华为认证 WLAN 系列教程

# **HCIP-WLAN**

# 实验指导手册(Web)

版本: 2.0



华为技术有限公司

### 版权所有 © 华为技术有限公司 2023。 保留一切权利。

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

### 商标声明

和其他华为商标均为华为技术有限公司的商标。本文档提及的其他所有商标或注册商标,由各自的所有人拥有。

### 注意

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

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

## 华为技术有限公司

- 地址: 深圳市龙岗区坂田华为总部办公楼 邮编: 518129
- 网址: https://e.huawei.com



## 华为认证体系介绍

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

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

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

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

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



	HCIE	Huawei Certified ICT Expert	HCIP		HCIA	Huawei Certified ICT Associate
	юТ	Kunpeng	MDC	Security		
	GaussDB	Ч	Digital Power		Access	LTE
职业证	Big Data	HarmonyOS	Intelligent Vision	WLAN		
华为	Cloud Service	openGauss	Collaboration		insmission	56
	Cloud Computing	openEuler	Storage	Datacom	Tre	
	云平台及云服务领域	基础软硬件领域	11基础设施领域	数通领域	光领域	无线领域
	云平台及云服务	基础软硬件		IC T 其 和 的 结		





# 简介

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

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

## 内容描述

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

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



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

# 读者知识背景

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

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







и iMaster NCE

iMaster NCE-Campus



接入交换机

STA



-6

iMaster NCE CampusInsight iMaster

NCE-CampusInsight



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
服冬哭	iMaster NCE-Campus	V300R021C00SPC110
	iMaster NCE-CampusInsight	V100R021C10SPC100

# 准备实验环境

检查设备

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

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



## 实验拓扑



实验拓扑说明如下:

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

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

WAC1~WAC3 旁挂于核心交换机 SW-Core 上。

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



# 目录

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



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



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



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



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



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



12.2.2 配置步骤	18
12.3 结果验证	53
12.3.1 检查 AP 上线状态	53
12.3.2 检查 VAP 信息	54
12.3.3 STA 关联无线信号,认证通过	55
12.4 配置参考	55
12.4.1 WAC1 配置	55
12.4.2 SW-Core 配置	59
12.4.3 SW-Access 配置	70
12.5 思考题	70



# 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





# 1.1.4 实验规划

设备	端口	端口类型	VLAN参数
	MultiGE0/0/1	Trunk	PVID:1
SIM Care			Allow-pass: VLAN 100 101
SVV-Core		- ·	PVID:1
	MulliGE0/0/9	Тгипк	Allow-pass: VLAN 100 101
		Trunk	PVID:1
	MultiGE0/0/9		Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100
			Allow-pass: VLAN 100 101
SW-Access	MultiGE0/0/2 Trunk	<b>T</b>	PVID:100
		Trunk	Allow-pass: VLAN 100 101
	MultiGE0/0/3 Trunk		PVID:100
		Trunk	Allow-pass: VLAN 100 101
	650/0/1	Turnels	PVID:1
WAC1	GEU/U/ I	Trunk	Allow-pass: VLAN 100 101

## 表1-1 VLAN 规划

## 表1-2 IP 地址规划

设备	端口	IP地址
SWL Corro	Vlanif100	10.23.100.254/24
Svv-Core	Vlanif101	10.23.101.254/24
	Vlanif100	10.23.100.1/24
VVACT	MEth0/0/1	172.21.39.4/24

## 表1-3 WLAN 业务参数规划

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



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

# 1.2 实验任务配置

## 1.2.1 配置思路

1.配置 SW-Core、SW-Access 设备的 VLAN 和 IP 地址。

2.初始化 WAC1 设备,并修改管理 IP 地址。

3.配置 WAC1 设备的 VLAN 和业务 IP 地址,确保网络互通。

4.在 SW-Core 上配置 DHCP 服务器,为 AP 及 STA 分配 IP 地址。

5.配置 AP 上线。

6.配置 WLAN 业务参数,实现 STA 接入 WLAN 网络。

## 1.2.2 配置步骤

步骤 1 配置交换机 VLAN 信息

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

#在SW-Access上创建VLAN 100、101。

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

# 配置 SW-Access 下行端口类型及允许通过的 VLAN。

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



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

# 配置 SW-Access 上行端口类型及允许通过的 VLAN。

[SW-Access] interface MultiGE 0/0/9 [SW-Access-MultiGE0/0/9] port link-type trunk

[SW-Access-MultiGE0/0/9] port trunk allow-pass vlan 100 101 [SW-Access-MultiGE0/0/9] quit

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

#在 SW-Core 上创建 VLAN 100 和 VLAN 101。

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

# 配置 SW-Core 下行端口类型及允许通过的 VLAN。

[SW-Core] interface MultiGE 0/0/9

[SW-Core-MultiGE 0/0/9] port link-type trunk

[SW-Core-MultiGE 0/0/9] port trunk allow-pass vlan 100 101

[SW-Core-MultiGE 0/0/9] quit

# 配置 SW-Core 与 WAC1 互联端口的类型及允许通过的 VLAN。

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

#### 步骤 2 配置交换机 IP 地址

#### # 配置 SW-Core 的 IP 地址。

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

### 步骤 3 初始化 WAC1 设备

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



Wireless LAN	用户名:	
Access Controller	密码:	0
	确认密码:	0
	串口认证类型: 〇 AAA认证 💿 密码认证	
	串口密码:	۲
	串口确认密码:	0
	注册	

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

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

Wireless LAN	用户名: admin	
Access Controller	密码:	•
	确认密码:	•
	串口认证类型: 🔘 AAA认	正 💿 密码认证
	串口密码:	0
	串口确认密码:	۲
	注:	₩

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



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

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

Wireless LAN 。 设备名称: AirEngine9700	AirEngine9700-M1 I-M1	监控	D ☆ ≊	[+] 诊断	 维护
● 配置向导	物理接口	逻辑接口 4	管理网口		
2 AC配置	接口名称:	M	th 0/0/1		
基本配置	接口状态:	C	ON		
VLAN	IP地址:	6	172 . 21 . 3	39.4	0
3 接口管理	6 应用				1
IP					
PNP					

#### #修改管理 IP,需要重新登录,点击"确定"。

警告		×
	修改设备当前管理IP地址将导致系统超时,需 要重新登录,是否继续?	
	确定取消	



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

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

Wireless LAN 。 设备名称: AirEngine9700	AirEngine9700-M1 -M1	监控	↔	(十) 诊断	┃↓↓ 维护
● 配置向导	物理接口	逻辑接口	管理网口		
● AC配置	按口夕物.		ME+b 0/0/1		
基本配置	接口状态:				
VLAN	IP地址:		172 . 21 .	39.4	0
接口管理	应用				
IP					
PNP					

# 为了实验方便,进一步修改 Web 网管的超时时间,本实验配置为 60 分钟(缺省为 10 分钟),注意,实际的生产网络中出于安全考虑,不建议将 Web 网管的超时时间配置过长。
# 选择"维护 > AC 维护 > 系统管理",选择"服务管理"选项卡,将 Web 服务的超时时间修改为 60 分钟,然后点击"应用",如下所示。

