultBasic'. A dropdown menu shows '10' items per page, and a total of '3 items' are listed. Below the list, there is a section for 'View Rules'.

11.3.2 查看 WAC1 的 AP 状态和 VAP 信息

选择“监控 > AP”，选择“AP 统计”选项卡，可以查看 AP 的状态信息，其中“normal”代表 AP 已正常上线。


```
defence engine enable
sysname WAC1
#
http timeout 10080
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif100
http server enable
#
vlan batch 100 to 101
#
stp enable
#
management-port isolate enable
management-plane isolate enable
#
mgmt isolate disable
#
interface Vlanif1
 ip address dhcp-alloc unicast
#
interface Vlanif100
 ip address 10.23.100.1 255.255.255.0
 management-interface
#
interface MEth0/0/1
 ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
 ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
snmp-agent local-engineid 800007DB039CB2E8B5A224
snmp-agent group v3 test-group privacy write-view HCIP-test notify-view HCIP-test
snmp-agent mib-view HCIP-test include iso
snmp-agent usm-user version v3 test-user
snmp-agent usm-user version v3 test-user group test-group
snmp-agent usm-user version v3 test-user authentication-mode sha2-
256 %^%#FuNM(|kva(w1dtRftXo#jiNM&VK`F7+0:q4pgdO$%^%#
snmp-agent usm-user version v3 test-user privacy-mode
aes256 %^%#88a5+3fR_HZ%+$U&6[3W!,{6V{#@8!/e(uKgo%MD%^%#
snmp-agent protocol source-interface Vlanif100
snmp-agent
#
```

```
ssh server-source -i all
sftp server enable
stelnet server enable
undo telnet server enable
undo telnet ipv6 server enable
telnet server-source -i MEth0/0/1
ssh server secure-algorithms cipher aes256_ctr aes128_ctr
ssh server secure-algorithms hmac sha2_256
ssh server key-exchange dh_group16_sha512 dh_group15_sha512 dh_group_exchange_sha256
ssh client secure-algorithms cipher aes256_ctr aes128_ctr
ssh client secure-algorithms hmac sha2_256
ssh client key-exchange dh_group16_sha512 dh_group15_sha512 dh_group_exchange_sha256
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif100 10.23.100.254
ip route-static 172.21.39.99 255.255.255.255 Vlanif100 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%#
capwap dtls inter-controller psk %^%#tc.5LFZ\oJ^bM8'YYv#<te,1Oq8kAl.}J+v{puP%^%#
capwap message-integrity psk %^%#eJ&eRx\$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x*%^%#
capwap sensitive-info psk %^%#;,L1<.L'e+li6MX,^QxH{6z#&#z[v4Oe"pCPrFJ'%^%#
capwap inter-controller sensitive-info psk %^%#ji6gT7>2y3dm}n~Bb"%8z$0]B62~|NkD,WJF[n2U%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
wmi-server
server ip-address 172.21.39.99 port 27371
log module mid fe030000 name WMP_RFM
log module mid ffee0000 name WCWP
log module mid ffc10000 name CLOUD_MNG
log module mid ff8c0000 name ENTITYTRAP
log module mid ff050000 name IFPDT
log module mid ffd10000 name VCON
log module mid d0410000 name SHELL
log module mid fff30000 name WLAN
log module mid fe050000 name WSTA
log module mid ffa30000 name WEBS
log module mid ff760000 name WEB
log module mid ff630000 name CM
log module mid ff620000 name DHCP
log module mid ff600000 name PORTAL
log module mid ff5f0000 name DOT1X
log module mid ff5b0000 name RDS
log module mid ff5a0000 name AAA
log module mid c1480000 name TACACS
#
wmi-server2
#
```

```
wlan
  calibrate flexible-radio auto-switch
  temporary-management psk %^%#PwFE@vw_"@n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
  ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)I%^%#
  traffic-profile name default
  security-profile name default
  security-profile name wlan-net
    security wpa-wpa2 psk pass-phrase %^%#914c;d4z)+#$JD3kxgr@w>*(.lMo~Sf}H8U2\c[E%^%# aes
  security-profile name default-wds
  security-profile name default-mesh
  ssid-profile name default
  ssid-profile name wlan-net
    ssid wlan-net
  vap-profile name default
  vap-profile name wlan-net
    service-vlan vlan-id 101
    ssid-profile wlan-net
    security-profile wlan-net
  wds-profile name default
  mesh-handover-profile name default
  mesh-profile name default
  regulatory-domain-profile name default
  regulatory-domain-profile name domain1
  air-scan-profile name default
  rrm-profile name default
  radio-2g-profile name default
  radio-5g-profile name default
  wids-spoof-profile name default
  wids-whitelist-profile name default
  wids-profile name default
  wireless-access-specification
wmi-server name test
  server ip-address 172.21.39.99 port 27371
  collect-item location-data enable
  collect-item terminal-dhcp-option-data enable
  collect-item terminal-http-ua-data enable
  collect-item terminal-mdns-data enable
  collect-item dns-data enable
  collect-item non-wifi-data enable
  ap log module mid C1480000 name TACACS
  ap log module mid FF600000 name PORTAL
  ap log module mid FF620000 name DHCP
  ap log module mid FE050000 name WSTA
  ap log module mid FFEF0000 name WSRV
  ap log module mid FFF30000 name WLAN
  ap log module mid D0410000 name SHELL
  ap log module mid FF050000 name IFPDT
  ap log module mid FFED0000 name SEA
```

```
ap log module mid FFEE0000 name WCWP
ap log module mid FE030000 name WMP_RFM
ap-system-profile name default
lldp report enable
wmi-server test index 2
port-link-profile name default
wired-port-profile name default
ap-group name default
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile wlan-net wlan 1
wids device detect enable
spectrum-analysis enable
channel-monitor enable
radio 1
vap-profile wlan-net wlan 1
wids device detect enable
spectrum-analysis enable
channel-monitor enable
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
ap-name AP1
ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
ap-name AP2
ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
ap-name AP3
ap-group ap-group1
provision-ap
#
return
```

