

华为认证 WLAN 系列教程

HCIP-WLAN

实验指导手册

版本：2.0



华为技术有限公司

版权所有 © 华为技术有限公司 2022。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技术架构与应用认证、云服务与平台认证两类认证。

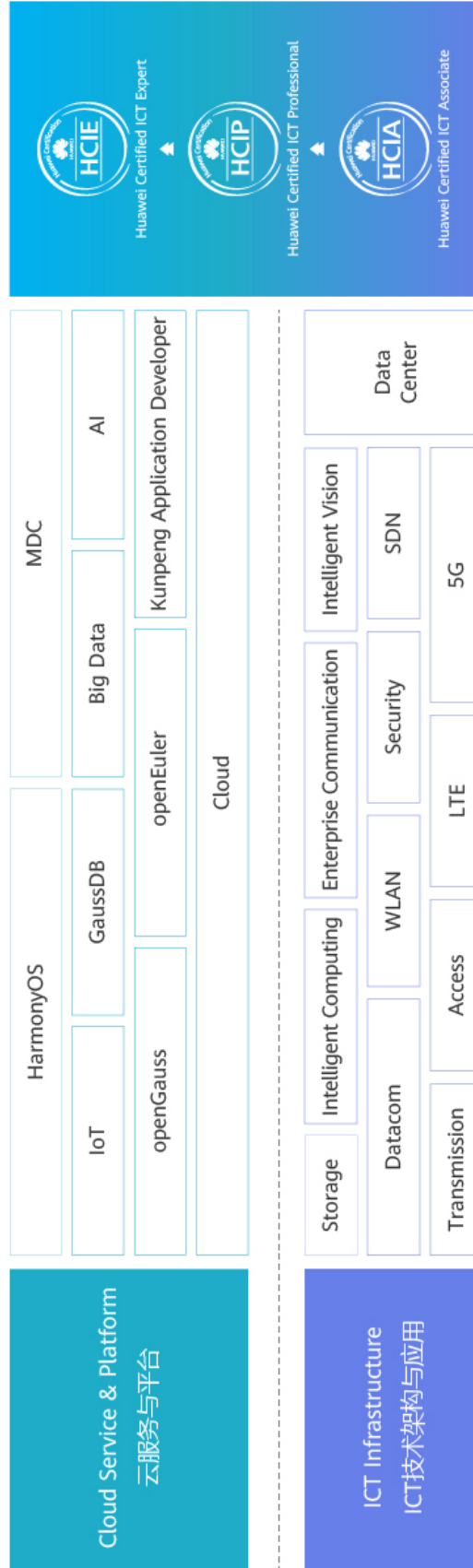
根据ICT从业者的学习和进阶需求，华为认证分为工程师级别、高级工程师级别和专家级别三个认证等级。

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。

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

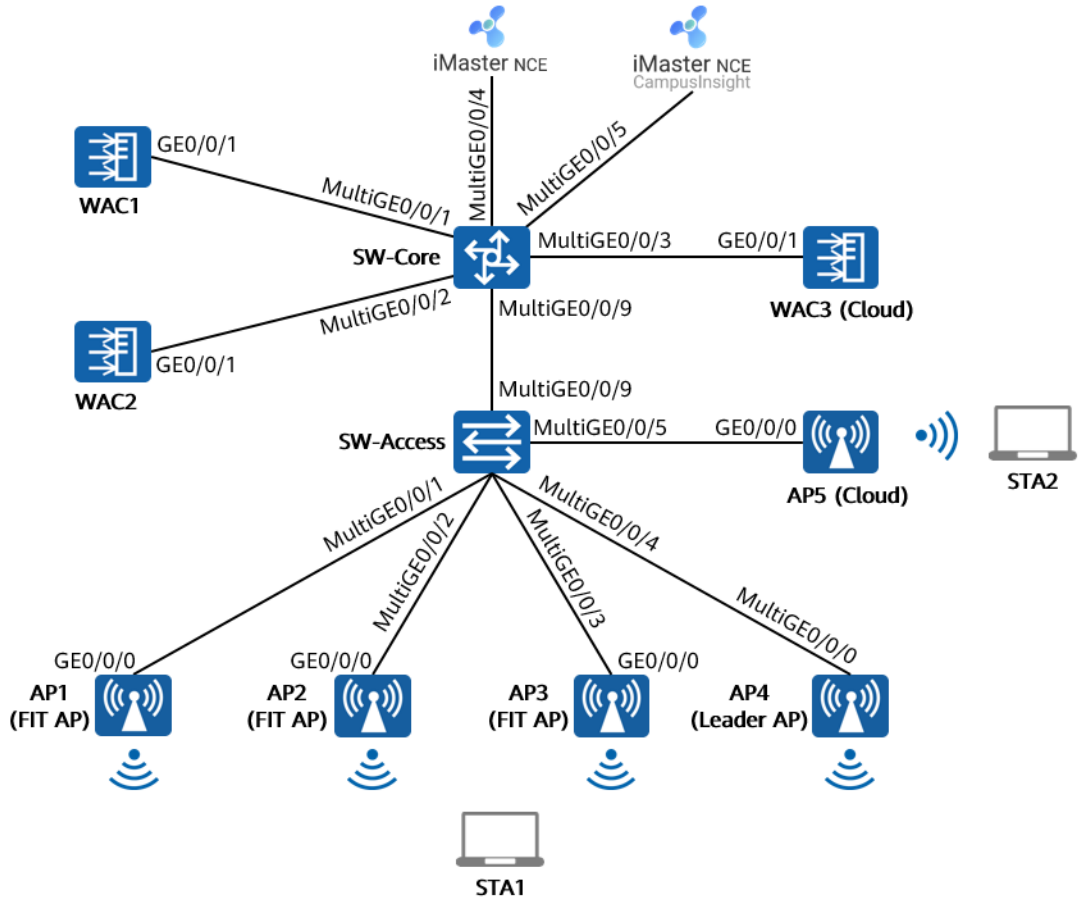
准备实验环境

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.....	21
1.3.1 查看 AP 上线情况、SSID 等信息.....	21
1.3.2 终端关联无线信号，测试网络连通性.....	22
1.4 配置参考.....	22
1.4.1 WAC1 配置.....	22
1.4.2 SW-Core 配置.....	25
1.4.3 SW-Access 配置.....	25
1.5 思考题.....	26
2 Leader AP 组网实验	27
2.1 实验介绍.....	27
2.1.1 关于本实验.....	27
2.1.2 实验目的.....	27
2.1.3 实验组网介绍.....	27
2.1.4 实验规划.....	28
2.2 实验任务配置.....	29

2.2.1 配置思路.....	29
2.2.2 配置步骤.....	29
2.3 结果验证.....	38
2.3.1 查看 AP 上线状态、SSID 等信息.....	38
2.3.2 查看射频状态信息.....	39
2.3.3 查看 VLAN 信息.....	39
2.3.4 STA 接入无线网络，测试网络连通性.....	40
2.4 配置参考.....	40
2.4.1 SW-Core 配置.....	40
2.4.2 SW-Access 配置.....	41
2.4.3 Leader AP 配置.....	42
2.5 思考题.....	44
3 VRRP 热备份实验.....	45
3.1 实验介绍.....	45
3.1.1 关于本实验.....	45
3.1.2 实验目的.....	45
3.1.3 实验组网介绍.....	45
3.1.4 实验规划.....	46
3.2 实验任务配置.....	47
3.2.1 配置思路.....	47
3.2.2 配置步骤.....	47
3.3 结果验证.....	55
3.3.1 检查 AP 上线状态.....	55
3.3.2 检查 VAP 信息.....	55
3.3.3 检查 VRRP 状态信息.....	56
3.3.4 检查 HSB 主备服务状态信息.....	57
3.3.5 检查 HSB 备份组状态信息.....	58
3.3.6 检查无线配置同步状态信息.....	59
3.3.7 STA 关联无线信号，测试网络连通性.....	60
3.4 配置参考.....	60
3.4.1 WAC1 配置.....	60
3.4.2 WAC2 配置.....	62
3.4.3 SW-Core 配置.....	64
3.4.4 SW-Access 配置.....	65
3.5 思考题.....	66

4 云管理组网实验	67
4.1 实验介绍.....	67
4.1.1 关于本实验.....	67
4.1.2 实验目的.....	67
4.1.3 实验组网介绍.....	67
4.1.4 实验规划.....	68
4.2 实验任务配置.....	70
4.2.1 配置思路.....	70
4.2.2 配置步骤.....	70
4.3 结果验证.....	86
4.3.1 在 WAC3 上检查云管理信息.....	86
4.3.2 STA 接入无线网络，测试网络连通性.....	87
4.3.3 在 NCE 上查看设备运行状态.....	88
4.3.4 在 NCE 上查看终端接入状况.....	88
4.4 配置参考.....	89
4.4.1 WAC3 配置.....	89
4.4.2 AP5 配置.....	91
4.4.3 SW-Core 配置.....	94
4.4.4 SW-Access 配置.....	96
4.5 思考题.....	97
5 802.1X 认证实验	98
5.1 实验介绍.....	98
5.1.1 关于本实验.....	98
5.1.2 实验目的.....	98
5.1.3 实验组网介绍.....	98
5.1.4 实验规划.....	99
5.2 实验任务配置.....	100
5.2.1 配置思路.....	100
5.2.2 配置步骤.....	101
5.3 结果验证.....	112
5.3.1 检查 AP 上线状态.....	112
5.3.2 检查 VAP 信息.....	113
5.3.3 STA 关联无线信号，认证成功.....	113
5.3.4 查看 NCE 终端认证日志.....	121
5.3.5 在 WAC1 检查终端认证情况.....	122

5.4 配置参考	123
5.4.1 WAC1 配置.....	123
5.4.2 SW-Core 配置.....	126
5.4.3 SW-Access 配置.....	127
5.5 思考题	128
6 Portal 认证实验	129
6.1 实验介绍	129
6.1.1 关于本实验	129
6.1.2 实验目的.....	129
6.1.3 实验组网介绍.....	129
6.1.4 实验规划.....	130
6.2 实验任务	132
6.2.1 配置思路配置.....	132
6.2.2 配置步骤.....	132
6.3 结果验证	144
6.3.1 检查 AP 上线状态	144
6.3.2 检查 VAP 信息	144
6.3.3 STA 通过 Portal 认证方式接入无线网络	145
6.3.4 查看 NCE 终端认证日志	146
6.3.5 在 WAC1 上检查终端认证情况.....	147
6.4 配置参考	148
6.4.1 WAC1 配置.....	148
6.4.2 SW-Core 配置.....	151
6.4.3 SW-Access 配置.....	152
6.5 思考题	153
7 WLAN 漫游实验	154
7.1 实验介绍	154
7.1.1 关于本实验	154
7.1.2 实验目的.....	154
7.1.3 实验组网介绍.....	154
7.1.4 实验规划.....	155
7.2 实验任务配置	157
7.2.1 配置思路.....	157
7.2.2 配置步骤.....	157
7.3 结果验证	164

7.3.1 检查 AP 上线.....	164
7.3.2 检查 VAP 状态.....	165
7.3.3 检查漫游组状态.....	165
7.3.4 观察 STA 漫游情况.....	166
7.4 配置参考.....	167
7.4.1 WAC1 配置.....	167
7.4.2 WAC2 配置.....	170
7.4.3 SW-Core 配置.....	172
7.4.4 SW-Access 配置.....	173
7.5 思考题.....	174
8 射频资源管理实验.....	175
8.1 实验介绍.....	175
8.1.1 关于本实验.....	175
8.1.2 实验目的.....	175
8.1.3 实验组网介绍.....	175
8.1.4 实验规划.....	176
8.2 实验任务配置.....	177
8.2.1 配置思路.....	177
8.2.2 配置步骤.....	177
8.3 结果验证.....	179
8.3.1 查看 RRM 模板信息.....	179
8.3.2 查看 2G 射频模板信息.....	181
8.3.3 查看 5G 射频模板信息.....	182
8.3.4 查看当前射频状态信息.....	183
8.4 配置参考.....	184
8.4.1 WAC1 配置.....	184
8.4.2 SW-Core 配置.....	187
8.4.3 SW-Access 配置.....	188
8.5 思考题.....	188
9 室内网络规划实验.....	190
9.1 实验介绍.....	190
9.1.1 关于本实验.....	190
9.1.2 实验目的.....	190
9.1.3 实验场景介绍.....	190
9.1.4 前期准备工作.....	191

9.2 实验任务配置	193
9.2.1 配置思路	193
9.2.2 配置步骤	193
9.3 思考题	218
10 室外网络规划实验	220
10.1 实验介绍	220
10.1.1 关于本实验	220
10.1.2 实验目的	220
10.1.3 实验场景介绍	220
10.1.4 前期准备工作	221
10.2 实验任务配置	223
10.2.1 配置思路	223
10.2.2 配置步骤	223
10.3 思考题	240
11 CampusInsight 智能运维实验	242
11.1 实验介绍	242
11.1.1 关于本实验	242
11.1.2 实验目的	242
11.1.3 实验组网介绍	242
11.1.4 实验规划	243
11.2 实验任务配置	244
11.2.1 配置思路	244
11.2.2 配置步骤	244
11.3 结果验证	257
11.3.1 查看 WAC1 的 SNMP 协议	257
11.3.2 查看 WAC1 的 VAP 信息	257
11.4 配置参考	258
11.4.1 WAC1 配置	258
11.4.2 SW-Core 配置	261
11.4.3 SW-Access 配置	262
11.5 思考题	263
12 故障排查综合实验	264
12.1 实验介绍	264
12.1.1 关于本实验	264
12.1.2 实验目的	264

12.1.3 实验组网介绍	264
12.1.4 实验规划	265
12.2 实验任务配置	267
12.2.1 配置思路	267
12.2.2 配置步骤	267
12.3 结果验证	276
12.3.1 检查 VAP 信息	276
12.3.2 STA 关联无线信号，认证通过	277
12.4 配置参考	278
12.4.1 WAC1 配置	278
12.4.2 SW-Core 配置	281
12.4.3 SW-Access 配置	282
12.5 思考题	283

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

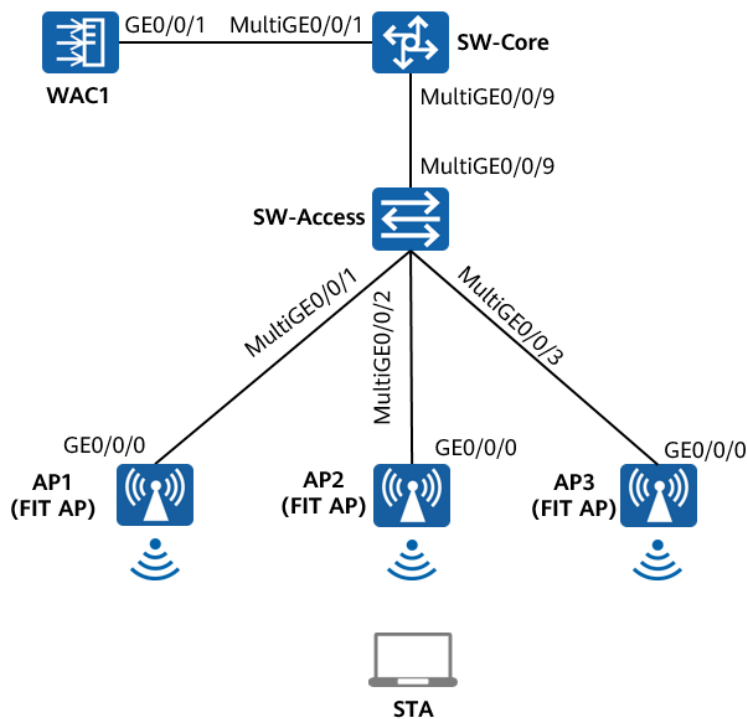


图1-1 WAC+FIT AP 组网实验拓扑图

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

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、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 可以获取管理 IP 地址。
- 4.在 WAC1 上配置 CAPWAP 源端口或源地址，以及 AP 认证方式。
- 5.配置 WLAN 业务参数，实现 STA 接入。

1.2.2 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
```

配置 WAC1 设备。创建 VLAN 100、101，GE0/0/1 端口类型修改为 Trunk，并允许通过 VLAN 100、101。

在 WAC1 上创建 VLAN 100、101。

```
<AirEngine9700-M1> system-view
[AirEngine9700-M1] sysname WAC1
[WAC1] vlan batch 100 101
```

配置 WAC1 的 GE0/0/1 端口类型及允许通过的 VLAN。

```
[WAC1] interface GigabitEthernet 0/0/1
[WAC1-GigabitEthernet /0/1] port link-type trunk
[WAC1-GigabitEthernet /0/1] port trunk allow-pass vlan 100 101
[WAC1-GigabitEthernet /0/1] quit
```

步骤 2 配置设备 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
```

配置 WAC1 的 IP 地址。

```
[WAC1] interface vlan 100
[WAC1-Vlanif100] ip address 10.23.100.1 24
[WAC1-Vlanif100] quit
```

步骤 3 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 4 配置 AP 上线

开启 CAPWAP DTLS 不认证。（V200R021C00 及之后版本）

```
[WAC1] capwap dtls no-auth enable
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is
enabled and brings security risks. After the device goes online for the first time, disable this function to
prevent security risks. Continue? [Y/N]: y
```

在 WAC1 上配置 CAPWAP 源端口，需要提前配置以下参数：

DTLS 预共享密钥：此处配置为 a1234567；

WAC 间 DTLS 预共享密钥：此处配置为 a1234567；

FIT AP 的管理参数（用户名/密码）：此处配置为 admin/Huawei@123；

全局离线管理 VAP 的登录密码：此处配置为 a1234567。

```
[WAC1] capwap dtls psk a1234567
[WAC1] capwap dtls inter-controller psk a1234567
[WAC1] capwap source interface vlanif 100
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters,
underscores, and digits, and must start with a letter):admin
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a combination of at least three of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters):Huawei@123
Confirm password:Huawei@123
Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text
characters that must be a combination of at least two of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters):a1234567
Confirm PSK:a1234567
```


Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.

Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.

创建 AP 组。

```
[WAC1] wlan
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

在 WAC1 上配置 AP 认证方式为 MAC 认证。

```
[WAC1] wlan
[WAC1-wlan-view] ap auth-mode mac-auth
[WAC1-wlan-view] quit
```

在 WAC1 上添加 AP (AP 的 MAC 地址以实际情况为准)。

```
[WAC1] wlan
[WAC1-wlan-view] ap-id 0 ap-mac 9cb2-e82d-54f0
[WAC1-wlan-ap-0] ap-group ap-group1
[WAC1-wlan-ap-0] ap-name AP1
[WAC1-wlan-ap-0] quit
[WAC1-wlan-view] ap-id 1 ap-mac 9cb2-e82d-5410
[WAC1-wlan-ap-1] ap-group ap-group1
[WAC1-wlan-ap-1] ap-name AP2
[WAC1-wlan-ap-1] quit
[WAC1-wlan-view] ap-id 2 ap-mac 9cb2-e82d-5110
[WAC1-wlan-ap-2] ap-group ap-group1
[WAC1-wlan-ap-2] ap-name AP3
[WAC1-wlan-ap-2] quit
[WAC1-wlan-view] quit
```

使用 display ap all 命令可以检查三个 AP 均已上线, 状态为 normal。

```
[WAC1] display ap all
Total AP information:
nor   : normal           [3]
ExtraInfo : Extra information
-----
ID    MAC                Name Group      IP           Type          State  STA  Uptime ExtraInfo
-----
0     9cb2-e82d-54f0 AP1  ap-group1 10.23.100.177 AirEngine5761-11 nor   0    9M:47S -
1     9cb2-e82d-5410 AP2  ap-group1 10.23.100.36  AirEngine5761-11 nor   0    7M:14S -
2     9cb2-e82d-5110 AP3  ap-group1 10.23.100.211 AirEngine5761-11 nor   0    7M:18S -
-----
Total: 3
```

步骤 5 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成对应的国家码）。

```
[WAC1] wlan
[WAC1-wlan-view] regulatory-domain-profile name domain1
[WAC1-wlan-regulate-domain-domain1] country-code CN
[WAC1-wlan-regulate-domain-domain1] quit
```

在 ap-group 中引用域管理模板。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may
restart APs. Continue?[Y/N]: y
[WAC1-wlan-ap-group-ap-group1] quit
```

创建名为“wlan-net”的安全模板，并配置安全策略。

```
[WAC1] wlan
[WAC1-wlan-view] security-profile name wlan-net
[WAC1-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a12345678 aes
[WAC1-wlan-sec-prof-wlan-net] quit
```

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

```
[WAC1-wlan-view] ssid-profile name wlan-net
[WAC1-wlan-ssid-prof-wlan-net] ssid wlan-net
[WAC1-wlan-ssid-prof-wlan-net] quit
```

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。

```
[WAC1-wlan-view] vap-profile name wlan-net
[WAC1-wlan-vap-prof-wlan-net] forward-mode direct-forward
[WAC1-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[WAC1-wlan-vap-prof-wlan-net] security-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] quit
```

配置 AP 组引用 VAP 模板，AP 上射频 0 和射频 1 都使用 VAP 模板“wlan-net”的配置。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

检查 VAP 状态。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID          Status  Auth type   STA   SSID
-----
```

0	AP1	0	1	9CB2-E82D-54F0	ON	WPA/WPA2-PSK	0	wlan-net
0	AP1	1	1	9CB2-E82D-5500	ON	WPA/WPA2-PSK	0	wlan-net
1	AP2	0	1	9CB2-E82D-5410	ON	WPA/WPA2-PSK	0	wlan-net
1	AP2	1	1	9CB2-E82D-5420	ON	WPA/WPA2-PSK	0	wlan-net
2	AP3	0	1	9CB2-E82D-5110	ON	WPA/WPA2-PSK	0	wlan-net
2	AP3	1	1	9CB2-E82D-5120	ON	WPA/WPA2-PSK	0	wlan-net

Total:								

1.3 结果验证

1.3.1 查看 AP 上线情况、SSID 等信息

在 WAC1 上执行 display ap all 命令，查看 AP 的上线结果。

```
[WAC1] display ap all
Total AP information:
nor : normal          [3]
ExtraInfo : Extra information
-----
ID   MAC           Name Group   IP           Type           State STA  Uptime ExtraInfo
-----
0    9cb2-e82d-54f0 AP1  ap-group1 10.23.100.177 AirEngine5761-11 nor   0    9M:47S -
1    9cb2-e82d-5410 AP2  ap-group1 10.23.100.36  AirEngine5761-11 nor   0    7M:14S -
2    9cb2-e82d-5110 AP3  ap-group1 10.23.100.211 AirEngine5761-11 nor   0    7M:18S -
-----
Total: 3
```

以上显示中，可以看到 AP 的 MAC 地址，加入的 AP 组名称，AP 动态获取的 IP 地址和 AP 的型号以及 AP 上线状态。

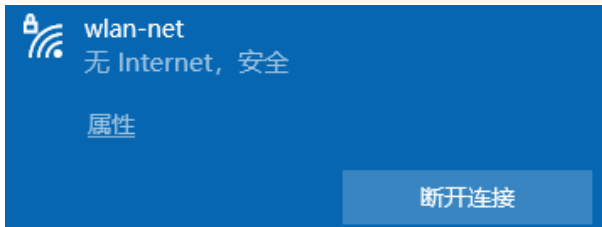
在 WAC1 上执行 display vap all 命令，查看 VAP 信息如下。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID           Status Auth type   STA  SSID
-----
0     AP1     0    1    9CB2-E82D-54F0 ON      WPA/WPA2-PSK 0    wlan-net
0     AP1     1    1    9CB2-E82D-5500 ON      WPA/WPA2-PSK 0    wlan-net
1     AP2     0    1    9CB2-E82D-5410 ON      WPA/WPA2-PSK 0    wlan-net
1     AP2     1    1    9CB2-E82D-5420 ON      WPA/WPA2-PSK 0    wlan-net
2     AP3     0    1    9CB2-E82D-5110 ON      WPA/WPA2-PSK 0    wlan-net
2     AP3     1    1    9CB2-E82D-5120 ON      WPA/WPA2-PSK 0    wlan-net
-----
Total: 6
```

以上显示中，可以查看 VAP 关联的 AP 名称、BSSID 名称、SSID 名称、认证方式等。

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
  management-interface
#
interface MEth0/0/1
  ip address 169.254.1.1 255.255.255.0
#
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 %^%#yo9h*3&U`Ry!ihRA+uol~E6l,`g2w1U~T9Z3-A^+%^%#
capwap dtls inter-controller psk %^%#Vro-.X&7';8.D+~k{]a0*6,H7.{2[McU1_Q1qxPY%^%#
capwap dtls no-auth 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)|%^%#
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

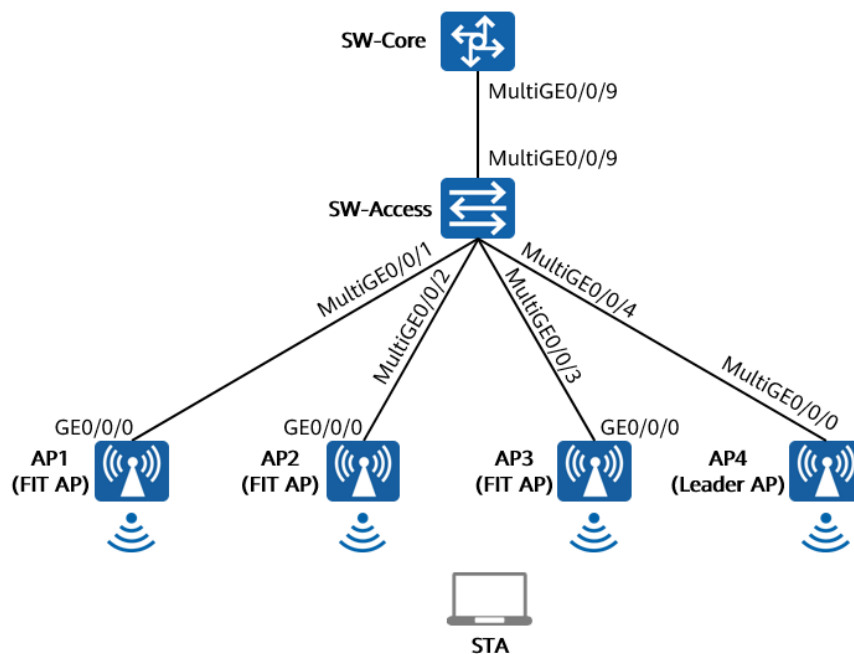


图2-1 Leader AP 组网实验拓扑图

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

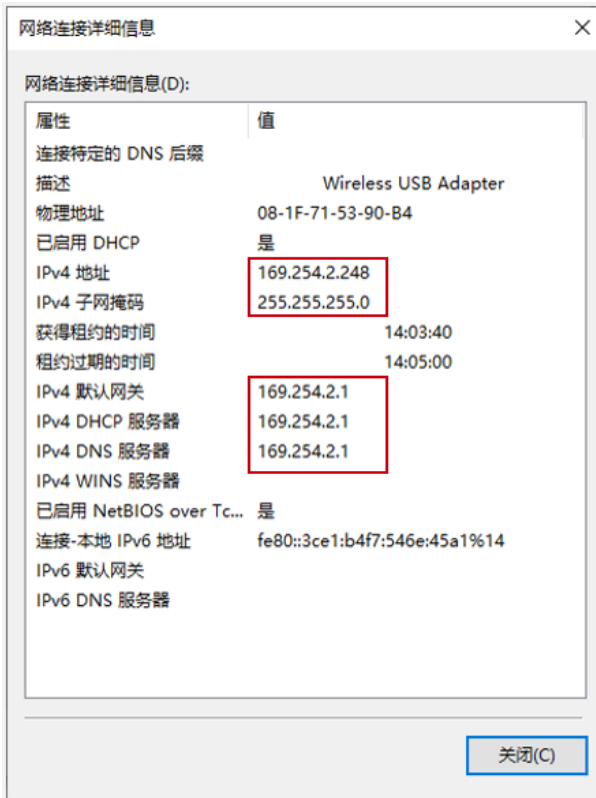
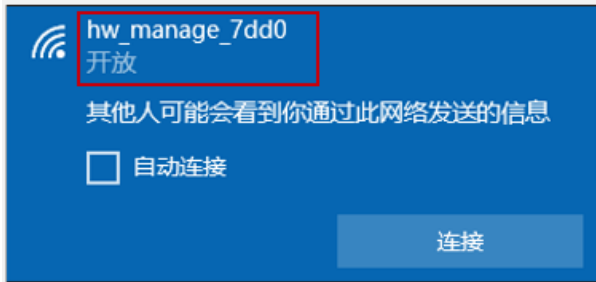
可以看到 AP1~AP4 均获取到 IP 地址（获取地址以实际情况为准）。

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。





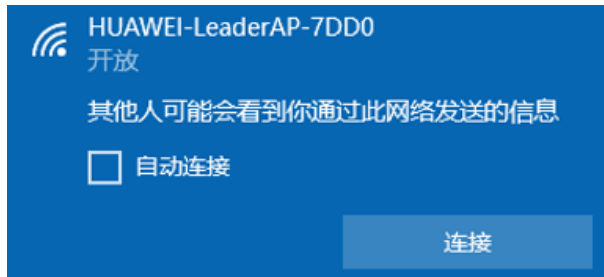
重新登录 AP4，如下所示。



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。

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

监控 向导 配置 维护 高级

上网配置 无线网络配置 接入点配置 系统配置

AP配置 AP接入安全

AP列表

添加 替换 删除 闪灯 导出 刷新

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

10 共4条

未认证AP列表

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。

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

监控 向导 配置 维护 高级

配置向导

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:

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

共4条

网络 (Networks) Section:

- Navigation: SSID名称
- Table:

SSID名称 ▲	用户数 ▲
wlan-net	0
HUAWEI-LeaderAP-7DD0	1

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

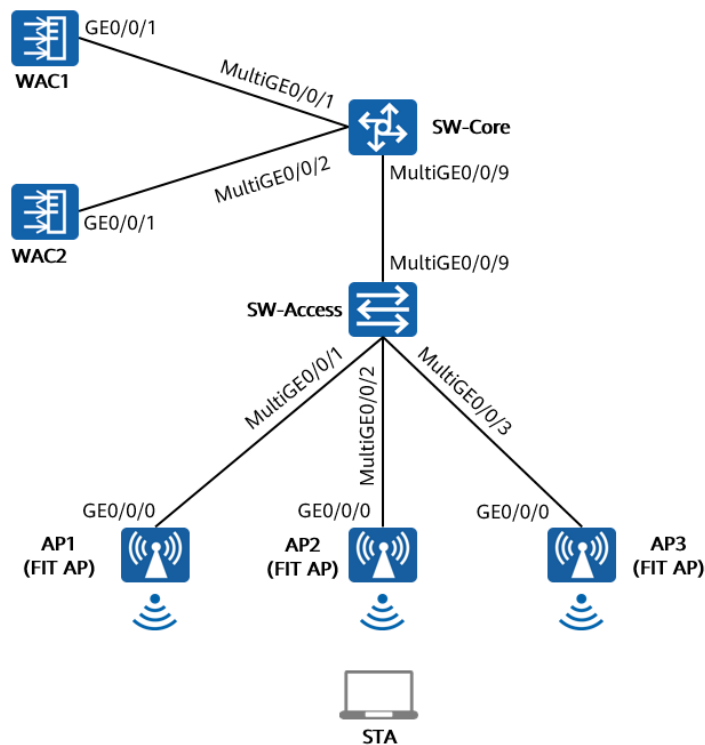


图3-1 VRRP 热备份实验拓扑图

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 配置网络互通

- # 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 WAC1 设备，创建 VLAN 100、101，GE0/0/1 端口类型修改为 Trunk，并允许通过 VLAN 100、101。

在 WAC1 上创建 VLAN 100、101。

```
<AirEngine9700-M1> system-view
[AirEngine9700-M1] sysname WAC1
[WAC1] vlan batch 100 101
```

配置 WAC1 的 GE0/0/1 端口类型及允许通过的 VLAN。

```
[WAC1] interface GigabitEthernet 0/0/1
[WAC1-GigabitEthernet /0/1] port link-type trunk
[WAC1-GigabitEthernet /0/1] port trunk allow-pass vlan 100 101
[WAC1-GigabitEthernet /0/1] quit
```

配置 WAC2 设备，创建 VLAN 100、101，GE0/0/1 端口类型修改为 Trunk，并允许通过 VLAN 100、101。

在 WAC2 上创建 VLAN 100、101。

```
<AirEngine9700-M1> system-view
[AirEngine9700-M1] sysname WAC2
[WAC2] vlan batch 100 101
```

配置 WAC2 的 GE0/0/1 端口类型及允许通过的 VLAN。

```
[WAC2] interface GigabitEthernet 0/0/1
[WAC2-GigabitEthernet /0/1] port link-type trunk
[WAC2-GigabitEthernet /0/1] port trunk allow-pass vlan 100 101
[WAC2-GigabitEthernet /0/1] quit
```

配置 SW-Core、WAC1、WAC2 的 IP 地址。

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
```

配置 WAC1 的 IP 地址。

```
[WAC1] interface vlan 100
[WAC1-Vlanif100] ip address 10.23.100.1 24
[WAC1-Vlanif100] quit
```

配置 WAC2 的 IP 地址。

```
[WAC2] interface vlan 100
[WAC2-Vlanif100] ip address 10.23.100.2 24
[WAC2-Vlanif100] quit
```

步骤 2 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（后续的 VRRP 协议使用），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 10.23.100.9
[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 3 配置 VRRP 双机热备（WAC1）

配置 VRRP 备份组的状态恢复延迟时间为 60 秒。

```
[WAC1] vrrp recover-delay 60
```

在 WAC1 上创建管理 VRRP 备份组，配置 WAC1 在该备份组中的优先级为 120，并配置抢占时间为 1800 秒。

```
[WAC1] interface vlanif 100
[WAC1-Vlanif100] ip address 10.23.100.1 255.255.255.0
[WAC1-Vlanif100] vrrp vrid 1 virtual-ip 10.23.100.33
[WAC1-Vlanif100] vrrp vrid 1 priority 120
[WAC1-Vlanif100] vrrp vrid 1 preempt-mode timer delay 1800
[WAC1-Vlanif100] admin-vrrp vrid 1
[WAC1-Vlanif100] quit
```

在 WAC1 上创建 HSB 主备服务，并配置其主备通道 IP 地址和端口号，配置 HSB 主备服务报文的重传次数和发送间隔。

```
[WAC1] hsb-service 0
[WAC1-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
[WAC1-hsb-service-0] service-keep-alive detect retransmit 3 interval 6
[WAC1-hsb-service-0] quit
```

在 WAC1 上创建 HSB 备份组，并配置其绑定 HSB 主备服务和管理 VRRP 备份组。

```
[WAC1] hsb-group 0
[WAC1-hsb-group-0] bind-service 0
[WAC1-hsb-group-0] track vrrp vrid 1 interface vlanif 100
[WAC1-hsb-group-0] quit
```

配置 NAC 业务绑定 HSB 备份组。

```
[WAC1] hsb-service-type access-user hsb-group 0
```

配置 WLAN 业务绑定 HSB 备份组。

```
[WAC1] hsb-service-type ap hsb-group 0
```


配置 DHCP 业务绑定 HSB 备份组。

```
[WAC1] hsb-service-type dhcp hsb-group 0
```

使能双机热备功能。

```
[WAC1] hsb-group 0
[WAC1-hsb-group-0] hsb enable
[WAC1-hsb-group-0] quit
```

步骤 4 配置 VRRP 双机热备 (WAC2)

配置 VRRP 备份组的状态恢复延迟时间为 60 秒。

```
[WAC2] vrrp recover-delay 60
```

在 WAC2 上创建管理 VRRP 备份组。

```
[WAC2] interface vlanif 100
[WAC2-Vlanif100] ip address 10.23.100.2 255.255.255.0
[WAC2-Vlanif100] vrrp vrid 1 virtual-ip 10.23.100.33
[WAC2-Vlanif100] admin-vrrp vrid 1
[WAC2-Vlanif100] quit
```

在 WAC2 上创建 HSB 主备服务，并配置其主备通道 IP 地址和端口号，配置 HSB 主备服务报文的重传次数和发送间隔。

```
[WAC2] hsb-service 0
[WAC2-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
[WAC2-hsb-service-0] service-keep-alive detect retransmit 3 interval 6
[WAC2-hsb-service-0] quit
```

在 WAC2 上创建 HSB 备份组，并配置其绑定 HSB 主备服务和管理 VRRP 备份组。

```
[WAC2] hsb-group 0
[WAC2-hsb-group-0] bind-service 0
[WAC2-hsb-group-0] track vrrp vrid 1 interface vlanif 100
[WAC2-hsb-group-0] quit
```

配置 NAC 业务绑定 HSB 备份组。

```
[WAC2] hsb-service-type access-user hsb-group 0
```

配置 WLAN 业务绑定 HSB 备份组。

```
[WAC2] hsb-service-type ap hsb-group 0
```

配置 DHCP 业务绑定 HSB 备份组。

```
[WAC2] hsb-service-type dhcp hsb-group 0
```

使能双机热备功能

```
[WAC2] hsb-group 0
[WAC2-hsb-group-0] hsb enable
[WAC2-hsb-group-0] quit
```

步骤 5 配置无线配置同步功能

配置 WAC1 的无线配置同步功能。

```
[WAC1] wlan
[WAC1-wlan-view] master controller
[WAC1-master-controller] master-redundancy peer-ip ip-address 10.23.100.2 local-ip ip-address
10.23.100.1 psk Huawei@123
[WAC1-master-controller] master-redundancy track-vrrp vrid 1 interface Vlanif 100
[WAC1-master-controller] quit
```

配置 WAC2 的无线配置同步功能。

```
[WAC2] wlan
[WAC2-wlan-view] master controller
[WAC2-master-controller] master-redundancy peer-ip ip-address 10.23.100.1 local-ip ip-address
10.23.100.2 psk Huawei@123
[WAC2-master-controller] master-redundancy track-vrrp vrid 1 interface Vlanif 100
[WAC2-master-controller] quit
```

步骤 6 配置 CAPWAP 源地址

配置 WAC1 参数。

在 WAC1 上开启 CAPWAP DTLS 不认证。（V200R021C00 及之后版本）

```
[WAC1] capwap dtls no-auth enable
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is
enabled and brings security risks. After the device goes online for the first time, disable this function to
prevent security risks. Continue? [Y/N]: y
```

在 WAC1 上配置 CAPWAP 源地址，需要提前配置以下参数：

DTLS 预共享密钥：此处配置为 a1234567；

WAC 间 DTLS 预共享密钥：此处配置为 a1234567；

FIT AP 的管理参数（用户名/密码）：此处配置为 admin/Huawei@123；

全局离线管理 VAP 的登录密码：此处配置为 a1234567。

```
[WAC1] capwap dtls psk a1234567
[WAC1] capwap dtls inter-controller psk a1234567
[WAC1] capwap source ip-address 10.23.100.33
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters,
underscores, and digits, and must start with a letter):admin
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a combination of at least three of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters):Huawei@123
Confirm password:Huawei@123
Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text
characters that must be a combination of at least two of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters):a1234567
Confirm PSK:a1234567
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be
interrupted.
Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version
earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.
```

配置 WAC2 参数。

在 WAC2 上开启 CAPWAP DTLS 不认证。（V200R021C00 及之后版本）