WEB服务		
HTTPS服务端源接口:	○ 所有接口 💿 指定接口	○无
	MEth0/0/1	
WEB服务器超时时间(分钟):	60	
应用		

步骤 4 配置 WAC1 设备的 VLAN 和 IP 地址

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

# 修改 WAC1 的设备名称。



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

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

重命名		×
*设备名称:	WAC1	
	确定取消	

#在WAC1上创建VLAN 100、101。

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN A 设备名称: WAC1	irEngine9700-M1	 监控	なる	☐÷ 诊断	\$ <b>↓</b> } 维护
▶ 配置向导	全局IPv6: OFF				
● AC配置	VLAN VLA	ANIF VLA	AN Pool		
基本配置	新建 删除	批量新建	批量删除	刷新	
VLAN	VLAN ID +	VLAN 描述 ▲			VLAN 类型 ▲
接口管理	1	VLAN 0001			commonVlan
IP	10 ▼ 共1条				
Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	な配置	+ 诊断	<b>   </b> 维护
① 配置向导	AC配置 > VLAN >	VLAN > 批量新	≣VLAN		
O AC配置	*VLAN ID:	[	100,101		)(1-4094,格式: 1,3 <mark>-</mark> 5,7)
基本配置	确定取消	)			
VLAN					
Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	な配置	(十) 诊断	┃↓↓ 维护
① 配置向导	全局IPv6: OFF				
O AC配置	VLAN V	LANIF V	LAN Pool		
基本配置	新建制除	批量新建	批量删除	刷新	
VLAN	VLAN ID +	VLAN 描述			VLAN 类型 *
接口管理	100	VLAN 0001			commonVlan
IP	101	VLAN 0101			commonVlan
● AP配置					
安全管理	10 ▼ 共3条				

# 配置 WAC1 的 GE0/0/1 端口类型及允许通过的 VLAN。



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

Wireless LAN A 设备名称: WAC1	irEngine9700-M1 🔄 🔅 🕂 🕌 监控 配置 诊断 维护	
● 配置向导	物理接口 逻辑接口 管理网口	
● AC配置	接口属性 LLDP	
基本配置	1 选择面板上的接口进行配置(Eth-Trunk接口也可点击紫色圆圈进行选中,或 点此 进行新建。	)
VLAN	2 4 6 8 10 12	6
接口管理		
IP		
● AP配置	1 3 5 7 9 11	5
● 安全管理	🚹 已选中 💼 Up 🗋 Down 💼 Shutdown	
QoS		
● 扩展业务	* 接口各杯: GigabitEthernet0/0/1	
● 可靠性配置	谜: 2 Trunk ▼	
	允许通过VLAN(Tagged): 3 100,101	
	高级 🕑	
	4 确定 取消	

# 创建 Vlanif100 接口,并配置接口 IP 地址。

# 选择 "配置 > AC 配置 > VLAN",选择 "VLANIF" 选项卡,点击"新建"。



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	- <u></u> 监控	<b>袋</b> 配置	[+] 诊断	 维护	
● 配置向导	全局IPv6: OFF					
● AC配置	VLAN VL	ANIF	VLAN Pool			
基本配置	新建 删除	刷新				
VLAN	接口名称 ▲	连拍	妾状态 ▲			IPv4地址/掩码 ▲
接口管理	Vlanif1	• :	不可用			
IP	10 ▼ 共1条					

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

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	监控	<b>☆</b> 配置	☐ 诊断	 维护	
● 配置向导	AC配置 > VLAN > V	'LANIF > 新建'	VLANIF			
● AC配置	* VLAN ID:	Γ	100			
基本配置	MTU (bytes):	(	1500			
VLAN	管理接口:	(	OFF ?	l.		
接口管理	IP地址格式:	[	✓ IPv4 IPv6	5		
IP	IPv4地址配置					
● AP配置	主IP地址/掩码:	L	10 . 23 . 1	100.1	/ 255 . 255 . 255	. 0
● 安全管理	从IP地址/掩码:		➡ 添加			<b>~</b>
QoS						. ^
● 扩展业务						
• 可靠性配置	開定則					



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	·····································	(十) 诊断	¦↓↓ 维护	
● 配置向导	全局IPv6: OFF				
● AC配置	VLAN VLAN	F VLAN Pool			
基本配置	新建创除	刷新			
VLAN	接口名称▲	连接状态 ◆		IPv	/4地址/掩码 ▲
位口等理	Vlanif1	• 不可用			
按口目理	Vlanif100	• 可用		10	.23.100.1/255.255.255.0
IP					
● AP配置	10 ▼ 共2条				

#### 步骤 5 配置 DHCP 服务器

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

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

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

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

#### 步骤 6 配置 AP 上线

# 配置 WAC 基础信息。

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



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	<b>谷</b> 配置	(十) 诊断	<b>↓↓</b> 维护	
● 配置向导	AC基本信息	AC间漫游	Navi-AC			
O AC配置	*AC源地址IP类型:		● IPv4 ○	IPv6 O IPv4	l&IP∨6	
基本配置	*AC源地址:	0	• VLANIF	O LoopBack	○ IP地址	
VLAN					2 🕈 😗	
接口管理			接口	IPv4地址	IPv6地址	×
IP		3	Vlanif100	10.23.100.1		
● AP配置	AP数据缓存:		OFF			
● 安全管理	AP认证方式:	4	MAC认证		添加AP	
QoS	无线用户IPv6业务:		OFF			
● 扩展业务	高级 🕑					
• 可靠性配置	应用					

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

高级 🕤				
↓ CAPWAP链路配置				
AC - AP				
AC到AP的CAPWAP管理报文优先级: 7	<b>*</b>	AP到AC的CAPWAP管理报文优先级:	7	*
允许AP以预置证书与AC进行DTLS会 () 话:		允许AP以不认证方式与AC进行DTLS 会话:		
AC-AP间控制隧道DTLS加密: 自动	×	AC-AP间数据隧道DTLS加密:	OFF 💡	
*AC-AP间DTLS加密预共享密钥:	•	AC-AP间敏感信息加密预共享密钥:		• •
报文完整性校验:		报文完整性预共享密钥:		۲
AC - AC				
AC-AC间控制隧道DTLS加密: 自动	<b>*</b>	AC-AC间数据隧道DTLS加密:	OFF	
*AC-AC间DTLS加密预共享密钥:	۲	AC-AC间敏感信息加密预共享密钥:		۲
CAPWAP心跳检测时间间隔(秒): 25		CAPWAP心跳检测次数:	6	

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



配置密钥			×
1 为提高系统安全性,请完成如7	下配置。		
AP帐号			
()为提高访问AP的安全性,请配	置AP的用户名和密码,同时该配置属于全	局配置,对所有AP有效。	
*用户名:	admin	*密码:	 •
离线VAP			
ⅰAP离线时会发出管理SSID,便	于管理员使用无线连接AP,为保证连接的	安全性,配置连接管理SSID的密钥。	
* 离线VAP密钥:	•••••		
	确定	取消	