11.4.2 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101
#
dhcp enable
#
vlan 99
name Manage
#
interface Vlanif1
#
```

```
interface Vlanif99
 ip address 172.21.39.253 255.255.128.0
#
interface Vlanif100
 ip address 10.23.100.254 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.254 255.255.255.0
 dhcp select interface
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/5
 port link-type access
 port default vlan 99
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
return
```

11.4.3 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
```

```
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

11.5 思考题

上述实验采用 CampusInsight 平台对无线网络进行智能运维，请思考，智能运维相较于传统运维方式（WAC Web 界面）有哪些优势？

参考答案：

体验可视化：基于 Telemetry 秒级数据采集，每用户每应用每时刻体验可视。

分钟级潜在故障识别和根因定位：基于动态基线、大数据关联等识别潜在故障；KPI 关联分析和协议回放，精准定位问题根因。

网络预测性调优：通过 AI 智能分析 AP 的负载趋势，完成无线网络的预测性调优闭环。

12 故障排查综合实验

12.1 实验介绍

12.1.1 关于本实验

本实验通过对已有实验的故障进行排查，使学员掌握故障排查的一般方法。

12.1.2 实验目的

- 描述故障的现象和相关配置
- 掌握排查故障的方法

12.1.3 实验组网介绍

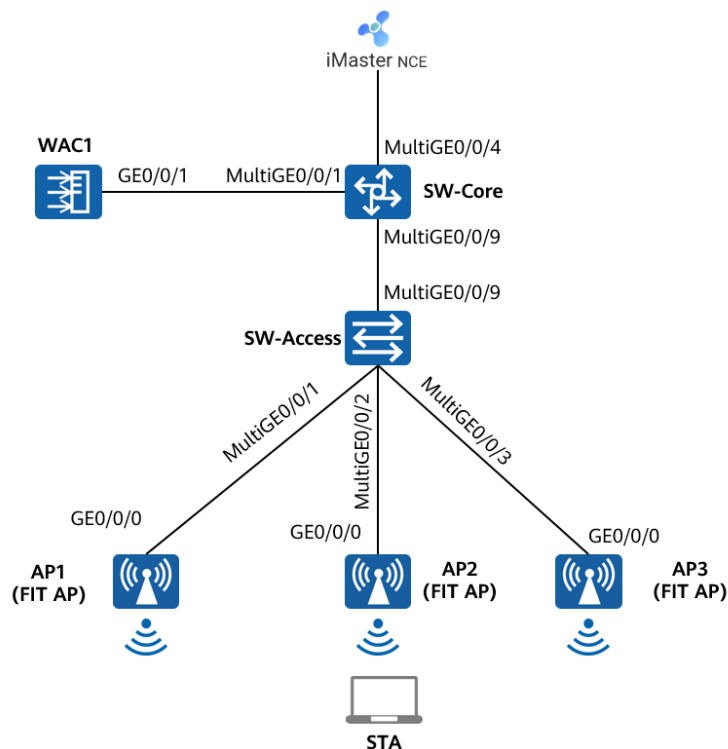


图12-1 故障排查综合实验拓扑图

12.1.4 实验规划

表12-1 VLAN 规划

设备	端口	端口类型	VLAN参数
SW-Core	MultiGE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/4	Access	PVID: 99
SW-Access	MultiGE0/0/9	Trunk	PVID:1 Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trunk	PVID:100 Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100 Allow-pass: VLAN 100 101
WAC1	GE0/0/1	Trunk	PVID:1 Allow-pass: VLAN 100 101

表12-2 IP 地址规划

设备	端口	IP地址
SW-Core	Vlanif100	10.23.100.254/24
	Vlanif101	10.23.101.254/24
	Vlanif99	172.21.39.253/17
WAC1	Vlanif100	10.23.100.1/24
iMaster NCE-Campus	/	172.21.39.88/17

表12-3 WLAN 业务参数规划

WLAN业务	参数
转发模式	隧道转发
管理VLAN	100

业务VLAN	101
AP组	ap-group1
VAP模板	wlan-net
安全模板	wlan-net
安全策略	OPEN
SSID模板	wlan-net
SSID	wlan-net
RADIUS认证参数	RADIUS认证方案名称: radius_huawei RADIUS计费方案名称: scheme1 RADIUS服务器模板名称: radius_huawei, 其中: IP地址: 172.21.39.88 认证端口号: 1812 计费端口号: 1813 共享密钥: Huawei@123
Portal服务器模板	名称: abc IP地址: 172.21.39.88 Portal认证共享密钥: Huawei@123
Portal接入模板	名称: portal1 绑定的模板: Portal服务器模板abc
免认证规则模板	名称: default_free_rule
认证模板	名称: p1 绑定的模板和认证方案: Portal接入模板portal1 RADIUS服务器模板radius_huawei RADIUS认证方案radius_huawei RADIUS计费方案scheme1 免认证规则模板default_free_rule

12.2 实验任务配置

12.2.1 配置思路

- 1.导入预配置。
- 2.依据故障现象进行排错。

12.2.2 配置步骤

步骤 1 导入预配置

导入 WAC1 的预配置。