```
[WAC2] capwap dtls no-auth enable
```

Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is enabled and brings security risks. After the device goes online for the first time, disable this function to prevent security risks. Continue? [Y/N]: y

在 WAC2 上配置 CAPWAP 源地址，需要提前配置以下参数：

DTLS 预共享密钥：此处配置为 a1234567；

WAC 间 DTLS 预共享密钥：此处配置为 a1234567；

FIT AP 的管理参数（用户名/密码）：此处配置为 admin/Huawei@123；

全局离线管理 VAP 的登录密码：此处配置为 a1234567。

```
[WAC2] capwap dtls psk a1234567
```

```
[WAC2] capwap dtls inter-controller psk a1234567
```

```
[WAC2] capwap source ip-address 10.23.100.33
```

Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters, underscores, and digits, and must start with a letter):**admin**

Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):**Huawei@123**

Confirm password:**Huawei@123**

Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):**a1234567**

Confirm PSK:**a1234567**

Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.

Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.

步骤 7 配置 AP 上线（WAC1）

创建 AP 组。

```
[WAC1] wlan
```

```
[WAC1-wlan-view] ap-group name ap-group1
```

```
[WAC1-wlan-ap-group-ap-group1] quit
```

```
[WAC1-wlan-view] quit
```

在 WAC1 上配置 AP 认证方式为 MAC 认证。

```
[WAC1] wlan
```

```
[WAC1-wlan-view] ap auth-mode mac-auth
```

```
[WAC1-wlan-view] quit
```

在 WAC1 上添加 AP（AP 的 MAC 地址以实际情况为准）。

```
[WAC1] wlan
```

```
[WAC1-wlan-view] ap-id 0 ap-mac 9cb2-e82d-54f0
```

```
[WAC1-wlan-ap-0] ap-group ap-group1
```

```
[WAC1-wlan-ap-0] ap-name AP1
[WAC1-wlan-ap-0] quit
[WAC1-wlan-view] ap-id 1 ap-mac 9cb2-e82d-5410
[WAC1-wlan-ap-1] ap-group ap-group1
[WAC1-wlan-ap-1] ap-name AP2
[WAC1-wlan-ap-1] quit
[WAC1-wlan-view] ap-id 2 ap-mac 9cb2-e82d-5110
[WAC1-wlan-ap-2] ap-group ap-group1
[WAC1-wlan-ap-2] ap-name AP3
[WAC1-wlan-ap-2] quit
[WAC1-wlan-view] quit
```

步骤 8 配置无线业务（WAC1）

创建名为“wlan-net”的安全模板，并配置安全策略。

```
[WAC1] wlan
[WAC1-wlan-view] security-profile name wlan-net
[WAC1-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a12345678 aes
[WAC1-wlan-sec-prof-wlan-net] quit
```

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

```
[WAC1-wlan-view] ssid-profile name wlan-net
[WAC1-wlan-ssid-prof-wlan-net] ssid wlan-net
[WAC1-wlan-ssid-prof-wlan-net] quit
```

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。

```
[WAC1-wlan-view] vap-profile name wlan-net
[WAC1-wlan-vap-prof-wlan-net] forward-mode direct-forward
[WAC1-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[WAC1-wlan-vap-prof-wlan-net] security-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] quit
```

配置 AP 组引用 VAP 模板，AP 上射频 0 和射频 1 都使用 VAP 模板“wlan-net”的配置。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

步骤 9 触发配置同步

```
[WAC1] synchronize-configuration
```

3.3 结果验证

3.3.1 检查 AP 上线状态

在 WAC1 上使用 display ap all 命令可以检查三个 AP 均已上线，状态为 normal。

```
[WAC1] display ap all
Total AP information:
nor : normal          [3]
ExtraInfo : Extra information
-----
ID   MAC           Name   Group   IP           Type           State STA  Uptime  ExtraInfo
-----
0    9cb2-e82d-54f0 AP1    ap-group1 10.23.100.225 AirEngine5761-11 nor    0    28M:38S -
1    9cb2-e82d-5410 AP2    ap-group1 10.23.100.214 AirEngine5761-11 nor    0    28M:45S -
2    9cb2-e82d-5110 AP3    ap-group1 10.23.100.117 AirEngine5761-11 nor    0    28M:58S -
-----
Total: 3
```

在 WAC2 上使用 display ap all 命令可以看到三个 AP 的状态为 standby。

```
[WAC2] display ap all
Total AP information:
stdby : standby      [3]
ExtraInfo : Extra information
-----
ID   MAC           Name   Group   IP           Type           State STA  Uptime  ExtraInfo
-----
0    9cb2-e82d-54f0 AP1    ap-group1 10.23.100.225 AirEngine5761-11 stdby  0    -      -
1    9cb2-e82d-5410 AP2    ap-group1 10.23.100.214 AirEngine5761-11 stdby  0    -      -
2    9cb2-e82d-5110 AP3    ap-group1 10.23.100.117 AirEngine5761-11 stdby  0    -      -
-----
Total: 3
```

3.3.2 检查 VAP 信息

在 WAC1 上检查 VAP 状态信息。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID           Status  Auth type  STA  SSID
-----
0     AP1     0    1    9CB2-E82D-54F0 ON      WPA/WPA2-PSK  0    wlan-net
0     AP1     1    1    9CB2-E82D-5500 ON      WPA/WPA2-PSK  0    wlan-net
1     AP2     0    1    9CB2-E82D-5410 ON      WPA/WPA2-PSK  0    wlan-net
1     AP2     1    1    9CB2-E82D-5420 ON      WPA/WPA2-PSK  0    wlan-net
2     AP3     0    1    9CB2-E82D-5110 ON      WPA/WPA2-PSK  0    wlan-net
2     AP3     1    1    9CB2-E82D-5120 ON      WPA/WPA2-PSK  0    wlan-net
```

```
-----
Total: 6
```

在 WAC2 上检查 VAP 状态信息。

```
[WAC2] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID           Status  Auth type      STA  SSID
-----
0     AP1     0    1    9CB2-E82D-54F0 ON      WPA/WPA2-PSK  0    wlan-net
0     AP1     1    1    9CB2-E82D-5500 ON      WPA/WPA2-PSK  0    wlan-net
1     AP2     0    1    9CB2-E82D-5410 ON      WPA/WPA2-PSK  0    wlan-net
1     AP2     1    1    9CB2-E82D-5420 ON      WPA/WPA2-PSK  0    wlan-net
2     AP3     0    1    9CB2-E82D-5110 ON      WPA/WPA2-PSK  0    wlan-net
2     AP3     1    1    9CB2-E82D-5120 ON      WPA/WPA2-PSK  0    wlan-net
-----
Total: 6
```

3.3.3 检查 VRRP 状态信息

在 WAC1 和 WAC2 上分别执行 display vrrp 命令，可以看到 WAC1 的 State 字段显示为 Master，WAC2 的 State 字段显示为 Backup。

WAC1 显示如下。

```
[WAC1] display vrrp
Vlanif100 | Virtual Router 1
  State : Master
  Virtual IP : 10.23.100.33
  Master IP : 10.23.100.1
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay Time : 1800 s
  TimerRun : 2 s
  TimerConfig : 2 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : admin-vrrp
  Backup-forward : disabled
  Track SysHealth Priority reduced : 254
  SysHealth state : UP
```

WAC2 显示如下。

```
[WAC2] display vrrp
Vlanif100 | Virtual Router 1
  State : Backup
```

```
Virtual IP : 10.23.100.33
Master IP : 10.23.100.1
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt : YES   Delay Time : 0 s
TimerRun : 2 s
TimerConfig : 2 s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : admin-vrrp
Backup-forward : disabled
Track SysHealth Priority reduced : 254
SysHealth state : UP
```

3.3.4 检查 HSB 主备服务状态信息

在 WAC1 和 WAC2 上执行 display hsb-service 0 命令，查看主备服务的建立情况。可以看到 Service State 字段的显示为 Connected，说明主备服务通道已经成功建立。

WAC1 显示如下。

```
[WAC1] display hsb-service 0
Hot Standby Service Information:
```

```
-----
Local IP Address      : 10.23.100.1
Peer IP Address       : 10.23.100.2
Source Port           : 10241
Destination Port      : 10241
Keep Alive Times      : 3
Keep Alive Interval   : 6
Service State         : Connected
Service Batch Modules :
Shared-key             : -
-----
```

WAC2 显示如下。

```
[WAC2] display hsb-service 0
Hot Standby Service Information:
```

```
-----
Local IP Address      : 10.23.100.2
Peer IP Address       : 10.23.100.1
Source Port           : 10241
Destination Port      : 10241
Keep Alive Times      : 3
Keep Alive Interval   : 6
Service State         : Connected
Service Batch Modules :
```


3.3.6 检查无线配置同步状态信息

在 WAC1 上查看无线配置同步的状态信息，其中 UP 字段表示配置已同步。

```
[WAC1] display sync-configuration status
Info: This operation may take a few seconds. Please wait for a moment.done.
Controller role:Master/Backup/Local
-----
Controller IP Role   Device Type          Version              Status Last synced
-----
10.23.100.2   Backup  AirEngine9700-M1    V200R021C00SPC100B171 up    XXXX-XX-XX/17:21:06
-----
Total: 1
```

在 WAC1 上查看无线配置同步的配置信息。

```
[WAC1] display sync-configuration master-redundancy
Master redundancy configuration:
-----
Peer IP Version      : IPV4
Peer IP              : 10.23.100.2
VRRP Interface       : Vlanif100
VRRP Vrid            : 1
VRRP Status          : Master
VRRP Type            : VRRPv4
-----
```

在 WAC2 上查看无线配置同步的状态信息，其中 UP 字段表示配置已同步。

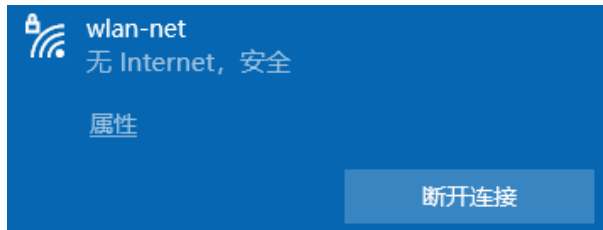
```
[WAC2] display sync-configuration status
Info: This operation may take a few seconds. Please wait for a moment.done.
Controller role:Master/Backup/Local
-----
Controller IP Role   Device Type          Version              Status Last synced
-----
10.23.100.1   Master  AirEngine9700-M1    V200R021C00SPC100B171 up    XXXX-XX-XX /17:21:16
-----
Total: 1
```

在 WAC2 上查看无线配置同步的配置信息。

```
[WAC2] display sync-configuration master-redundancy
Master redundancy configuration:
-----
Peer IP Version      : IPV4
Peer IP              : 10.23.100.1
VRRP Interface       : Vlanif100
VRRP Vrid            : 1
VRRP Status          : Backup
VRRP Type            : VRRPv4
-----
```

3.3.7 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 169.254.1.1 255.255.255.0
#
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 169.254.1.1 255.255.255.0
#
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 10.23.100.9
#
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

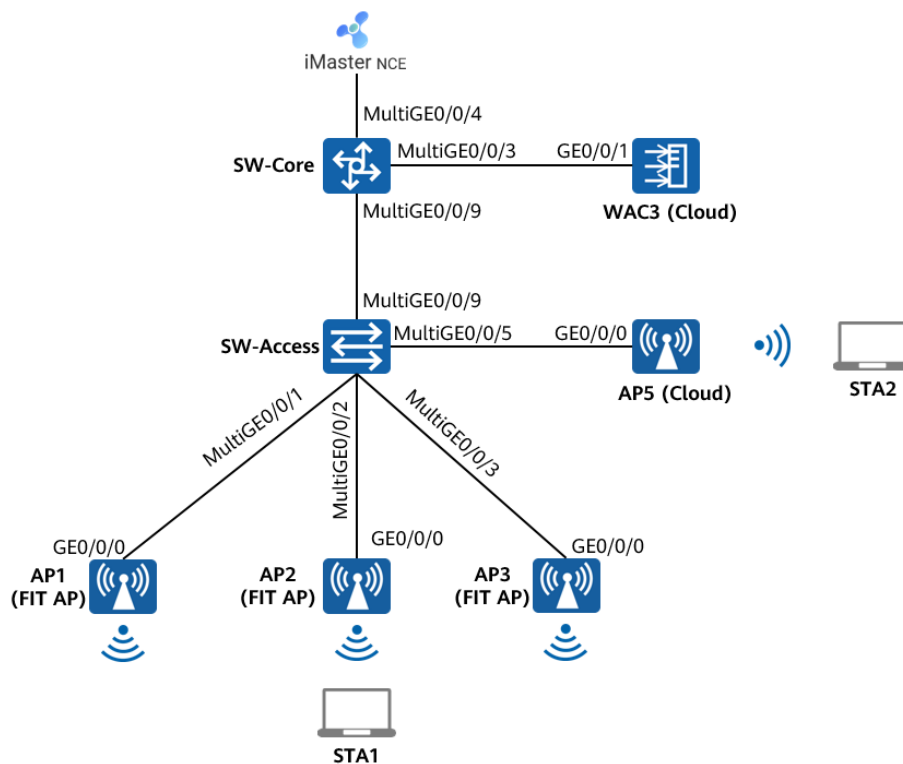


图4-1 云管理组网实验拓扑图

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 配置网络互通

- # 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 WAC3 设备。创建 VLAN 100、101，GE0/0/1 端口类型修改为 Trunk，并允许通过 VLAN 100、101。

在 WAC3 上创建 VLAN 100、101。

```
<AirEngine9700-M1> system-view
[AirEngine9700-M1] sysname WAC3
[WAC3] vlan batch 100 101
```

配置 WAC3 的 GE0/0/1 端口类型及相应 VLAN。

```
[WAC3] interface GigabitEthernet 0/0/1
[WAC3-GigabitEthernet0/0/1] port link-type trunk
[WAC3-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101
[WAC3-GigabitEthernet0/0/1] quit
```

配置 SW-Core、WAC3 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
```

配置 WAC3 的 IP 地址。

```
[WAC3] interface Vlanif 100
[WAC3-Vlanif100] ip address 10.23.100.3 24
[WAC3-Vlanif100] quit
```

步骤 2 配置 iMaster NCE-Campus 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。

```
[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 的默认路由，下一跳地址指向 SW-Core 设备。

```
[WAC3] ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
```

步骤 3 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。

```
[WAC3] ac-mode cloud
Warning: This operation will switch the AC mode to cloud, Continue? [Y/N] y
This operation will take several minutes, please wait...
Warning: The authentication mode is switched to SN authentication. Ensure that the APs added offline
have SN information. Otherwise, configurations of these APs may be lost..
[WAC3] cloud-mng controller ip-address 172.21.39.88 port 10020 source-interface Vlanif 100
[WAC3] pnp startup-vlan receive enable
```

测试 WAC3 与 NCE 的网络连通性。

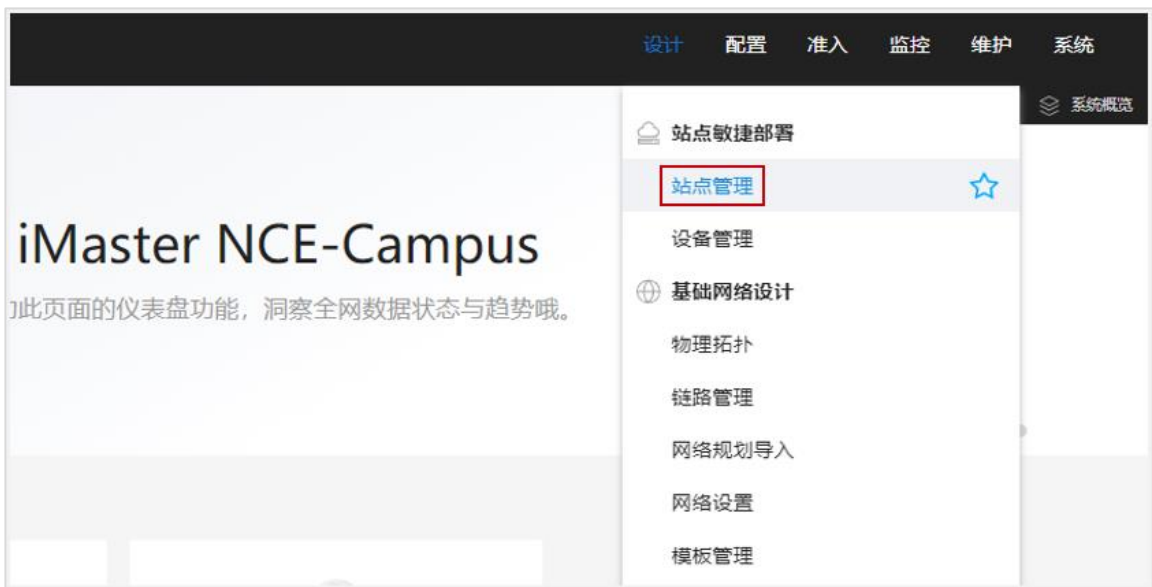
```
[WAC3] ping -a 10.23.100.3 172.21.39.88
PING 172.21.39.88: 56 data bytes, press CTRL_C to break
Reply from 172.21.39.88: bytes=56 Sequence=1 ttl=62 time=1 ms
Reply from 172.21.39.88: bytes=56 Sequence=2 ttl=62 time=1 ms
Reply from 172.21.39.88: bytes=56 Sequence=3 ttl=62 time=1 ms
```

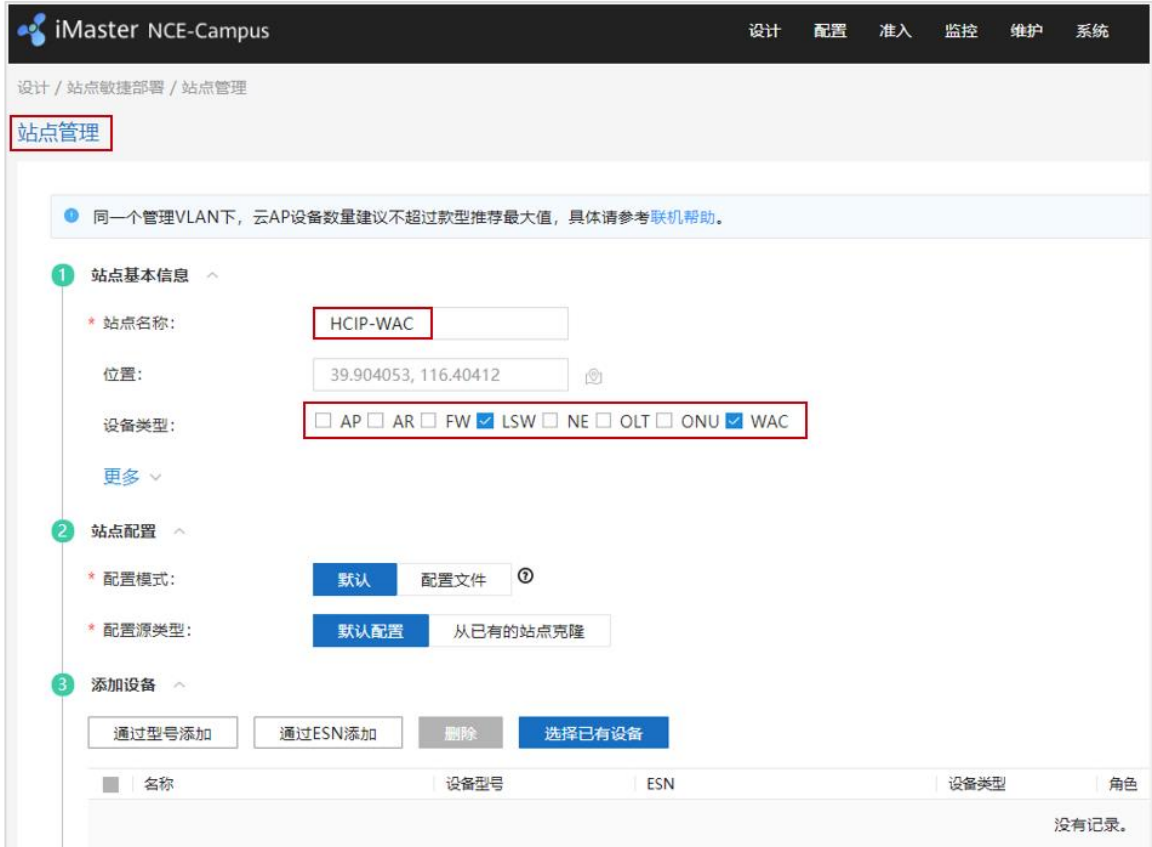
```
Reply from 172.21.39.88: bytes=56 Sequence=4 ttl=62 time=1 ms
Reply from 172.21.39.88: bytes=56 Sequence=5 ttl=62 time=1 ms

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

步骤 4 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”。





在 WAC3 上查询设备的 ESN 编号。

```
[WAC3] display esn
ESN of device: 102257532207
```

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。





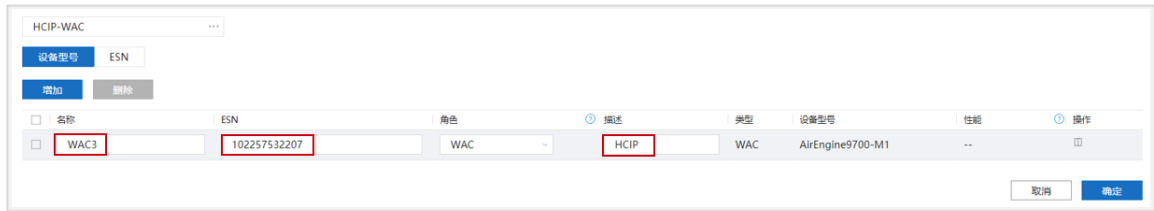
在弹出的手动添加界面，协议类型选择“NETCONF 协议”，站点选择“HCIP-WAC”，模式选择“设备型号”，然后点击“增加”按钮。



在弹出的页面中，按照以下参数进行配置，点击“确定”。



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”。



名称	ESN	角色	描述	类型	设备型号	性能	操作
WAC3	102257532207	WAC	HCIP	WAC	AirEngine9700-M1	--	

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。



名称	ESN	状态	角色
WAC3	102257532207	正常	WAC

步骤 5 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 6 配置无线业务 (WAC3)

NCE 纳管设备后，AP 上线以及 WLAN 业务依然在 WAC3 设备上配置，此处以 CLI 命令行为例进行配置。

配置 AP1、AP2、AP3 在 WAC3 中上线。开启 CAPWAP DTLS 不认证。(V200R021C00 及之后版本)

```
[WAC3] capwap dtls no-auth enable
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is enabled and brings security risks. After the device goes online for the first time, disable this function to prevent security risks. Continue? [Y/N]: y
```

在 WAC3 上配置 CAPWAP 源端口，需要提前配置以下参数：

DTLS 预共享密钥：此处配置为 a1234567；

WAC 间 DTLS 预共享密钥：此处配置为 a1234567；

FIT AP 的管理参数（用户名/密码）：此处配置为 admin/Huawei@123；

全局离线管理 VAP 的登录密码：此处配置为 a1234567。

```
[WAC3] capwap dtls psk a1234567
[WAC3] capwap dtls inter-controller psk a1234567
[WAC3] capwap source interface vlanif 100
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters,
underscores, and digits, and must start with a letter):admin
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a combination of at least three of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters):Huawei@123
Confirm password:Huawei@123
Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text
characters that must be a combination of at least two of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters):a1234567
Confirm PSK:a1234567
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be
interrupted.
Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version
earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.
```

在 WAC3 上配置 AP 认证方式为 SN 认证（WAC 在云模式下仅支持 SN 认证方式）。

```
[WAC3] wlan
[WAC3-wlan-view] ap auth-mode sn-auth
[WAC3-wlan-view] quit
```

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。



发现有三台未被纳管的设备，同时选中三台设备，点击“修复”。

AP列表

筛选条件

解绑 修复

<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”。

选择站点

选择站点 | 设置角色

请输入关键字

站点	描述	类型
<input checked="" type="radio"/> HCIP-WAC		WAC,LSW

共1条

10 条/页

取消 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 “ap-group1”，并将 AP1、AP2、AP3 加入此 AP 组。

```
[WAC3] wlan
[WAC3-wlan-view] ap-group name ap-group1
[WAC3-wlan-ap-group-ap-group1] quit
[WAC3-wlan-view] ap-id 0
```

```
[WAC3-wlan-ap-0] ap-group ap-group1
[WAC3-wlan-ap-0] quit
[WAC3-wlan-view] ap-id 1
[WAC3-wlan-ap-1] ap-group ap-group1
[WAC3-wlan-ap-1] quit
[WAC3-wlan-view] ap-id 2
[WAC3-wlan-ap-2] ap-group ap-group1
[WAC3-wlan-ap-2] quit
```

使用 display ap all 命令可以检查三个 AP 均已上线，状态为 normal。

```
[WAC3] display ap all
Total AP information:
nor   : normal           [3]
ExtraInfo : Extra information
-----
ID   MAC           Name  Group   IP           Type           State STA  Uptime  ExtraInfo
-----
0   9cb2-e82d-5110 AP3   ap-group1 10.23.100.218 AirEngine5761-11 nor   0    11M:29S -
1   9cb2-e82d-54f0 AP1   ap-group1 10.23.100.27  AirEngine5761-11 nor   0    11M:11S -
2   9cb2-e82d-5410 AP2   ap-group1 10.23.100.222 AirEngine5761-11 nor   0    11M:5S  -
-----
Total: 3
```

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成对应的国家码）。

```
[WAC3] wlan
[WAC3-wlan-view] regulatory-domain-profile name domain1
[WAC3-wlan-regulate-domain-domain1] country-code CN
[WAC3-wlan-regulate-domain-domain1] quit
```

在 AP 组中引用域管理模板。

```
[WAC3-wlan-view] ap-group name ap-group1
[WAC3-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]: y
[WAC3-wlan-ap-group-ap-group1] quit
```

创建名为“wlan-net”的安全模板，并配置安全策略。

```
[WAC3] wlan
[WAC3-wlan-view] security-profile name wlan-net
[WAC3-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a12345678 aes
[WAC3-wlan-sec-prof-wlan-net] quit
```

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

```
[WAC3-wlan-view] ssid-profile name wlan-net
[WAC3-wlan-ssid-prof-wlan-net] ssid wlan-net
[WAC3-wlan-ssid-prof-wlan-net] quit
```

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。

```
[WAC3-wlan-view] vap-profile name wlan-net
[WAC3-wlan-vap-prof-wlan-net] forward-mode direct-forward
[WAC3-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[WAC3-wlan-vap-prof-wlan-net] security-profile wlan-net
[WAC3-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[WAC3-wlan-vap-prof-wlan-net] quit
```

配置 AP 组引用 VAP 模板，AP 上射频 0 和射频 1 都使用 VAP 模板“wlan-net”的配置。

```
[WAC3-wlan-view] ap-group name ap-group1
[WAC3-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[WAC3-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[WAC3-wlan-ap-group-ap-group1] quit
[WAC3-wlan-view] quit
```

检查 VAP 状态。

```
[WAC3] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID          Status  Auth type   STA  SSID
-----
0     AP3      0   1   9CB2-E82D-5110 ON       WPA/WPA2-PSK  0   wlan-net
0     AP3      1   1   9CB2-E82D-5120 ON       WPA/WPA2-PSK  0   wlan-net
1     AP1      0   1   9CB2-E82D-54F0 ON       WPA/WPA2-PSK  0   wlan-net
1     AP1      1   1   9CB2-E82D-5500 ON       WPA/WPA2-PSK  0   wlan-net
2     AP2      0   1   9CB2-E82D-5410 ON       WPA/WPA2-PSK  0   wlan-net
2     AP2      1   1   9CB2-E82D-5420 ON       WPA/WPA2-PSK  1   wlan-net
-----
Total: 6
```

步骤 7 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
-----

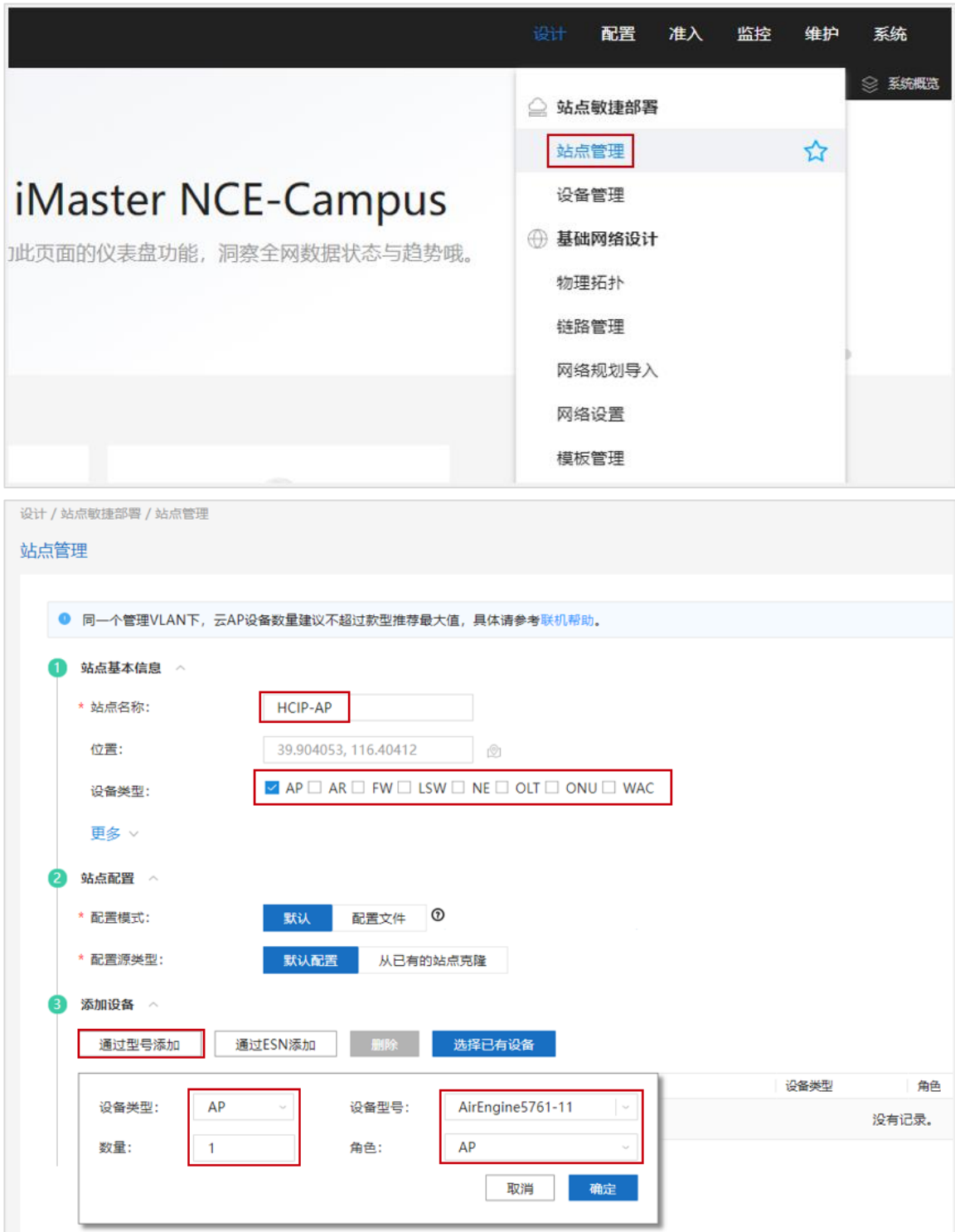
Index      IP          Client-ID  Type      Left  Status
-----
221      10.23.200.222 9cb2-e82d-5230 DHCP      86400  Used
-----
```

步骤 8 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，也可以通过命令行获取。

```
<9cb2-e82d-5230> display esn
ESN of device: 2102353VUR10N5119348
```

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 / 站点敏捷部署 / 站点管理

站点管理

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: HCIP-AP
 - 位置: 39.904053, 116.40412
 - 设备类型: AP AR FW LSW NE OLT ONU WAC
- 2 站点配置**
 - * 配置模式: 默认 配置文件
 - * 配置源类型: 默认配置 从已有的站点克隆
- 3 添加设备**
 - 通过型号添加 通过ESN添加 删除 选择已有设备

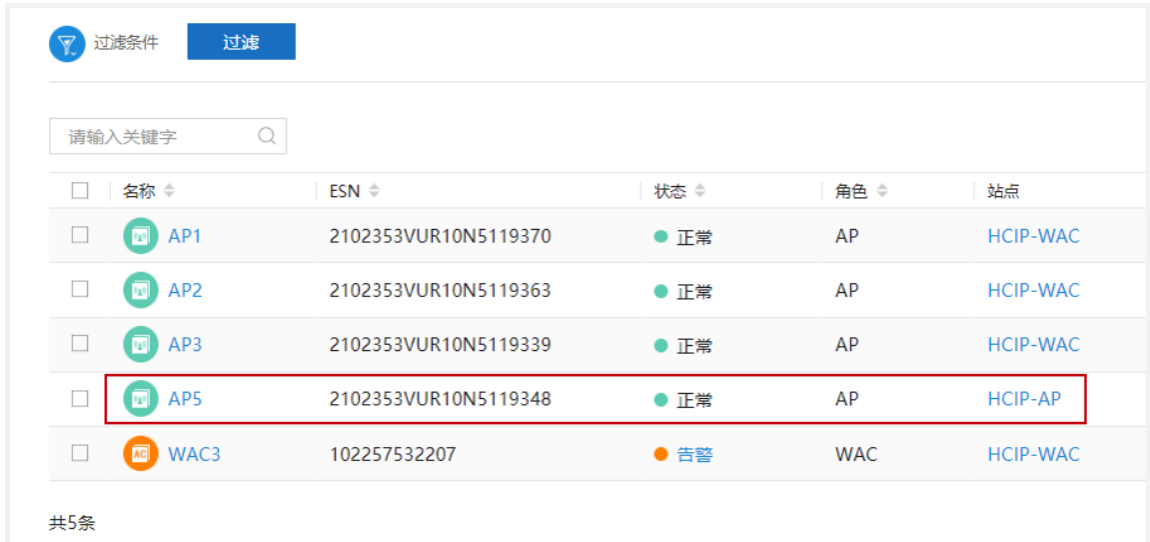
设备类型:	AP	设备型号:	AirEngine5761-11
数量:	1	角色:	AP

取消 确定

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”。



选择“设计 > 设备管理”，可以看到 AP5 已经被正常纳管。



步骤 9 配置无线业务（AP5）

选择“设计 > 设备管理”，点击 AP5，进入 AP5 的管理界面，点击右上角的“命令行”，可以对 AP5 进行 CLI 配置。



创建 VLAN 信息。

```
<AP5> system-view
[AP5] vlan batch 200 201
```

创建名为“ap5”的安全模板，并配置安全策略。

```
[AP5] wlan
[AP5-wlan-view] security-profile name ap5
[AP5-wlan-sec-prof-ap5] security wpa-wpa2 psk pass-phrase a12345678 aes
[AP5-wlan-sec-prof-ap5] quit
```

创建名为“ap5”的 SSID 模板，并配置 SSID 名称为“ap5”。

```
[AP5-wlan-view] ssid-profile name ap5
[AP5-wlan-ssid-prof-ap5] ssid ap5
[AP5-wlan-ssid-prof-ap5] quit
```

创建名为“ap5”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。

```
[AP5-wlan-view] vap-profile name ap5
[AP5-wlan-vap-prof-ap5] forward-mode direct-forward
[AP5-wlan-vap-prof-ap5] service-vlan vlan-id 201
[AP5-wlan-vap-prof-ap5] security-profile ap5
[AP5-wlan-vap-prof-ap5] ssid-profile ap5
[AP5-wlan-vap-prof-ap5] quit
```

在 AP5 中引用 VAP 模板（AP5 对应的 ap-id 为 0）。

```
[AP5-wlan-view] ap-id 0
[AP5-wlan-ap-0] vap-profile ap5 wlan 1 radio 0
[AP5-wlan-ap-0] vap-profile ap5 wlan 1 radio 1
[AP5-wlan-ap-0] quit
[AP5-wlan-view] quit
```

查看 AP5 的上线信息。

```
[AP5] display ap all
Total AP information:
nor   : normal           [1]
ExtraInfo : Extra information
-----
ID  MAC      Name  Group  IP          Type          State  STA  Uptime  ExtraInfo
-----
0*  9cb2-e82d-5230 AP5   default 10.23.200.222 AirEngine5761-11 nor    0    2H:21M:19S -
-----
Total: 1
```

查看 AP5 的 VAP 状态信息

```
[AP5] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID          Status  Auth type      STA  SSID
-----
0     AP5     0    1    9CB2-E82D-5230 ON      WPA/WPA2-PSK  0    ap5
0     AP5     1    1    9CB2-E82D-5240 ON      WPA/WPA2-PSK  0    ap5
-----
Total: 2
```

4.3 结果验证

4.3.1 在 WAC3 上检查云管理信息

在 WAC3 上通过命令 display cloud-mng info 查看云管理配置及状态信息。

```
[WAC3] display cloud-mng info
-----
```

```
AC status           : Online
Controller URL      : -
Controller IP address : 172.21.39.88
Controller port     : 10020
Source interface    : Vlanif100
Controller address source: configuration
-----
```

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。



设备终端监控

站点 / VN / 终端 : HCIP-AP

① 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



① 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 169.254.1.1 255.255.255.0
#
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 %^%#<-{((EfVe"O\.(U8m`1UkQ208k_{B11\RcJi_`+9%^%#
capwap dtls inter-controller psk %^%#nCH6FI3FFyITcANdQoW0UpB3/zU7Hao]JQS\m_4%^%#
capwap dtls no-auth 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<GIQ]Ln'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`+@0a5GB%^%#
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 切换到云模式？

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

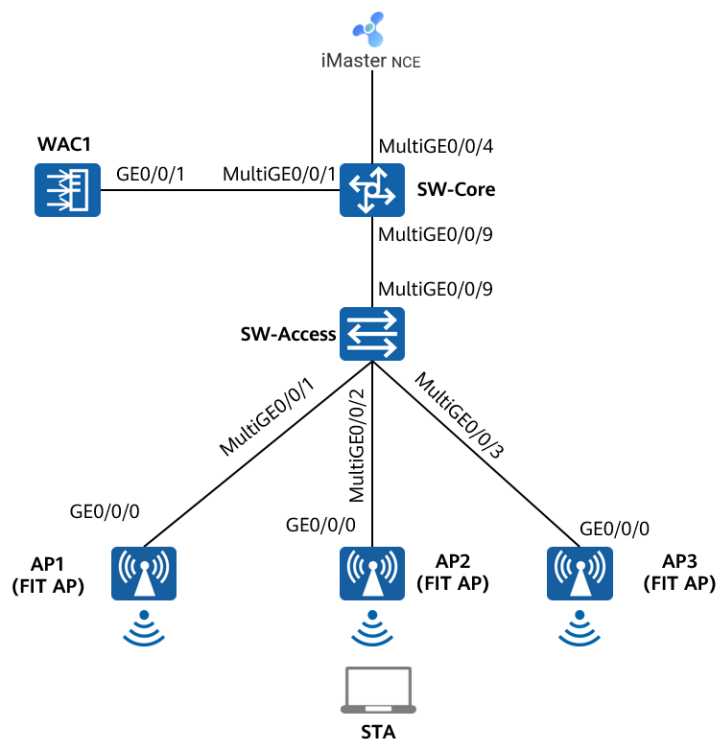


图5-1 802.1X 认证实验拓扑图

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 SW-Core 作为 DHCP 服务器，为 AP 和 STA 分配地址。
- 3.配置 NCE 与 WAC1 网络互通。

- 4.配置 AP 上线。
- 5.在 WAC1 上配置 802.1X 认证。
- 6.配置 WLAN 基本业务。
- 7.在 NCE 服务器上配置 802.1X 认证。
- 8.验证 802.1X 准入认证。

5.2.2 配置步骤

步骤 1 配置网络互通

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
```

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 下行端口类型及相应 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
```

配置 WAC1 设备。创建 VLAN 100、101，GE0/0/1 端口类型修改为 Trunk，并允许 VLAN 100、101。

在 WAC1 上创建 VLAN 100、101。

```
<AirEngine9700-M1> system-view
[AirEngine9700-M1] sysname WAC1
[WAC1] vlan batch 100 101
```

配置 WAC1 的 GE0/0/1 端口类型及相应 VLAN。

```
[WAC1] interface GigabitEthernet 0/0/1
[WAC1-GigabitEthernet /0/1] port link-type trunk
[WAC1-GigabitEthernet /0/1] port trunk allow-pass vlan 100 101
[WAC1-GigabitEthernet /0/1] quit
```

配置 SW-Core、WAC1 的 IP 地址。

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
```

配置 WAC1 的 IP 地址。

```
[WAC1] interface vlan 100
[WAC1-Vlanif100] ip address 10.23.100.1 24
[WAC1-Vlanif100] quit
```

步骤 2 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，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 3 配置 iMaster NCE-Campus 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。

```
[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 的默认路由，下一跳地址指向 SW-Core 设备。

```
[WAC1] ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
```

步骤 4 配置 AP 上线

开启 CAPWAP DTLS 不认证。（V200R021C00 及之后版本）

```
[WAC1] capwap dtls no-auth enable
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is
enabled and brings security risks. After the device goes online for the first time, disable this function to
prevent security risks. Continue? [Y/N]: y
```

在 WAC1 上配置 CAPWAP 源端口，需要提前配置以下参数：

DTLS 预共享密钥：此处配置为 a1234567；

WAC 间 DTLS 预共享密钥：此处配置为 a1234567；

FIT AP 的管理参数（用户名/密码）：此处配置为 admin/Huawei@123；

全局离线管理 VAP 的登录密码：此处配置为 a1234567。

```
[WAC1] capwap dtls psk a1234567
[WAC1] capwap dtls inter-controller psk a1234567
[WAC1] capwap source interface vlanif 100
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters,
underscores, and digits, and must start with a letter):admin
```

Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):**Huawei@123**

Confirm password:**Huawei@123**

Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):**a1234567**

Confirm PSK:**a1234567**

Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.

Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.

创建 AP 组。

```
[WAC1] wlan
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

在 WAC1 上配置 AP 认证方式为 MAC 认证。

```
[WAC1] wlan
[WAC1-wlan-view] ap auth-mode mac-auth
[WAC1-wlan-view] quit
```

在 WAC1 上添加 AP (AP 的 MAC 地址以实际情况为准)。

```
[WAC1] wlan
[WAC1-wlan-view] ap-id 0 ap-mac 9cb2-e82d-54f0
[WAC1-wlan-ap-0] ap-group ap-group1
[WAC1-wlan-ap-0] ap-name AP1
[WAC1-wlan-ap-0] quit
[WAC1-wlan-view] ap-id 1 ap-mac 9cb2-e82d-5410
[WAC1-wlan-ap-1] ap-group ap-group1
[WAC1-wlan-ap-1] ap-name AP2
[WAC1-wlan-ap-1] quit
[WAC1-wlan-view] ap-id 2 ap-mac 9cb2-e82d-5110
[WAC1-wlan-ap-2] ap-group ap-group1
[WAC1-wlan-ap-2] ap-name AP3
[WAC1-wlan-ap-2] quit
[WAC1-wlan-view] quit
```

使用 display ap all 命令可以检查三个 AP 均已上线, 状态为 normal。

```
<WAC1> display ap all
Total AP information:
nor   : normal           [3]
ExtraInfo : Extra information
-----
ID    MAC      Name   Group   IP           Type          State STA   Uptime   ExtraInfo
-----
0    9cb2-e82d-54f0 AP1    ap-group1 10.23.100.225 AirEngine5761-11 nor    0    3D:16H:14M:57S -
```

```

1 9cb2-e82d-5410 AP2 ap-group1 10.23.100.214 AirEngine5761-11 nor 0 3D:16H:13M:31S -
2 9cb2-e82d-5110 AP3 ap-group1 10.23.100.117 AirEngine5761-11 nor 0 3D:16H:14M:44S -
-----
Total: 3
    
```

步骤 5 配置 802.1X 认证 (WAC1)

配置 RADIUS 服务器模板。

```

[WAC1] radius-server template radius_huawei
[WAC1-radius-radius_huawei] radius-server authentication 172.21.39.88 1812 source vlanif 100
[WAC1-radius-radius_huawei] radius-server accounting 172.21.39.88 1813 source vlanif 100
[WAC1-radius-radius_huawei] radius-server shared-key cipher Huawei@123
[WAC1-radius-radius_huawei] quit
[WAC1] radius-server authorization 172.21.39.88 shared-key cipher Huawei@123 server-group
radius_huawei
[WAC1] radius-server authorization server-source all-interface
Warning: All interface listening has security risks.
If configured, the configuration of the specified listening IP address will be removed. Continue?[Y/N] y
Info: This operation may take some time, please wait for a moment .....
    
```

配置 RADIUS 方式的认证方案。

```

[WAC1] aaa
[WAC1-aaa] authentication-scheme radius_huawei
[WAC1-aaa-authen-radius_huawei] authentication-mode radius
[WAC1-aaa-authen-radius_huawei] quit
    
```

配置 RADIUS 方式的计费方案。

```

[WAC1-aaa] accounting-scheme scheme1
[WAC1-aaa-accounting-scheme1] accounting-mode radius
[WAC1-aaa-accounting-scheme1] accounting realtime 3
[WAC1-aaa-accounting-scheme1] quit
[WAC1-aaa] quit
    
```

accounting realtime 命令用来配置实时计费间隔，单位是分钟。

配置 802.1X 接入模板 “d1”。

```

[WAC1] dot1x-access-profile name d1
[WAC1-dot1x-access-profile-d1] dot1x authentication-method eap
[WAC1-dot1x-access-profile-d1] quit
    
```

配置认证模板 “p1”。新建认证模板 “p1”，并在认证模板中引用 802.1X 接入模板 “d1”、RADIUS 服务器模板 “radius_huawei”、认证方案 “radius_huawei”、计费方案 “scheme1”。

```

[WAC1] authentication-profile name p1
[WAC1-authentication-profile-p1] dot1x-access-profile d1
[WAC1-authentication-profile-p1] radius-server radius_huawei
[WAC1-authentication-profile-p1] authentication-scheme radius_huawei
[WAC1-authentication-profile-p1] accounting-scheme scheme1
[WAC1-authentication-profile-p1] quit
    
```

步骤 6 配置无线业务

创建名为“wlan-net”的安全模板，并配置安全策略。

```
[WAC1] wlan
[WAC1-wlan-view] security-profile name wlan-net
[WAC1-wlan-sec-prof-wlan-net] security wpa2 dot1x aes
[WAC1-wlan-sec-prof-wlan-net] quit
```

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

```
[WAC1-wlan-view] ssid-profile name wlan-net
[WAC1-wlan-ssid-prof-wlan-net] ssid wlan-net
[WAC1-wlan-ssid-prof-wlan-net] quit
```

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、SSID 模板、认证模板。

```
[WAC1-wlan-view] vap-profile name wlan-net
[WAC1-wlan-vap-prof-wlan-net] forward-mode tunnel
[WAC1-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[WAC1-wlan-vap-prof-wlan-net] security-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] authentication-profile p1
[WAC1-wlan-vap-prof-wlan-net] quit
```

配置 AP 组引用 VAP 模板。

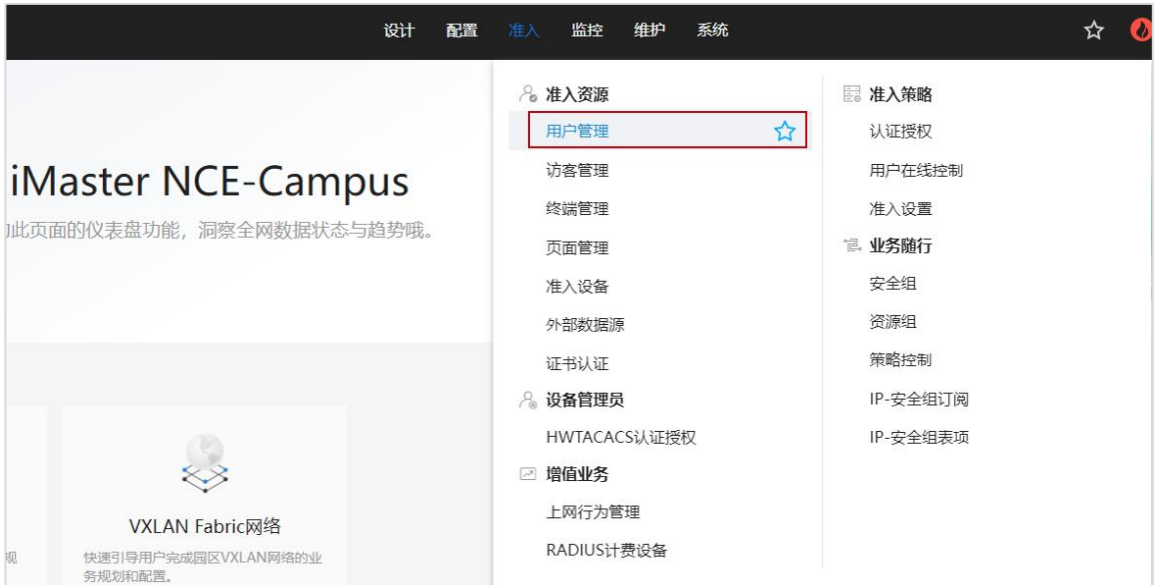
```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

步骤 7 配置 802.1X 认证（NCE）

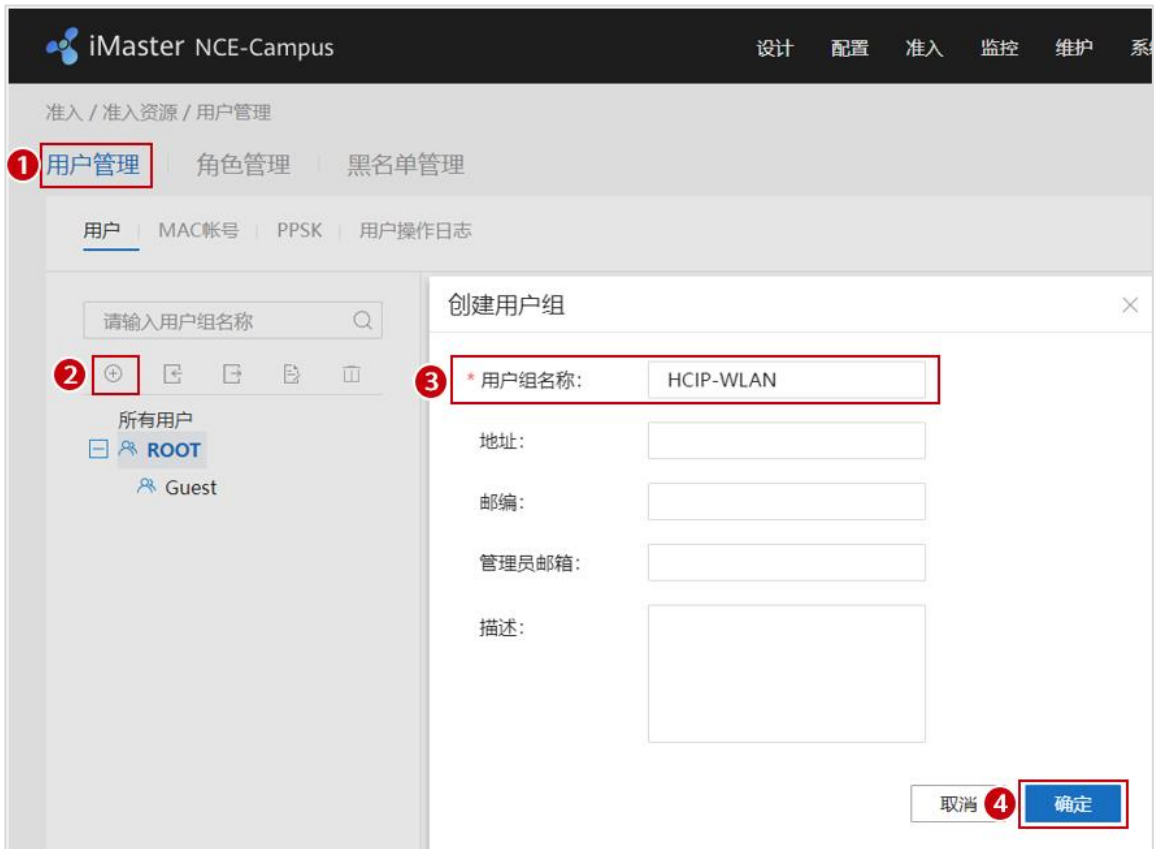
在 NCE 上配置准入认证，需要提前创建租户账号/密码，本文不再赘述。

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”。

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: dot1x-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）。

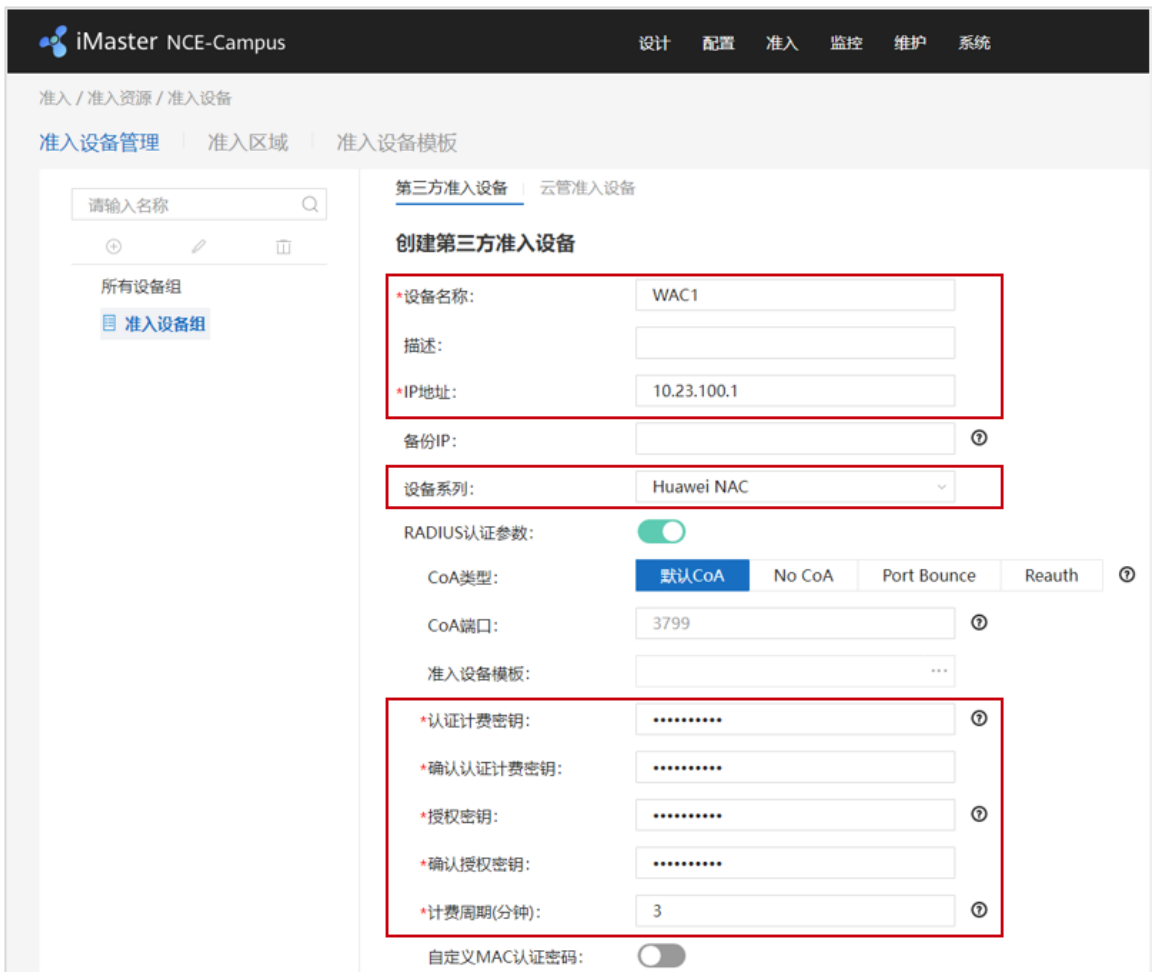
选择“准入 > 准入资源 > 准入设备”，配置准入设备。

iMaster NCE-Campus
 此页面的仪表盘功能，洞察全网数据状态与趋势哦。
 VXLAN Fabric网络
 快速引导用户完成园区VXLAN网络的业务规划和配置。
 设计 配置 准入 监控 维护 系统
 准入资源
 用户管理
 访客管理
 终端管理
 页面管理
准入设备 ☆
 外部数据源
 证书认证
 设备管理员
 HWTACACS认证授权
 增值业务
 上网行为管理
 RADIUS计费设备
 准入策略
 认证授权
 用户在线控制
 准入设置
 业务随行
 安全组
 资源组
 策略控制
 IP-安全组订阅
 IP-安全组表项

选择“第三方准入设备”，点击“创建”，创建第三方准入设备。

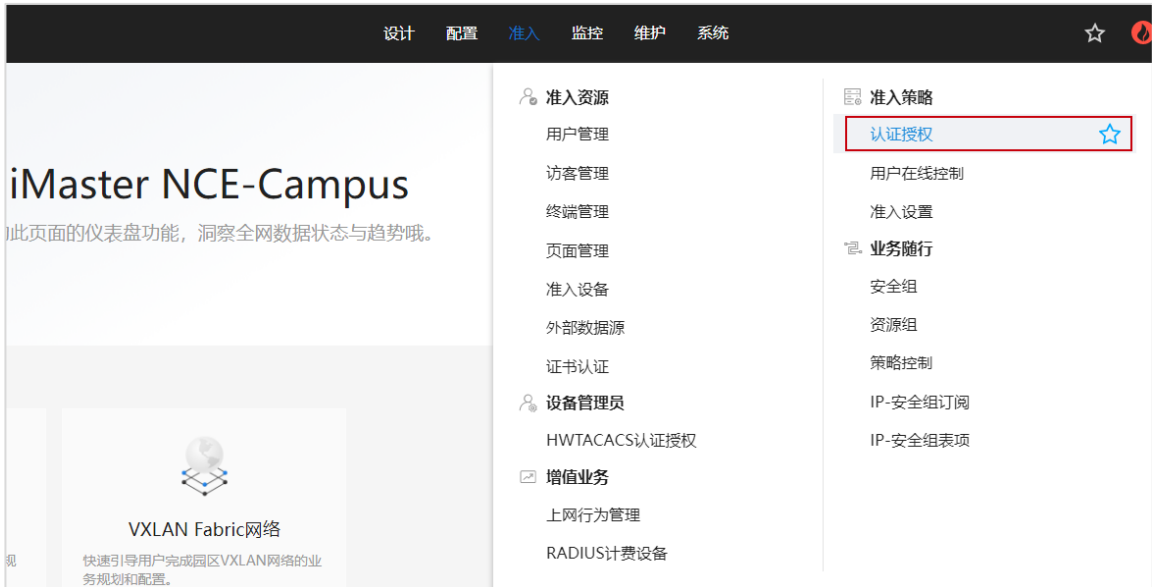


按照如下参数进行配置，其中“认证计费密钥”与“授权密钥”均为 Huawei@123，计费周期设置为 3 分钟，与 WAC1 中配置的参数保持一致。

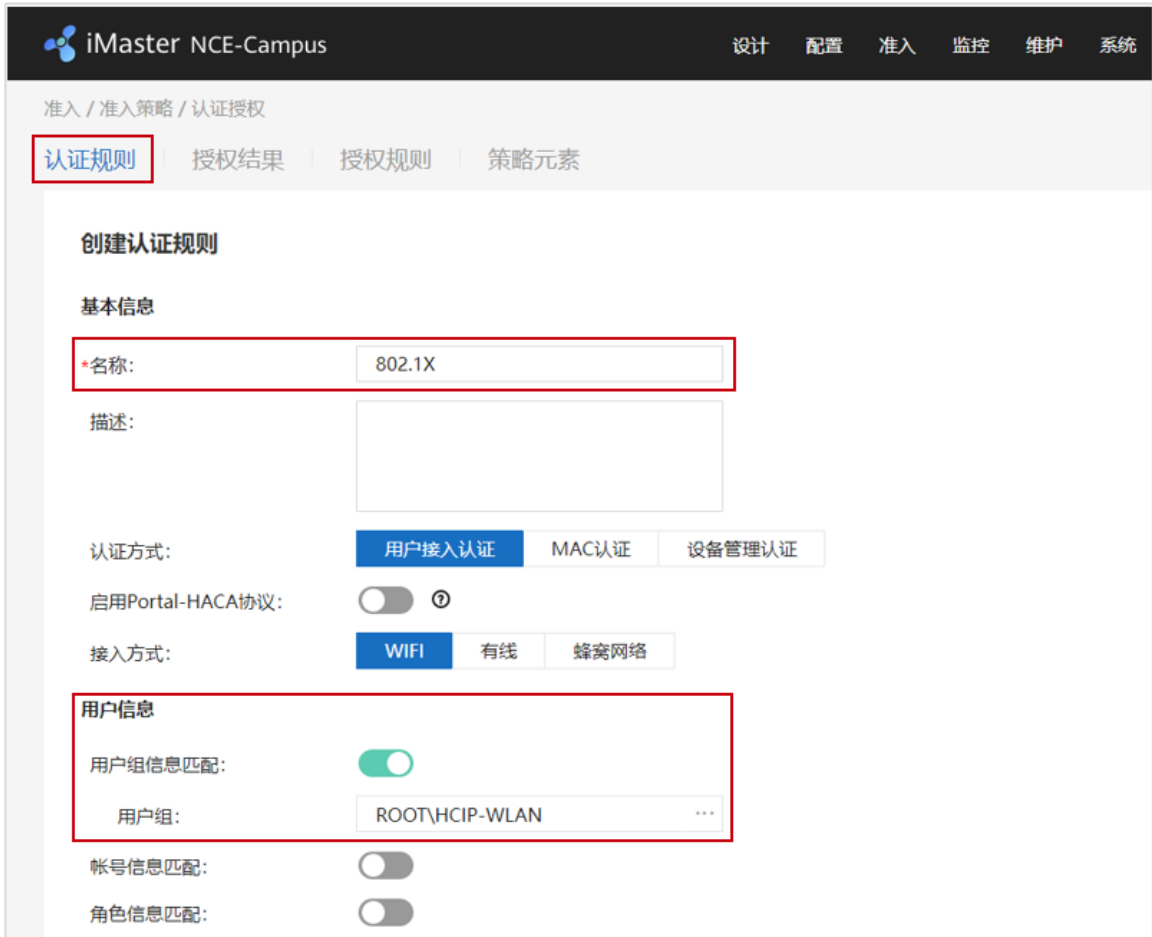


在 NCE 上创建认证授权、授权规则、授权结果。

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。



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)

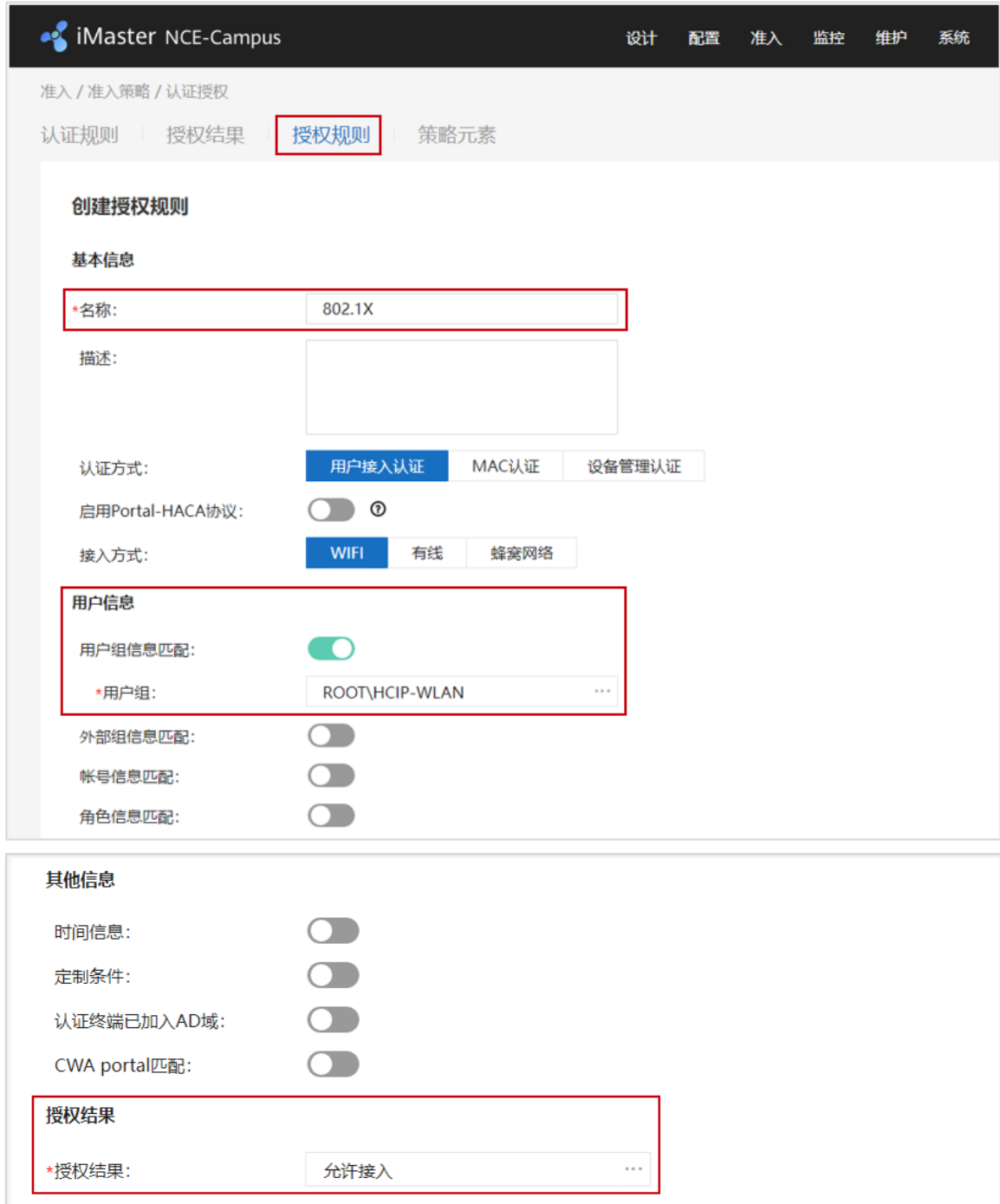
PAP协议, CHAP协议和EAP-MD5协议为不安全协议, 请谨慎选择。

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。



The screenshot shows the iMaster NCE-Campus web interface for configuring an authorization rule. The interface is in Chinese and includes a navigation bar at the top with options like '设计', '配置', '准入', '监控', '维护', and '系统'. The main content area is titled '准入 / 准入策略 / 认证授权' and has tabs for '认证规则', '授权结果', '授权规则', and '策略元素'. The '授权规则' tab is active, and a red box highlights the '创建授权规则' section. This section is divided into '基本信息' and '其他信息'.

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 (selected), MAC认证, 设备管理认证
- 启用Portal-HACA协议:
- 接入方式: WIFI (selected), 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:

其他信息

- 时间信息:
- 定制条件:
- 认证终端已加入AD域:
- CWA portal匹配:

授权结果

- *授权结果: 允许接入

5.3 结果验证

5.3.1 检查 AP 上线状态

在 WAC1 上执行 display vap all 命令，查看 VAP 信息如下。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID          Status  Auth type  STA  SSID
-----
0     AP1      0   1   9CB2-E82D-54F0 ON      WPA2+802.1X  0   wlan-net
0     AP1      1   1   9CB2-E82D-5500 ON      WPA2+802.1X  1   wlan-net
1     AP2      0   1   9CB2-E82D-5410 ON      WPA2+802.1X  0   wlan-net
1     AP2      1   1   9CB2-E82D-5420 ON      WPA2+802.1X  0   wlan-net
2     AP3      0   1   9CB2-E82D-5110 ON      WPA2+802.1X  0   wlan-net
2     AP3      1   1   9CB2-E82D-5120 ON      WPA2+802.1X  0   wlan-net
-----
Total: 6
```

5.3.2 检查 VAP 信息

在 WAC1 上执行 display vap all 命令，查看 VAP 信息如下。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID          Status  Auth type  STA  SSID
-----
0     AP1      0   1   9CB2-E82D-54F0 ON      WPA2+802.1X  0   wlan-net
0     AP1      1   1   9CB2-E82D-5500 ON      WPA2+802.1X  1   wlan-net
1     AP2      0   1   9CB2-E82D-5410 ON      WPA2+802.1X  0   wlan-net
1     AP2      1   1   9CB2-E82D-5420 ON      WPA2+802.1X  0   wlan-net
2     AP3      0   1   9CB2-E82D-5110 ON      WPA2+802.1X  0   wlan-net
2     AP3      1   1   9CB2-E82D-5120 ON      WPA2+802.1X  0   wlan-net
-----
Total: 6
```

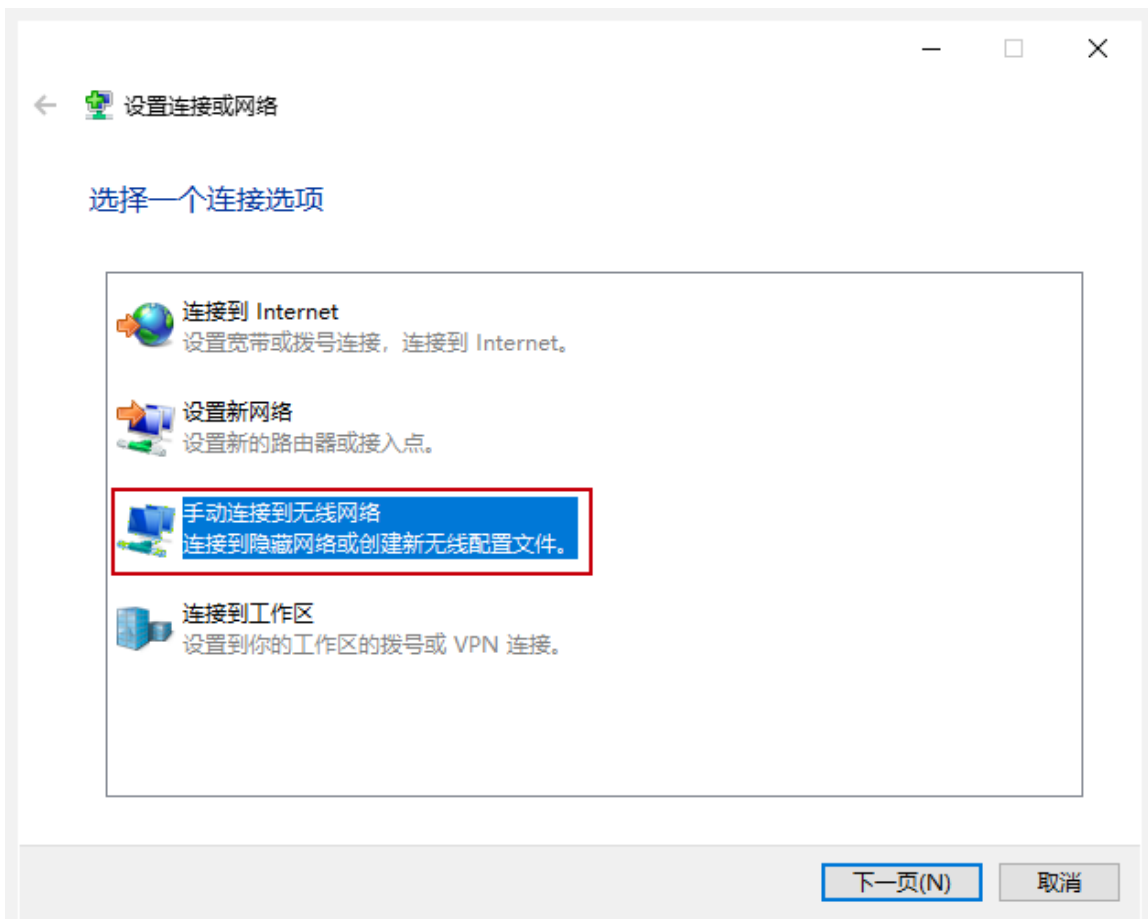
5.3.3 STA 关联无线信号，认证成功

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。

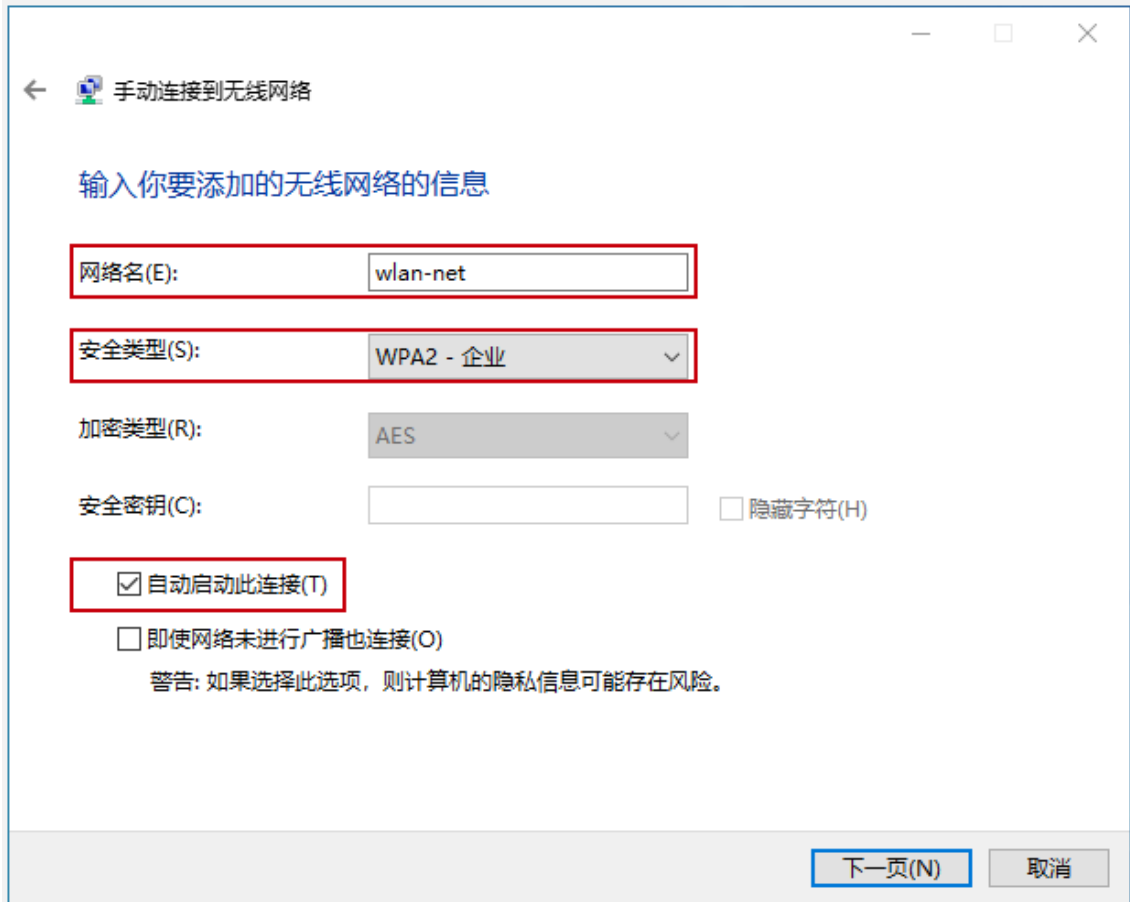
选择“控制面板 > 网络和 Internet > 网络和共享中心”（控制面板的“查看方式”选择“类别”时可显示“网络和 Internet”），单击“设置新的连接或网络”。