# 创建 AP 组。选择"配置 > AP 配置 > AP 组配置",选择"AP 组"选项卡,点击"新 建"按钮,配置 AP 组名称为 ap-group1,然后点击"确定",如下所示。

Wireless LAN A 设备名称: WAC1	\irEngine9700-M1	 监控	<b>谷</b> 配置	(十) 诊断	↓↓ 维护
● 配置向导	AP组 静态	负载均衡组			
● AC配置	修改新建	删除	刷新		
⊙ AP配置	组名称 ▲	VAP	奠板 ▲		射频0模板▲
AP组配置	default				2.4G-default
AP配置	20 🔻 共1条				
Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	<b>☆</b> 配置	(十) 诊断	<b>   </b> 维护
● 配置向导	AP配置 > AP组配置	置 > AP组 > 新	書AP组		
● AC配置	* AP组名称:	ap	aroup1		
⊙ AP配置	···· 2 日 ···· · · · · · · · · · · · · ·	E Cob	9.0001		
AP组配置	WOAL PAA				
AP配置					

# 在 WAC1 上添加 AP ( AP 的 MAC 地址以实际情况为准 )。



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

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	监控	な	(十) 诊断	↓  维护
● 配置向导	AP信息	AP白名单	AP黑名单	AP邻居关系	AP设备类型
● AC配置	↓ AP列表				
⊙ AP配置	i 点击AP ID列	可进入AP的个	生化配置页面。		
AP组配置	修改AP配置		替換し制除	加入黑名单	
AP配置	AP ID -	AP MACABAE	AP	<b>台</b> 小 ~	AP
射频规划/调优					
分支AP组配置	→未认证AP列	则表			
Wireless LAN AirEngine 设备名称: WAC1	9700-M1 监控	<b>☆</b> 配置	<ul> <li>□</li> <li>□</li></ul>		
<ul> <li>● 配置向导 AP配</li> </ul>	置 > AP配置 > AP信息 > 添加	ΠΑΡ			
● AC配置 *添	加方式: • 手动派	泰加 🔿 批量导入			
✓ AP配置 *关	建字: • AP M	IAC O AP SN			
AP组配置	添加AP				
AP配置 *AF	MAC地址: 9cb2 -	e82d - 54f0	AP ID : 0		AP名称: AP1
射频规划/调优 AF	类型: - none -	•	AP SN :		
分支AP组配置	Real Final				
模板管理	NUAL AXIE				

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

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN Air 设备名称: WAC1	Engine9700-M1 监控		(十) 诊断	 维护			
● 配置向导	AP信息 AP白名单	单 AP黑名单	AP邻居关系	AP设备类型			
● AC配置	↓AP列表						
● AP配置	1 点击AP ID列可进入APA	的个性化配置页面。					
AP组配置	修改AP配置 添加		加入黑名单	闪灯   清空所	有AP 刷新		
AP配置	✓ AP ID × AP MACA ✓ Ø 0 9cb2-e82	d-54f0 AP	/西称 * 21	default 1	о.23.100.174		
射频规划/调优	✓ 💯 1 9cb2-e82	d-5410 AP	2	default 1	0.23.100.45		
分支AP组配置	✓ 💯 2 9cb2-e82	d-5110 AP	3	default 1	0.23.100.38		
模板管理	10 🔻 共3条						
Wireless LAN 设备名称: WAC1	Wireless     LAN     AirEngine9700-M1     Image: Comparison of the state of t						
▶ 配置向导	AP配置 > AP配置 > A	AP信息 > 修改AP					
● AC配置	AP组:	ap-group1					
⊙ AP配置	AC地址列表:	🛨 添加					
AP组配置				×			
AP配置	已选AP列表						
射频规划/调优	AP AP MAC地	AP名称	AP组 ▲	IP地址获取方式	IP地址		
分支▲P细融罢	0 9cb2-e82d	-54 AP1	default	- none -	· ·		
	1 9cb2-e82d-	-54 AP2	default	- none -	· ·		
模板管理	2 9cb2-e82d	-51 AP3	default	- none -	·		
<ul> <li>安全管理</li> </ul>	(∢						
QoS	10 ▼ 共3条						
● 扩展业务	确定						

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



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	<b>☆</b> 配置		<b>┃↓</b> 维护
● 配置向导	AP信息	AP白名单	AP黑名单	AP邻居关系	AP设备类型
● AC配置	↓ AP列表				
▼ AP配置	i 点击AP ID列	列可进入AP的个性们	和置页面。		
AP组配置	修改AP配置	添加	換删除	加入黑名单	闪灯  清空所有AP
	AP ID 🔺	AP MAC地址	AP名称 ▲	AP组 ▲	IP地址
AP配置	<b>(19</b> )	9cb2-e82d-54f0	AP1	ap-group	1 10.23.100.174
射频规划/调优	0.00 1	9cb2-e82d-5410	AP2	ap-group	1 10.23.100.45
分支AP组配置	2	9cb2-e82d-5110	AP3	ap-group	1 10.23.100.38
模板管理	10 🔻 共3	条			

### 步骤 7 配置 WLAN 业务

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

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

新建域管理模板		
*模板名称:	domain1	
确定取消		

# 然后选中 domain1 模板,配置国家码为中国,点击"应用",如下所示。



域管理模板:	domain1 展示模板引用关系	
🚺 模板介绍信息: 域管理	莫板提供对国家码、调优信道集合和调优带宽等的配置。	
国家码:	中国	
4.9G频段使能:	OFF ?	
→ 2.4GHZ DCA信道	合	
→ 5GHZ DCA信道集	≙	
应用		

# 在 AP 组中引用域管理模板。

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

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	 监控	なる	(土) 诊断	 维护
● 配置向导	AP组 静态	负载均衡组			
● AC配置	修改新建	删除	刷新		
● AP配置	组名称 ▲	VAP	模板 ▲		射频0模板▲
AP组配置	default				2.4G-default
	ap-group1				2.4G-default
AP配置					
射频规划/调优	20 🔻 共2条				

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



AP配置 > AP组配置 > AP组				
AP组配置: ap-group1 ▼ 查看成员		*城管理模板:	domain1	Ŧ
显示所有模板	置模型介绍	模板介绍信息:域	管理模板提供对国家码、调合	尤信道集合和调你
<ul> <li></li></ul>		国家码:	中国	*
<b>夏</b> 域管理模板	[default]	4.9G频段使能:	OFF ?	
<ul> <li></li></ul>		→ 2.4GHZ DCA信	道集合	
田 <b>一</b> 射频2		→ 5GHZ DCA信道	首集合	
🗄 🔚 AP				
I IIIII		应用		

# 创建名为 "wlan-net"的安全模板,并配置安全策略。

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

模板管理	
	新建安全模板
団 ■ VAP模板	
Image: Base of the second	*模板名称: wlan-net
■ 1000000000000000000000000000000000000	
🖪 default	确定取消
📮 default-wds	
🛃 default-mesh	

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

安全模板:	wlan-net 展示模板引用关系
● 模板介绍信息:配置	WLAN安全策略,可以对无线终端进行身份验证,对用户的报文进行加密,保护WLAN网络和用户的安全。WLAN安全策略支
基础配置	高级配置
🌗 Open认证方式存在	一定的安全风险,建议采用其他认证方式。安全级别由高到低。
*安全策略: ○ WPA3	WPA2-WPA3 WAPI WPA2 WPA-WPA2 WPA WPA OWE OPEN
认证方式:	O Dot1x O DPSK PPSK O PSK
WPA加密方式:	AES AES-TKIP TKIP
WPA2加密方式:	AES AES-TKIP TKIP
密钥类型:	PASS-PHRASE     HEX
*密钥:	•••••
应用	