```
Software Version V200R021C00SPC100
#
defence engine enable
sysname WAC1
#
vlan batch 100
#
authentication-profile name p1
authentication-scheme radius_huawei
accounting-scheme scheme1
radius-server radius_huawei
#
web-auth-server server-source all-interface
#
management-port isolate enable
management-plane isolate enable
#
radius-server template default
radius-server template radius_huawei
radius-server shared-key cipher Huawei@123
radius-server authentication 172.21.39.88 1812 source Vlanif 100 weight 80
radius-server accounting 172.21.39.88 1813 source Vlanif 100 weight 80
radius-server authorization 172.21.39.88 shared-key cipher Huawei@123 server-group radius_huawei
radius-server authorization server-source all-interface
#
url-template name url1
url https://172.21.39.88:8445/portal
url-parameter redirect-url redirect-url ssid ssid user-ipaddress userip user-mac usermac device-ip ac-ip
#
web-auth-server abc
server-ip 172.21.39.89
port 50100
shared-key cipher Huawei@456
url-template url1
```

```
source-ip 10.23.100.1
server-detect
#
portal-access-profile name portal1
web-auth-server abc direct
#
portal-access-profile name portal_access_profile
#
aaa
authentication-scheme radius_huawei
authentication-mode radius
accounting-scheme scheme1
accounting-mode radius
accounting realtime 3
local-aaa-user password policy administrator
domain default
authentication-scheme default
accounting-scheme default
radius-server default
domain default_admin
authentication-scheme default
accounting-scheme default
#
interface Vlanif1
ip address dhcp-alloc unicast
#
interface Vlanif100
ip address 10.23.100.1 255.255.255.0
management-interface
#
interface MEth0/0/1
ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk a1234567
capwap dtls inter-controller psk a1234567
capwap dtls no-auth enable
```

```
#
wlan
  calibrate flexible-radio auto-switch
  temporary-management psk a1234567
  ap username admin password cipher %^%#\4Y*HdY5jU={"Q,)V{2J[=sNPG-eG$TI_.'>AvM%^%#
  traffic-profile name default
  security-profile name default
  security-profile name wlan-net
    security open
  security-profile name default-wds
  security-profile name default-mesh
  ssid-profile name default
  ssid-profile name wlan-net
    ssid wlan-net
  vap-profile name default
  vap-profile name wlan-net
    forward-mode tunnel
    service-vlan vlan-id 101
    ssid-profile wlan-net
    security-profile wlan-net
    authentication-profile p1
  wds-profile name default
  mesh-handover-profile name default
  mesh-profile name default
  regulatory-domain-profile name default
  regulatory-domain-profile name domain1
  air-scan-profile name default
  rrm-profile name default
  radio-2g-profile name default
  radio-5g-profile name default
  wids-spoof-profile name default
  wids-whitelist-profile name default
  wids-profile name default
  wireless-access-specification
  ap-system-profile name default
  port-link-profile name default
  wired-port-profile name default
  ap-group name default
  ap-group name ap-group1
    regulatory-domain-profile domain1
  radio 1
    radio disable
  ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
    ap-name AP1
    ap-group ap-group1
  ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
    ap-name AP2
    ap-group ap-group1
```