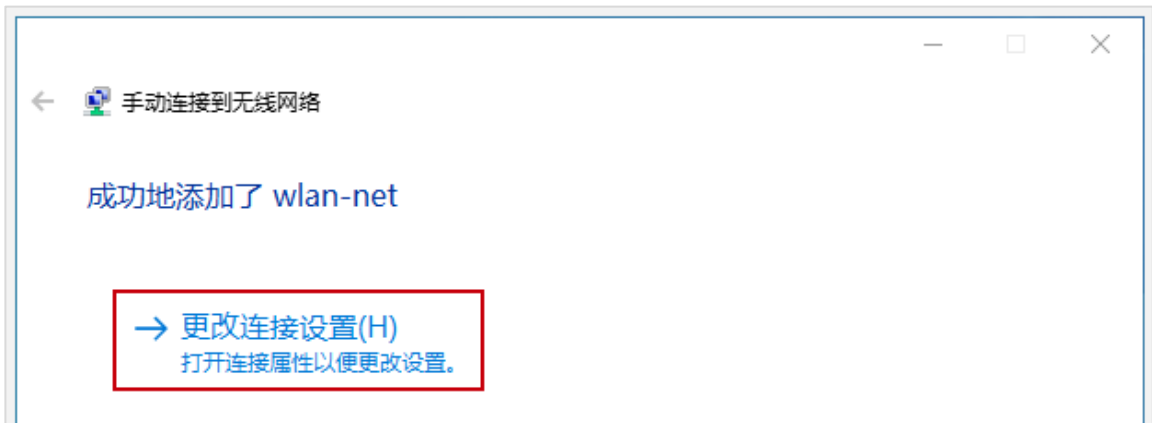
在弹出的对话框中选择“手动连接到无线网络”，然后单击“下一页”。



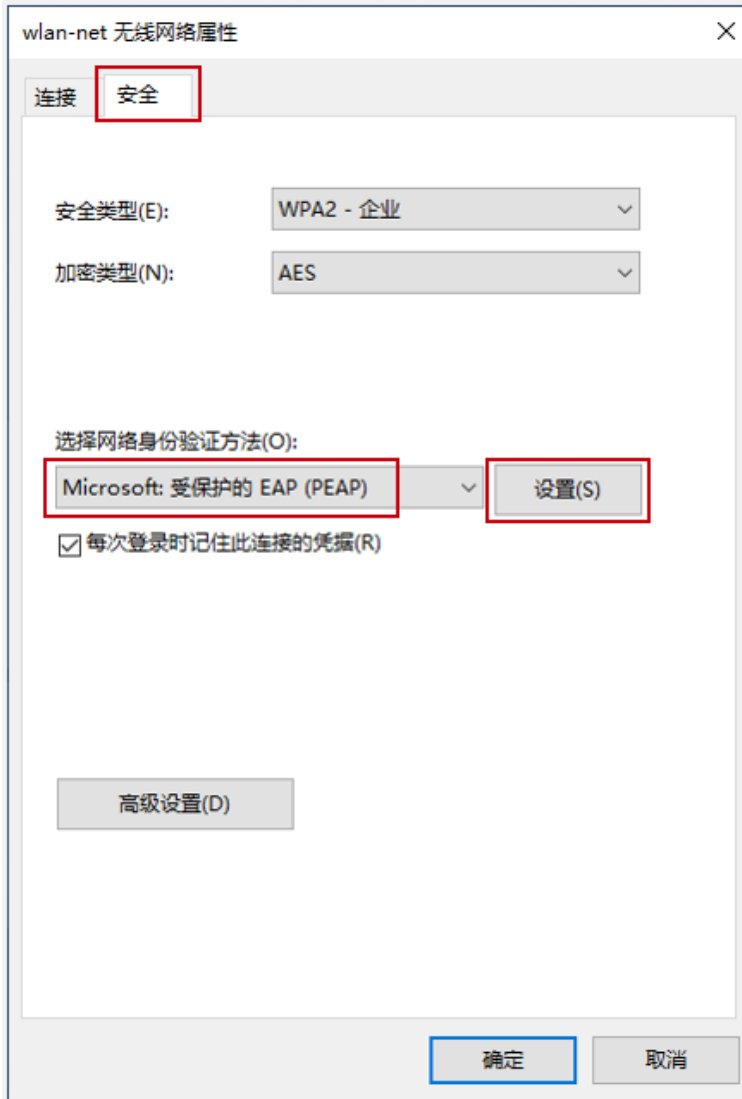
手动添加“网络名”，设置“安全类型”和“加密类型”，并选中“自动启动此连接”，单击“下一页”完成设置。



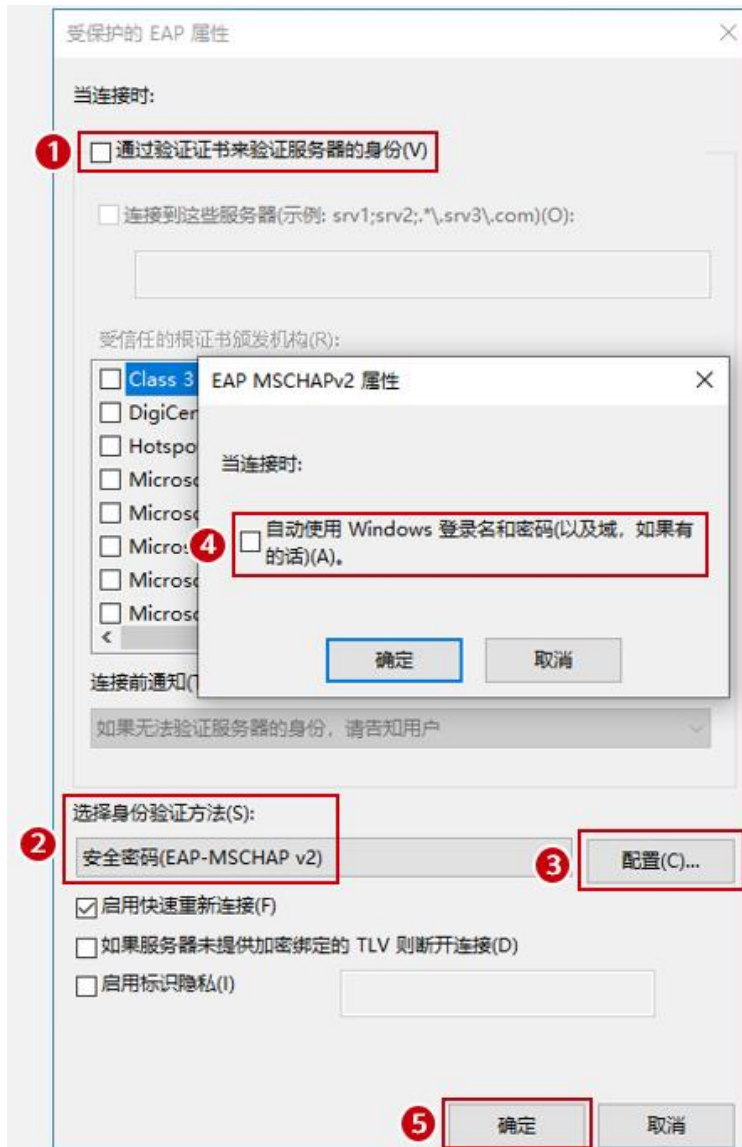
显示已成功添加了“wlan-net”无线网络，然后点击“更改连接设置”。



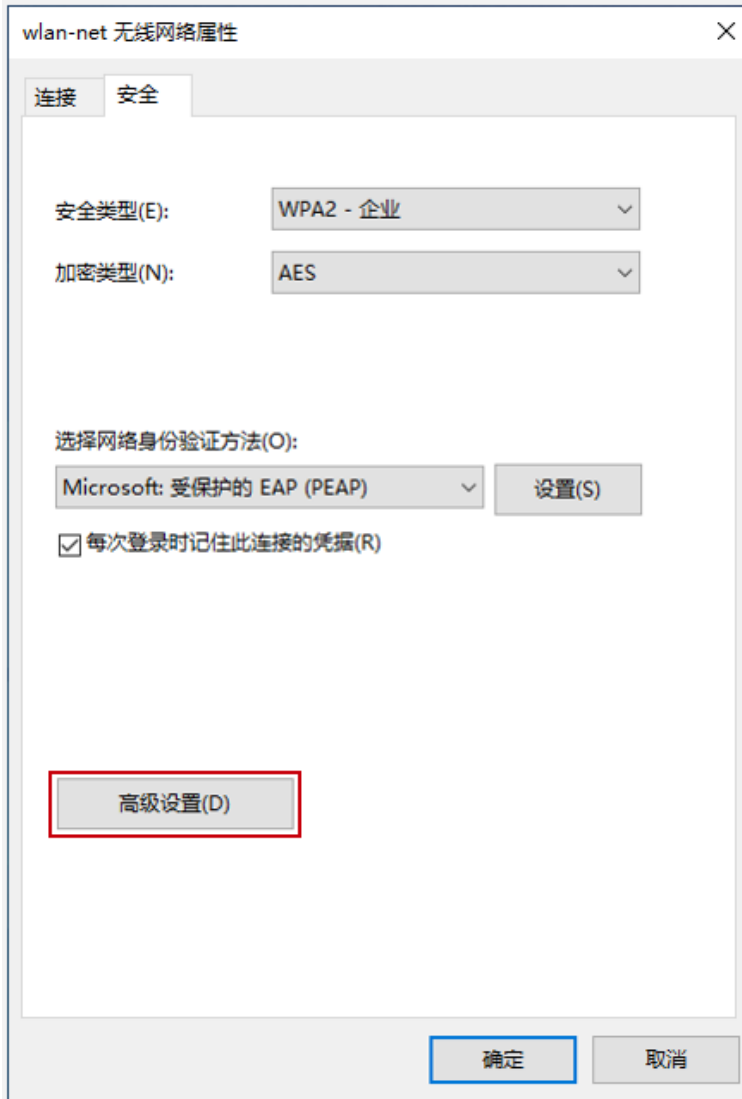
点击“安全”页签，“选择网络身份验证方法”设置为“Microsoft: 受保护的 EAP (PEAP)”，然后单击“设置”。



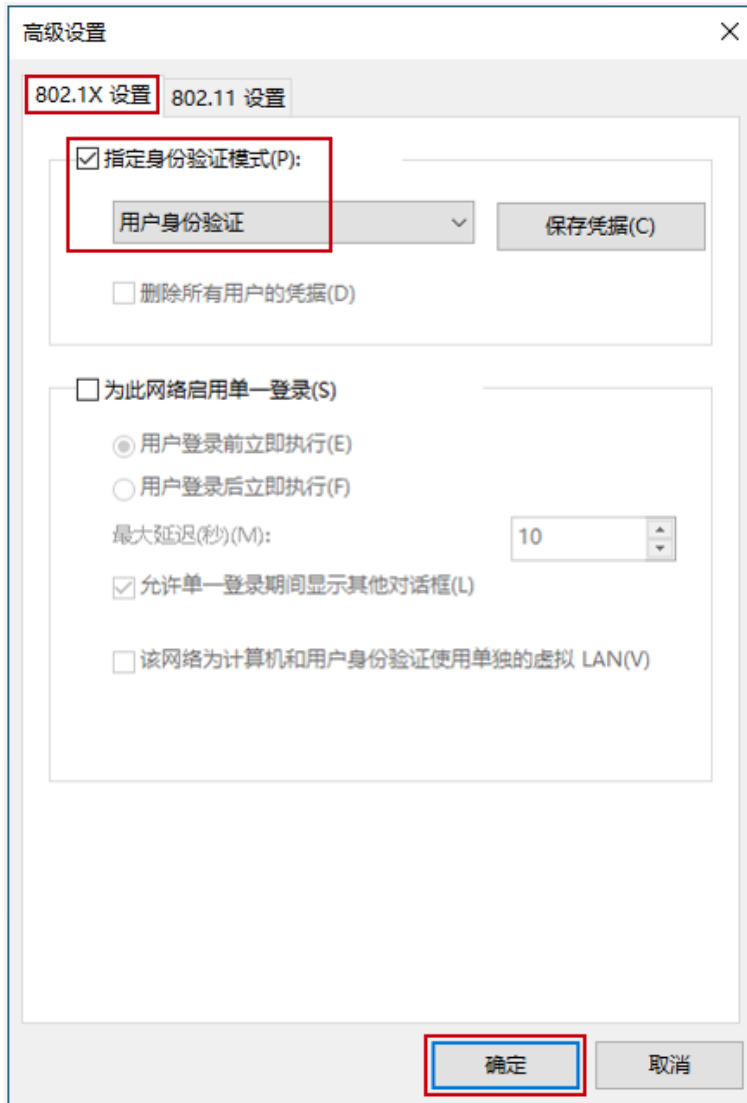
取消勾选“通过验证证书来验证服务器的身份”，“选择身份验证方法”选择“安全密码（EAP-MSCHAP v2）”，然后单击“配置”，在弹出的对话框中，取消勾选“自动使用 Windows 登录名和密码”，最后点击“确定”。



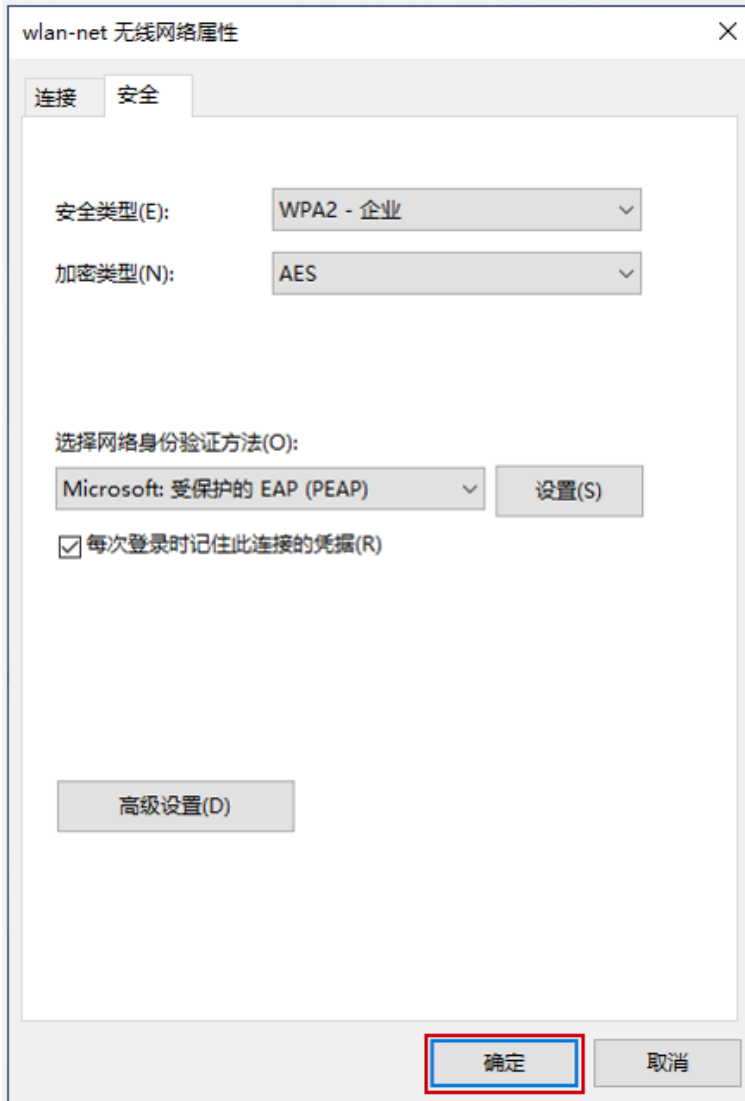
在“安全”页签，单击“高级设置”。



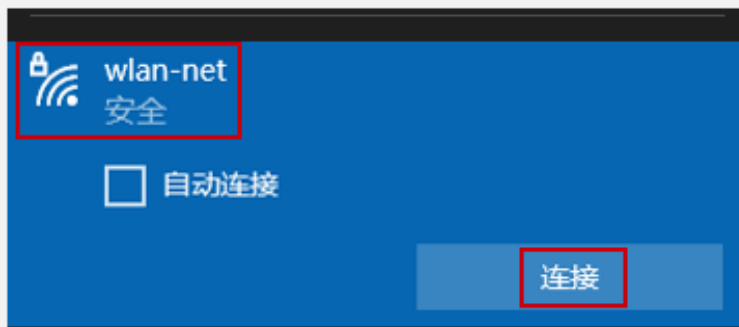
在弹出的对话框中点击“802.1X 设置”页签，设置“指定身份验证模式”为“用户身份验证”，单击“确定”。



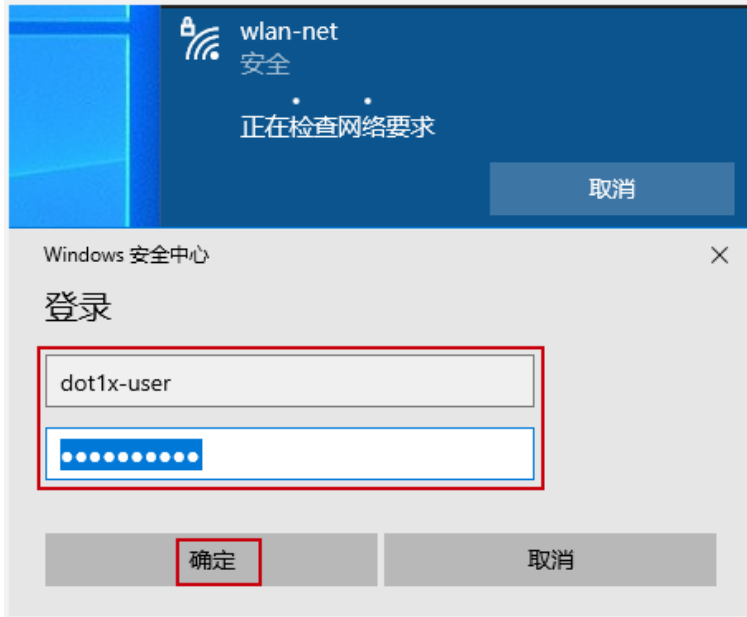
最后点击“确定”，完成 Windows 10 操作系统中的 802.1X 参数设置。



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

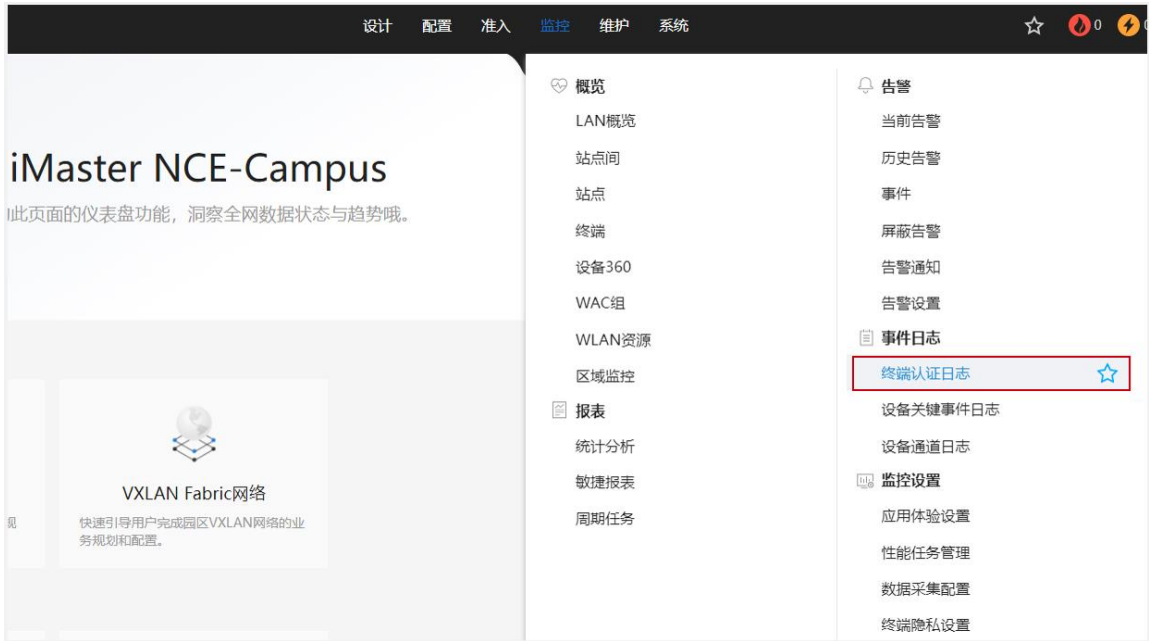
C:\Windows\system32>ping 10.23.101.254

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，“Success”表示成功接入，如下所示。

```
[WAC1] display access-user detail
Basic:
  User ID           : 65613
  User name         : dot1x-user
  User MAC          : 081f-7153-90b4
  User IP address   : 10.23.101.196
  User vpn-instance : -
  User IPv6 address : -
  User access Interface : Wlan-Dbss17497
  User vlan event   : Success
  QinQVlan/UserVlan : 0/101
  User vlan source  : user request
```



```
User access time           : XXXX
User accounting session ID  : WAC1000000000001011d****010004d
User accounting mult session ID : 9CB2E82D54F0081F715390B46321B****F061063
User access type           : 802.1x
AP name                     : AP1
Radio ID                   : 1
AP MAC                      : 9cb2-e82d-54f0
SSID                       : wlan-net
Online time                 : 788(s)
User Group Priority         : 0

AAA:
User authentication type    : 802.1x authentication
Current authentication method : RADIUS
Current authorization method  : -
Current accounting method    : RADIUS
-----
Total: 1, printed: 1
```

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 default
radius-server template radius_huawei
```

```
radius-server shared-key cipher %^%#3:KT&'SI#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-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>j|^%# server-group radius_huawei
radius-server authorization server-source all-interface
#
aaa
authentication-scheme radius_huawei
authentication-mode radius
authorization-scheme default
authorization-mode local
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
management-interface
#
interface MEth0/0/1
ip address 169.254.1.1 255.255.255.0
#
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 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)!%^%#
traffic-profile name default
security-profile name default
security-profile name wlan-net
  security wpa2 dot1x 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
  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
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
  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

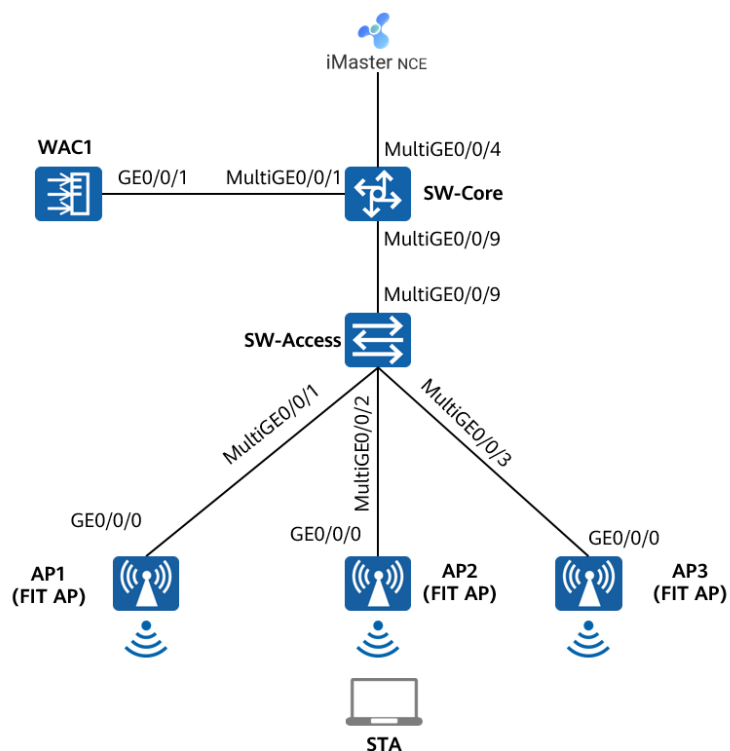


图6-1 Portal 认证实验拓扑图

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 SW-Core 作为 DHCP 服务器，为 AP 和 STA 分配地址。
- 3.配置 iMaster NCE-Campus 与 WAC1 网络互通。
- 4.配置 AP 上线。
- 5.在 WAC1 上配置 Portal 认证。
- 6.配置 WLAN 基本业务。
- 7.在 NCE 服务器上配置 Portal 认证。
- 8.验证 Portal 认证。

6.2.2 配置步骤

步骤 1 配置网络互通

此配置步骤请参考 5.2.2 章节中的步骤 1，此处不再赘述。

步骤 2 配置 DHCP 服务器

此配置步骤请参考 5.2.2 章节中的步骤 2，此处不再赘述。

步骤 3 配置 iMaster NCE-Campus 与 WAC1 之间网络互通

此配置步骤请参考 5.2.2 章节中的步骤 3，此处不再赘述。

步骤 4 配置 AP 上线

此配置步骤请参考 5.2.2 章节中的步骤 4，此处不再赘述。

步骤 5 配置 Portal 认证 (WAC1)

配置 RADIUS 服务器模板。

```
[WAC1] radius-server template radius_huawei
[WAC1-radius-radius_huawei] radius-server authentication 172.21.39.88 1812 source vlanif 100
[WAC1-radius-radius_huawei] radius-server accounting 172.21.39.88 1813 source vlanif 100
[WAC1-radius-radius_huawei] radius-server shared-key cipher Huawei@123
[WAC1-radius-radius_huawei] quit
[WAC1] radius-server authorization 172.21.39.88 shared-key cipher Huawei@123 server-group
radius_huawei
[WAC1] radius-server authorization server-source all-interface
Warning: All interface listening has security risks.
If configured, the configuration of the specified listening IP address will be removed. Continue?[Y/N] y
Info: This operation may take some time, please wait for a moment .....
```

配置 RADIUS 方式的认证方案。

```
[WAC1] aaa
[WAC1-aaa] authentication-scheme radius_huawei
[WAC1-aaa-authen-radius_huawei] authentication-mode radius
[WAC1-aaa-authen-radius_huawei] quit
```

配置 RADIUS 方式的计费方案。

```
[WAC1-aaa] accounting-scheme scheme1
[WAC1-aaa-accounting-scheme1] accounting-mode radius
[WAC1-aaa-accounting-scheme1] accounting realtime 3
[WAC1-aaa-accounting-scheme1] quit
[WAC1-aaa] quit
```

配置 URL 模板。NCE 作为 Portal 服务器时，Portal 页面的默认端口号为 19008。

```
[WAC1] url-template name url1
[WAC1-url-template-url1] url https://172.21.39.88:19008/portal
[WAC1-url-template-url1] url-parameter redirect-url redirect-url ssid ssid user-ipaddress userip user-mac
usermac device-ip ac-ip
[WAC1-url-template-url1] quit
```

配置 Portal 服务器模板。NCE 作为 Portal 服务器时，默认监听 50200 端口。

```
[WAC1] web-auth-server server-source all-interface
Warning: All interface listening has security risks.
If configured, the configuration of the specified listening IP address will be removed. Continue?[Y/N] y
[WAC1] web-auth-server abc
[WAC1-web-auth-server-abc] server-ip 172.21.39.88
[WAC1-web-auth-server-abc] source-ip 10.23.100.1
[WAC1-web-auth-server-abc] shared-key cipher Huawei@123
[WAC1-web-auth-server-abc] port 50200
[WAC1-web-auth-server-abc] url-template url1
[WAC1-web-auth-server-abc] quit
```

创建 Portal 接入模板“portal1”，并配置 Portal 认证为二层 Portal 认证。

```
[WAC1] portal-access-profile name portal1
[WAC1-portal-access-profile-portal1] web-auth-server abc direct
[WAC1-portal-access-profile-portal1] quit
```

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。

```
[WAC1] free-rule-template name free1
[WAC1-free-rule-free1] free-rule 1 destination ip 172.21.39.88 mask 32
[WAC1-free-rule-free1] quit
```

新建认证模板“p1”，并在认证模板中引用 Portal 接入模板“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”。

```
[WAC1] authentication-profile name p1
[WAC1-authentication-profile-p1] portal-access-profile portal1
```

```
[WAC1-authentication-profile-p1] free-rule-template free1
[WAC1-authentication-profile-p1] radius-server radius_huawei
[WAC1-authentication-profile-p1] authentication-scheme radius_huawei
[WAC1-authentication-profile-p1] accounting-scheme scheme1
[WAC1-authentication-profile-p1] quit
```

步骤 6 配置无线业务

创建名为“wlan-net”的安全模板，并配置安全策略。

```
[WAC1] wlan
[WAC1-wlan-view] security-profile name wlan-net
[WAC1-wlan-sec-prof-wlan-net] security open
[WAC1-wlan-sec-prof-wlan-net] quit
```

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

```
[WAC1-wlan-view] ssid-profile name wlan-net
[WAC1-wlan-ssid-prof-wlan-net] ssid wlan-net
[WAC1-wlan-ssid-prof-wlan-net] quit
```

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、SSID 模板、认证模板。

```
[WAC1-wlan-view] vap-profile name wlan-net
[WAC1-wlan-vap-prof-wlan-net] forward-mode tunnel
[WAC1-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[WAC1-wlan-vap-prof-wlan-net] security-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net] authentication-profile p1
[WAC1-wlan-vap-prof-wlan-net] quit
```

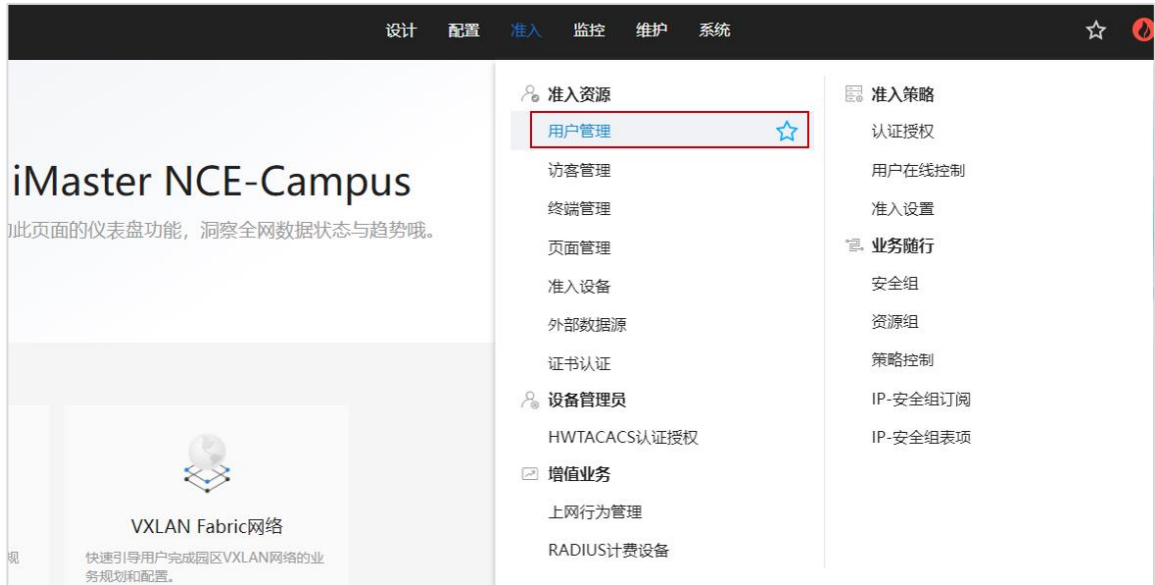
配置 AP 组引用 VAP 模板。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

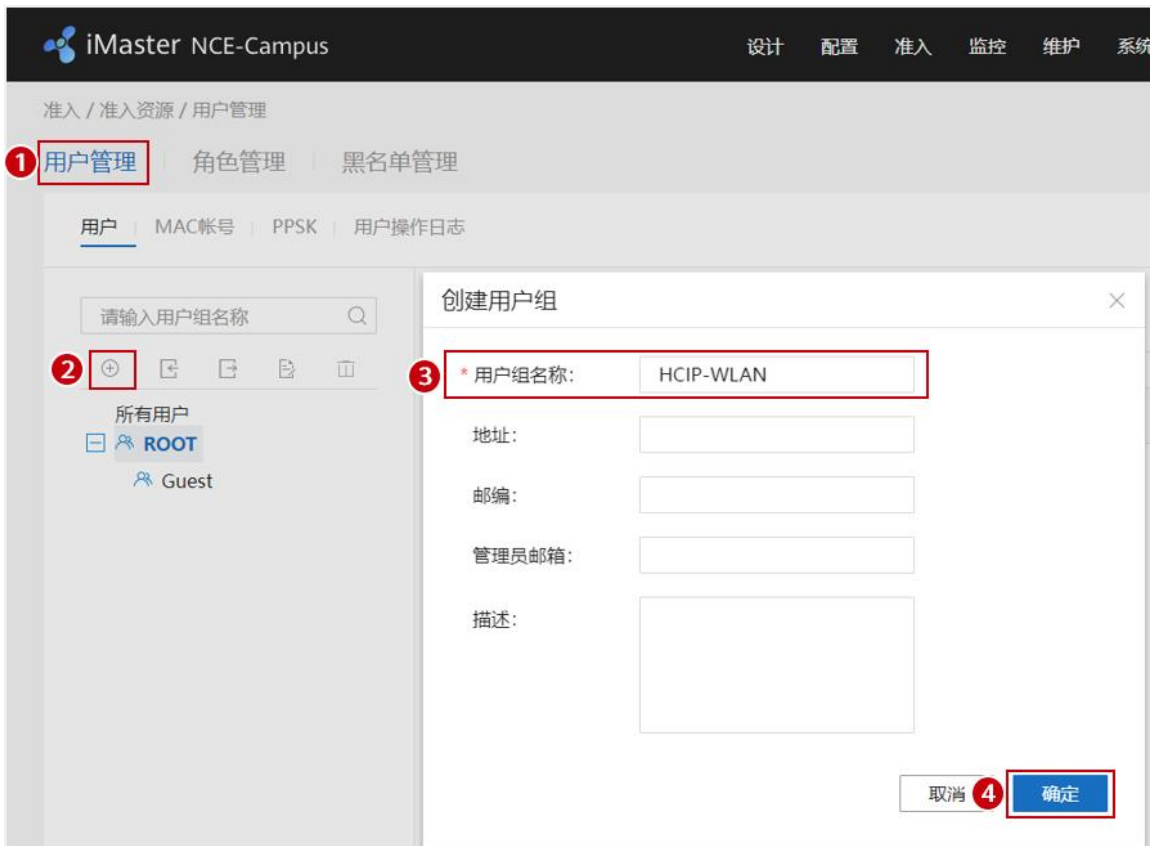
步骤 7 配置 Portal 认证（NCE）

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”。

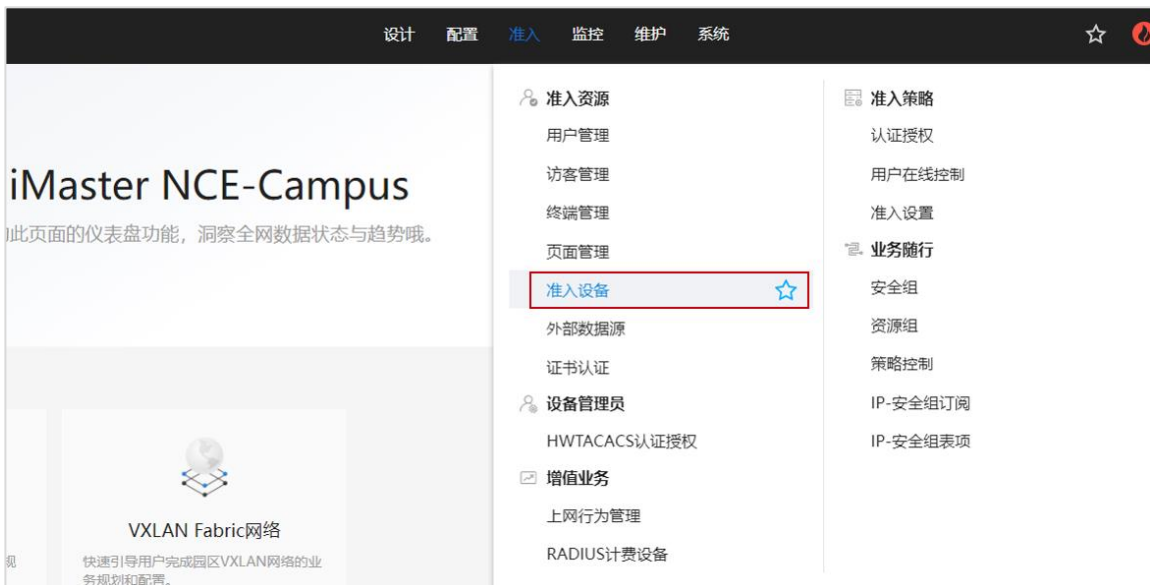


选中“HCIP-WLAN”用户组，单击“创建”，新增用于 Portal 认证的用户名“portal-user”，密码设置为“Huawei@123”，允许登录方式勾选“Portal”和“802.1X & Portal 2.0”，最后点击“确定”。

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）。

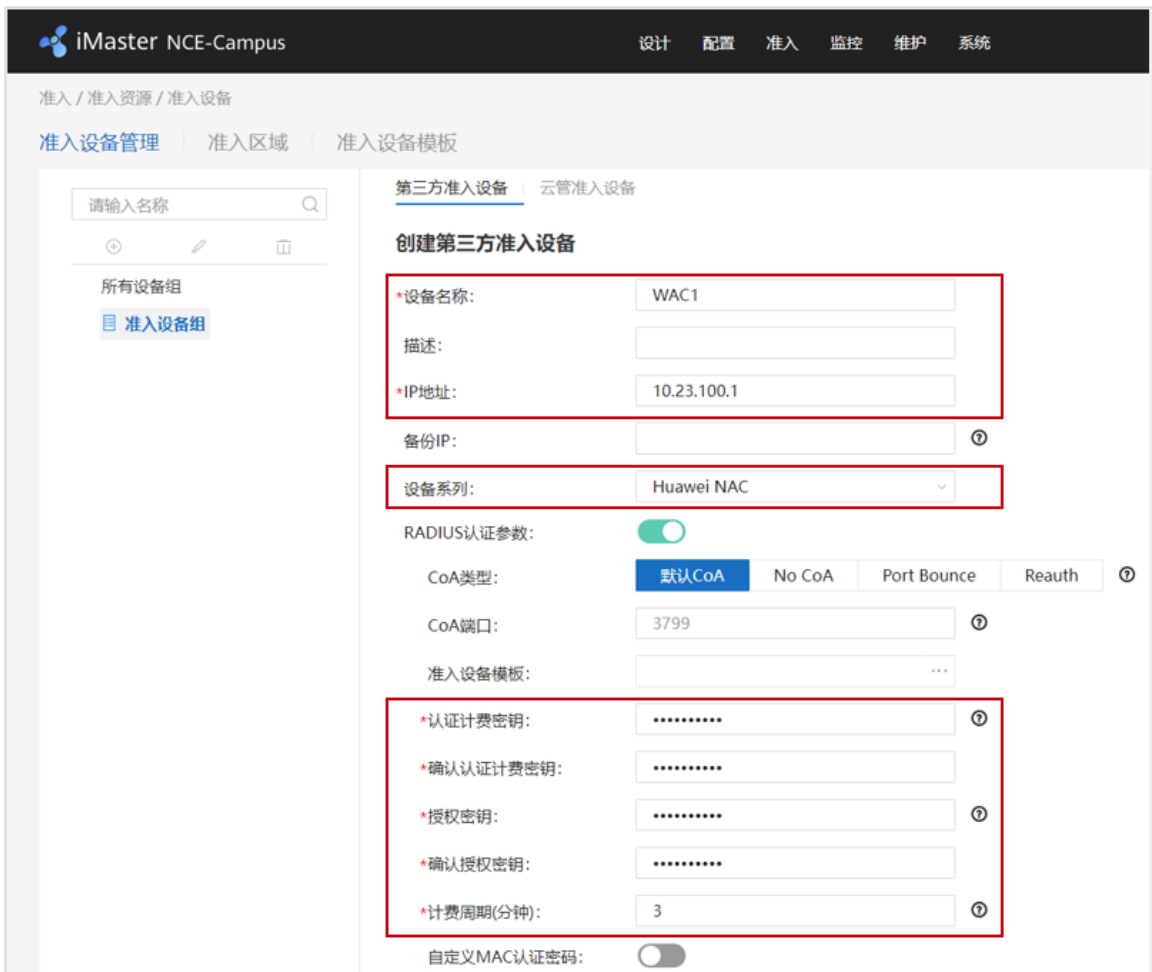
选择“准入 > 准入资源 > 准入设备”，配置准入设备。



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:

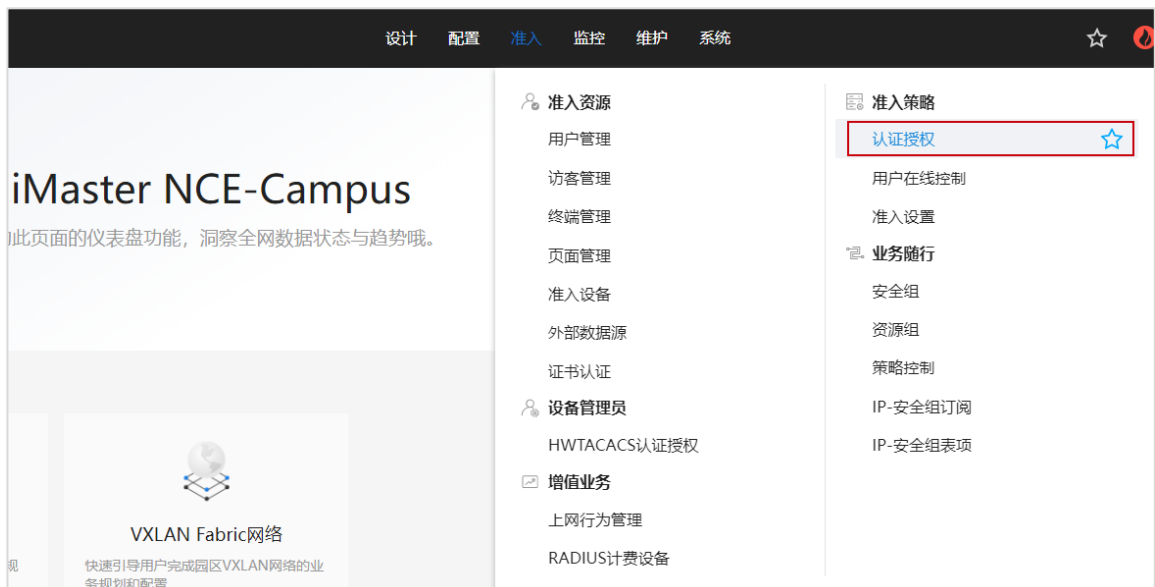
*Portal认证端口: 2000

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: 选择 移除

<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:

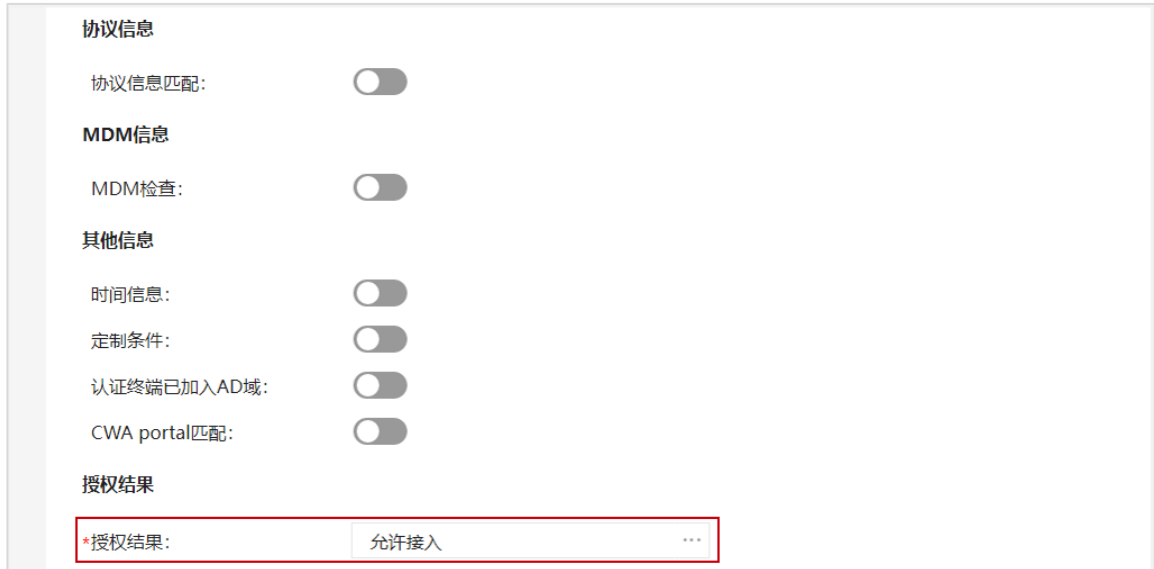
SSID: 增加

wlan-net

终端信息匹配:

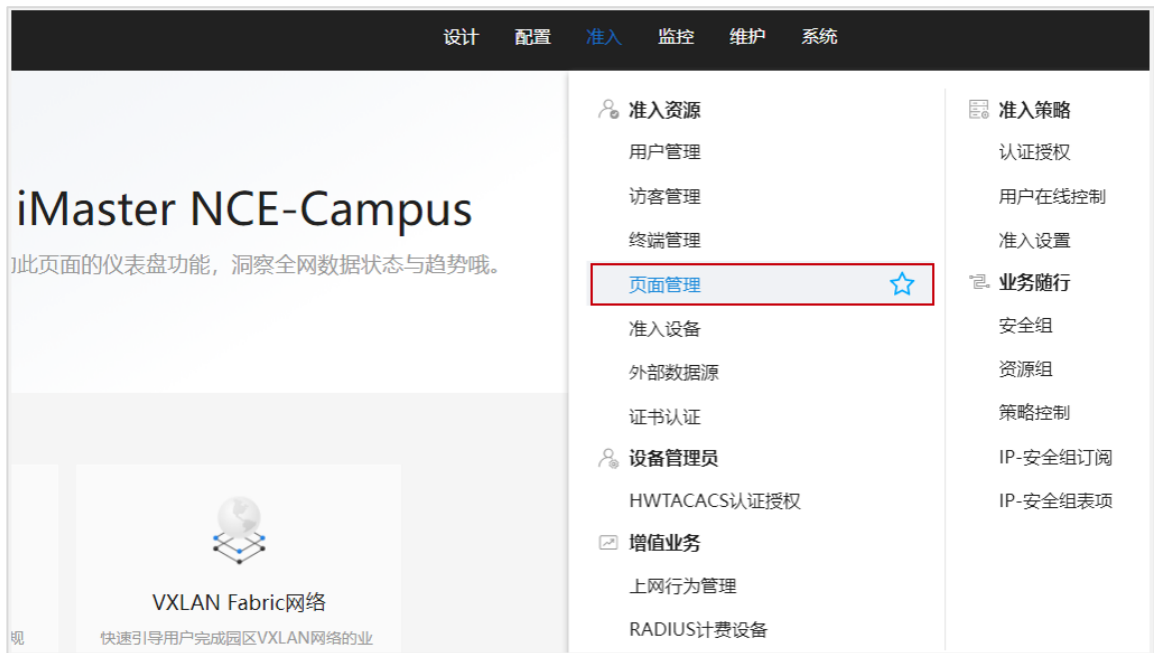
终端IP范围: 通过换行符分隔IP地址, 请输入IP地址/掩码(如192.168.1.1/32或2001:0DB8:0:0:0:1428:57AB/64)或IP地址段(如192.168.1.1-

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”。

iMaster NCE-Campus 设计 配置 准入 监控 维护 系统

准入 / 准入资源 / 页面管理

页面定制 | Portal页面推送策略 | 语言模板 | 门户管理

* 名称: Portal

描述:

接入方式: 有线 **无线**

推送规则 ^

站点信息匹配:

接入设备类型: 请选择...

SSID匹配:

SSID: **增加**

wlan-net

准入设备组:

操作系统匹配:

Windows PC IOS Android Linux/Unix

Windows Phone MAC OS Other

推送页面规则 ^

* 认证方式: 用户名密码认证

* 推送页面: 请输入推送页面名称 没有合适的页面? 跳转到 准入 > 准入资源 > 页面管理 > 页面定制 规划新的页面。



默认用户名密码认...

* 首推页面: **认证页面** 注册页面 用户须知页面

* 认证成功后跳转: 不跳转

查看 Portal 页面推送策略，如下所示。



6.3 结果验证

6.3.1 检查 AP 上线状态

在 WAC1 上执行 `display ap all` 命令，查看 AP 的上线状态。“State”为 normal 表示 AP 成功上线。AP 的 IP 地址通过 DHCP 动态获取，实际中以实验结果为准。

```
[WAC1] display ap all
Total AP information:
nor : normal          [3]
ExtralInfo : Extra information
-----
ID  MAC      Name  Group  IP           Type           State STA  Uptime  ExtralInfo
-----
0   9cb2-e82d-54f0 AP1   ap-group1 10.23.100.225 AirEngine5761-11 nor   0   6D:18H:42M:59S -
1   9cb2-e82d-5410 AP2   ap-group1 10.23.100.214 AirEngine5761-11 nor   0   6D:18H:41M:33S -
2   9cb2-e82d-5110 AP3   ap-group1 10.23.100.117 AirEngine5761-11 nor   0   6D:18H:42M:46S -
-----
Total: 3
```

6.3.2 检查 VAP 信息

在 WAC1 上执行 `display vap all` 命令，查看 VAP 信息如下。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID           Status  Auth type  STA  SSID
-----
0     AP1     0    1    9CB2-E82D-54F0 ON      Open+Portal 0    wlan-net
0     AP1     1    1    9CB2-E82D-5500 ON      Open+Portal 0    wlan-net
1     AP2     0    1    9CB2-E82D-5410 ON      Open+Portal 0    wlan-net
1     AP2     1    1    9CB2-E82D-5420 ON      Open+Portal 0    wlan-net
2     AP3     0    1    9CB2-E82D-5110 ON      Open+Portal 0    wlan-net
```

2	AP3	1	1	9CB2-E82D-5120 ON	Open+Portal	0	wlan-net

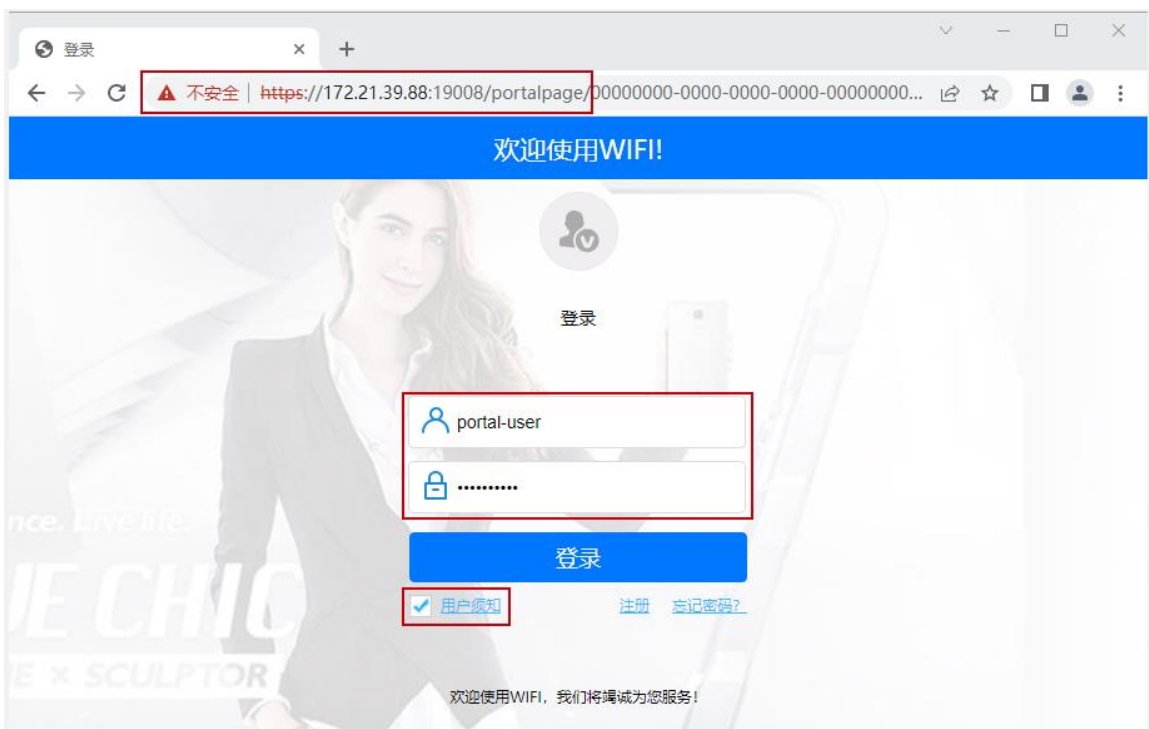
Total: 6							

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。

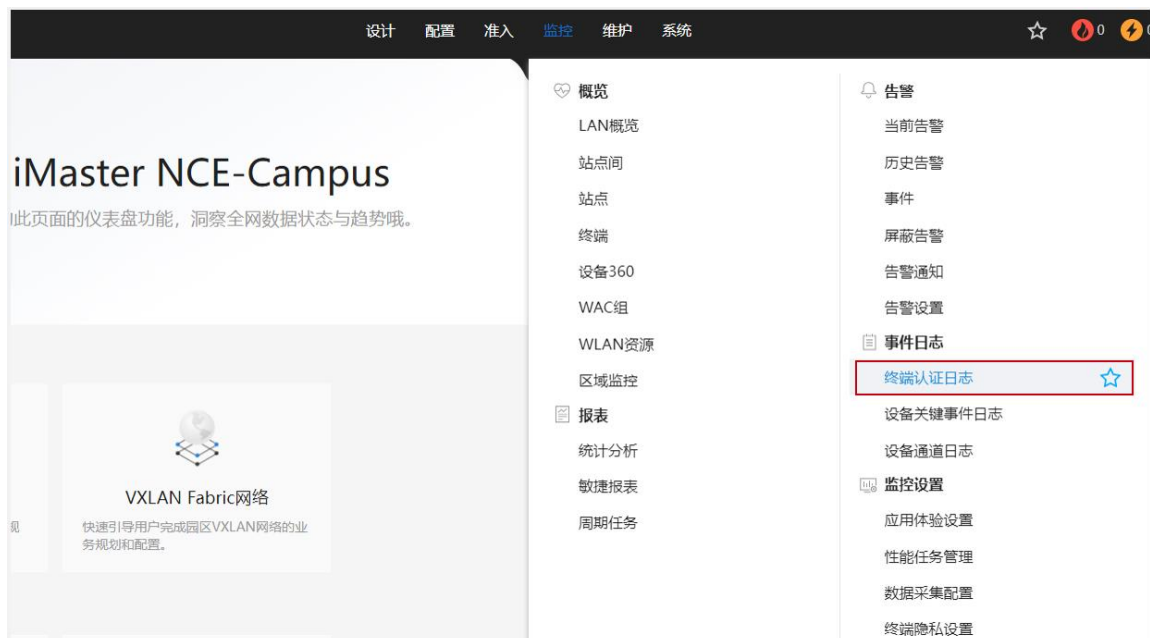


显示认证成功，后续即可正常访问网络资源。



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，“Success”表示成功接入，如下所示。

```
[WAC1] display access-user detail
Basic:
  User ID                : 65623
  User name               : portal-user
  User MAC                : 081f-7153-90b4
  User IP address         : 10.23.101.196
  User vpn-instance       : -
  User IPv6 address       : -
  User access Interface   : Wlan-Dbss17499
  User vlan event         : Success
  QinQVlan/UserVlan      : 0/101
  User vlan source        : user request
  User access time        : XXXX 09:21:06
  User accounting session ID : WAC10000000000010194****0100057
  User accounting mult session ID : 9CB2E82D5410081F715390B463283****8D7D1C1
  User access type        : WEB
  AP name                 : AP2
  Radio ID                : 1
  AP MAC                  : 9cb2-e82d-5410
  SSID                    : wlan-net
  Online time              : 1166(s)
  Web-server IP address   : 172.21.39.88
  User Group Priority      : 0

AAA:
  User authentication type : WEB authentication
  Current authentication method : RADIUS
  Current authorization method : -
  Current accounting method  : RADIUS

-----
Total: 1, printed: 1
```

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 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 169.254.1.1 255.255.255.0
#
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
```

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

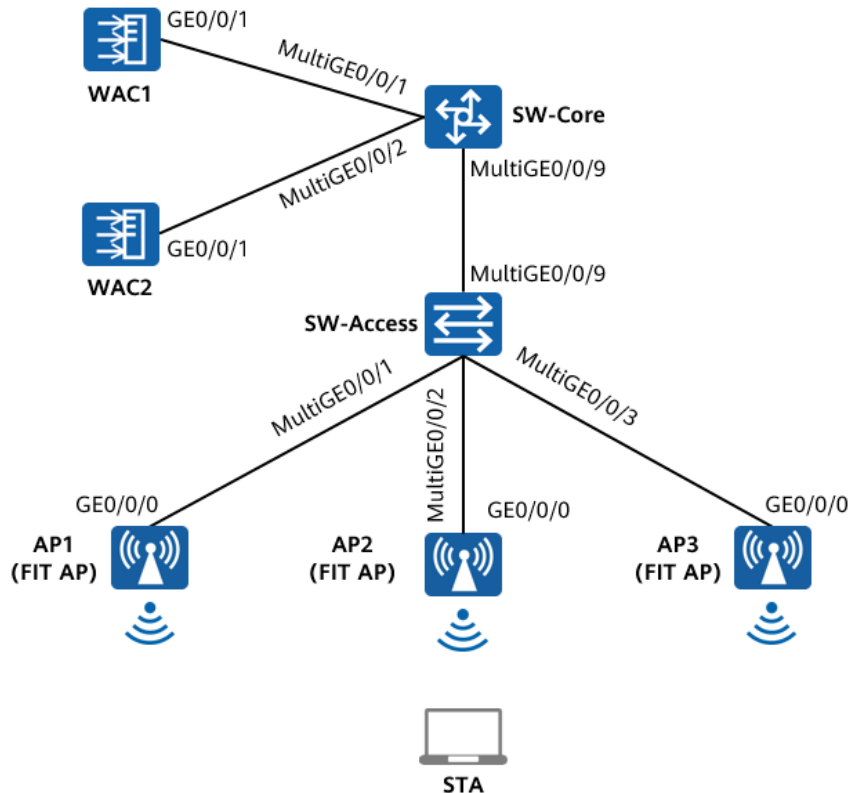


图7-1 WLAN 漫游实验拓扑图

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.配置各个设备 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 配置网络互通

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
```

配置 WAC1 设备。

在 WAC1 上创建 VLAN 100、101。

```
<AirEngine9700-M1> system-view
[AirEngine9700-M1] sysname WAC1
[WAC1] vlan batch 100 101
```

配置 WAC1 的 GE0/0/1 端口类型及允许通过的 VLAN。

```
[WAC1] interface GigabitEthernet 0/0/1
[WAC1-GigabitEthernet /0/1] port link-type trunk
[WAC1-GigabitEthernet /0/1] port trunk allow-pass vlan 100 101
[WAC1-GigabitEthernet /0/1] quit
```

配置 WAC2 设备。

在 WAC2 上创建 VLAN 200、201。

```
<AirEngine9700-M1> system-view
[AirEngine9700-M1] sysname WAC2
[WAC2] vlan batch 200 201
```

配置 WAC2 的 GE0/0/1 端口类型及允许通过的 VLAN。

```
[WAC2] interface GigabitEthernet 0/0/1
[WAC2-GigabitEthernet /0/1] port link-type trunk
[WAC2-GigabitEthernet /0/1] port trunk allow-pass vlan 200 201
[WAC2-GigabitEthernet /0/1] quit
```

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。

```
[WAC1] interface vlanif 100
[WAC1-Vlanif100] ip address 10.23.100.1 24
[WAC1-Vlanif100] quit
[WAC1] interface Vlanif 101
[WAC1-Vlanif101] ip address 10.23.101.254 24
[WAC1-Vlanif101] quit
```

配置 WAC2 的 IP 地址。

```
[WAC2] interface vlan 200
[WAC2-Vlanif200] ip address 10.23.200.1 24
[WAC2-Vlanif200] quit
[WAC2] interface vlan 201
[WAC2-Vlanif201] ip address 10.23.201.254 24
[WAC2-Vlanif201] quit
```

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。

```
[WAC1] ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
```

在 WAC2 上配置缺省路由。

```
[WAC2] ip route-static 0.0.0.0 0.0.0.0 10.23.200.254
```

步骤 2 配置 DHCP 服务器

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

```
[WAC1] dhcp enable
[WAC1] interface Vlanif 100
[WAC1-Vlanif100] dhcp select interface
[WAC1-Vlanif100] quit
[WAC1] interface Vlanif 101
[WAC1-Vlanif101] dhcp select interface
[WAC1-Vlanif101] quit
```

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

```
[WAC2] dhcp enable
[WAC2] interface Vlanif 200
[WAC2-Vlanif200] dhcp select interface
```

```
[WAC2-Vlanif200] quit
[WAC2] interface Vlanif 201
[WAC2-Vlanif201] dhcp select interface
[WAC2-Vlanif201] quit
```

步骤 3 配置 AP1、AP2 上线

在 WAC1 上开启 CAPWAP DTLS 不认证。（V200R021C00 及之后版本）

```
[WAC1] capwap dtls no-auth enable
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is
enabled and brings security risks. After the device goes online for the first time, disable this function to
prevent security risks. Continue? [Y/N]: y
```

在 WAC1 上配置 CAPWAP 源端口，需要提前配置以下参数：

DTLS 预共享密钥：此处配置为 a1234567；

WAC 间 DTLS 预共享密钥：此处配置为 a1234567；

FIT AP 的管理参数（用户名/密码）：此处配置为 admin/Huawei@123；

全局离线管理 VAP 的登录密码：此处配置为 a1234567。

```
[WAC1] capwap dtls psk a1234567
[WAC1] capwap dtls inter-controller psk a1234567
[WAC1] wlan
[WAC1-wlan-view] temporary-management psk a1234567
[WAC1-wlan-view] ap username admin password cipher
Enter the password (plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a combination of at least three of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm password: Huawei@123
[WAC1-wlan-view] quit
[WAC1] capwap source interface vlanif 100
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be
interrupted.
Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version
earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.
```

创建 AP 组“ap-group1”，后续将 AP1、AP2 加入同一 AP 组中。

```
[WAC1] wlan
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

在 WAC1 上配置 AP 认证方式为 MAC 认证。

```
[WAC1] wlan
[WAC1-wlan-view] ap auth-mode mac-auth
[WAC1-wlan-view] quit
```

在 WAC1 上添加 AP（AP 的 MAC 地址以实际情况为准）。

```
[WAC1] wlan
[WAC1-wlan-view] ap-id 0 ap-mac 9cb2-e82d-54f0
```

```
[WAC1-wlan-ap-0] ap-group ap-group1
[WAC1-wlan-ap-0] ap-name AP1
[WAC1-wlan-ap-0] quit
[WAC1-wlan-view] ap-id 1 ap-mac 9cb2-e82d-5410
[WAC1-wlan-ap-1] ap-group ap-group1
[WAC1-wlan-ap-1] ap-name AP2
[WAC1-wlan-ap-1] quit
[WAC1-wlan-view] quit
```

步骤 4 配置 AP3 上线

在 WAC2 上开启 CAPWAP DTLS 不认证。（V200R021C00 及之后版本）

```
[WAC2] capwap dtls no-auth enable
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is
enabled and brings security risks. After the device goes online for the first time, disable this function to
prevent security risks. Continue?[Y/N]: y
```

在 WAC2 上配置 CAPWAP 源端口，需要提前配置以下参数：

DTLS 预共享密钥：此处配置为 a1234567；

WAC 间 DTLS 预共享密钥：此处配置为 a1234567；

FIT AP 的管理参数（用户名/密码）：此处配置为 admin/Huawei@123；

全局离线管理 VAP 的登录密码：此处配置为 a1234567。

```
[WAC2] capwap dtls psk a1234567
[WAC2] capwap dtls inter-controller psk a1234567
[WAC2] wlan
[WAC2-wlan-view] temporary-management psk a1234567
[WAC2-wlan-view] ap username admin password cipher
Enter the password (plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a combination of at least three of the following: lowercase letters a to z,
uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm password: Huawei@123
[WAC2-wlan-view] quit
[WAC2] capwap source interface vlanif 200
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be
interrupted.
Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version
earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.
```

创建 AP 组 “ap-group2”。

```
[WAC2] wlan
[WAC2-wlan-view] ap-group name ap-group2
[WAC2-wlan-ap-group-ap-group2] quit
[WAC2-wlan-view] quit
```

在 WAC2 上配置 AP 认证方式为 MAC 认证。

```
[WAC2] wlan
[WAC2-wlan-view] ap auth-mode mac-auth
[WAC2-wlan-view] quit
```

在 WAC2 上添加 AP（AP 的 MAC 地址以实际情况为准）。

```
[WAC2] wlan
[WAC2-wlan-view] ap-id 0 ap-mac 9cb2-e82d-5110
[WAC2-wlan-ap-0] ap-group ap-group2
[WAC2-wlan-ap-0] ap-name AP3
[WAC2-wlan-ap-0] quit
[WAC2-wlan-view] quit
```

步骤 5 配置无线业务（WAC1）

通过域管理模板配置国家码，缺省国家代码为中国（如果设备在中国以外地区则需要改成对应的国家码）。

```
[WAC1] wlan
[WAC1-wlan-view] regulatory-domain-profile name domain1
[WAC1-wlan-regulate-domain-domain1] country-code CN
[WAC1-wlan-regulate-domain-domain1] quit
```

在 AP 组中引用域管理模板。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]: y
[WAC1-wlan-ap-group-ap-group1] quit
```

创建名为“wlan-net”的安全模板，并配置安全策略。

```
[WAC1] wlan
[WAC1-wlan-view] security-profile name wlan-net
[WAC1-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a12345678 aes
[WAC1-wlan-sec-prof-wlan-net] quit
```

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

```
[WAC1-wlan-view] ssid-profile name wlan-net
[WAC1-wlan-ssid-prof-wlan-net] ssid wlan-net
[WAC1-wlan-ssid-prof-wlan-net] quit
```

创建名为“wlan-net1”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。

```
[WAC1-wlan-view] vap-profile name wlan-net1
[WAC1-wlan-vap-prof-wlan-net1] forward-mode direct-forward
[WAC1-wlan-vap-prof-wlan-net1] service-vlan vlan-id 101
[WAC1-wlan-vap-prof-wlan-net1] security-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net1] ssid-profile wlan-net
[WAC1-wlan-vap-prof-wlan-net1] quit
```

配置 AP 组引用 VAP 模板。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net1 wlan 1 radio 0
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net1 wlan 1 radio 1
```



```
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] quit
```

步骤 6 配置无线业务（WAC2）

通过域管理模板配置国家码，缺省国家代码为中国（如果设备在中国以外地区则需要改成对应的国家码）。

```
[WAC2] wlan
[WAC2-wlan-view] regulatory-domain-profile name domain1
[WAC2-wlan-regulate-domain-domain1] country-code CN
[WAC2-wlan-regulate-domain-domain1] quit
```

在 AP 组中引用域管理模板。

```
[WAC2-wlan-view] ap-group name ap-group2
[WAC2-wlan-ap-group-ap-group2] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may
restart APs. Continue?[Y/N]: y
[WAC2-wlan-ap-group-ap-group2] quit
```

创建名为“wlan-net”的安全模板，并配置安全策略。

```
[WAC2] wlan
[WAC2-wlan-view] security-profile name wlan-net
[WAC2-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a12345678 aes
[WAC2-wlan-sec-prof-wlan-net] quit
```

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

```
[WAC2-wlan-view] ssid-profile name wlan-net
[WAC2-wlan-ssid-prof-wlan-net] ssid wlan-net
[WAC2-wlan-ssid-prof-wlan-net] quit
```

创建名为“wlan-net2”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。

```
[WAC2-wlan-view] vap-profile name wlan-net2
[WAC2-wlan-vap-prof-wlan-net2] forward-mode direct-forward
[WAC2-wlan-vap-prof-wlan-net2] service-vlan vlan-id 201
[WAC2-wlan-vap-prof-wlan-net2] security-profile wlan-net
[WAC2-wlan-vap-prof-wlan-net2] ssid-profile wlan-net
[WAC2-wlan-vap-prof-wlan-net2] quit
```

配置 AP 组引用 VAP 模板。

```
[WAC2-wlan-view] ap-group name ap-group2
[WAC2-wlan-ap-group-ap-group2] vap-profile wlan-net2 wlan 1 radio 0
[WAC2-wlan-ap-group-ap-group2] vap-profile wlan-net2 wlan 1 radio 1
[WAC2-wlan-ap-group-ap-group2] quit
```

步骤 7 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。

```
[WAC1] wlan
```

```
[WAC1-wlan-view] mobility-group name mob1
[WAC1-mc-mg-mob1] member ip-address 10.23.100.1
[WAC1-mc-mg-mob1] member ip-address 10.23.200.1
[WAC1-mc-mg-mob1] quit
```

在 WAC2 上创建漫游组，并配置 WAC1 和 WAC2 为漫游组成员。

```
[WAC2] wlan
[WAC2-wlan-view] mobility-group name mob1
[WAC2-mc-mg-mob1] member ip-address 10.23.100.1
[WAC2-mc-mg-mob1] member ip-address 10.23.200.1
[WAC2-mc-mg-mob1] quit
```

步骤 8 配置 WAC 间隧道 DTLS 加密

由于之前的步骤中，已经配置了 WAC 间 DTLS 加密的预共享密钥，此处无需重复配置。

在 WAC1 上启用 WAC 间隧道加密。

```
[WAC1] capwap dtls inter-controller control-link encrypt on
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue?
[Y/N]: y
```

在 WAC2 上启用 WAC 间隧道加密。

```
[WAC2] capwap dtls inter-controller control-link encrypt on
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue?
[Y/N]: y
```

7.3 结果验证

7.3.1 检查 AP 上线

在 WAC1 上使用 display ap all 命令检查 AP1、AP2 的上线状态。

```
[WAC1] display ap all
Total AP information:
nor   : normal           [2]
ExtraInfo : Extra information
-----
ID    MAC          Name  Group   IP          Type          State  STA  Uptime  ExtraInfo
-----
0     9cb2-e82d-54f0 AP1   ap-group1 10.23.100.97 AirEngine5761-11 nor  0    2M:44S -
1     9cb2-e82d-5410 AP2   ap-group1 10.23.100.85 AirEngine5761-11 nor  0    2M:32S -
-----
Total: 2
```

在 WAC2 上使用 display ap all 命令检查 AP3 的上线状态。

```
[WAC2] display ap all
Total AP information:
nor   : normal           [1]
```

ExtralInfo : Extra information

ID	MAC	Name	Group	IP	Type	State	STA	Uptime	ExtralInfo
0	9cb2-e82d-5110	AP3	ap-group2	10.23.200.249	AirEngine5761-11	nor	0	1M:28S	-

Total: 1

7.3.2 检查 VAP 状态

在 WAC1 上执行 display vap all 命令，查看 VAP 信息如下。

[WAC1] display vap all

Info: This operation may take a few seconds, please wait.

WID : WLAN ID

AP ID	AP name	RfID	WID	BSSID	Status	Auth type	STA	SSID
0	AP1	0	1	9CB2-E82D-54F0	ON	WPA/WPA2-PSK	0	wlan-net
0	AP1	1	1	9CB2-E82D-5500	ON	WPA/WPA2-PSK	0	wlan-net
1	AP2	0	1	9CB2-E82D-5410	ON	WPA/WPA2-PSK	0	wlan-net
1	AP2	1	1	9CB2-E82D-5420	ON	WPA/WPA2-PSK	0	wlan-net

Total: 4

在 WAC2 上执行 display vap all 命令，查看 VAP 信息如下。

[WAC2] display vap all

Info: This operation may take a few seconds, please wait.

WID : WLAN ID

AP ID	AP name	RfID	WID	BSSID	Status	Auth type	STA	SSID
0	AP3	0	1	9CB2-E82D-5110	ON	WPA/WPA2-PSK	0	wlan-net
0	AP3	1	1	9CB2-E82D-5120	ON	WPA/WPA2-PSK	0	wlan-net

Total: 2

7.3.3 检查漫游组状态

在 WAC1/WAC2 上执行 display mobility-group name mob1 命令，检查漫游组状态。其中“State”为 normal，表示正常，以 WAC1 为例，显示如下。

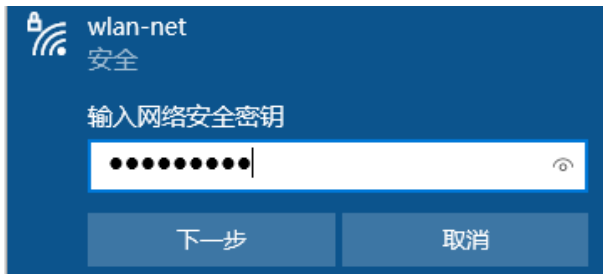
[WAC1] display mobility-group name mob1

State	IP address	Description
normal	10.23.100.1	-
normal	10.23.200.1	-

Total: 2

7.3.4 观察 STA 漫游情况

在 AP1 的信号覆盖范围之内，STA 搜索无线信号“wlan-net”，输入共享密钥“a12345678”，接入 WLAN 网络。



在 WAC1 上查看 STA 接入情况，发现 STA 接入了 AP1。

```
[WAC1] display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-----
STA MAC   AP ID   Ap name  Rf/WLAN  Band  Type  Rx/Tx RSSI  VLAN  IP address  SSID
-----
081f-7153-90b4  0   AP1    1/1     5G   11ac  156/144  -31  101  10.23.101.83  wlan-net
-----
Total: 1 2.4G: 0 5G: 1
```

随着 STA 逐渐向 AP2 的覆盖区域移动，发现 STA 漫游到了 AP2。

```
[WAC1] display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-----
STA MAC   AP ID   Ap name  Rf/WLAN  Band  Type  Rx/Tx RSSI  VLAN  IP address  SSID
-----
081f-7153-90b4  1   AP2    1/1     5G   11ac  156/115  -17  101  10.23.101.83  wlan-net
-----
Total: 1 2.4G: 0 5G: 1
```

在 WAC1 上查看漫游轨迹如下所示（WAC 内二层漫游）。

```
[WAC1] display station roam-track sta-mac 081f-7153-90b4
Access SSID:wlan-net
Rx/Tx: link receive rate/link transmit rate(Mbps)
s:Same Frequency Network c:PMK Cache Roam
r:802.11r Roam d:802.11r over ds Roam p:proprietary 802.11r Roam
-----
L2/L3      AP-AC IP          AC-AC IP          Ap name  Radio ID
BSSID      TIME              In/Out RSSI       Out Rx/Tx
-----
--         10.23.100.1      -                  AP1      1
9cb2-e82d-5500  XXXX-XX-XX/19:58:10  -22/-23          156/130
```

```

L2          10.23.100.1          -          AP2      1
9cb2-e82d-5420 XXXX-XX-XX /20:00:02 -31/-      -/-
-----
Number: 1
    
```

然后随着 STA 继续向 AP3 的覆盖区域移动，发现 STA 漫游到了 AP3。

```

[WAC2] display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-----
STA MAC    AP ID    Ap name  Rf/WLAN  Band  Type  Rx/Tx RSSI  VLAN  IP address  SSID
-----
081f-7153-90b4  0    AP3     1/1     5G   -   -/-      -    101  10.23.101.83 wlan-net
-----
Total: 1 2.4G: 0 5G: 1
    
```

在 WAC2 上查看漫游轨迹如下所示（WAC 间三层漫游）。

```

[WAC2] display station roam-track sta-mac 081f-7153-90b4
Access SSID:wlan-net
Rx/Tx: link receive rate/link transmit rate(Mbps)
s:Same Frequency Network c:PMK Cache Roam
r:802.11r Roam d:802.11r over ds Roam p:proprietary 802.11r Roam
-----
L2/L3      AP-AC IP          AC-AC IP          Ap name  Radio ID
BSSID      TIME              In/Out RSSI       Out Rx/Tx
-----
--         10.23.100.1      -                  AP1      1
9cb2-e82d-5500 XXXX-XX-XX /19:58:10 -22/-23         156/130
L2         10.23.100.1      -                  AP2      1
9cb2-e82d-5420 XXXX-XX-XX /20:00:02 -31/-27         156/115
L3         10.23.200.1      10.23.200.1      AP3      1
9cb2-e82d-5120 XXXX-XX-XX /20:01:58 -26/-           -/-
-----
Number: 2
    
```

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.$n|ec5XhLvJw,(]KNf[B%K[0I1J[:\T2~Fl/&R&(T$
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 169.254.1.1 255.255.255.0
#
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>xRRT}{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 169.254.1.1 255.255.255.0
#
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#i1%`PR@S60sh\SOH2r69%^%#
capwap dtls inter-controller psk %^%#ia.O&Gj]IXF|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

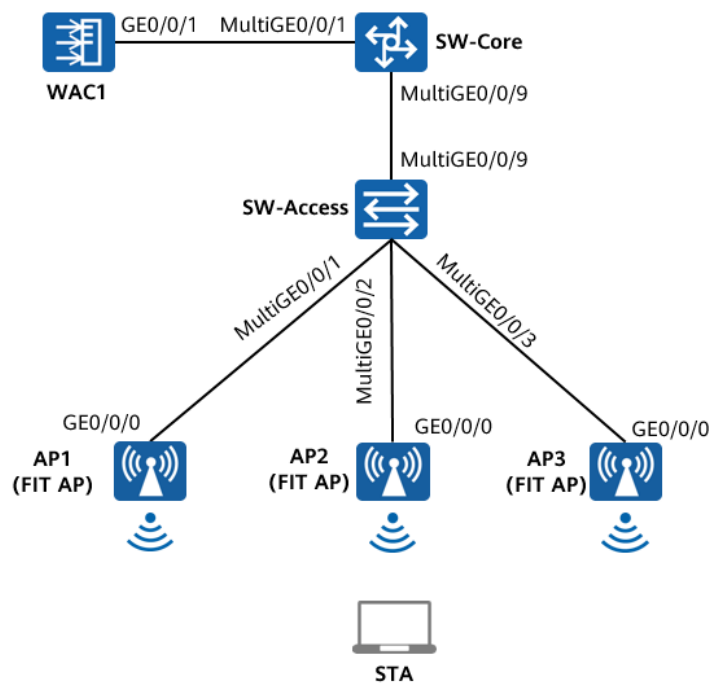


图8-1 射频资源管理实验拓扑图

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

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.配置信道、频率自动调优范围。
- 5.配置频谱导航功能。
- 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

此配置步骤请参考 1.2.2 章节（配置步骤）中的步骤 1~步骤 5，此处不再赘述。

步骤 2 配置射频调优

配置射频调优模式为 auto 模式，缺省的调优时间间隔为 1440 分钟。

```
[WAC1-wlan-view] calibrate enable auto
```

开启全局 DFA 功能，冗余射频的处理模式为 auto-switch 模式。

```
[WAC1-wlan-view] calibrate flexible-radio auto-switch
```

在 2.4G 频段开启信道、功率动态调整功能。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] radio 0
[WAC1-wlan-group-radio-ap-group1/0] calibrate auto-channel-select enable
[WAC1-wlan-group-radio-ap-group1/0] calibrate auto-txpower-select enable
[WAC1-wlan-group-radio-ap-group1/0] quit
```

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）

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] radio 1
[WAC1-wlan-group-radio-ap-group1/1] calibrate auto-channel-select enable
[WAC1-wlan-group-radio-ap-group1/1] calibrate auto-tpower-select enable
[WAC1-wlan-group-radio-ap-group1/1] calibrate auto-bandwidth-select enable
[WAC1-wlan-group-radio-ap-group1/1] quit
```

手动触发射频调优。

```
[WAC1-wlan-view] calibrate manual startup
Warning: The operation may cause business interruption, continue? [y/n]: y
```