# 创建名为 "wlan-net"的 SSID 模板,并配置 SSID 名称为 "wlan-net"。

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

模板管理		
	新建SSID模板	
<ul> <li>■ IB VAP 爆吹</li> <li>■ IBSSID 模板</li> </ul>	* 模板名称:	wlan-net
I default ● I 安全模板	确定取消	

# 选择 "wlan-net" SSID 模板,配置 SSID 名称为 "wlan-net",点击"应用"。

SSID模板:	wlan-net 展示模板引用关系
模板介绍信息: SSII	D用来指定不同的无线网络。在STA上搜索可接入的无线网络时,显示出来的网络名称就是SSID。
基础配置	高级配置
*SSID名称:	wlan-net
最大用户数:	64
应用	

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

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

模板管理	
□ □无线业务	新建VAP模板
■ <b>I</b> VAP模板	
🗉 🧧 default	×模板名称; wlan-pet
∃ SSID模板	
∃ 📴 安全模板	确定取消
∃ <mark>  </mark> 流量模板	

# 选择"wlan-net"VAP 模板,配置转发模式为直接转发,业务 VLAN 为 101,点击"应 用"。





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

日 / 无线业务		*SSID模板:	wlan-net	~
回 <b>I</b> VAP模板				
🕑 📑 default		模板介绍信息: SSII	D用来指定不同的无线网络	。在STA上搜索可
🖃 📮 wlan-net				
BSID模板	[default]	基础配置	高级配置	
■ 安全模板	[default]			
■流量模板	[default]	*SSID名称:	wlan-net	
🗉 🧧 认证模板				
■终端黑白名单模板		最大用户数:	64	
■ 智能应用控制模板		「市田		
		152755		

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

模板管理				
		*安全模板:	wlan-net	-
□ <mark>■</mark> VAP模板				
🖭 📃 default		<ul> <li>         ·</li></ul>	冒WLAN安全策略,可以对无线线	冬端进行身
🗉 📑 wlan-net		0		
<mark>■</mark> SSID模板	[wlan-ne]	基础配置	高级配置	
目安全模板	[default]			
■ 流量模板	[default]	🌔 Open认证方式存在	至一定的安全风险,建议采用其(	也认证方式
🗉 🥫 认证模板				
■ 终端黑白名单模板		*安全策略: 🔘 WPA3	○ WPA2-WPA3 ○ W	
■ 智能应用控制模板				
<mark>■</mark> UCC模板		认证方式:	🔿 Dot1x 🔹 DPSK	O PPS
田 ■ Hotspot2.0模板     日本     日本				
🕙 📑 攻击防御模板		WPA加密方式:	AES AES-TKIF	∘⊙тк
CPE隧道模板			0 450 0 450 FM	
∃ SSID模板		WPA2加密方式:	AES AES-TKIP	
🗆 📙 安全模板		· 成何 米田 - 利。	PASS-PHRASE	HEX
📃 default		省初关室:		
🛃 wlan-net		*密钥:		0
default-wds				
🛃 default-mesh		应用		
∃ <mark>同</mark> 流量模板				


#### # 配置 AP 组引用 VAP 模板。

# 选择 "配置 > AP 配置 > AP 组配置",选择 "AP 组"选项卡,点击 "ap-group1",进 入此 AP 组的配置界面。

Wireless LAN A 设备名称: WAC1	AirEngine9700-M1	上 <u>小</u> 监控	なる	(十) 诊断	↓  维护
● 配置向导	AP组 静态	负载均衡组			
● AC配置	修改新建	删除	刷新		
⊙ AP配置	组名称 ▲	VAP	模板 ▲	射频	0模板 ▲
AP组配置	default			2.40	ò-default
	ap-group1			2.40	i-default
Areue					
射频规划/调优	20 ▼ 共2条				

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

AP配置 > AP组配置 > AP组	
AP组配置: ap-group1 ▼ 查看成员	VAP 模板列表
显示所有模板 配置模型介绍	④ 相关配置
	新建 添加 移除 展示模板引用关系
🗉 🖿 射频管理	
🕀 👝 AP	
🗉 🧮 WIDS	

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

添加VAP模板					
9 添加					
*VAP模板名称:	wlan-net 🔻	*WLAN ID: 1	*射频:	0,1 💌	×
高级 🕑					
确定取消					

# 然后查看"VAP 模板列表"如下。



VAP 模板列表								
<ul> <li>相关配置</li> </ul>								
新建 添加 移降	展示模板引用关系							
模板名称 ▲	SSID模板 ≜	认证模板▲	安全模板 ▲	WLAN ID +	射频▲	转发模式 ▲	业务VLAN ▲	使能状
wlan-net	wlan-net		wlan-net	1	0	直接转发	101	●开启
wlan-net	wlan-net		wlan-net	1	1	直接转发	101	●开启
10 ▼ 共2条							<	1 >

# 1.3 结果验证

## 1.3.1 查看 AP 上线状况、SSID 等信息

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

AP列表			
智能诊断	上线失败记录	SoftGRE隧道状态	导出信息 loT插卡信息
AP ID 🔺 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 🔺 🍸
0	AP1	ap-group1	normal
1	AP2	ap-group1	• normal
2	AP3	ap-group1	• normal
10 ▼ 共3条	ŧ		
总AP数:3		normal : 3	
AirEngine5761-1	1:3		

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



AP型VAP教	列表							
应用统计	清零							
AP ID *	AP名称 =	射频ID -	WLAN ID +	SSID +	BSSID *	认证方式 🔺	接入用户数 -	状态
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA/WPA2-PSK	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA/WPA2-PSK	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA/WPA2-PSK	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA/WPA2-PSK	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA/WPA2-PSK	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA/WPA2-PSK	0	on

# 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"。

°77.	<b>wlan-net</b> 无 Internet,安全		
	<u>属性</u>		
		断开连接	
# 测i	式 STA 与业务网关的网	<b>]</b> 络连通性。	
C:\₩i	ndows\system32>ping 1	0. 23. 101. 254	
正来来来来 在自自自自	Ping 10.23.101.254 具 10.23.101.254 的回复: 10.23.101.254 的回复: 10.23.101.254 的回复: 10.23.101.254 的回复: 10.23.101.254 的回复:	有 32 字节的数据: 字节=32 时间=4ms TTI 字节=32 时间=6ms TTI 字节=32 时间=7ms TTI 字节=32 时间=8ms TTI 字节=32 时间=8ms TTI	.=254 .=254 .=254 .=254
10.23 娄 往返行	.101.254 的 Ping 统计 奴据包: 已发送 = 4, 已 冠程的估计时间(以毫秒为 短 = 4ms, 最长 = 8ms	信息: 接收 = 4, 丢失 = 0 (0 9单位): , 平均 = 6ms	% 丢失),

# 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#*{";)Ik6$LUMXJS;VWR$p7mWZtx|EN3q#M`}27Bg+[8<)ELp.$
local-user admin privilege level 15
local-user admin service-type telnet ssh http
#
interface Vlanif100
ip address 10.23.100.1 255.255.255.0
#
interface MEth0/0/1
```