```
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
  ap-name AP3
#
return
```

导入 SW-Core 的预配置。

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101
#
dhcp enable
#
vlan 99
  name Manage
#
interface Vlanif1
#
interface Vlanif99
  ip address 172.21.39.253 255.255.128.0
#
interface Vlanif100
  ip address 10.23.100.254 255.255.255.0
  dhcp select interface
#
interface Vlanif101
  ip address 10.23.101.254 255.255.255.0
  dhcp select interface
#
interface MEth0/0/1
  ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
  port link-type access
  port default vlan 99
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
```

```
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
return
```

导入 SW-Access 的预配置。

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
return
```

认证服务器 NCE 的预配置与 6.2.2 步骤 5 配置一致，本实验不再赘述。

步骤 2 排查故障：终端无法搜索到无线信号

在 STA 上搜索 SSID 信号，发现并未搜索到“wlan-net”的无线信号，此时需要排查 AP 是否已经上线，在 WAC1 上选择“监控 > AP”，选择“AP 统计”选项卡，查看 AP 列表如下所示：

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 AP配置 > AP配置 > AP信息 > 修改AP

AC配置 AP组: ap-group1

AP配置 AC地址列表: + 添加

AP组配置

AP配置 已选AP列表

AP ID	AP MAC地址	AP名称	AP组	IP地址获取方式
2	9cb2-e82d-5110	AP3	default	- none -

模板管理 10 共1条

安全管理 确定 取消

再次查看，发现三台 AP 均属于“ap-group1”组，并且已正常上线。

AP列表

智能诊断 上线失败记录 下线记录 SoftGRE隧道状态 导出信息 IoT插卡信息

AP ID	AP名称	AP组	状态名称
0	AP1	ap-group1	● normal
1	AP2	ap-group1	● normal
2	AP3	ap-group1	● normal

10 共3条

总AP数: 3 normal: 3

AirEngine5761-11: 3

由于当前 STA 仍然无法搜索到 SSID，所以继续查看 VAP 的状态信息，选择“监控 > SSID > VAP”，查看 VAP 信息如下：

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

概览 SSID **VAP**

网络KPI 自动刷新: OFF

AC

用户

射频

AP

SSID

应用统计清零

AP ID ▲	AP名称 ▲	射频ID ▲	WLAN ID ▲	SSID ▲	BSSID ▲
---------	--------	--------	-----------	--------	---------

注: 选择列表中的VAP,查看该VAP应用统计信息。

发现所有 AP 均没有关联任何 VAP 信息，所以进一步查看 AP 组中是否引用了 VAP 模板，选择“配置 > AP 配置 > AP 组配置”，在“AP 组”选项卡中发现“ap-group1”并未引用任何 VAP 模板，如下所示。

Wireless LAN AirEngine9700-M1
设备名称: WAC1

监控 配置 诊断 维护

配置向导 AP组 静态负载均衡组

AC配置 修改 新建 删除 刷新

AP配置

AP组配置

AP配置

射频规划/调优

组名称 ▲	VAP模板 ▲	射频0模板 ▲
<input type="checkbox"/> default		2.4G-default
<input type="checkbox"/> ap-group1		2.4G-default

20 共2条

然后在当前页面中，点击“ap-group1”，进入 AP 组配置页面。选择“VAP 配置”，点击“添加”，添加已经预配的 VAP 模板“wlan-net”，最后点击“确定”，如下所示。

AP配置 > AP组配置 > AP组

AP组配置: ap-group1 [查看成员](#)

显示所有模板 [配置模型介绍](#)

VAP配置

- 射频管理
- AP
- WIDS

VAP 模板列表

[相关配置](#)

[新建](#) [添加](#) [移除](#)

模板名称 ▲

添加VAP模板

[+ 添加](#)

*VAP模板名称: wlan-net *WLAN ID: 1 *射频: 0,1

[高级](#)

[确定](#) [取消](#)

再次查看 VAP 信息，发现三台 AP 均已释放名称为“wlan-net”的 SSID，但是 AP 的 Radio 1 的状态为“OFF”，说明 5G 射频被关闭，需要手动打开。

Wireless LAN AirEngine9700-M1

设备名称: WAC1 [监控](#) [配置](#) [诊断](#) [维护](#)

概览

网络KPI

AC

用户

射频

AP

SSID

CPE隧道

Mesh&WDS

潜在问题

WIDS

频谱分析

SSID VAP

自动刷新: OFF

AP型VAP列表

[应用统计清零](#)

AP ID ▲	AP名称 ▲	射频ID ▲	WLAN ID ▲	SSID ▲	BSSID ▲	认证方式 ▲	接入用户数 ▲	状态 ▲
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	Open	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	Open	0	off
1	AP2	0	1	wlan-net	9cb2-e82d-5410	Open	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	Open	0	off
2	AP3	0	1	wlan-net	9cb2-e82d-5110	Open	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	Open	0	off

10 共6条

注: 选择列表中的VAP查看该VAP应用统计信息。

手动开启 5G 射频，选择“配置 > AP 配置 > AP 组配置”，选中“ap-group1” AP 组，选择“射频管理 > 射频 1”，将射频 1 的工作状态配置为“ON”，然后点击“应用”，如下所示。

查看 VAP 状态信息，均已正常，如下所示：

AP ID	AP名称	射频ID	WLAN ID	SSID	BSSID	认证方式	接入用户数	状态
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	Open	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	Open	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	Open	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	Open	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	Open	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	Open	0	on

步骤 3 排查故障：终端关联无线信号，无法获取地址

STA 连接“wlan-net”信号后，无法获取 IP 地址，检查发现 VAP 的数据转发方式为隧道转发，但是 WAC1 上缺少业务 VLAN 信息（即缺少 VLAN 101），如下所示。



Wireless LAN AirEngine9700-M1
设备名称: WAC1

全局IPv6: OFF

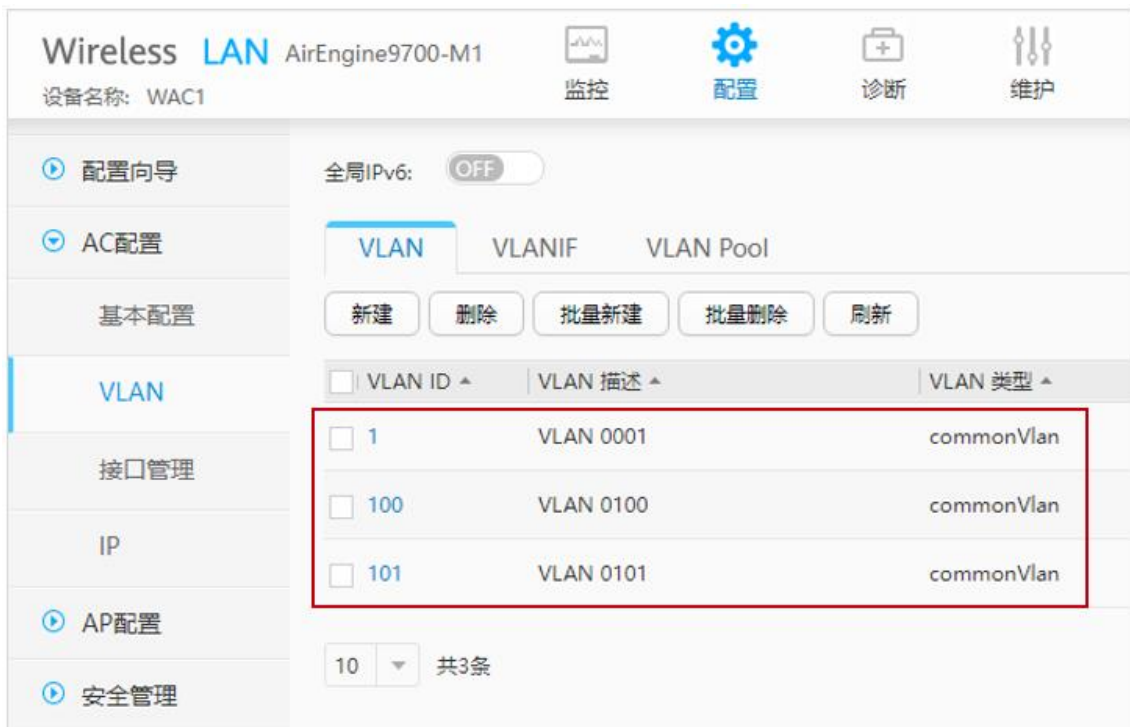
VLAN VLANIF VLAN Pool

新建 删除 批量新建 批量删除 刷新

VLAN ID	VLAN 描述	VLAN 类型
1	VLAN 0001	commonVlan
100	VLAN 0100	commonVlan

10 共2条

在 WAC1 上手动创建 VLAN 101，创建成功后，检查 VLAN 信息如下所示。（创建 VLAN 的步骤请参考 1.2.2 步骤 4，此处不再赘述）



Wireless LAN AirEngine9700-M1
设备名称: WAC1

全局IPv6: OFF

VLAN VLANIF VLAN Pool

新建 删除 批量新建 批量删除 刷新

VLAN ID	VLAN 描述	VLAN 类型
1	VLAN 0001	commonVlan
100	VLAN 0100	commonVlan
101	VLAN 0101	commonVlan

10 共3条

STA 断开 “wlan-net” 信号，然后重新连接，可以正常获取 IP 地址，使用 “ipconfig” 命令验证如下。