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）

```
[WAC1-wlan-view] vap-profile name wlan-net
[WAC1-wlan-vap-prof-wlan-net] undo band-steer disable
[WAC1-wlan-vap-prof-wlan-net] quit
```

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。

```
[WAC1-wlan-view] rrm-profile name wlan-rrm
[WAC1-wlan-rrm-prof-wlan-rrm] band-steer balance start-threshold 90
[WAC1-wlan-rrm-prof-wlan-rrm] band-steer balance gap-threshold 80
[WAC1-wlan-rrm-prof-wlan-rrm] band-steer snr-threshold 18
```

创建射频模板，引用 RRM 模板。

```
[WAC1-wlan-view] radio-2g-profile name wlan-2g
[WAC1-wlan-radio-2g-prof-wlan-2g] rrm-profile wlan-rrm
[WAC1-wlan-radio-2g-prof-wlan-2g] quit
[WAC1-wlan-view] radio-5g-profile name wlan-5g
[WAC1-wlan-radio-5g-prof-wlan-5g] rrm-profile wlan-rrm
[WAC1-wlan-radio-5g-prof-wlan-5g] quit
```

将 2G 射频模板 “wlan-2g” 引用至 AP 组的 radio 0 中，将 5G 射频模板 “wlan-5g” 引用至 AP 组的 radio 1 中。

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] radio-2g-profile wlan-2g radio 0
Warning: This action may cause service interruption. Continue?[Y/N] y
[WAC1-wlan-ap-group-ap-group1] radio-5g-profile wlan-5g radio 1
Warning: This action may cause service interruption. Continue?[Y/N] y
```

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。

```
[WAC1-wlan-view] rrm-profile name wlan-rrm
[WAC1-wlan-rrm-prof-wlan-rrm] undo sta-load-balance dynamic disable
[WAC1-wlan-rrm-prof-wlan-rrm] sta-load-balance dynamic sta-number start-threshold 12
```



```
[WAC1-wlan-rrm-prof-wlan-rrm] sta-load-balance dynamic sta-number gap-threshold number 5
[WAC1-wlan-rrm-prof-wlan-rrm] sta-load-balance dynamic rssi-threshold -63
[WAC1-wlan-rrm-prof-wlan-rrm] quit
```

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。

启用当接入终端达到阈值时自动隐藏 SSID 的功能。

```
[WAC1-wlan-view] rrm-profile name wlan-rrm
[WAC1-wlan-rrm-prof-wlan-rrm] uac client-number enable
[WAC1-wlan-rrm-prof-wlan-rrm] uac client-number threshold access 40 roam 40
[WAC1-wlan-rrm-prof-wlan-rrm] uac client-snr enable
[WAC1-wlan-rrm-prof-wlan-rrm] uac client-snr threshold 13
[WAC1-wlan-rrm-prof-wlan-rrm] uac reach-access-threshold hide-ssid
[WAC1-wlan-rrm-prof-wlan-rrm] quit
```

8.3 结果验证

8.3.1 查看 RRM 模板信息

在 WAC1 上查看 RRM 模板的配置信息，如下所示。

```
[WAC1] display rrm-profile name wlan-rrm
-----
Retransmission rate threshold for trigger channel/power select(%) : 60
Noise-floor threshold for trigger channel/power select(dBm) : -75
Calibrate tpc threshold(dBm): : -60
Maximum 2.4G calibration TX power(dBm) : 127
Maximum 5G calibration TX power(dBm) : 127
Minimum 2.4G calibration TX power(dBm) : 9
Minimum 5G calibration TX power(dBm) : 12
Calibrate retransmission rate check interval(min) : 1
Calibrate retransmission rate check traffic threshold(kbps) : 1250
Airtime fairness schedule : disable
Dynamic adjust EDCA parameter : disable
Dynamic EDCA be-service threshold : 6
UAC check client's SNR : enable
UAC client's SNR threshold(dB) : 13
UAC check client number : enable
UAC client number access threshold : 40
UAC client number roam threshold : 40
Action upon reaching the UAC threshold : SSID hide
Band steer deny threshold : 0
Band steer SNR threshold(dB) : 18
Band balance start threshold : 90
```

Band balance gap threshold(%)	: 80
Client's band expire based on continuous probe counts	: 35
Station load balance	: enable
Station load balance mode	: sta-number
Station load balance RSSI threshold(dBm)	: -63
Station load balance RSSI-diff-gap threshold(dBm)	: 5
Station load balance sta-number start threshold	: 12
Station load balance sta-number gap threshold(percentage)	: -
Station load balance sta-number gap threshold(number)	: 5
Station load balance deauth fail times	: 0
Station load balance BTM fail times	: 5
Station load balance steer-restrict restrict time(s)	: 5
Station load balance steer-restrict probe threshold	: 5
Station load balance steer-restrict auth threshold	: 0
Station load balance probe-report interval(s)	: 120
BSS color switch	: enable
Spatial reuse switch	: enable
Smart-roam	: enable
Smart-roam AI mode	: enable
Smart-roam quick kickoff	: enable
Smart-roam check SNR	: enable
Smart-roam quick kickoff check SNR	: enable
Smart-roam check rate	: disable
Smart-roam quick kickoff check rate	: disable
Smart-roam standing SNR threshold(dB)	: 20
Smart-roam SNR quick-kickoff-threshold(dB)	: 15
Smart-roam rate threshold(%)	: 20
Smart-roam rate quick-kickoff-threshold(%)	: 20
Smart-roam high level SNR margin(dB)	: 15
Smart-roam low level SNR margin(dB)	: 6
Smart-roam SNR check interval(s)	: 3
Smart-roam unable roam client expire time(min)	: 120
Smart-roam quick-kickoff SNR check interval(ms)	: 500
Smart-roam quick-kickoff SNR P-N observe time	: 6
Smart-roam quick-kickoff SNR P-N qualify time	: 4
Smart-roam advanced scan	: enable
Smart-roam quick-kickoff back off time	: 60
AMC policy	: auto-balance
High density AMC optimize	: disable
Antenna-mode	: omnidirection
SFN roam check high threshold(dBm)	: -55
SFN roam check low threshold(dBm)	: -60
SFN roam check interval(ms)	: 700
SFN roam report interval(ms)	: 400
SFN roam check rssi-accumulate threshold(dB)	: 8
SFN roam check sta-holding times	: 3
SFN roam check gap-rssi(dB)	: 6
SFN roam check better-times	: 2

```

DFS smart select                : enable
DFS recover delay time(min)     : 0
Multimedia air optimize
  Switch                         : disable
  Voice threshold                : 30
  Video threshold                : 100
  Voice downlink-slice-ratio    : medium
  Video downlink-slice-ratio    : medium
  Voice downlink-delay-guarantee : medium
  Video downlink-delay-guarantee : medium
  Congestion-control tcp-window-tuning switch : enable
Rate limit dynamic interval     : 5
Rate limit dynamic threshold    : 80
-----
    
```

8.3.2 查看 2G 射频模板信息

在 WAC1 上查看 2G 射频模板的配置信息，如下所示。

```

[WAC1] display radio-2g-profile name wlan-2g
-----
Radio type                : 802.11ax
Power auto adjust         : disable
Beacon interval(TUs)     : 100
Beamforming switch        : disable
Support short preamble    : support
Fragmentation threshold(Byte) : 2346
Channel switch announcement : enable
Channel switch mode       : continue
Guard interval mode      : short
802.11ax Guard interval mode : dot8
A-MPDU switch             : enable
HT A-MPDU length limit   : 3
A-MSDU switch             : auto
RTS-CTS-mode              : rts-cts
RTS-CTS-threshold        : 1400
802.11bg basic rate      : 1 2
802.11bg support rate    : 1 2 5 6 9 11 12 18 24 36 48 54
Multicast rate 2.4G      : auto adapt
Interference detect switch : enable
Co-channel frequency interference threshold(%) : 60
Adjacent-channel frequency interference threshold(%) : 60
Station interference threshold : 25
WMM switch                : enable
Mandatory switch          : disable
Auto-off start time       : -
Auto-off end time         : -
Auto-off time-range       : -
    
```

```

Wifi-light mode                : signal-strength
Utmost power switch            : auto
Rrm-profile                    : wlan-rrm
Air-scan-profile               : default
Smart-antenna                  : default
Agile-antenna-polarization    : disable
CCA threshold(dBm)            : -
High PER threshold(%)          : 80
Low PER threshold(%)           : 20
Training interval(s)          : auto
Training mpdu num              : 640
Throughput trigger training threshold (%) : 10
Autonavigation roam optimize beacon interval(TUs): 60
VIP user bandwidth reservation ratio (%) : 20
    
```

AP EDCA parameters:

	ECWmax	ECWmin	AIFSN	TXOPLimit(32us)	Ack-Policy
AC_VO	3	2	1	47	normal
AC_VI	4	3	1	94	normal
AC_BE	6	4	3	0	normal
AC_BK	10	4	7	0	normal

8.3.3 查看 5G 射频模板信息

在 WAC1 上查看 5G 射频模板的配置信息，如下所示。

```

[WAC1] display radio-5g-profile name wlan-5g
-----
Radio type                : 802.11ax
Power auto adjust         : disable
Beacon interval(TUs)     : 100
Beamforming switch        : disable
Fragmentation threshold(Byte) : 2346
Channel switch announcement : enable
Channel switch mode       : continue
Guard interval mode      : short
802.11ax guard interval mode : dot8
A-MPDU switch             : enable
HT A-MPDU length limit   : 3
VHT A-MPDU length limit  : 7
A-MSDU switch            : auto
VHT A-MSDU Max frame number : 2
RTS-CTS-mode              : RTS-CTS
RTS-CTS-threshold        : 1400
802.11a basic rate       : 6 12 24
802.11a support rate     : 6 9 12 18 24 36 48 54
    
```

```

Multicast rate 5G                : auto adapt
VHT mcs                          : 9 9 9 9 9 9 9
Interference detect switch       : enable
Co-channel frequency interference threshold(%) : 60
Adjacent-channel frequency interference threshold(%) : 60
Station interference threshold    : 25
WMM switch                       : enable
Mandatory switch                 : disable
Auto-off start time              : -
Auto-off end time                : -
Auto-off time-range              : -
WiFi-light mode                  : signal-strength
Utmost power switch              : auto
Rrm-profile                      : wlan-rrm
Air-scan-profile                 : default
Smart-antenna                    : default
Agile-antenna-polarization       : disable
CCA threshold(dBm)               : -
High PER threshold(%)            : 80
Low PER threshold(%)             : 20
Training interval(s)             : auto
Training mpdu num                : 640
Throughput trigger training threshold (%) : 10
Autonavigation roam optimize beacon interval(TUs): 60
VIP user bandwidth reservation ratio (%) : 20
    
```

AP EDCA parameters:

	ECWmax	ECWmin	AIFSN	TXOPLimit(32us)	Ack-Policy
AC_VO	3	2	1	47	normal
AC_VI	4	3	1	94	normal
AC_BE	6	4	3	0	normal
AC_BK	10	4	7	0	normal

8.3.4 查看当前射频状态信息

在 WAC1 上查看当前射频的状态信息，重点关注信道使用率，如下所示。

```

[WAC1] display radio all
Info: This operation may take a few seconds. Please wait for a moment.done.
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
WM:Working mode (normal/monitor/monitor dual-band-scan/monitor proxy dual-band-scan)
    