```
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
capwap source interface vlanif100
capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%#
capwap dtls inter-controller psk %^%#tc.5LFZ\oJ^bM8'*YYv#<te,1Oq8kAl.}J+v{puP%^%#
capwap message-integrity psk %^%#eJ&eRx\$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x*%^%#
capwap sensitive-info psk %^%#;,L1<.L'e+li6MX,^QxH{6z#&#z[v4Oe"pCPrFJ'%^%#
capwap inter-controller sensitive-info psk %^%#ji6gT7>2y3dm}n~Bb"%8z$0]B62~|NkD,WJF[n2U%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
wlan
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=+!I"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	VL	AN	规划
------	----	----	----

设备	端口	端口类型	VLAN参数
		Truple	PVID:1
SW-Core	MultiGE0/0/9	ттипк	Allow-pass: VLAN 100 101
		Truple	PVID:1
	MultiGE0/0/9	ттипк	Allow-pass: VLAN 100 101
SW-Access		Taunal	PVID:100
	MultiGE0/0/1	ттипк	Allow-pass: VLAN 100 101
		Trupk	PVID:100
	MultiGE0/0/2	пинк	Allow-pass: VLAN 100 101
		Trupk	PVID:100
	MultiGE0/0/5	пинк	Allow-pass: VLAN 100 101
		Trupk	PVID:100
	wiulliGE0/0/4		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



系统自动生成
WPA/WPA2+PSK+AES
a12345678
系统自动生成

# 2.2 实验任务配置

安全模板

安全策略

密码

SSID模板

SSID

AP Zone

### 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。

wlan-net

default

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] 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 H	lours 0 Minu	tes				
Domain-name	: -						
DNS-server0	: -						
NBNS-server0	: -						
Netbios-type	:-						
Position	: Interface						
Status	: Unlocked						
Gateway-0	: -						
Network	: 10.23.100	.0					
Mask	: 255.255.2	55.0					
VPN instance	:						
Logging	: Disable						
Conflicted addres	ss recycle inte	rval: -					
Address Statistic:	Total	:254 L	Jsed	:4			
	Idle	:250	Expired	:0			
	Conflict	:0	Disabled	d: 0			
Network section						-	
Start	End	Total	l Ised Io	lle(Evnir	ed) Conflict	t Disahl	led
						-	icu
10.23.100.1	10.23.100.25	4 254	4	25	0(0)	0	0
Client-ID format a	as follows:						
DHCP : mac-a	ddress	Р	PPoE :	mac-add	ress		
IPSec : user-id/p	ortnumber/vr	f PPP	: inte	face ind	ex		
L2TP : cpu-slo	t/session-id	SSL-V	/PN : user	-id/sessi	on-id		
Index	IP	Client	-ID Ty	pe	Left St	atus	
116 10.23.10	00.117	9cb2-e82d-	5110	DHCP	86299	- Usec	ł
170 10.23.10	00.171	eca1-d1f7-	7dd0 I	OHCP	86299	Used	
213 10.23.10	00.214	9cb2-e82d-	5410	DHCP	86329	Usec	ł
224 10.23.10	00.225	9cb2-e82d-	54f0 I	ОНСР	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。

Wireless LAN Access Point	用户名: 密码: 确认实码:	admin
		注册



提示		×
<b></b>	注册用户成功。	

### # 重新登录 AP4,如下所示。

Wireless LAN	用户名:	admin	
Access Point	密 码:		忘记室
	语 言:	中文 ▼ 登录	

### #修改 AP4 的模式为 FAT AP,然后 AP4 将会自动重启。

Wireless LAN 设备型号: AirEngine676	L-21T 监控
概览	
	AP工作模式
	<ul> <li>① 切換AP工作模式后,AP将会复位井工作在新的工作模式下。</li> <li>T作標框式:</li> <li>○ FAT ○ Cloud</li> </ul>
	应用
警告	×
<u> </u>	确认切换工作模式?
	确定取消



# 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"。

	Wireless LAN	用户名:	admin
	Access Point	密码:	••••••
		确认密码:	
		串口认证类型:	<ul> <li>AAA认证</li> <li>密码认证</li> </ul>
		串口密码:	•••••••
		串口确认密码:	••••••
			注册
提示		×	
1	当前串口认证类型选择为密码认证,注册用# STelnet和Web网管登录。 确定	□将用于	

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



第51	页
-----	---

配置密钥	×
1 为提高系统安全性,请完成如下配置。	
FIT AP帐号	
1 为提高访问FIT AP的安全性,请配置FIT AP的用户名和密码,同时该配置属于全局配置,对所有FIT AP有效。	
*用户名: admin *密码: ••••••• ••	
离线VAP	
● FIT AP离线时会发出管理SSID,便于管理员使用无线连接FIT AP,为保证连接的安全性,配置连接管理SSID的密钥。	
* 高线 VAP密钥: ③	
确定取消	

#### 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"。

國本信息	基本信息		
	AP版本:	V200R021C10SPC100	
	AP设备名称:	Leader AP	
	所在国家/地区:	中国	0
	*选择时区:	(UTC +08:00:00) Default 💌	
	系统时间:	● 手动设置 ○ 自动同步	
	*日期和时间:	22:26:25 🛗	使用PC当前时间

#### 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 Air 设备名称: Leader AP	Engine6761-21T	<u>~~</u> 监控	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	<b>    </b> 维护	高级		
上网配置	AP配置	AP接入安全					
无线网络配置	↓ AP列表						
接入点配置	添加 替换	も、別除(闪	灯	新			
	AP ID +	AP MAC地址	AP名称 ▲	AP Zone 🔺	IP地址	类型 ▲	版本
系统配置	<u>(100</u> 0	eca1-d1f7-7dd0	Lead (Leader AP	) default	10.23.100.165	AirEngine6761-21T	V200R021C
	<u>(r)</u> 1	9cb2-e82d-5410	AP2	default	10.23.100.207	AirEngine5761-11	V200R021C
	<u>(1)</u> 2	9cb2-e82d-5110	AP3	default	10.23.100.120	AirEngine5761-11	V200R021C
	<u>(1</u> ) 3	9cb2-e82d-54f0	AP1	default	10.23.100.220	AirEngine5761-11	V200R021C
	10 ▼ 共4条	:					
	→未认证AP列表	ŧ					

#### 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。



# 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 设备名称: Leader AP	AirEngine6761-21T	」 上述	□ <b>☆</b> 向导	なる	┃↓ 维护	高级
配置向导	*上网模式:		桥接模式		2	
	L网连接设置	Fit AP	Fit AP			
	MultiGE0 GE0	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"。

*无线网络名称:	wlan-net		
业务VLAN ID:	101	0	
加密方式:	密码认证	×	
*密钥:		0 Ø	
生效射频:	✓ 2.4GHz	5GHz(Radio1) 🛛 🖌 5G/60	GHz(Radio2)
单用户上行限速(Kbps):	不限速		
单用户下行限速(Kbps):	不限速	×	



# 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。

Wireless LAN AirEr 设备名称: Leader-AP	ngine6761-21T 些		設置	↓  维护	高级
概览	接入点				Ð
			接入点	Ŧ	Q
	接入点 ▲	用户数 ▲	AP Zone 🔺	状态 ▲	
	Leader (Leader AP)	1	default	<ul> <li>normal</li> </ul>	
	AP1	0	default	<ul> <li>normal</li> </ul>	
	AP2	0	default	<ul> <li>normal</li> </ul>	
	AP3	0	default	<ul> <li>normal</li> </ul>	
	5 ▼ 共4条			< 1	>