```

无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
本地连接 IPv6 地址 . . . . . : fe80::3ce1:b4f7:546e:45a1%12
IPv4 地址 . . . . . : 10.23.101.196
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 10.23.101.254
    
```

步骤 4 排查故障：Portal 认证无法弹出 Portal 认证页面

STA 搜索到“wlan-net”信号后，进行连接，然后打开浏览器，输入任意 IP 地址，发现无法弹出 Portal 认证页面。



无法弹出 Portal 认证页面的原因较多，大多数情况下都是由于认证模板配置错误导致，所以首先检查 VAP 模板是否正确引用了认证模板。

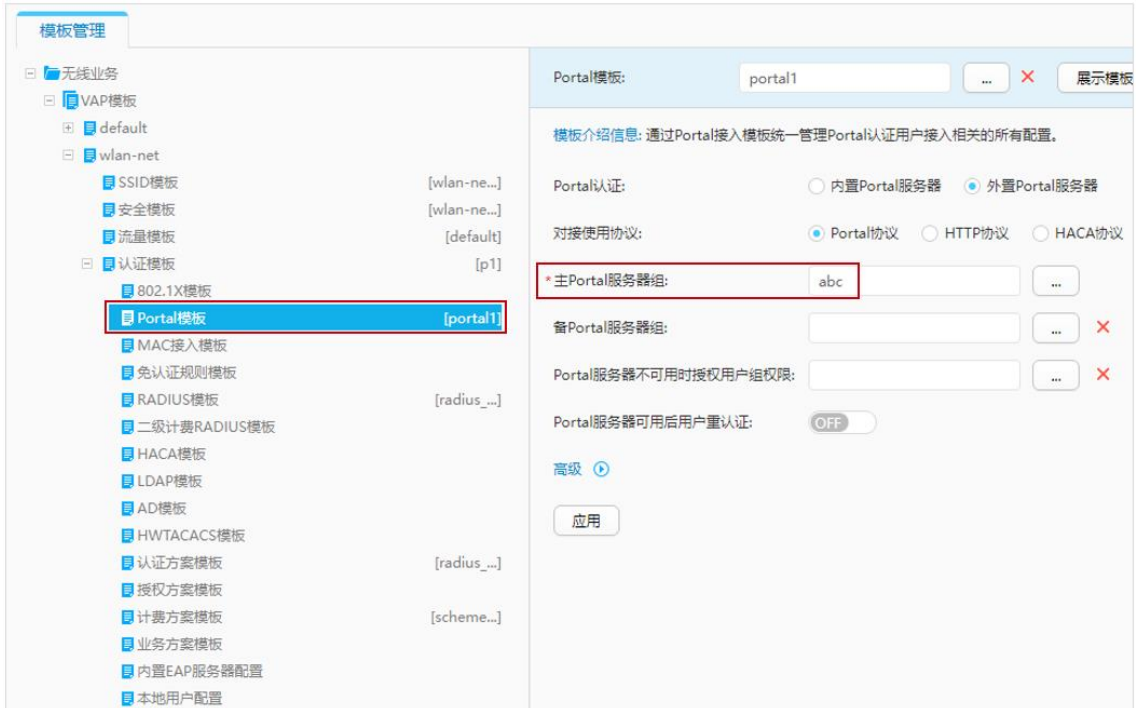
选择“配置 > AP 配置 > 模板管理 > 无线业务 > VAP 模板”，发现 VAP 模板“wlan-net”中引用了认证模板“p1”，但是认证模板“p1”中没有引用 Portal 模板，如下所示。



The screenshot displays the configuration interface for a Huawei AirEngine9700-M1 device, specifically for the Wireless LAN section. The device name is WAC1. The interface includes navigation icons for Monitoring, Configuration, Diagnosis, and Maintenance. On the left, a sidebar lists various configuration categories, with 'Template Management' (模板管理) selected. The main area shows a tree view of templates under 'Wireless Services' (无线业务). The 'Authentication Templates' (认证模板) folder is expanded, and the 'Portal Template' (Portal模板) is highlighted with a red box. Other templates listed include SSID, Security, Traffic, 802.1X, MAC Access, RADIUS, HWTACACS, and Local User configurations.

Template Name	Associated Name
SSID模板	[wlan-ne...]
安全模板	[wlan-ne...]
流量模板	[default]
认证模板	[p1]
802.1X模板	
Portal模板	
MAC接入模板	
免认证规则模板	
RADIUS模板	[radius_...]
二级计费RADIUS模板	
HACA模板	
LDAP模板	
AD模板	
HWTACACS模板	
认证方案模板	[radius_...]