```

AP ID	Name	Rfid	Band	Type	ST	CH/BW	CE/ME	STA	CU	WM
0	AP1	0	2.4G	11ax	on	1/20M	9/29	0	15%	normal
0	AP1	1	5G	11ax	on	56/20M	12/30	0	5%	normal
1	AP2	0	2.4G	11ax	on	6/20M	9/29	0	20%	normal
1	AP2	1	5G	11ax	on	44/20M	12/30	0	5%	normal
2	AP3	0	2.4G	11ax	on	11/20M	9/29	0	33%	normal
2	AP3	1	5G	11ax	on	161/20M	12/30	1	6%	normal

Total:6										

8.4 配置参考

8.4.1 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
#
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
#
management-port isolate enable
management-plane isolate enable
#
diffserv domain default
#
radius-server template 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 169.254.1.1 255.255.255.0
#
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 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。

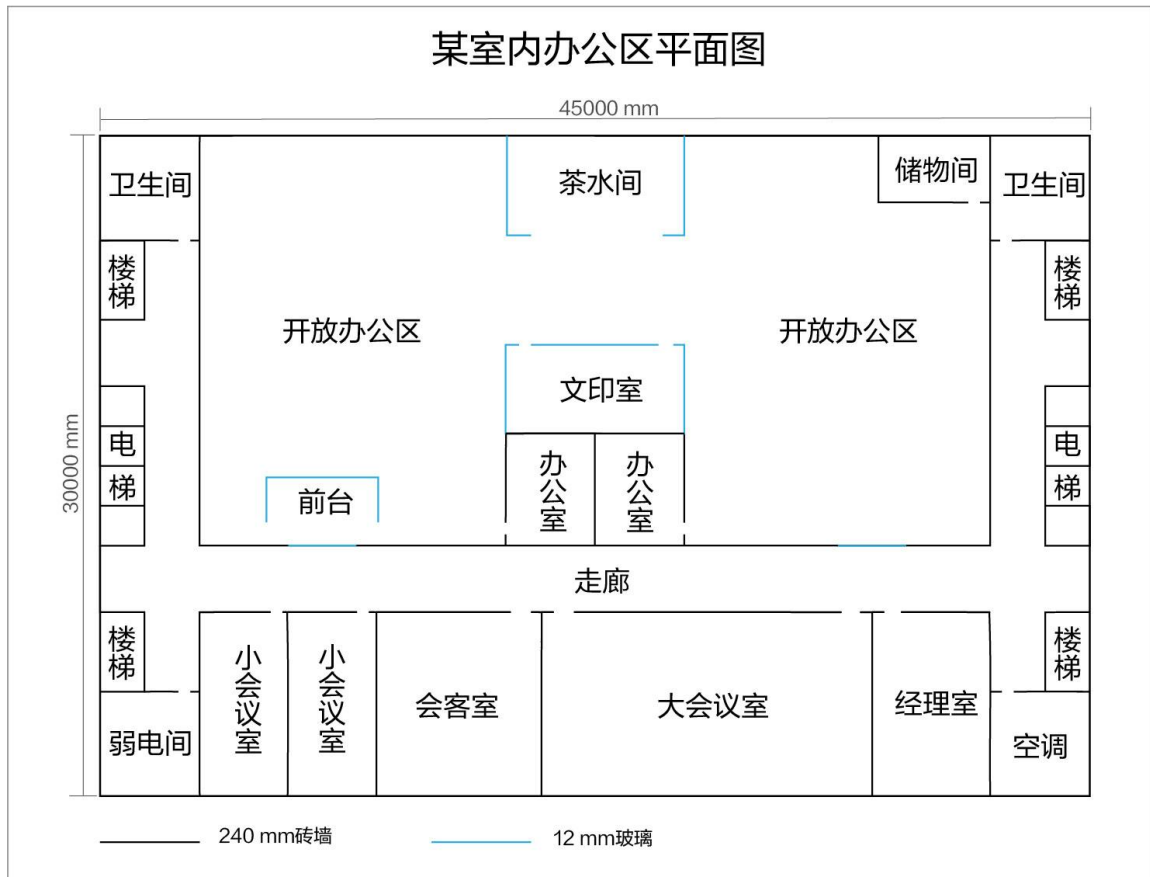


图9-1 WLAN 室内网规建筑图纸

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。

* 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

客户名称：HCIP-WLAN Q

* 项目名称：Huawei

* 项目经理：请输入完整的账号或邮箱

交付工程师：请输入完整的账号或邮箱

* 国家/地区：中国

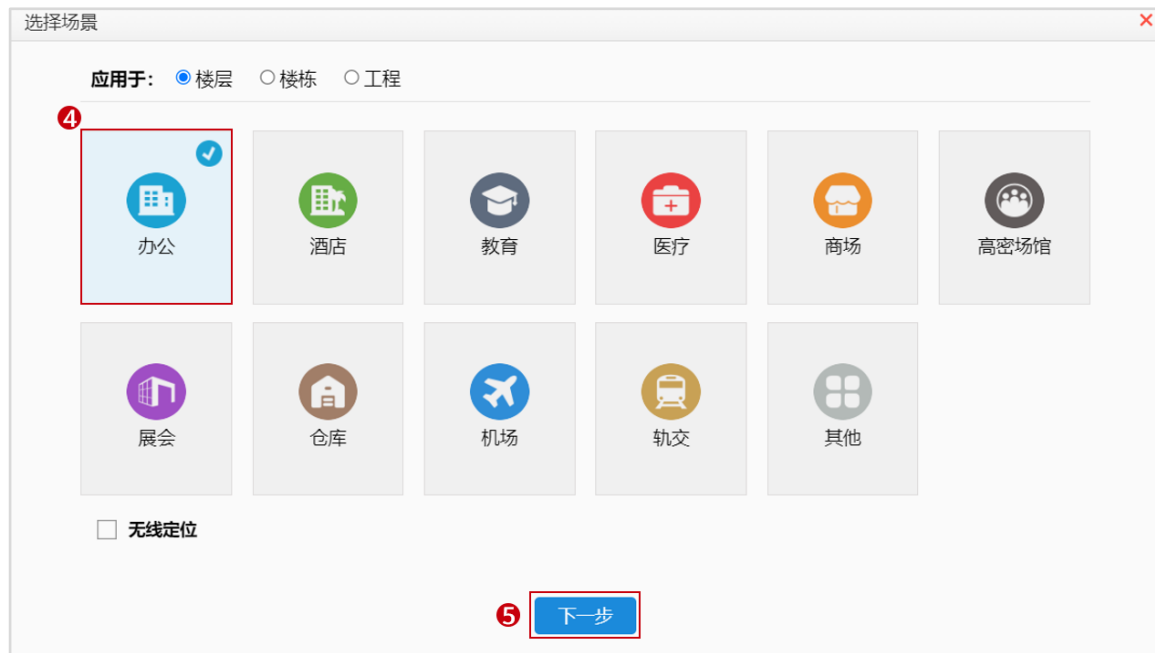
* 我已阅读并同意《法律声明》

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。

确定 取消

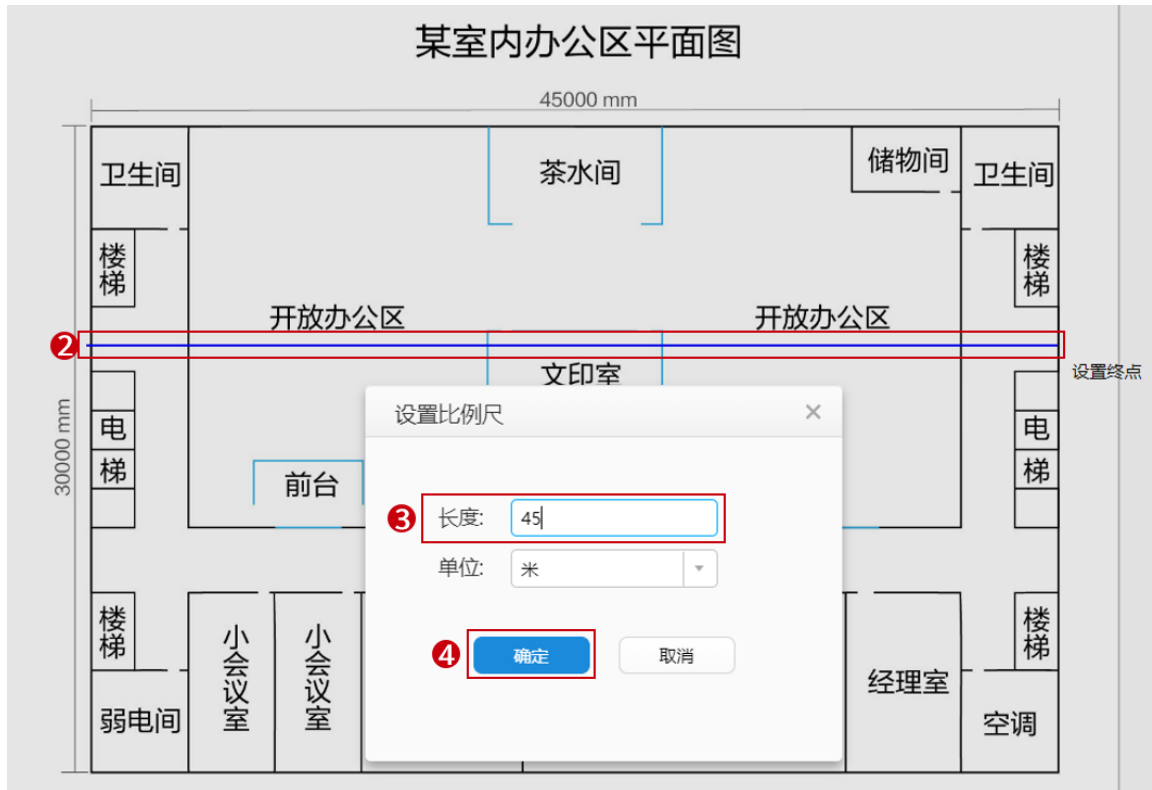
步骤 5 环境设置

根据客户需求收集 checklist 表和工勘信息进行环境及区域设置。

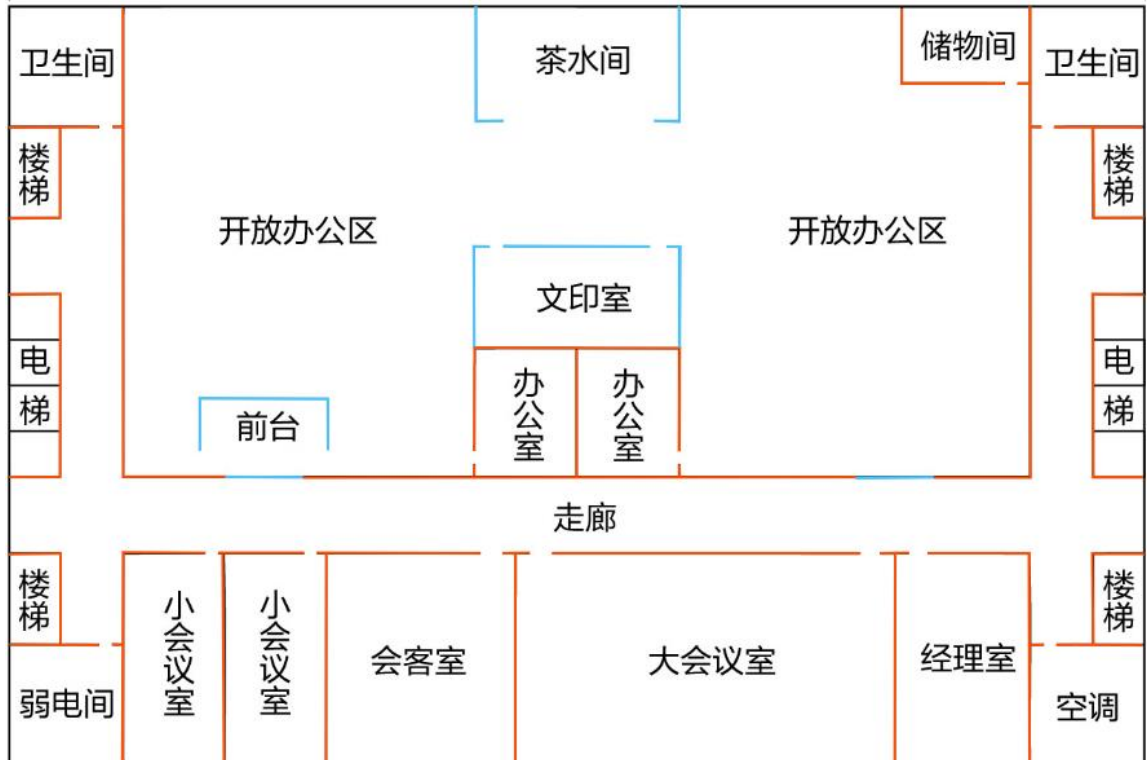
#设置比例尺。



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。

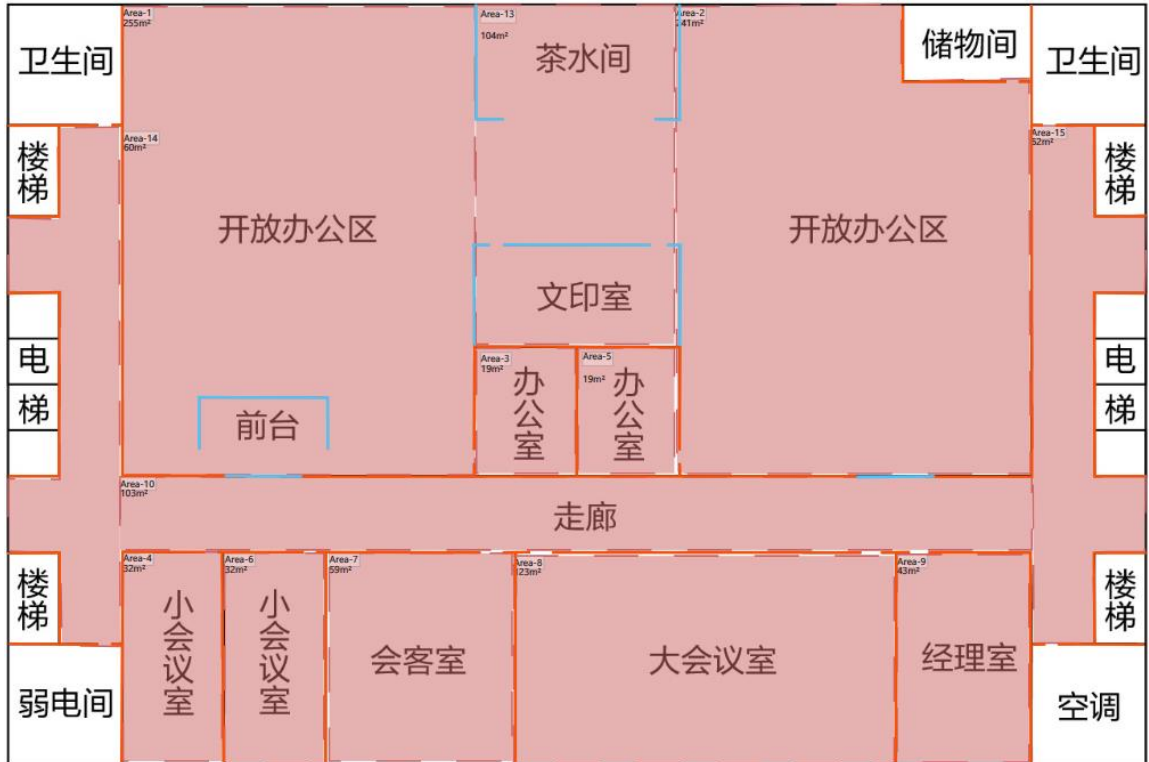


绘制障碍物，图纸边框使用绝缘边界绘制，室内墙体用 240 mm 加厚砖墙绘制，茶水间、前台和文印室使用 12 mm 加厚玻璃绘制，最终效果如下所示。



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

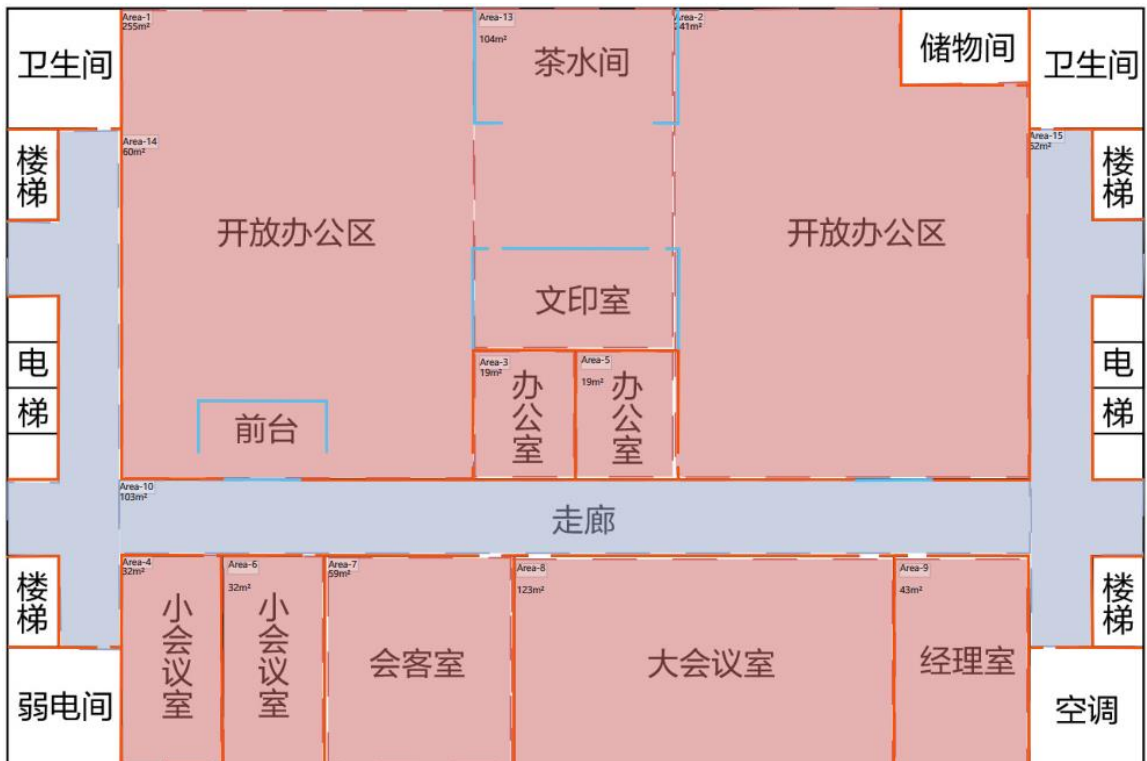
并发率(%):

终端情况

总带宽需求 40Mbps * 30%

[删除](#)

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。

自动布放配置

区域选择 AP选型 信道设置 功率设置

保留现有AP位置

场景推荐 最近使用

AirEngine6761-21 AirEngine5761-21 AirEngine5762-12 AirEngine5760-51

选择其他AP款型

当前仅支持内置全向AP布放

上一步 下一步

设置信道参数。

自动布放配置

区域选择 AP选型 信道设置 功率设置

信道计算 (每100AP信道计算的时间约为40秒)

2.4G 5G

选择信道计算方式

1/6/11信道

1/5/9/13信道

HT20

36 40 44 48 52*

56* 60* 64* 149 153

157 161 165

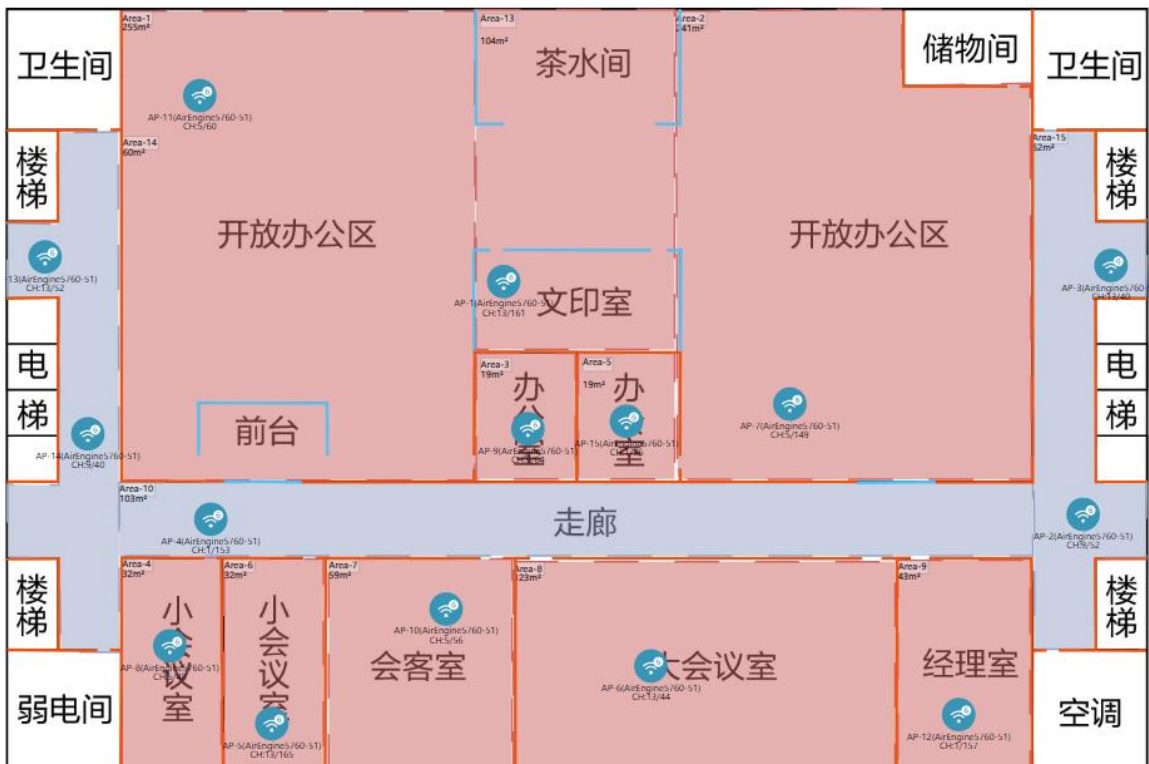
标注*的信道可能为雷达信道，请尽量避免。当前国家或地区，室内AP和室外AP所适用的信道不同，请正确选择信道

上一步 下一步

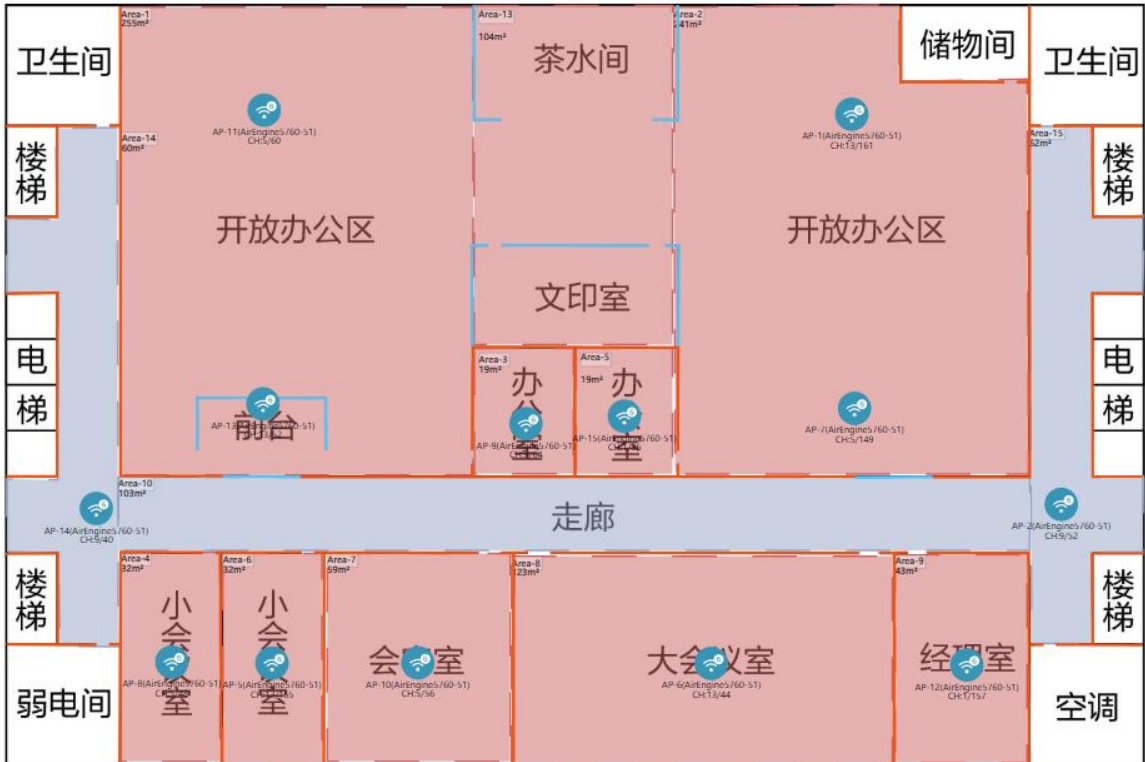
设置功率。



自动布放后，效果如下所示。

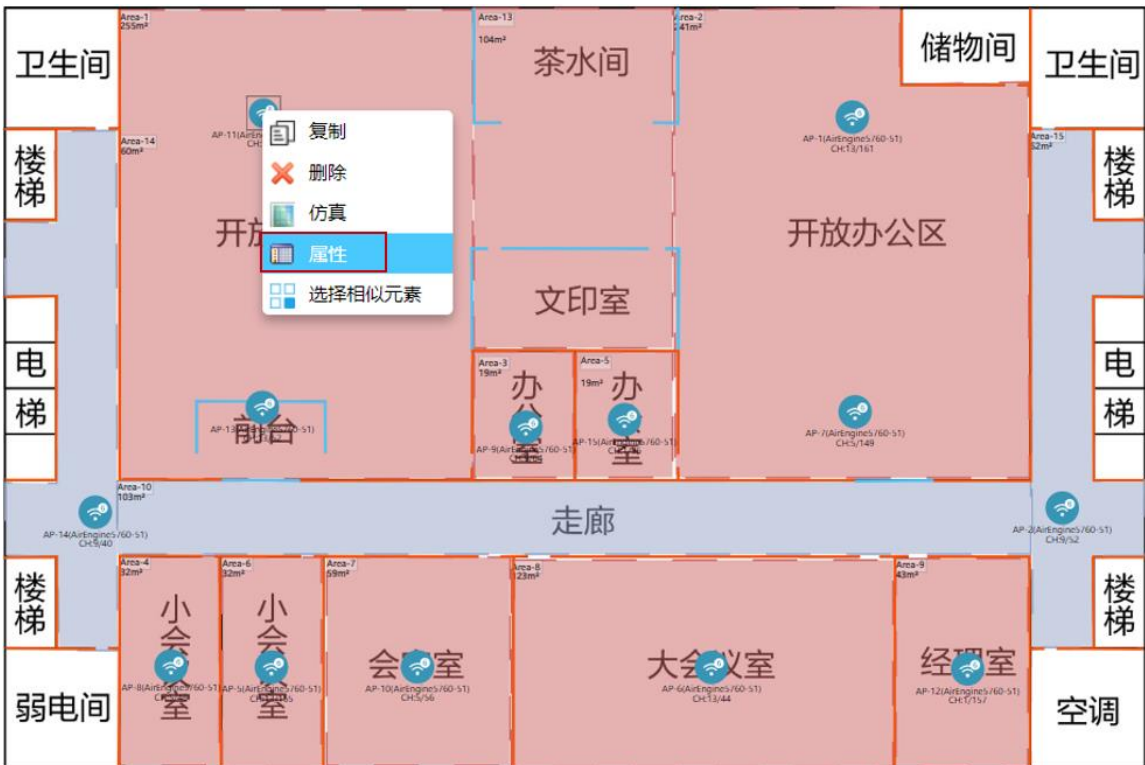


手动调整 AP 数量和位置后，最终效果如下所示。

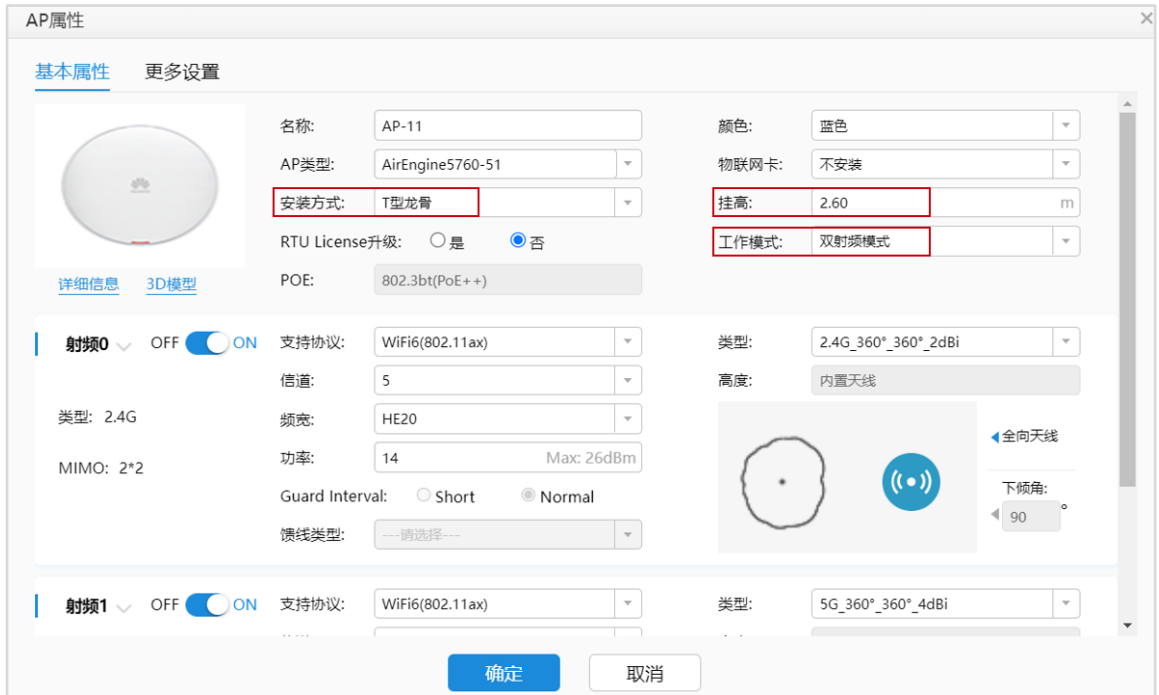


AP 参数调整。

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。

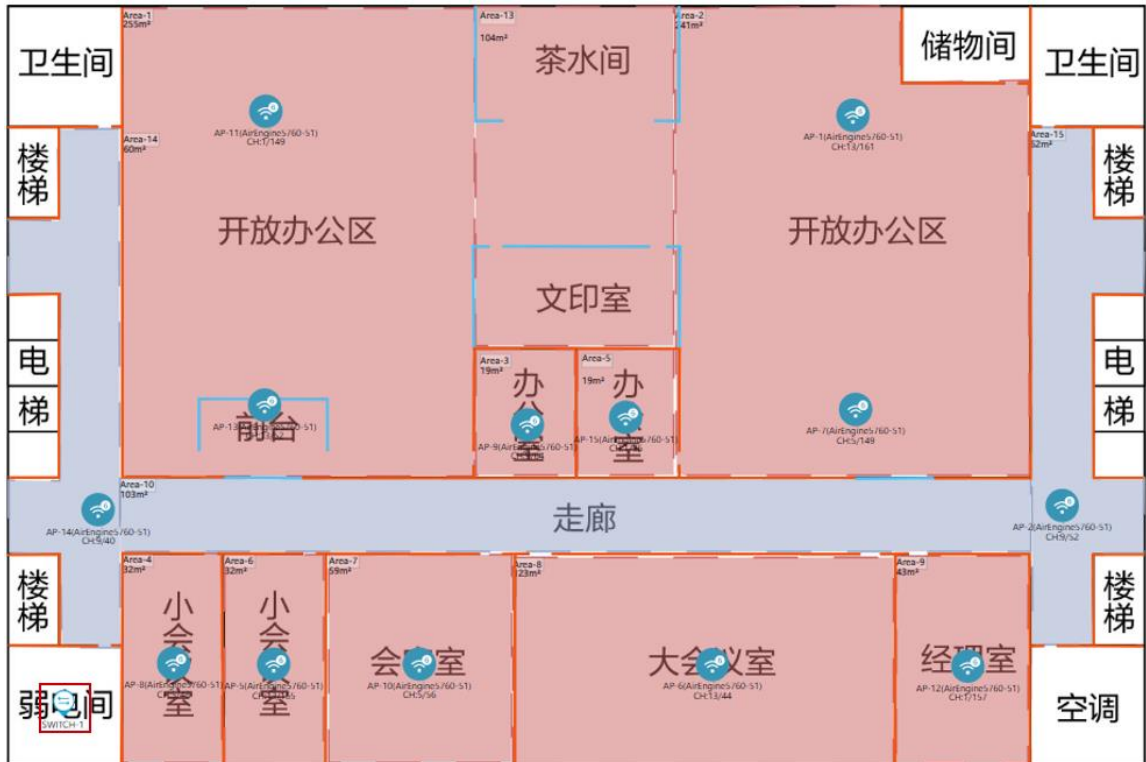


步骤 8 交换机摆放

选择交换机型号，本项目使用 S5731-S24P4X 交换机。

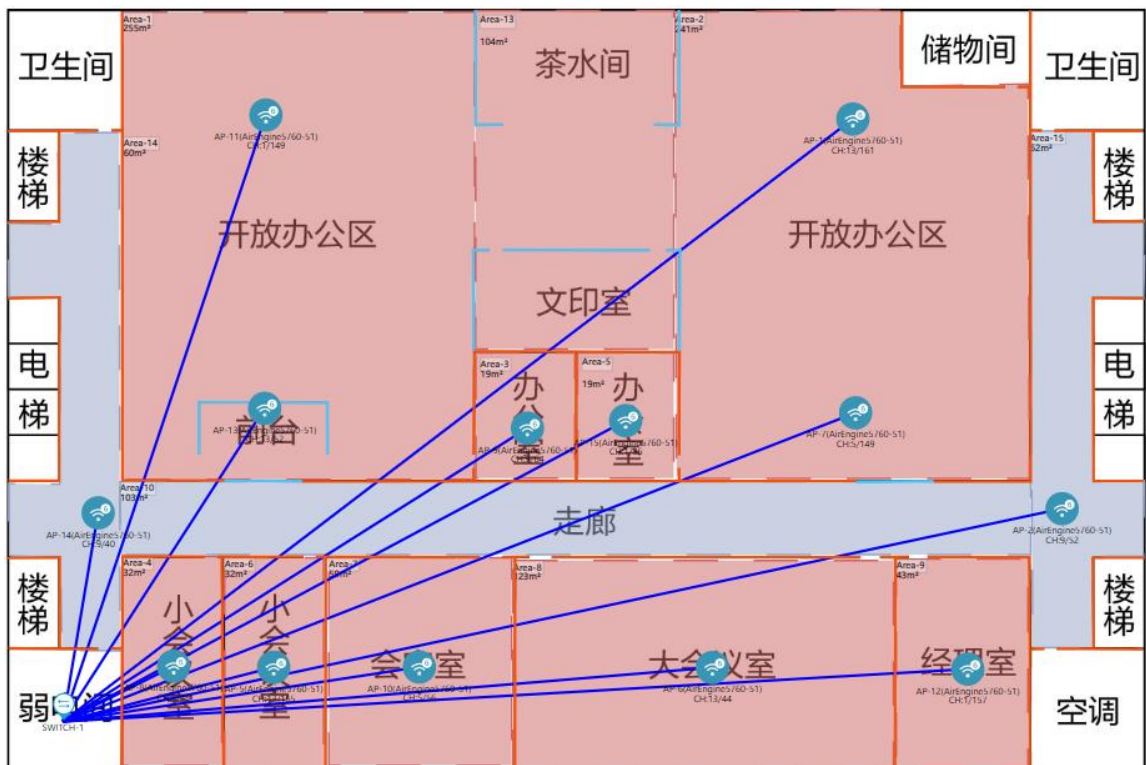


直接在左下角弱电间部署交换机即可。



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。

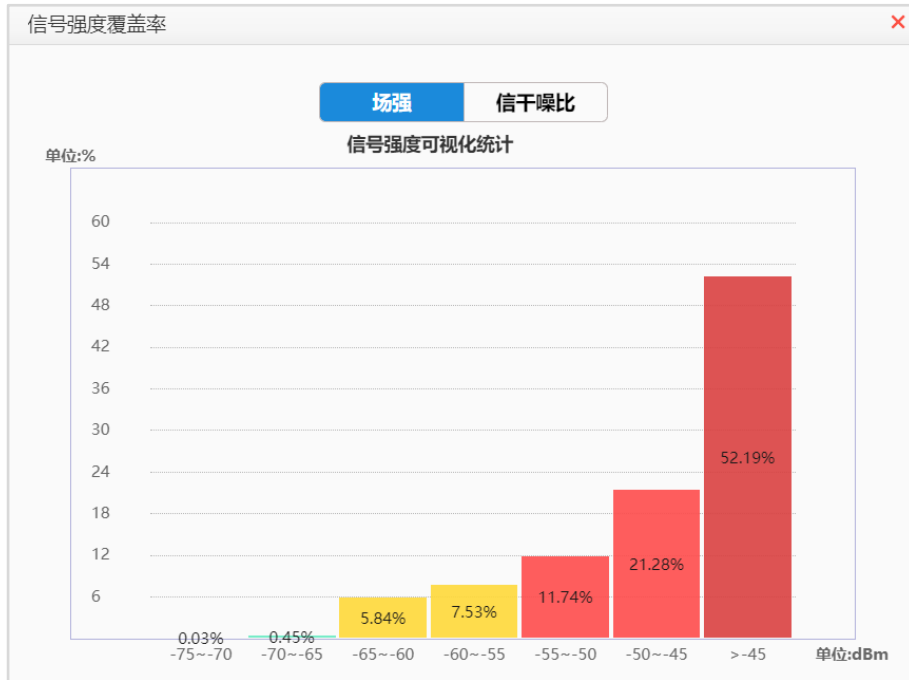


本项目只需关注走廊的信号覆盖情况。



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 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	<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	<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	<input checked="" type="checkbox"/> 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。 <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	<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	<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。 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

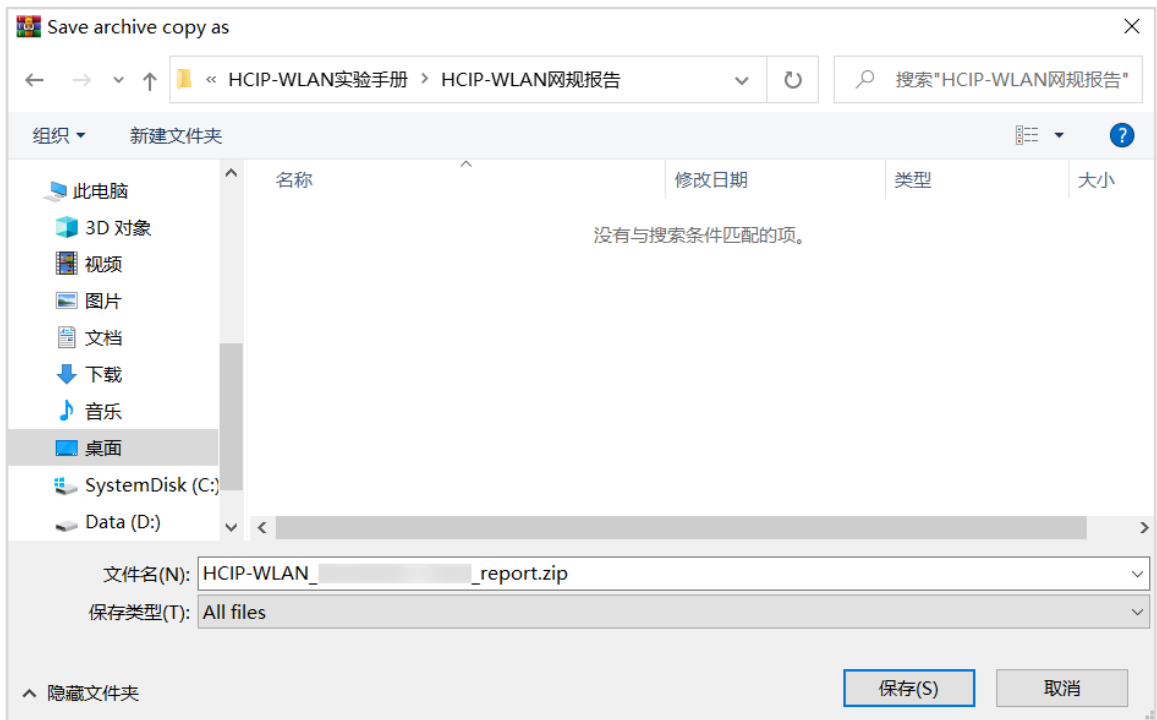
环境设置	<ul style="list-style-type: none"> ● 障碍物设置: 检查是否有图纸 (所有场景, 室内室外GIS等) 没有绘制障碍物。 ✓ ● 障碍物类型: 检查是否有图纸 (所有场景, 室内室外GIS等) 只绘制了一种障碍物。 ✓
设备布放	● AP布放过近: 检查AP间距, 如果有小于8m (26.25英尺), 并且AP间没有障碍物。 ✓
AP设置	<ul style="list-style-type: none"> ● 功率调优: 以楼层/室外区域维度查询AP功率是否均为默认功率。 ✓ ● 信道设置: 以楼层/室外区域维度查询AP信道是否均为默认信道。 ✓
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。 ✓ 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。

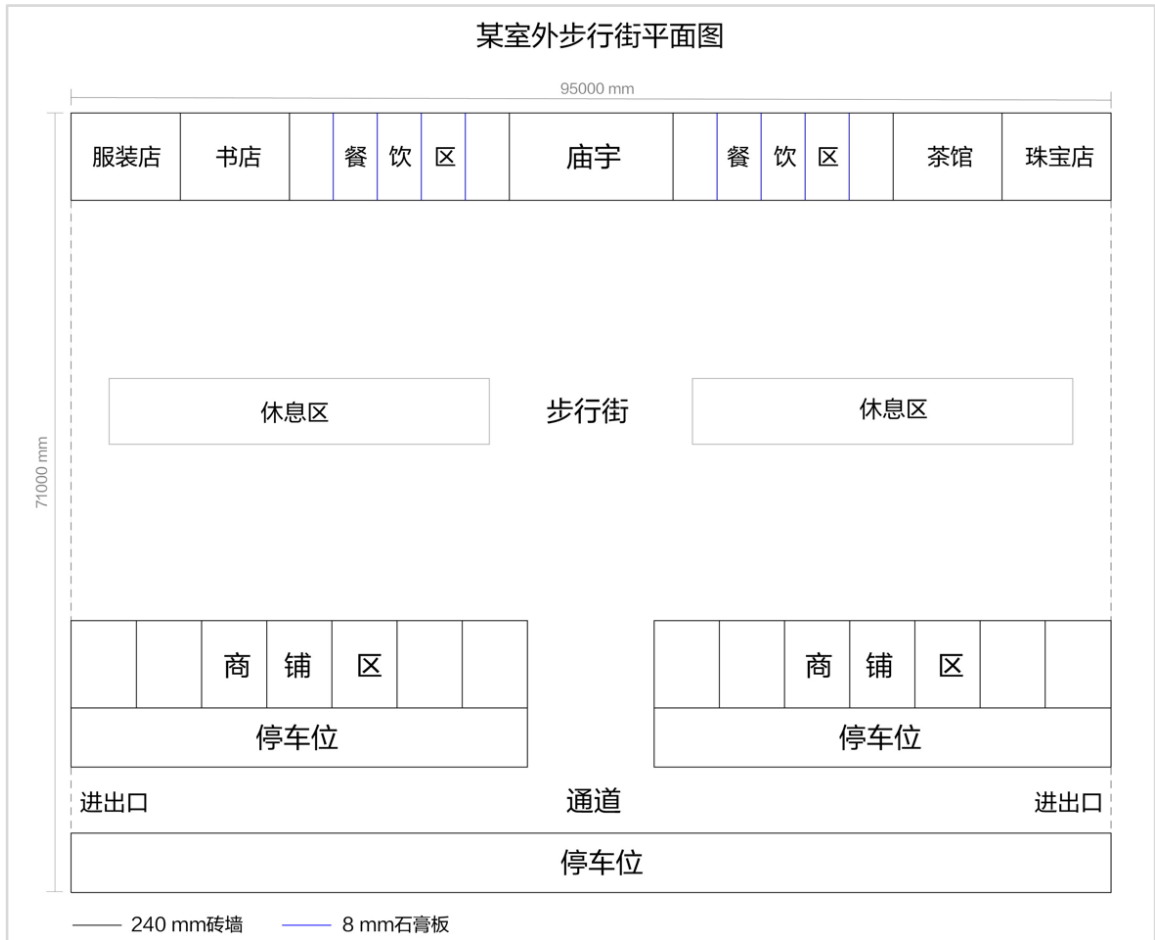


图10-1 WLAN 室外（步行街）网规建筑图纸

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：

步行街高峰期为 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。

— 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

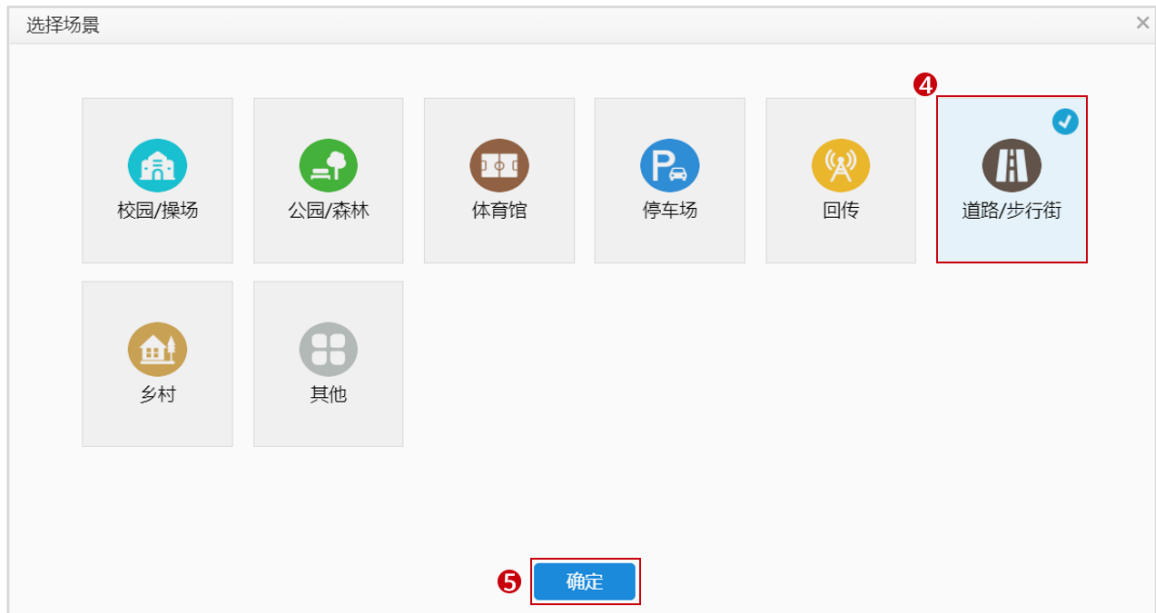
* 我已阅读并同意《法律声明》

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: HCIP-WLAN室外

* 选择场景: 道路/步行街 更改

室外类型: 平面图纸

楼层地图: 6 选择文件 HCI...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 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。



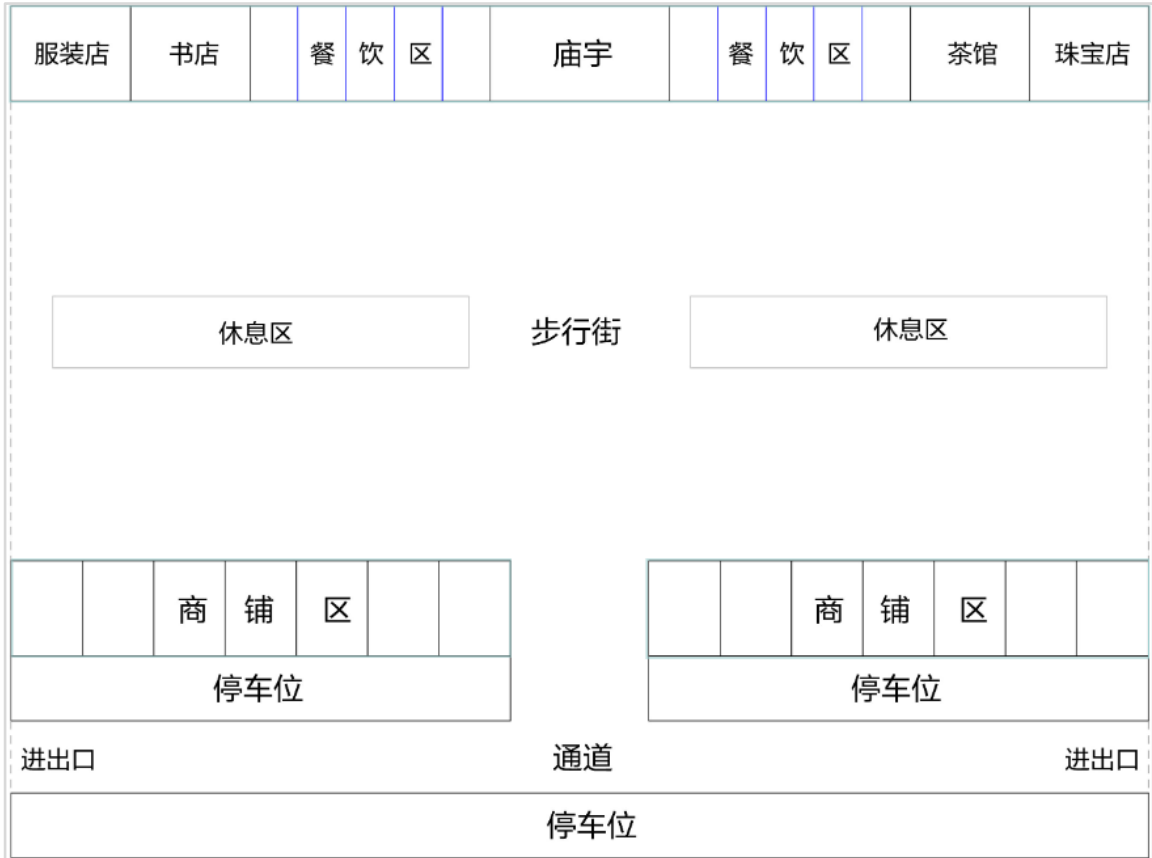
图纸宽度为 95 米，在图纸上选择任意位置，水平从左到右拉直设置比例尺长度为 95 米。



框选楼栋区域，设置障碍物高度。



环境设置后，效果如下所示。



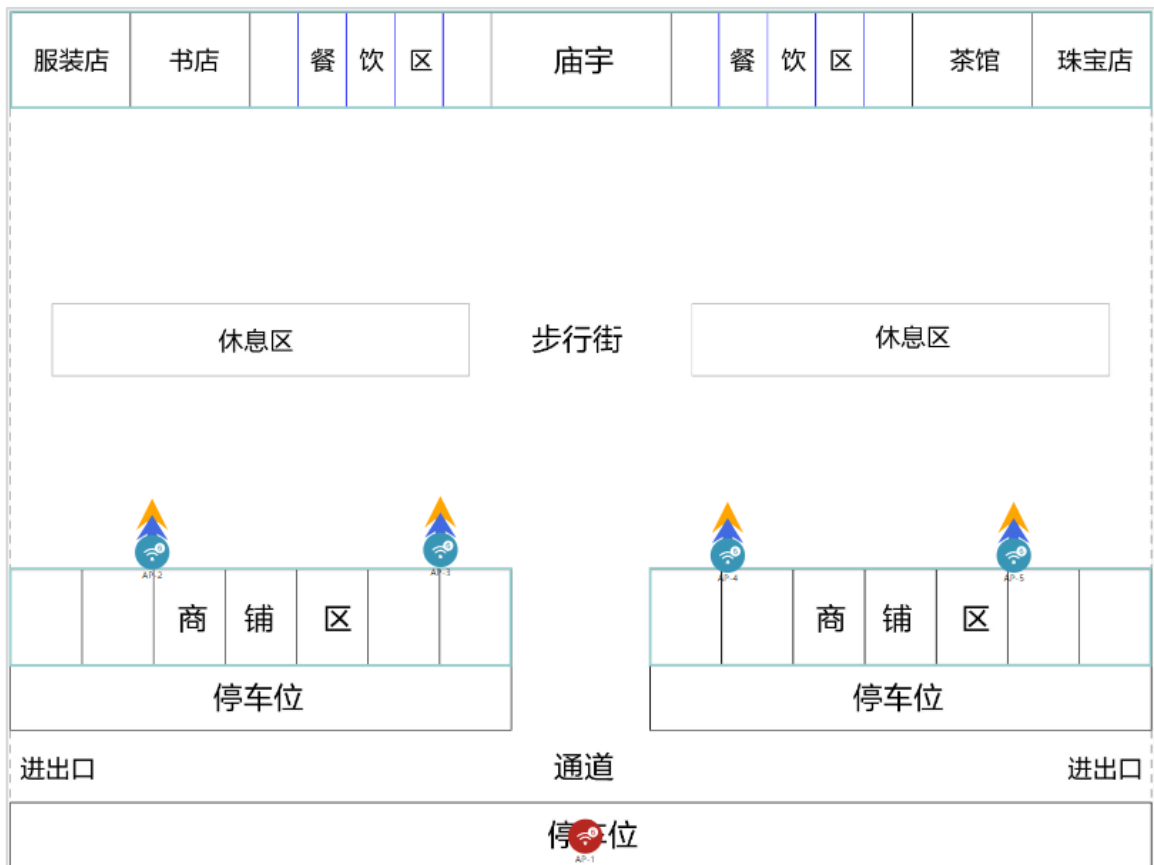
步骤 6 AP 布放，调整 AP 参数

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。

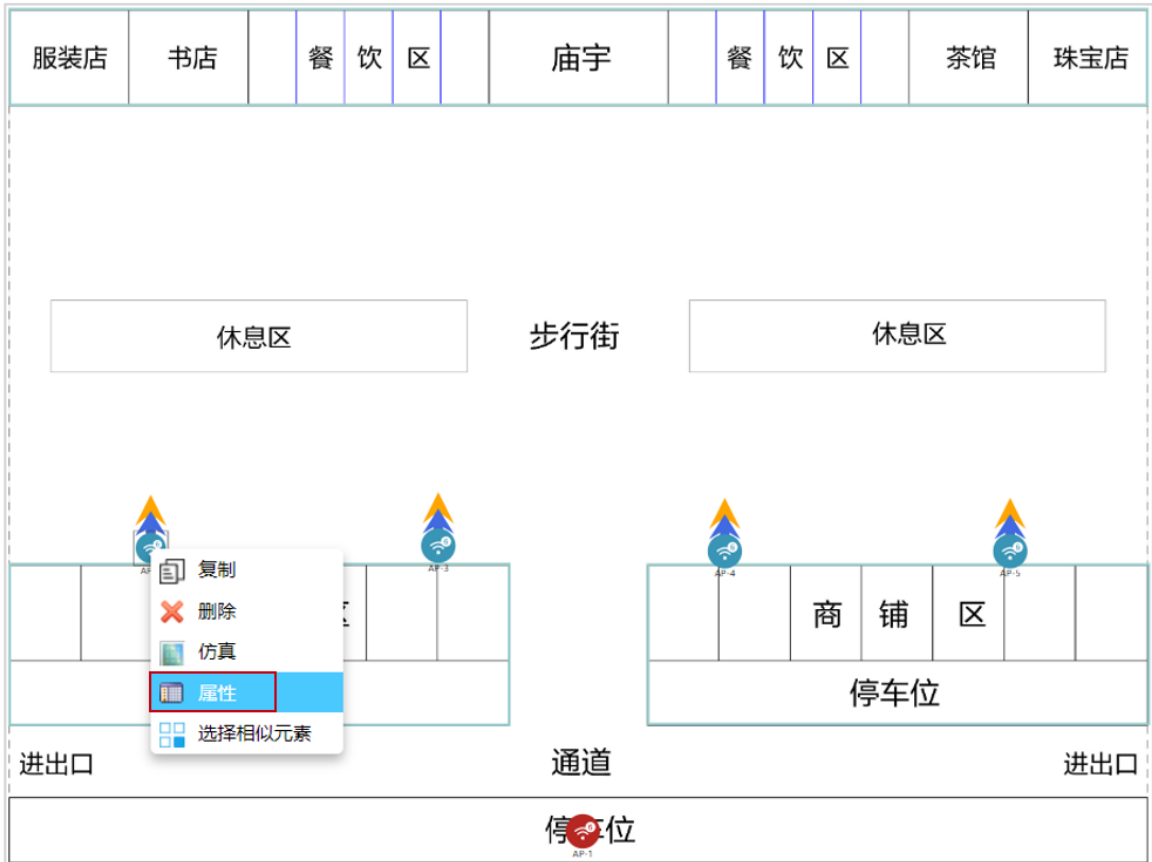


本项目壁挂 AP 使用 AirEngine5761R-11，抱杆 AP 使用 AirEngine5761R-11E，手动布放后效果如下。



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°

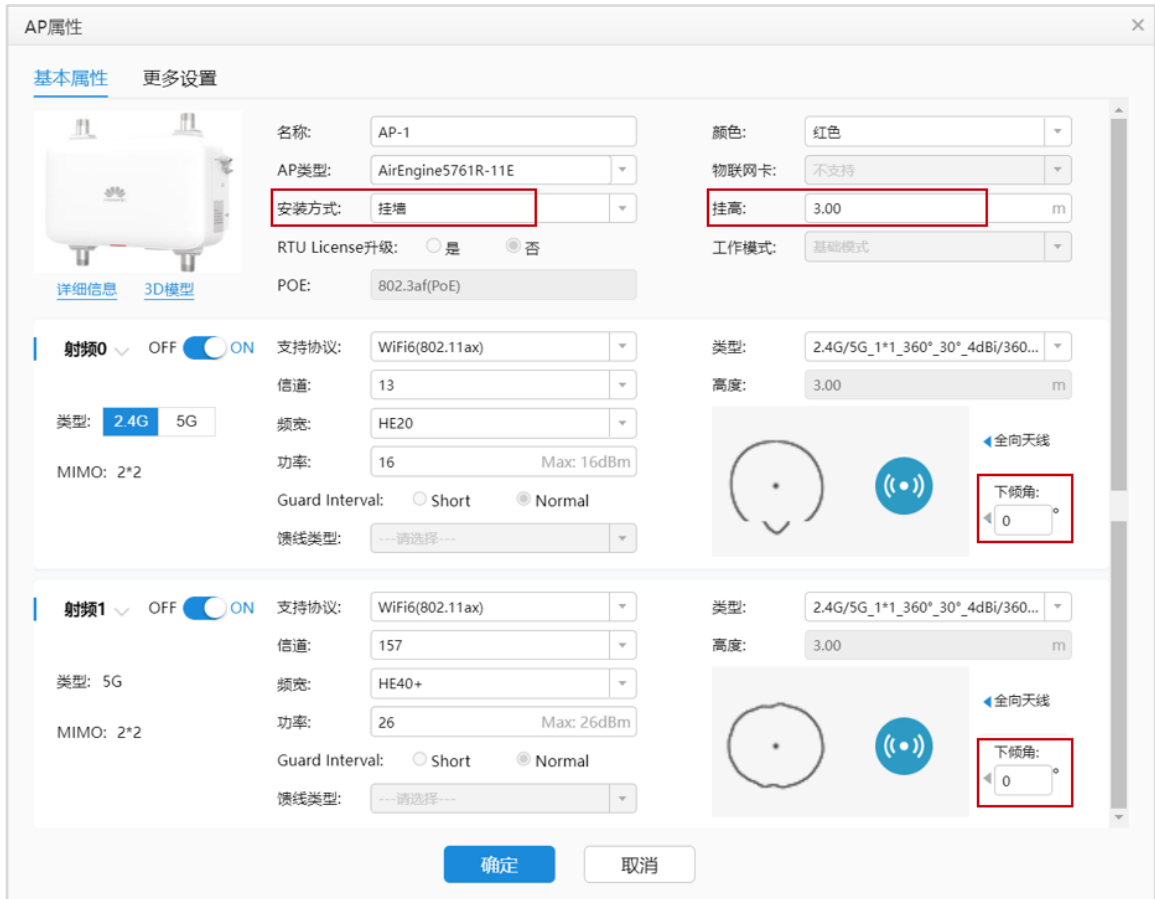
MIMO: 2*2 功率: 23 Max: 23dBm 下倾角: 15°

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。



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。

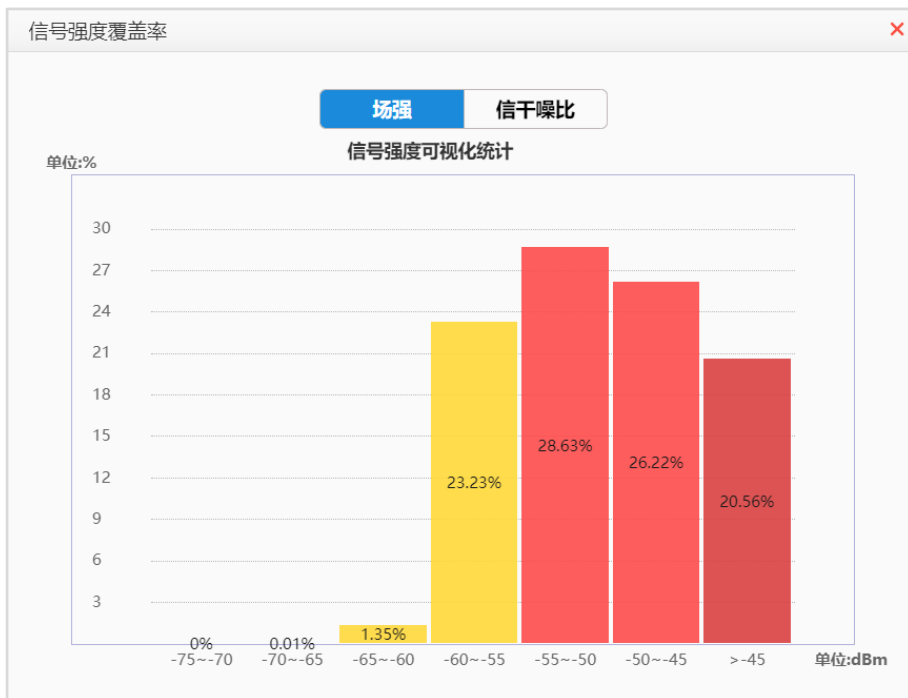
将仿真图示意中的信号强度调整为-70 dBm 即可。



本项目只需关注停车场的信号覆盖情况。



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 heatmap options. Below this is the 'Automatic Inspection' (网规自动检视) section, which lists several inspection items with checkboxes:

- 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**:
 - 定位AP间距是否满足小于等于15米。
 - 定位AP之间是否构成等三角形。
 - 定位AP与障碍物间距是否满足大于等于2米。
 - 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: <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">1.定位AP间距是否满足小于等于15米。</td> <td style="width: 50%;">2.定位AP之间是否构成等三角形形状。</td> </tr> <tr> <td>3.定位AP与障碍物间距是否满足大于等于2米。</td> <td>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...</td> </tr> </table> ✓ 	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...
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
导出报告
3

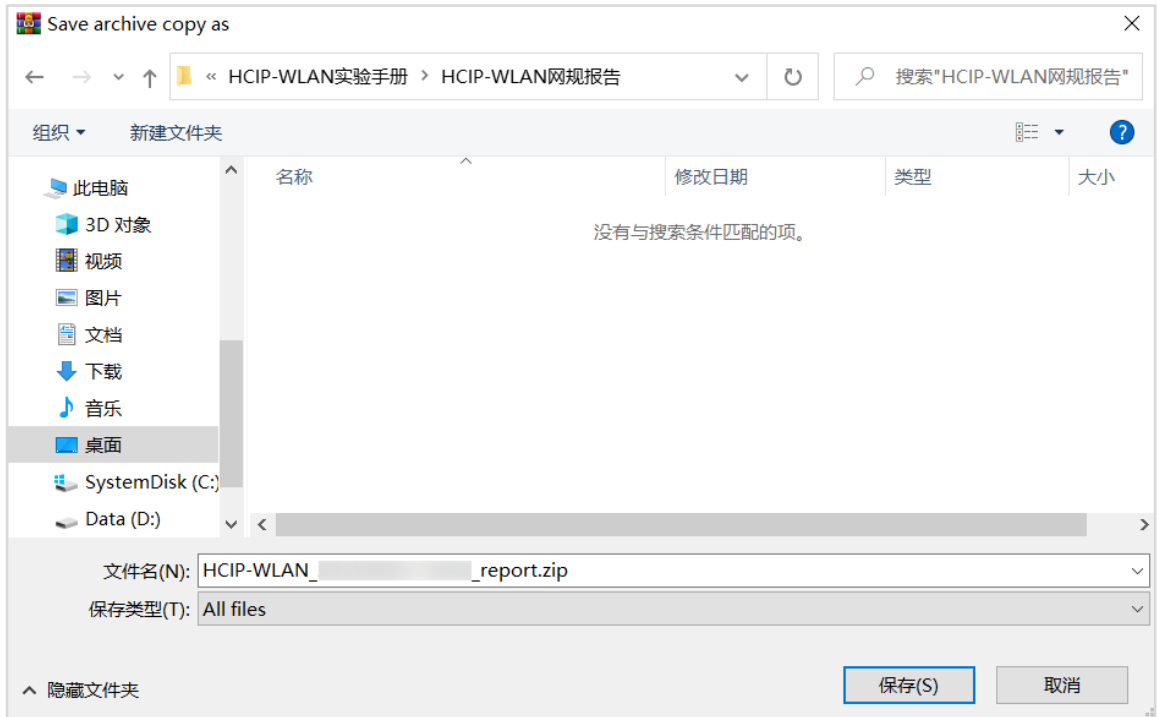
导出报告。

导出报告/导出报告计算中... 35%

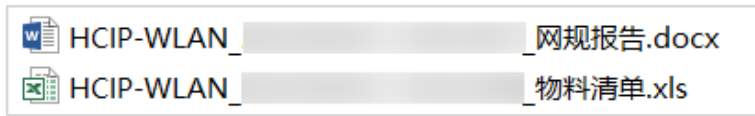


00:00:02 预计总耗时1分钟

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

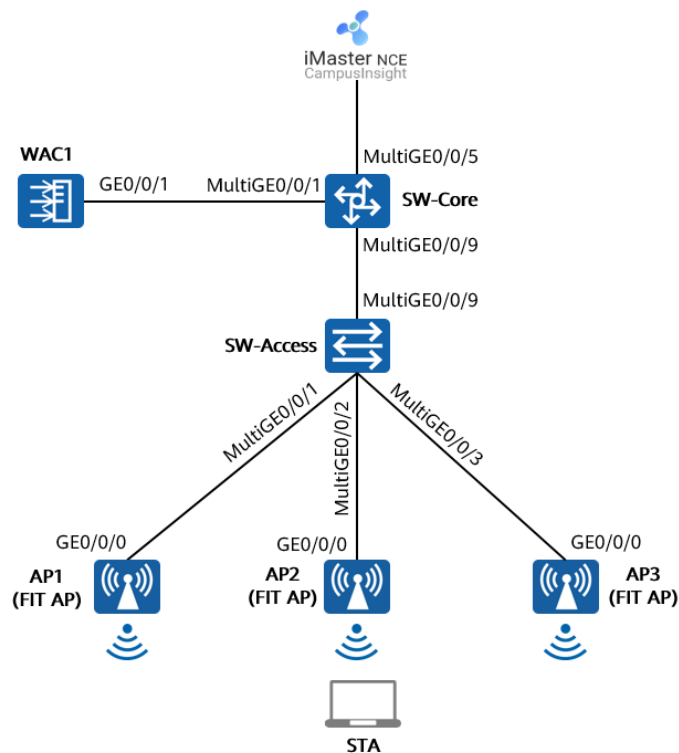


图11-1 CampusInsight 智能运维实验拓扑图

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 CampusInsight 相关网络，确保网络互通。
- 5.配置 WLAN 业务参数，实现 STA 接入。
- 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 配置基础网络互通、AP 上线、无线业务

此配置步骤请参考 1.2.2 章节（配置步骤）中的步骤 1~步骤 5，此处不再赘述。

步骤 2 配置 CampusInsight 与 WAC1 之间网络互通

CampusInsight 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
```