	SSID名称	<b>T</b>	٩
SSID名称 ▲	用户数 ▲		
wlan-net	0		
HUAWEI-LeaderAP-7DD0	1		





# 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。

D AP配置								
∋ 射频配置	→ 2.40	HZ DCA信道集	A					
射频规划	射频列表	Z DCA信道来古						
射频参数	立即调伤				浙 识别冗余	射频		
接口管理	AP ID +	AP名称 -	射频ID▲	频段 🔺	工作模式 -	射频状态▲	颜宽/	信道
D IP业务	2	AP3	0	2.4G	正常模式	on	自动	20M/1
安全管理	2	AP3	1	5G	正常模式	on	自动	20M/4
	1	AP2	0	2.4G	正常模式	on	自动	20M/1
	1	AP2	1	5G	正常模式	on	自动	20M/4
	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/1
	0	Leader AP	0	2.4G	正常模式	on	自动	20M/6
	o	Leader AP	1	5G	正常模式	on	自动	20M/1
	0	Leader AP	2	5G	正常模式	on	自动	20M/4

### 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。



Wireless LAN 设备名称: Leader AP	AirEngine6761-21T	「」」	「「「「「「「」」」。	なる	<b>↓↓</b> 维护	高级
● AP配置	VLAN V	LANIF				
● 射频配置	新建制除	批量新建	批量删除	刷新		
⊙ 接口管理	VLAN ID +	VLAN 描述 *			VLAN	类型 ▲
VLAN	1	VLAN 0001			comn	nonVlan
以大网接口	100	VLAN 0100			comn	nonVlan
	- 101	VLAN 0101			comn	nonVlan
U IPWS						
● 安全管理	10 ▼ 共3条					

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"。

٩//	wlan-net 无 Internet,	安全	
	<u>属性</u>		
			断开连接

# 测试 STA 与业务网关的网络连通性。

C:\\indows\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 MultiGE0/0/0 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<:I]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
		Trupk	PVID:1
	WulliGE0/0/1	пипк	Allow-pass: VLAN 100 101
SW/ Coro	Multic E0/0/2	Trupk	PVID:1
300-0016	WulliGL0/0/2	TTUTK	Allow-pass: VLAN 100 101
	Multice0/0/9	Trupk	PVID:1
	WULLIGE0/0/9	пипк	Allow-pass: VLAN 100 101
	MultiGE0/0/9	Trunk	PVID:1
			Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100
			Allow-pass: VLAN 100 101
SVV-ACCESS	MultiGE0/0/2	Trunk	PVID:100
			Allow-pass: VLAN 100 101
	MultiGE0/0/3	Trunk	PVID:100
			Allow-pass: VLAN 100 101
		Trupk	PVID:1
VVACI			Allow-pass: VLAN 100 101
	CE0/0/1	Trupk	PVID:1
VVAC2	GE0/0/1	Irunk	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
	Vlanif100	10.23.100.254/24	管理VLAN,DHCP启用
SW-Core	Vlanif101	10.23.101.254/24	业务VLAN,DHCP启用
VRRP虚地址	/	10.23.100.33	与AP建立CAPWAP隧道



#### 表3-3 WLAN 业务参数规划

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

# 3.2 实验任务配置

### 3.2.1 配置思路

1. 配置 WAC1、WAC2、AP、SW-Core、SW-Access 设备网络互通。

2.配置 DHCP 服务器。

- 3.配置 VRRP 双机热备。
- 4.配置无线配置同步功能。
- 5.配置 WLAN 业务。

### 3.2.2 配置步骤

步骤 1 配置交换机 VLAN 及 IP 地址

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

#在 SW-Core 上创建 VLAN 100 和 VLAN 101。

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



[SW-Core] vlan batch 100 101

#### # 配置 SW-Core 下行端口类型及允许通过的 VLAN。

[SW-Core] interface MultiGE 0/0/9

[SW-Core-MultiGE 0/0/9] port link-type trunk

[SW-Core-MultiGE 0/0/9] port trunk allow-pass vlan 100 101

[SW-Core-MultiGE 0/0/9] quit

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

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

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

#在 SW-Access 上创建 VLAN 100、101。

<Huawei> system-view

[Huawei] sysname SW-Access [SW-Access] vlan batch 100 101

# 配置 SW-Access 下行端口类型及允许通过的 VLAN。

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

# 配置 SW-Access 上行端口类型及允许通过的 VLAN。

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

# 配置 SW-Core 的 IP 地址。



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

#### 步骤 2 初始化 WAC 设备

#初始化 WAC1 和 WAC2 的配置过程请参考 1.2.2 步骤 3,不再赘述。

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

#### 步骤 3 配置 WAC 的 VLAN 及 IP 地址

# WAC1、WAC2 的 VLAN 及 IP 地址配置过程请参考 1.2.2 步骤 4,不再赘述。

# WAC1 的 Vlanif100 接口地址配置为 10.23.100.1/24,WAC2 的 Vlanif100 接口地址配置为 10.23.100.2/24。

#### 步骤 4 配置 DHCP 服务器

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

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

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

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

步骤 5 配置 VRRP 双机热备(WAC1)

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

# 注意: WAC1 为主用设备, VRRP 虚地址配置为 10.23.100.33, 优先级配置为 120。



#### HCIP-WLAN V2.0 实验指导手册(Web )

第66页

Wireless LAN 。 设备名称: WAC1	AirEngine9700-M1	监控	な配置	<b>中</b> 诊断	<b>   </b> 维护	
● 配置向导	VRRP列表	BFD				
● AC配置	√ 高级配置					
● AP配置	状态恢复响应延迟的	间(秒):	60			
● 安全管理	VRRP协议版本:		• 版本2 🔵	版本3	•	
QoS	免费ARP报文发送:					
● 扩展业务	2 应用					
⊙ 可靠性配置	VRRP V	RRP6				
可靠性配置	i VRRP基于IPv4	类型进行配置。				
VRRP/BFD	VRRP列表					
	3 新建 删除	刷新				
	VRID *	VLAN	IIF ≜	状态 🔺	虚拟IP地址▲	
新建VRID						×
i 普通VRRP组的主备状态可以	跟随管理VRRP组的主备状态	;建议先创建管理	VRRP组。			
*VLANIF/IP:	VLANIF100		/ 10 , 23 ,	100 , 1		
* VRID: 😯	1		VRRP类型:	謹	通VRRP组	•
*虚拟IP地址:	🛨 添加		优先级:	12	0	
	10 . 23 . 100 .	33 ×				
抢占模式:						
抢占延迟时间(秒):	1800(主设备建议值)	T				
● 绑定VRRP组						
管理VRID:	- none -	T	管理VRRP接口:			
○ 绑定BFD						
● 绑定BFD 高级 ●						
○ 現定BFD 高级 ●						