授权方案模板	
计费方案模板	[scheme...]
业务方案模板	
内置EAP服务器配置	
本地用户配置	

手动引用已经预配的 Portal 模板“portal1”后，如下所示。



同时检查 Portal 模板“portal1”中引用的 Portal 服务器组“abc”的配置是否正确，选择“配置 > 安全管理 > AAA > Portal 服务器全局设置 > 外置 Portal 全局设置”，点击 Portal 认证服务器列表中的“abc”，检查其配置，发现如下配置错误：

- Portal 服务器的 IP 地址配置错误，正确地址应该是 172.21.39.88；
- Portal 服务器的端口号配置错误，正确端口号应该是 50200；
- 为确保共享密钥与 NCE 一致，重新配置共享密钥为 Huawei@123；
- URL 中的端口号配置错误，正确端口应该是 19008（NCE 默认端口）；
- 需要关闭 Portal 服务器探测功能（因为 NCE 默认未开启探测功能）。

安全管理 > AAA > 外置Portal全局设置 > 修改认证服务器

* 服务器名称: abc

* 服务器IP地址: IPv4 . . . +

服务器IP地址 ×

① 172.21.39.89

协议类型: Portal HTTP HACA

* 共享密钥: ②

报文端口号: ③ 50100

本机网关地址: . . .

URL: ④ https://172.21.39.88:8445/p

URL配置结果: https://172.21.39.88:8445/portal?ac-ip=&redirect-url=redirect-url&usermac=user-mac

√ 服务器探测配置

Portal服务器探测: ⑤ ON

探测周期(秒): 60

状态为UP的Portal服务器最小数目: 0

探测失败超过最大次数后动作: 发送日志信息 发送告警信息

确定 取消

手动修改以上五处配置错误后，正确的配置如下所示：

安全管理 > AAA > 外置Portal全局设置 > 修改认证服务器

* 服务器名称:

* 服务器IP地址: IPv4

服务器IP地址

① 172.21.39.88

协议类型: Portal HTTP HACA

* 共享密钥: ②

报文端口号: ③

本机网关地址:

URL: ④

URL配置结果: https://172.21.39.88:19008/portal?ac-ip=&redirect-url=redirect-url&usermac=user-mac&

服务器探测配置

Portal服务器探测: ⑤ OFF

最后在 STA 上断开无线连接，然后重新连接“wlan-net”，发现已经可以弹出 Portal 认证页面，输入用户名/密码，Portal 认证成功。

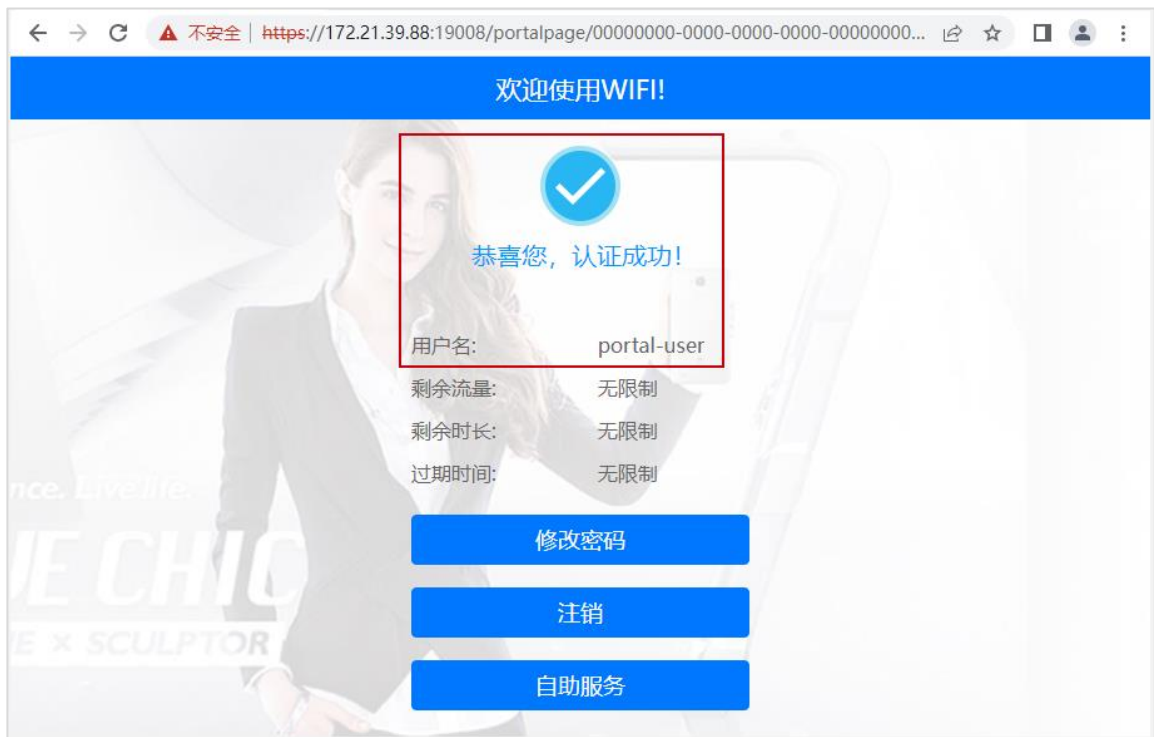
12.3 结果验证

12.3.1 检查 AP 上线状态

选择“监控 > AP”，选择“AP 统计”选项卡，可以查看 AP 的状态信息，其中“normal”代表 AP 已正常上线。

同时可以看到所有 AP 均属于 AP 组“ap-group1”。

12.3.3 STA 关联无线信号，认证通过



12.4 配置参考

12.4.1 WAC1 配置