配置 WAC1 的默认路由，下一跳地址指向 SW-Core 设备。

```
[WAC1] ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
```

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，建议配置安全的 SNMPv3 协议。

```
[WAC1] mgmt isolate disable
Warning: Disabling management plane isolation may bring security risks. Are you sure you want to
continue ? [y/n]: y
[WAC1] snmp-agent sys-info version v3
[WAC1] snmp-agent mib-view HCIP-test include iso
[WAC1] snmp-agent group v3 test-group privacy write-view HCIP-test notify-view HCIP-test
[WAC1] snmp-agent usm-user version v3 test-user group test-group
[WAC1] snmp-agent usm-user version v3 test-user authentication-mode sha2-256
Please configure the authentication password (<8-64>)
Enter Password: Huawei@123
Confirm password: Huawei@123
[WAC1] snmp-agent usm-user version v3 test-user privacy-mode aes256
Please configure the privacy password (<8-64>)
Enter Password: Huawei@456
Confirm password: Huawei@456
```

此处 SNMP 协议的用户名为 test-user，认证密码为 Huawei@123，加密密码为 Huawei@456，需与 CampusInsight 侧配置一致。

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。

```
[WAC1] ssh client first-time enable
```

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。

```
[WAC1] lldp enable
[WAC1] wlan
[WAC1-wlan-view] ap-system-profile name default
[WAC1-wlan-ap-system-prof-default] lldp report enable
[WAC1-wlan-ap-system-prof-default] quit
```

步骤 6 配置日志数据上报

设备日志上报功能默认支持 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

```
[WAC1] undo access-user syslog-restrain enable
[WAC1] wmi-server
[WAC1-wmi-server] server ip-address 172.21.39.99 port 27371
[WAC1-wmi-server] collect-item log-data interval 60
[WAC1-wmi-server] log module mid ff760000
[WAC1-wmi-server] log module mid ff5f0000
[WAC1-wmi-server] log module mid ff630000
[WAC1-wmi-server] log module mid fff30000
[WAC1-wmi-server] log module mid ff620000
[WAC1-wmi-server] log module mid ff050000
[WAC1-wmi-server] log module mid d0410000
[WAC1-wmi-server] log module mid ff5a0000
[WAC1-wmi-server] log module mid ff8c0000
[WAC1-wmi-server] log module mid ff5d0000
[WAC1-wmi-server] quit
```

配置 AP 设备的 HTTP/2 协议通道。

```
[WAC1] wlan
[WAC1-wlan-view] wmi-server name test
[WAC1-wlan-wmi-server-prof-test] server ip-address 172.21.39.99 port 27371
[WAC1-wlan-wmi-server-prof-test] collect-item log-data interval 60
[WAC1-wlan-wmi-server-prof-test] ap log module mid FF600000
[WAC1-wlan-wmi-server-prof-test] ap log module mid D0410000
[WAC1-wlan-wmi-server-prof-test] ap log module mid FF620000
[WAC1-wlan-wmi-server-prof-test] ap log module mid FFED0000
[WAC1-wlan-wmi-server-prof-test] ap log module mid FFEF0000
[WAC1-wlan-wmi-server-prof-test] ap log module mid FFF30000
[WAC1-wlan-wmi-server-prof-test] ap log module mid FF2B0000
[WAC1-wlan-wmi-server-prof-test] ap log module mid FE011004
[WAC1-wlan-wmi-server-prof-test] quit
[WAC1-wlan-view] ap-system-profile name default
[WAC1-wlan-ap-system-prof-default] wmi-server test index 2
[WAC1-wlan-ap-system-prof-default] quit
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] ap-system-profile default
[WAC1-wlan-ap-group-ap-group1] quit
```

步骤 7 配置 WLAN 业务性能指标数据上报

将设备上的 WLAN 业务性能指标数据主动上报至 CampusInsight 进行分析。

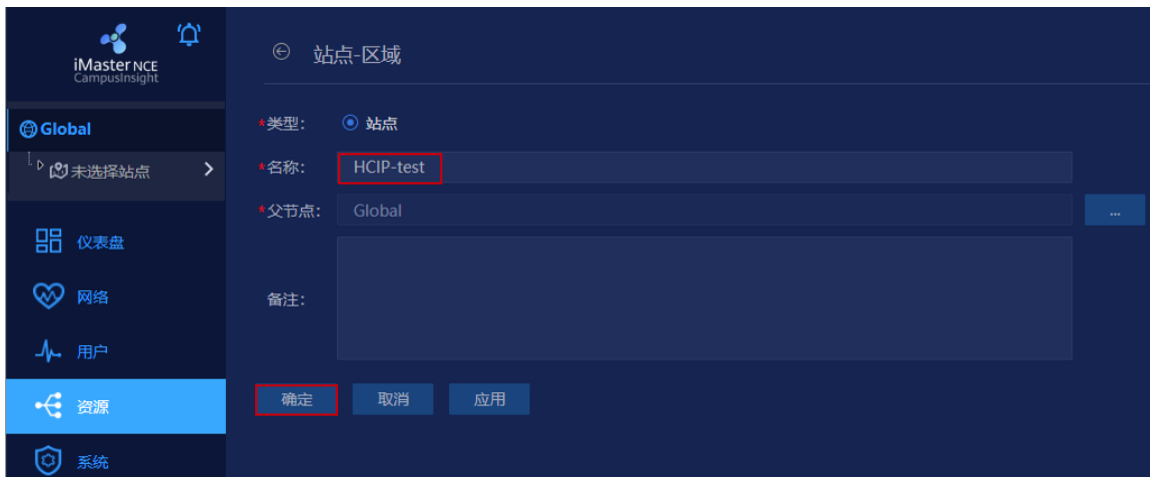
```
[WAC1] pki realm default
[WAC1-pki-realm-default] certificate-check none
[WAC1-pki-realm-default] quit
[WAC1] wmi-server
[WAC1-wmi-server] collect-item device-data interval 60
[WAC1-wmi-server] collect-item interface-data interval 60
[WAC1-wmi-server] collect-item cpcar-data interval 60
[WAC1-wmi-server] collect-item security-data interval 60
[WAC1-wmi-server] quit
[WAC1] wlan
[WAC1-wlan-view] wmi-server name test
[WAC1-wlan-wmi-server-prof-test] report-interval 60
[WAC1-wlan-wmi-server-prof-test] collect-item device-data interval 60
[WAC1-wlan-wmi-server-prof-test] collect-item radio-data interval 60
[WAC1-wlan-wmi-server-prof-test] collect-item ssid-data interval 60
[WAC1-wlan-wmi-server-prof-test] collect-item terminal-data interval 60
[WAC1-wlan-wmi-server-prof-test] collect-item non-wifi-data interval 60
[WAC1-wlan-wmi-server-prof-test] quit
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] radio 0
[WAC1-wlan-group-radio-ap-group1/0] wids device detect enable
[WAC1-wlan-group-radio-ap-group1/0] spectrum-analysis enable
[WAC1-wlan-group-radio-ap-group1/0] channel-monitor enable
[WAC1-wlan-ap-group-ap-group1] radio 1
[WAC1-wlan-group-radio-ap-group1/1] wids device detect enable
[WAC1-wlan-group-radio-ap-group1/1] spectrum-analysis enable
[WAC1-wlan-group-radio-ap-group1/1] channel-monitor enable
[WAC1-wlan-group-radio-ap-group1/1] quit
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] ap-system-profile default
[WAC1-wlan-ap-group-ap-group1] quit
```

步骤 8 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”。



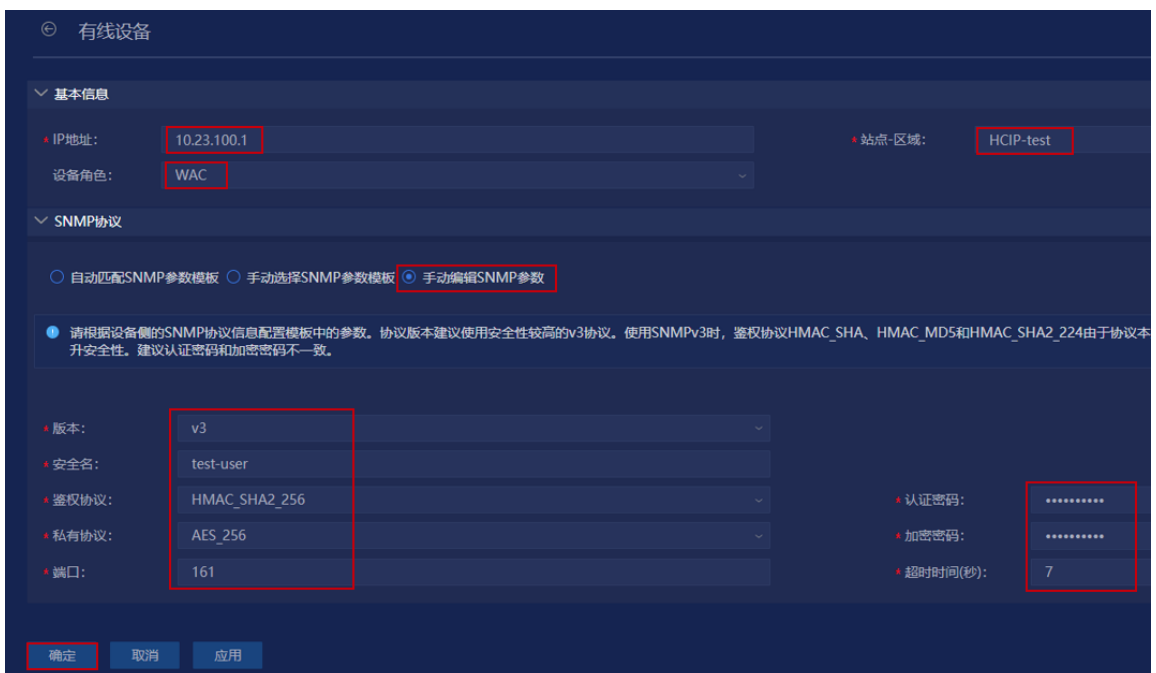
选择“资源 > 有线设备”，点击“增加设备”，选择“单个添加”。



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”。

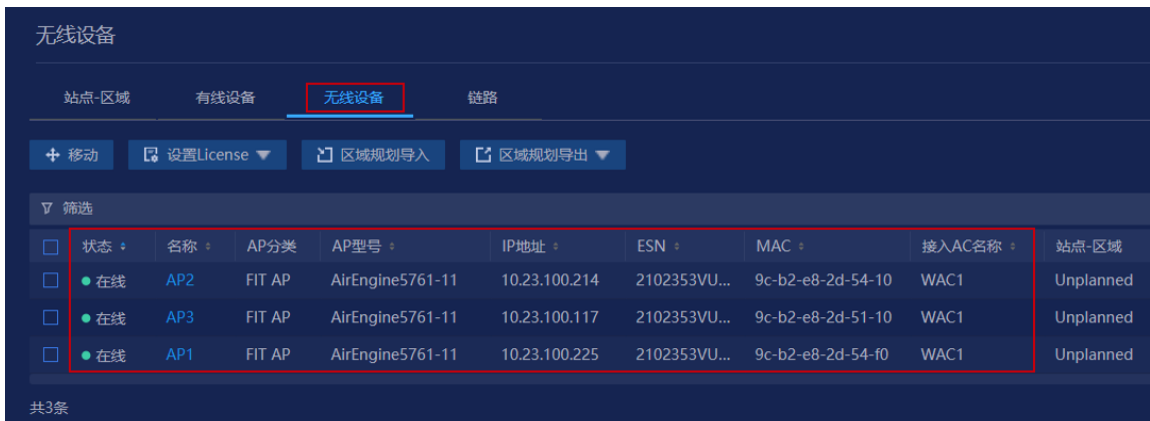
此处的安全名需要与 WAC1 上配置的 SNMP 用户名一致，其他参数也需要一致。



检查有线设备上线状态，发现 WAC1 已经在线。



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。



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”。



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 9 配置 CampusInsight 运维功能

查看整网状态。

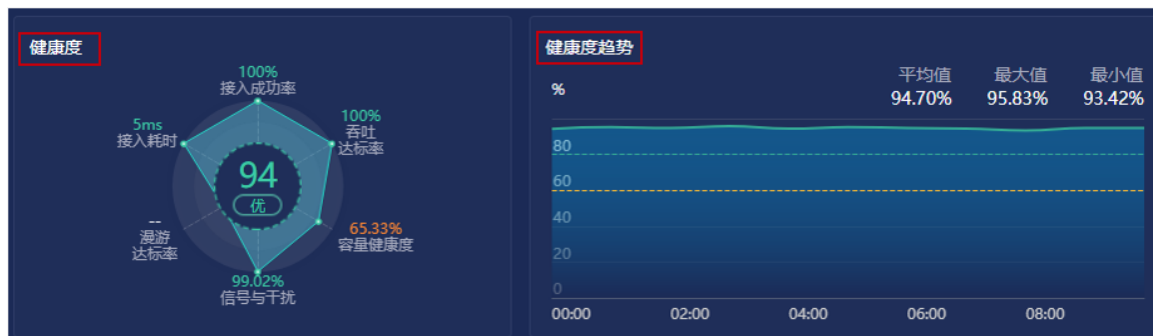
选择“仪表盘 > 概览”，可以查看“HCIP-test”站点的资源状态、健康度、用户数、流量、AP 速率/流量等关键信息，使管理员可以了解网络的整体运行情况。





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。

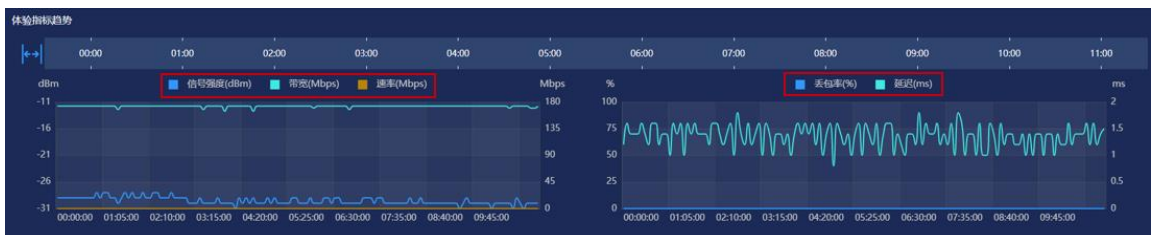
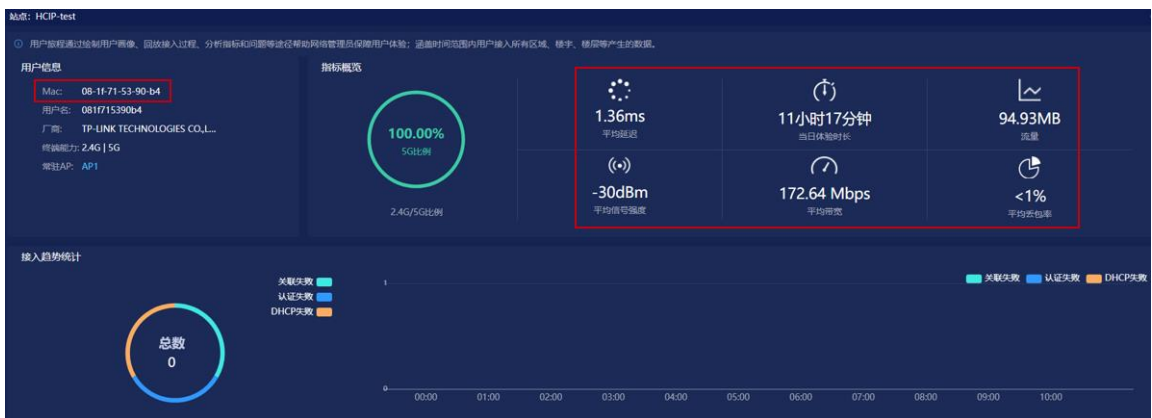
2个结果, 耗时: 260ms

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

在 WAC1 上执行 display snmp-agent mib-view 命令，查看 SNMP 的 MIB 信息。

```
[WAC1] display snmp-agent mib-view HCIP-test
View name: HCIP-test
MIB subtree: iso
Subtree mask:
Storage type: nonVolatile
View type: included
View status: active
```

在 WAC1 上执行 display snmp-agent group 命令，查看 SNMP 的组信息。

```
[WAC1] display snmp-agent group
Group name: test-group
Security model: v3 AuthPriv
Readview: ViewDefault
Writeview: HCIP-test
Notifyview: HCIP-test
Storage type: nonVolatile

Total number is 1
```

在 WAC1 上执行 display snmp-agent usm-user 命令，查看 SNMP 的用户信息。

```
[WAC1] display snmp-agent usm-user
User name: test-user
Engine ID: 800007DB039CB2E8B5A224
Group name: test-group
Authentication mode: sha2-256, Privacy mode: aes256
Storage type: nonVolatile
User status: active

Total number is 1
```

11.3.2 查看 WAC1 的 VAP 信息

在 WAC1 上执行 display vap all 命令，查看 VAP 信息。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID          Status  Auth type      STA  SSID
-----
0     AP1      0    1    9CB2-E82D-54F0 ON      WPA/WPA2-PSK  0    wlan-net
0     AP1      1    1    9CB2-E82D-5500 ON      WPA/WPA2-PSK  1    wlan-net
1     AP2      0    1    9CB2-E82D-5410 ON      WPA/WPA2-PSK  0    wlan-net
```

1	AP2	1	1	9CB2-E82D-5420 ON	WPA/WPA2-PSK	0	wlan-net
2	AP3	0	1	9CB2-E82D-5110 ON	WPA/WPA2-PSK	0	wlan-net
2	AP3	1	1	9CB2-E82D-5120 ON	WPA/WPA2-PSK	1	wlan-net

Total: 6							

11.4 配置参考

11.4.1 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
#
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 169.254.1.1 255.255.255.0
#
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 %^%#D~DQT_u@3&)9hQ=w|Y)lqQC6U0b-A,$Qj{:_f<eH%^%#
snmp-agent usm-user version v3 test-user privacy-mode
aes256 %^%#]W!A6{&Y1Tx4&s,{ex:0Be2EE[_Pw(V$%"&zwwQC%^%#
snmp-agent
#
ssh server-source -i Vlanif100
ssh client first-time enable
sftp server enable
stelnet server enable
#
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
#
wmi-server
server ip-address 172.21.39.99 port 27371
collect-item device-data interval 60
collect-item log-data interval 60
collect-item security-data interval 60
collect-item cpcar-data interval 60
log module mid ff760000 name WEB
log module mid ff5f0000 name DOT1X
log module mid ff630000 name CM
log module mid fff30000 name WLAN
log module mid ff620000 name DHCP
log module mid ff050000 name IFPDT
log module mid d0410000 name SHELL
log module mid ff5a0000 name AAA
log module mid ff8c0000 name ENTITYTRAP
log module mid ff5d0000 name AM
#
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)|%^%#
```

```
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 device-data interval 60
  collect-item radio-data interval 60
  collect-item terminal-data interval 60
  collect-item log-data interval 60
  collect-item non-wifi-data enable
  ap log module mid FF2B0000
  ap log module mid FE011004
  ap log module mid FF600000 name PORTAL
  ap log module mid D0410000 name SHELL
  ap log module mid FF620000 name DHCP
  ap log module mid FFED0000 name SEA
  ap log module mid FFEF0000 name WSRV
  ap log module mid FFF30000 name WLAN
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

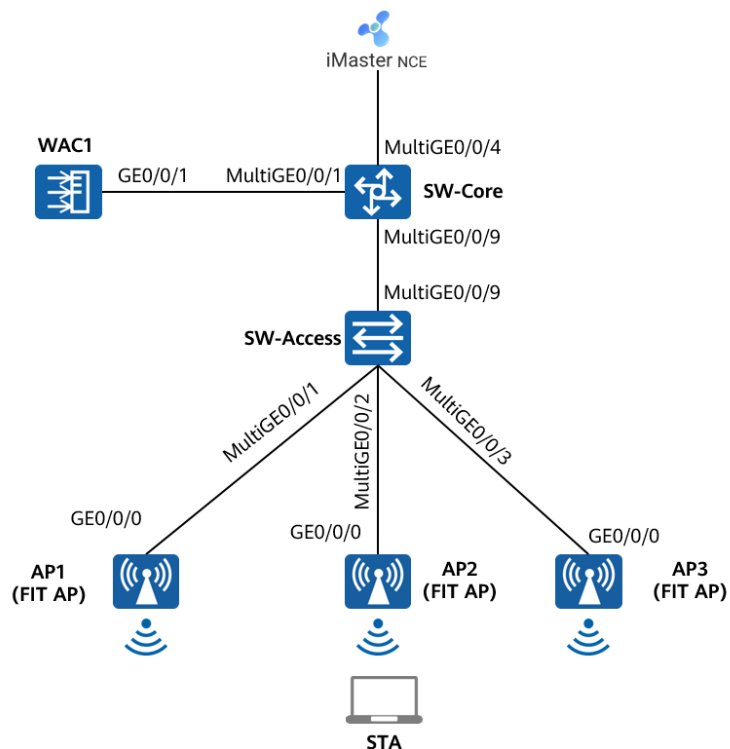


图12-1 故障排查综合实验拓扑图

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 %^%#]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
#
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 %^%#N[ePT/1o_2@zKz/>v:dTE_H%#s@Cy<{-|g:s'\&\8%^%#
```

```
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 169.254.1.1 255.255.255.0
#
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 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
```

认证服务器预配置与章节 6.2.2（配置步骤）中的步骤 7 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 上检查如下：

```
[WAC1] display ap all
Total AP information:
```

```

nor : normal [3]
ExtralInfo : Extra information
-----
ID   MAC           Name Group   IP           Type           State STA  Uptime  ExtralInfo
-----
0    9cb2-e82d-54f0 AP1  ap-group1 10.23.100.225 AirEngine5761-11 nor  0   10M:12S -
1    9cb2-e82d-5410 AP2  ap-group1 10.23.100.214 AirEngine5761-11 nor  0   9M:42S  -
2    9cb2-e82d-5110 AP3  default   10.23.100.117 AirEngine5761-11 nor  0   10M:16S -
-----
Total: 3
    
```

发现三台 AP 均已上线，但是其中 AP3 并未属于“ap-group1”组，为了确保后续 WAC1 下发至 AP 的策略统一，此处需要把 AP3 划分至正确的 AP 组中，配置如下：

```

[WAC1] wlan
[WAC1-wlan-view] ap-id 2
[WAC1-wlan-ap-2] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power
and antenna gain configurations of the radio, Whether to continue? [Y/N]: y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[WAC1-wlan-ap-2] quit
    
```

再次查看，发现三台 AP 均属于“ap-group1”组，并且已正常上线。

```

[WAC1] display ap all
Total AP information:
nor : normal [3]
ExtralInfo : Extra information
-----
ID   MAC           Name Group   IP           Type           State STA  Uptime  ExtralInfo
-----
0    9cb2-e82d-54f0 AP1  ap-group1 10.23.100.225 AirEngine5761-11 nor  0   17M:12S -
1    9cb2-e82d-5410 AP2  ap-group1 10.23.100.214 AirEngine5761-11 nor  0   16M:42S -
2    9cb2-e82d-5110 AP3  ap-group1 10.23.100.117 AirEngine5761-11 nor  0   10S    -
-----
Total: 3
    
```

由于当前无法搜索到 SSID，所以继续查看 VAP 的状态信息，如下：

```

[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID           Status  Auth type  STA  SSID
-----
-----
Total: 0
    
```

发现所有 AP 均没有关联任何 VAP 信息，通过查看 WAC1 的配置，发现 VAP 模板并未在 AP 组中引用，修改配置如下：

```

[WAC1] wlan
    
```

```
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[WAC1-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[WAC1-wlan-ap-group-ap-group1] quit
```

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。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID           Status  Auth type  STA  SSID
-----
0     AP1      0   1   9CB2-E82D-54F0 ON      Open      0     wlan-net
0     AP1      1   1   9CB2-E82D-5500 OFF     Open      0     wlan-net
1     AP2      0   1   9CB2-E82D-5410 ON      Open      0     wlan-net
1     AP2      1   1   9CB2-E82D-5420 OFF     Open      0     wlan-net
2     AP3      0   1   9CB2-E82D-5110 ON      Open      1     wlan-net
2     AP3      1   1   9CB2-E82D-5120 OFF     Open      0     wlan-net
-----
Total: 6
```

手动开启 5G 射频，配置如下：

```
[WAC1] wlan
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] radio 1
[WAC1-wlan-group-radio-ap-group1/1] undo radio disable
[WAC1-wlan-group-radio-ap-group1/1] quit
```

查看 VAP 状态信息，均已正常，如下所示：

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name  RfID WID  BSSID           Status  Auth type  STA  SSID
-----
0     AP1      0   1   9CB2-E82D-54F0 ON      Open      1     wlan-net
0     AP1      1   1   9CB2-E82D-5500 ON      Open      0     wlan-net
1     AP2      0   1   9CB2-E82D-5410 ON      Open      0     wlan-net
1     AP2      1   1   9CB2-E82D-5420 ON      Open      0     wlan-net
2     AP3      0   1   9CB2-E82D-5110 ON      Open      0     wlan-net
2     AP3      1   1   9CB2-E82D-5120 ON      Open      0     wlan-net
-----
Total: 6
```

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，在 WAC1 上手动创建 VLAN 101，配置如下：

```
[WAC1] vlan 101
[WAC1-vlan101] quit
```

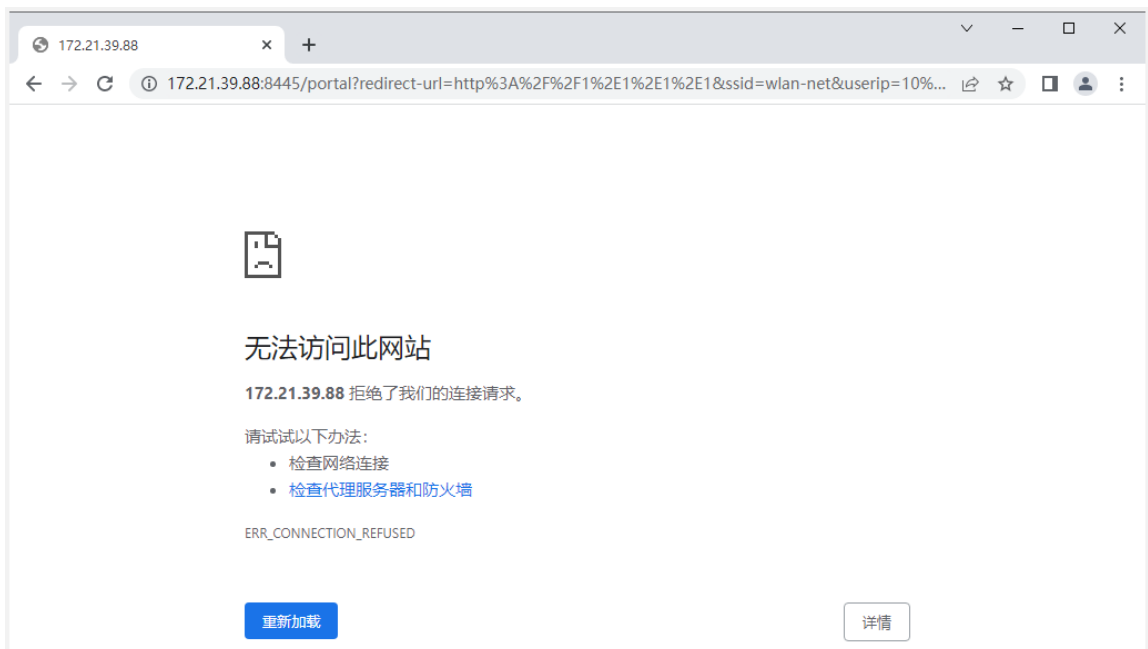
STA 断开 “wlan-net” 信号，然后重新连接，可以正常获取 IP 地址，使用 “ipconfig” 命令验证如下。

```
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，首先检查 VAP 模板是否正确引用了认证模板。VAP 下配置正常。

```
vap-profile name wlan-net
  forward-mode tunnel
  service-vlan vlan-id 101
  ssid-profile wlan-net
  security-profile wlan-net
  authentication-profile p1
```

检查认证模板是否配置正确。认证模板下未配置 Portal 接入模板。

```
authentication-profile name p1
```



```
authentication-scheme radius_huawei
accounting-scheme scheme1
radius-server radius_huawei
```

通过查询配置，WAC1 中已经预先配置 Portal 接入模板 “portal1”，在认证模板中引用 “portal1”，配置如下：

```
[WAC1] authentication-profile name p1
[WAC1-authentication-profile-p1] portal-access-profile portal1
Info: This operation may take a few minutes, please wait...
Warning: Changing the authentication profile will cause online users to go offline. Continue? [Y/N] y
Authentication profile p1 : done.
[WAC1-authentication-profile-p1] quit
```

此时发现 STA 仍然无法弹出 Portal 认证页面，查看 Portal 服务器模板的配置。Portal 服务器的地址和端口配置错误，正确地址应该是 172.21.39.88，端口号应该是 50200。

```
#
web-auth-server abc
server-ip 172.21.39.89
port 50100
shared-key cipher %^%#N[ePT/1o_2@zKz/>v:dTE_H%#s@Cy<{-|g:s'&\8%^%#
url-template url1
source-ip 10.23.100.1
server-detect
#
```

配置正确的服务器地址，同时为了确保共享密钥与 NCE 一致，重新配置共享密钥为 Huawei@123，配置如下：

```
[WAC1] web-auth-server abc
[WAC1-web-auth-server-abc] undo server-ip 172.21.39.89
Warning: Server-ip access-users will be offline, sure to continue?[Y/N] y
[WAC1-web-auth-server-abc] server-ip 172.21.39.88
[WAC1-web-auth-server-abc] port 50200
[WAC1-web-auth-server-abc] shared-key cipher Huawei@123
```

查看 Portal 服务状态，Portal 服务器的状态为 “DOWN”。

```
[WAC1] display portal-server state
Web-auth-server      :   abc
Total-servers        :   1
Live-servers          :   0
Critical-num          :   0
Status                :   Abnormal
Ip-address            :   Status
172.21.39.88         :   DOWN
```

检查配置确认当前设备开启 Portal 服务器探测功能，而认证服务器未配置。故需要手动关闭 Portal 服务器探测功能，配置如下：

```
[WAC1] web-auth-server abc
[WAC1-web-auth-server-abc] undo server-detect
```

```
[WAC1-web-auth-server-abc] quit
```

再次检查 Portal 服务器的状态，状态为“UP”，如下所示：

```
[WAC1] display portal-server state
Web-auth-server      :   abc
Total-servers        :   1
Live-servers         :   1
Critical-num         :   0
Status               :   Normal
Ip-address           Status
172.21.39.88         UP
```

采用 STA 再次测试，发现依旧无法弹出 Portal 认证页面，发现跳转页面的端口号为 8445，而 NCE 作为 Portal 服务器的默认端口为 19008。随后检查 WAC1 上的 URL 模板，发现 URL 地址中的端口号配置错误，如下所示：

```
#
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
#
```

修改 URL 端口为 19008，配置如下：

```
[WAC1] url-template name url1
[WAC1-url-template-url1] url https://172.21.39.88:19008/portal
[WAC1-url-template-url1] quit
```

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 VAP 信息

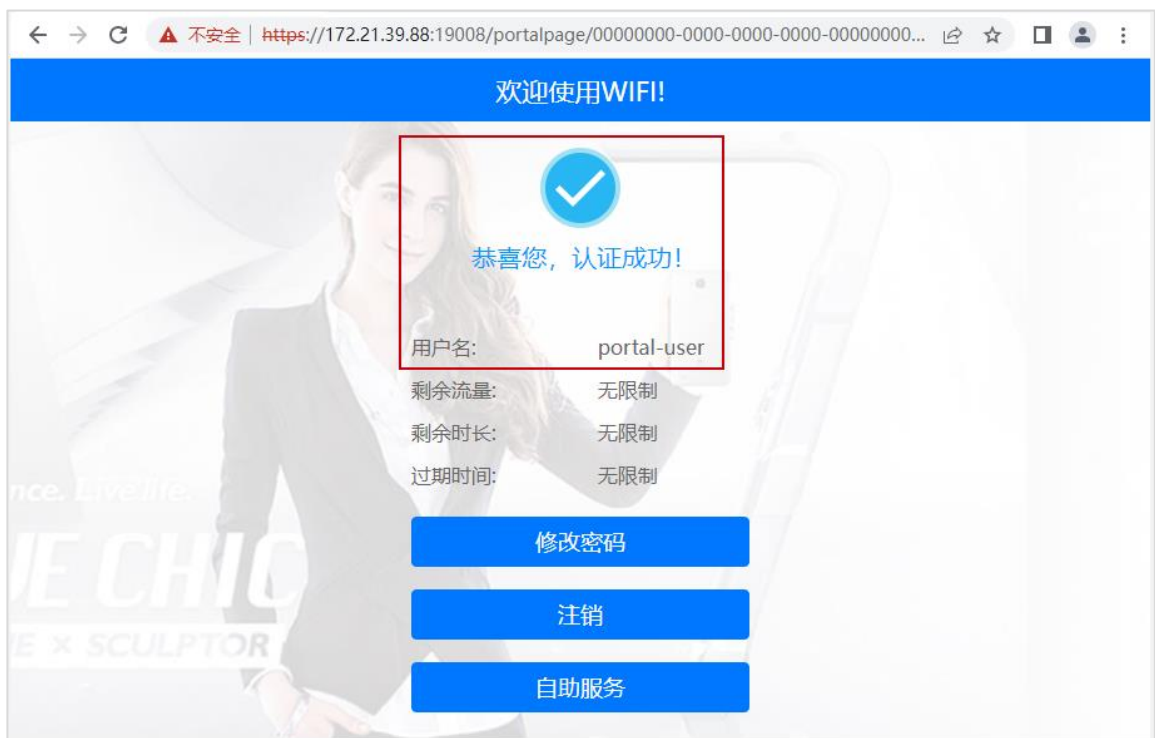
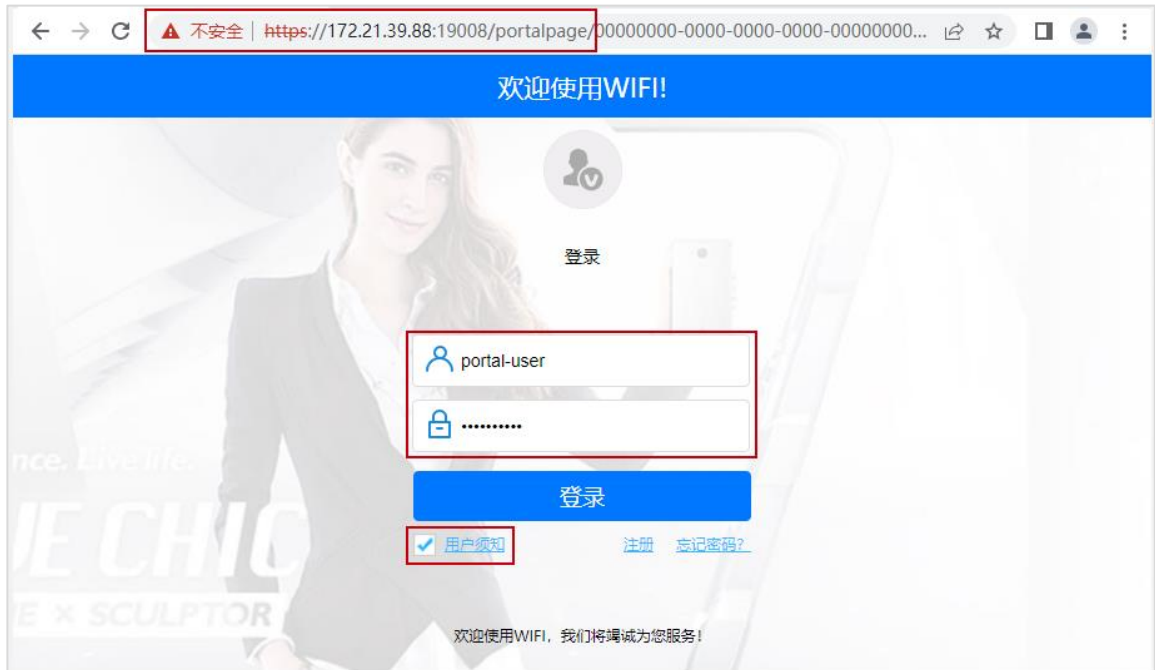
在 WAC1 上执行 display vap all 命令，查看 VAP 信息如下。

```
[WAC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
```

AP ID	AP name	RfID	WID	BSSID	Status	Auth type	STA	SSID
0	AP1	0	1	9CB2-E82D-54F0	ON	Open+Portal	0	wlan-net
0	AP1	1	1	9CB2-E82D-5500	ON	Open+Portal	0	wlan-net
1	AP2	0	1	9CB2-E82D-5410	ON	Open+Portal	0	wlan-net
1	AP2	1	1	9CB2-E82D-5420	ON	Open+Portal	0	wlan-net
2	AP3	0	1	9CB2-E82D-5110	ON	Open+Portal	0	wlan-net
2	AP3	1	1	9CB2-E82D-5120	ON	Open+Portal	0	wlan-net

Total: 6

12.3.2 STA 关联无线信号，认证通过



12.4 配置参考

12.4.1 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 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 169.254.1.1 255.255.255.0
#
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。