# 配置 HSB 通道,使能双机热备功能。

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



Wireless LAN 设备名称: WAC1	AirEngine9700-M1 空 管 111	
① 配置向导	可靠性配置 > 可靠性配置	
● AC配置	备份方式: ● VRRP热备份 ○ 双链路总备份 ② ○ 双链路总备份 ○ N+1备份/无	
● AP配置	热备份(HSB)通道配置	
• 安全管理	◆备份业务: WILAN业务 ✔ NAC业务 ✔ DHCP	
QoS	IP地址类型: IPv4 m	
<ul> <li>扩展业务</li> </ul>	*本辦ACIP地址: 10 . 23 . 100 . 1	*本辦週囗: 10241
◎ 可集性配置	* 对MAC IP地址: 10 , 23 , 100 , 2	* 对娴娴囗: 10241
-Jakitela	*关联VRID: 0	
可靠性能讓	HSB通道状态: 未配置	
VRRP/BFD	1 注意,配置了VRRP热备份后,要求AC源地址必须要配置跟HSB关联VRID相同的虚地址。 標改ACI界地址	
	高級 🕤	
	① 配置的HSB主备服务报文的重传次数和发送间隔的乘积不小于VRRP的Master_Down_Interval定时器的时间。建议HSB主备服务报文的重	传次数和发送间隔时间使用缺省值。
	<b>回传次载:</b> 3	(前)稿出(前)(杉少): 6
	无线配置同步	
	启用无线配置同步: OF	
	应用	

步骤 6 配置 VRRP 双机热备(WAC2)

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

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

Wireless LAN A 设备名称: WAC2	irEngine9700-M1	监控	<b>读</b> 配置	<b>(十</b> ) 诊断	<b>4</b> 维护	
● 配置向导	VRRP列表	BFD				
● AC配置	↓ 高级配置					
● AP配置	状态恢复响应延迟时间	](秒): 6	50			
● 安全管理	VRRP协议版本:	۲	版本2 🔵 版	本3		
Oos	免费ARP报文发送:	C	ON			
<ul> <li>扩展业务</li> </ul>	应用					
⊙ 可靠性配置	VRRP VR	RP6				
可靠性配置	i VRRP基于IPv4类	型进行配置。				
VRRP/BFD	VRRP列表					
•	新建删除	刷新				
	VRID *	VLANIF	▲ ¥	态 🔺	虚拟IP地址▲	



新建VRID				×			
1 普通VRRP组的主备状态可以跟随管理VRRP组的主备状态,建议先创建管理VRRP组。							
* VLANIF/IP:	VLANIF100						
*VRID: 😮	1	VRRP类型:	普通VRRP组	•			
*虚拟IP地址:	😌 添加	优先级:	100				
	10 . 23 . 100 . 33	×					
抢占模式:							
抢占延迟时间(秒):	0(备设备建议值)						
● 绑定VRRP组							
管理VRID:	- none - 🔻	管理VRRP接口:					
○ 绑定BFD							
高级 🕑							
	ä	<b>能</b> 取消					

#### # 配置 HSB 通道,使能双机热备功能。

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

2 配置向导	可靠性配置 > 可靠性配	1			
AC配置	备份方式	● VRRP热备份 ○ 双链路热备份 ② ○ 双链路冷备份 ○	N+1备份/无		
AP配置	热备份(HSB)通道配置				
安全管理	*备份业务:	☑ WLAN业务 ☑ NAC业务 ☑ DHCP			
QoS	IP地址类型:	ip <sub>V</sub> 4 *			
) 扩展业务	*本端AC IP地址:	10 . 23 . 100 . 2		*本號端口:	102
C C LL SI	* 对端AC IP地址:	10 . 23 . 100 . 1		* 又才如何的收口:	102
可靠性配置	* 关联VRID:	1			
可靠性配置	HSB通道状态	+記事			
VRRP/BFD	1 注意,配置了VRRP热备	分后,要求AC源地址必须要配置跟HSB关联VRID相同的虚地址。修改AC源	ueur.		
	高级 💿				
	1 配置的HSB主备服务指	文的重传次数和发送间隔的乘积不小于VRRP的Master_Down_Interval定	討醫的时间。建议HSB主备服务报文的重传次数和	发送间隔时间使用缺省值。	
	回传次数:	3		间隔时间(砂):	б
	无线配置同步				
	启用无线配置同步:	OFF			

#### 步骤 7 配置 CAPWAP 源地址

# 配置 WAC1 基本信息。

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	上 监控	な配置	<b>(+)</b> 诊断	<b>   </b> 维护		
● 配置向导	AC基本信息	AC间漫游	Navi-AC				
<ul><li>● AC配置</li></ul>	*AC源地址IP类型:		• IPv4	IPv6 O IPv	4&IPv6		
基本配置	* AC源地址:			O LoopBack	● IP地址		
VLAN			IPv4 💌			0 0	
接口管理			接口	IPv4地址		IPv6地址	×
IP				10.23.100.3	33		
● AP配置	AP数据缓存:		OFF				
● 安全管理	AP认证方式:		MAC认证		▼ 添加A	P	
QoS	无线用户IPv6业务:		OFF				
● 扩展业务	高级 🕟						
▶ 可靠性配置	应用						

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

高级 🕤				
↓ CAPWAP链路配置				
AC - AP				
AC到AP的CAPWAP管理报文优先级:	7 🔻	AP到AC的CAPWAP管理报文优先级:	7	*
允许AP以预置证书与AC进行DTLS会话:		允许AP以不认证方式与AC进行DTLS 会话:		
AC-AP间控制隧道DTLS加密:	自动	AC-AP间数据隧道DTLS加密:	OFF ?	
*AC-AP间DTLS加密预共享密钥:	•••••	AC-AP间敏感信息加密预共享密钥:		• ?
报文完整性校验:		报文完整性预共享密钥:		•
AC - AC				
AC-AC间控制隧道DTLS加密:	自动	AC-AC间数据隧道DTLS加密:	OFF	
*AC-AC间DTLS加密预共享密钥:		AC-AC间敏感信息加密预共享密钥:		•
CAPWAP心跳检测时间间隔(秒):	25	CAPWAP心翻检测次数:	6	

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



第	7	0	页
~ ~	•	-	~

配置密钥			×
1为提高系统安全性,请完成如7	下配置。		
AP帐号			
1)为提高访问AP的安全性,请配	置AP的用户名和密码,同时该配置属于全局	局配置,对所有AP有效。	
*用户名:	admin	*密码:	
离线VAP			
ⅰAP离线时会发出管理SSID,便	于管理员使用无线连接AP,为保证连接的多	e全性,配置连接管理SSID的密钥。	
* 离线VAP密钥:	•••••		
	确定	取消	

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

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

步骤 8 配置无线配置同步功能

# 配置 WAC1 的无线配置同步功能。

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

无线配置同步			
1 配置将会从VRRP主设备	同步到VRRP备设备,备设备相关的配置仅支持查看。配置同步复用热备份(HSB)通道配置。		
<b>启用无线配置同步</b> :			
定时同步开关:			
定时同步间隔(分钟):	1440	定时同步启动时间:	00 : 00 : 00 🗢
P地址类型:	IPv4 ×		
本婰AC IP地址:	10 . 23 . 100 . 1	汉封網AC IP地址:	10 . 23 . 100 . 2
/RID:	1	接口名称:	
PSK密钥:	Huawei@123		
应用			

# 配置 WAC2 的无线配置同步功能。

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

无线配置同步								
● 配置將会从VRRP主设备同步到VRRP备设备。各设备相关的配置仅支持查看。通道&VRID配置与可靠性配置不一致。但由应用后将会把配置替换成可靠性的配置。								
启用无线配置同步:								
定时同步开关:	ON							
定时同步间隔(分钟):	1440	定时同步启动时间:	00:00:00 \$					
IP地址类型:	IPv4 *							
本뻀AC IP地址:	10 . 23 . 100 . 2	又拉碘AC IP地址:	10 , 23 , 100 , 1					
VRID:		接口名称:	Vlanif100					
PSK密钥:	Huawei@123							
应用								