```
#
defence engine enable
sysname WAC1
#
http timeout 10080
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif100
http server enable
#
vlan batch 100 to 101
#
authentication-profile name p1
portal-access-profile portal1
free-rule-template free1
authentication-scheme radius_huawei
accounting-scheme scheme1
radius-server radius_huawei
#
web-auth-server server-source all-interface
#
management-port isolate enable
management-plane isolate enable
#
radius-server template default
radius-server template radius_huawei
radius-server shared-key cipher %^%#]gR#5-y9p=z#}}Pk4-L;WGPdIm[,VBkhjz&Wf<G%%^%#
radius-server authentication 172.21.39.88 1812 source Vlanif 100 weight 80
radius-server accounting 172.21.39.88 1813 source Vlanif 100 weight 80
radius-server authorization 172.21.39.88 shared-key cipher %^%#5jF1YZq(*OsX-2U&P}A<]'!XH,|-r15kUd$G}=]"%^%# server-group radius_huawei
radius-server authorization server-source all-interface
#
free-rule-template name default_free_rule
#
free-rule-template name free1
free-rule 1 destination ip 172.21.39.88 mask 255.255.255.255
#
url-template name url1
url https://172.21.39.88:19008/portal
url-parameter redirect-url redirect-url ssid ssid user-ipaddress userip user-mac usermac device-ip ac-ip
#
web-auth-server abc
server-ip 172.21.39.88
port 50200
shared-key cipher %^%#/H+oJc*rtC_]{{(WRUDt4un;&<1:g~NP{q(SD$ux#%^%#
url-template url1
source-ip 10.23.100.1
#
```

```
portal-access-profile name portal1
  web-auth-server abc direct
#
portal-access-profile name portal_access_profile
#
aaa
  authentication-scheme radius_huawei
  authentication-mode radius
  accounting-scheme scheme1
  accounting-mode radius
  accounting realtime 3
  local-aaa-user password policy administrator
  domain default
  authentication-scheme default
  accounting-scheme default
  radius-server default
  domain default_admin
  authentication-scheme default
  accounting-scheme default
#
interface Vlanif1
  ip address dhcp-alloc unicast
#
interface Vlanif100
  ip address 10.23.100.1 255.255.255.0
  management-interface
#
interface MEth0/0/1
  ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
  ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#EjVsX!hYu4YZ2_G4#DzXA@:RKv34&REZ}|-y_]mY%^%#
capwap dtls inter-controller psk %^%#{9Wo7!%#BFZ<@EQ:JG>Rp<|47s,v>YPa.#^!]A9%^%#
capwap dtls no-auth enable
#
wlan
  calibrate flexible-radio auto-switch
```

```
temporary-management psk %^%#PwFE@vw_"@n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\KXW7QH=Ogpvg'K*Y)I%^%#
traffic-profile name default
security-profile name default
security-profile name wlan-net
    security open
security-profile name default-wds
security-profile name default-mesh
ssid-profile name default
ssid-profile name wlan-net
    ssid wlan-net
vap-profile name default
vap-profile name wlan-net
    forward-mode tunnel
    service-vlan vlan-id 101
    ssid-profile wlan-net
    security-profile wlan-net
    authentication-profile p1
wds-profile name default
mesh-handover-profile name default
mesh-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-whitelist-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
ap-group name default
ap-group name ap-group1
    regulatory-domain-profile domain1
    radio 0
        vap-profile wlan-net wlan 1
    radio 1
        vap-profile wlan-net wlan 1
ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
    ap-name AP1
    ap-group ap-group1
ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
    ap-name AP2
    ap-group ap-group1
ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
```

```
ap-name AP3
ap-group ap-group1
provision-ap
#
return
```

12.4.2 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101
#
dhcp enable
#
vlan 99
 name Manage
#
interface Vlanif1
#
interface Vlanif99
 ip address 172.21.39.253 255.255.128.0
#
interface Vlanif100
 ip address 10.23.100.254 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 10.23.101.254 255.255.255.0
 dhcp select interface
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
 port link-type access
 port default vlan 99
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
```

```
#
interface MultiGE0/0/8
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
return
```

12.4.3 SW-Access 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Access
#
vlan batch 100 to 101
#
interface Vlanif1
#
interface MEth0/0/1
ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/3
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/9
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
return
```

12.5 思考题

本实验中，WAC1 上配置的 URL 地址由 Portal 服务器的 IP 地址表示，实际生产环境中，URL 地址常用域名来表示。此时，在部署 Portal 认证过程中，需要额外注意什么事项？

参考答案：

由于 STA 在访问 Portal 服务器的过程中，需要通过 DNS 服务器将域名解析为 IP 地址，所以在部署 Portal 认证过程中，需要额外配置免认证规则模板，事先放通 DNS 服务器的地址，保证 DNS 解析正确。