- 步骤 9 配置 AP 上线 (WAC1)
  - # 配置过程请参考 1.2.2 步骤 6 相关内容,不再赘述。
  - # 注意: 仅需要在主用 WAC1 上配置即可,备用 WAC2 无需配置。
- 步骤 10 配置无线业务(WAC1)
  - # 配置过程请参考 1.2.2 步骤 7 相关内容,不再赘述。
  - # 注意: 仅需要在主用 WAC1 上配置即可,备用 WAC2 无需配置。
- 步骤 11 触发配置同步

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

	AC概況	漫游用户数概》	兄 接口流量统计	无线配置同步信息	业务逃生	Navi-AC			
自动刷新: OFF									
无线配置同步信息									
	对端IP地址	对端角色	对端型号	对端版本	链路状态	配置同步状态	最后同步时间	操作	
	10.23.100.2	Backup	AirEngine9700-M1	V200R021C00SPC100B171	• up	同步成功	16:22:24		
	10 ▼ 共	1条							

# 3.3 结果验证

- 3.3.1 检查 AP 上线状态
  - # 在主用 WAC1 上选择 "监控 > AP ",选择 "AP 统计 "选项卡,查看 AP 的状态为 "normal ",如下所示。



AP ID 🔺 🍸	AD 字称▲▽	1		
	AL THIN - I	AP组 + 7	状态名称▲▽	用户数。了
0	AP1	ap-group1	normal	0
1	AP2	ap-group1	normal	0
2	AP3	ap-group1	normal	0

# 在备用 WAC2 上选择"监控 > AP",选择"AP 统计"选项卡,查看 AP 的状态为 "standby",如下所示。

智能诊断	上线失败记录	下线记录 Soft	tGRE隧道状态导出信息	息 loT插卡信息
AP ID * 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 ▲ ▽	用户数 🔺 🍸
0	AP1	ap-group1	standby	0
1	AP2	ap-group1	standby	0
2	AP3	ap-group1	standby	0

# 3.3.2 检查 VAP 信息

# 以 WAC1 为例,检查 VAP 状态信息。

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



自动	SSID VAP a动刷新: OFF AP型VAP列表								
	应用统计清	零							
	AP ID 🔺	AP名称 ▲	射频ID ▲	WLAN ID 🛎	SSID 🔺	BSSID 🔺	认证方式 ▲	接入用户数	状态 ▲
	0	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA/WPA2-PSK	0	on
	0	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA/WPA2-PSK	0	on
	1	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA/WPA2-PSK	0	on
	1	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA/WPA2-PSK	0	on
	2	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA/WPA2-PSK	0	on
	2	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA/WPA2-PSK	0	on
	10 💌 🛃	<b>ŧ6条</b> Þ的VAP,查看该\	/AP应用统计信题	<u>م</u> در •					

# 3.3.3 检查 HSB 通道状态

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

Wireless LAN A 设备名称: WAC1	irEngine9700-M1	Left     日     1       LEft     1       LEft     1       LEft     1       LEft     1
● 配置向导	可靠性配置 > 可靠性配	置
● AC配置	备份方式:	● VRRP热备份 ○ 双链路热备份 ? ○ 双链路冷备份 ○ N+1备份/无
● AP配置	热备份(HSB)通道配置	
<ul> <li>安全管理</li> </ul>	*备份业务:	✓ WLAN业务 ✓ NAC业务 ✓ DHCP
QoS	IP地址类型:	IPv4 ·
● 扩展业务	*本端AC IP地址:	10 . 23 . 100 . 1
⊙ 可靠性配置	*对端AC IP地址:	10 . 23 . 100 . 2
可靠性配置	*关联VRID:	1 0
VRRP/BFD	HSB通道状态:	已连接 备份后,要求AC源地址必须要配置跟HSB关联VRID相同的虚地址。修改AC源地址
	高级 🕑	

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



• 配置向导	可靠性配置 > 可靠性配置	Ĩ			
● AC配置	备份方式:	● VRRP热备份	○ 双链路热备份	😚 🕜 🔵 双链路冷备份	○ N+1备份/決
● AP配置	热备份(HSB)通道配置				
● 安全管理	*备份业务:	WLAN业务	NAC业务	JHCP	
QoS	IP地址类型:	IPv4 T			
● 扩展业务	*本端AC IP地址:	10 . 23	. 100 . 2		
● 可靠性配置	* 对端AC IP地址:	10 . 23	. 100 . 1		
可靠性配置	*关联VRID:	1		😮	
	HSB通道状态:	已连接			

# 3.3.4 检查无线配置同步状态信息

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

	AC概况	漫游用户数概况	记 接口流量统计	无线配置同步信息	业务逃生	Navi-AC		
自动	加刷新: OFF							
	无线配置同步	信息						
	对端IP地址	对端角色	对端型号	对端版本	链路状态	配置同步状态	最后同步时间	操作
	10.23.100.2	Backup	AirEngine9700-M1	V200R021C00SPC100B171	• up	同步成功	16:22:24	
	10 ▼ 共	1条						

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

	AC概況	漫游用户数概况	记 接口流量统计	无线配置同步信息	业务逃生	Navi-AC		
自动	刷新: OFF							
	无线配置同步	信息						
	对端IP地址	对端角色	对端型号	对端版本	链路状态	配置同步状态	最后同步时间	操作
	10.23.100.1	Master	AirEngine9700-M1	V200R021C00SPC100B171	• up	同步成功	16:23:57	
	10 🍷 共	1条						



# 3.3.5 STA 关联无线信号,测试网络连通性

#### # STA 扫描接入无线网络"wlan-net"。

	٩//	wlar 无 I	n-net nterne	et, ≸	全							
		属性										
							断	开连接	ŧ			
#	测记	ζ STA	、与业	务网	关的网	络连	通性	ŧ.				
C	:\Win	dows	∖syste	m32>j	ping 1	0.23.	101.	254				
	王在 P: 王自 10 王自 10 王自 10	ing 1 0.23. 0.23. 0.23. 0.23. 0.23.	10.23. 101.2 101.2 101.2 101.2	101. 54 的 54 的 54 的 54 的	254 具 9回复复复 9回复复	有 32 字字字字字字字字	字 <sup>±</sup> =32 =32 =32 =32	市的数 时间: 时间: 时间:	文据: =4ms / =6ms / =7ms / =8ms /	TTL= TTL= TTL= TTL=	254 254 254 254 254	
1) 行	0.23. 数 E返行 最	101.2 据包: 短目 1011	254 的 : 已发 古计时 4ms,	Pin 送 = (1) 最长	g 统计 4, 已 《毫秒为 = 8ms	信息: 接收, 9 单位, 9 平均	= 4, ): ] =	丢失 6ms	₹ = 0	(0%	丢失	),

# 3.4 配置参考

# 3.4.1 WAC1 配置

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





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



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

## 3.4.2 WAC2 配置

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



```
interface MEth0/0/1
ip address 172.21.39.5 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source ip-address 10.23.100.33
capwap dtls psk %^%#EJVsX!hYu4YZ2_G4#DzXA@:RKv34&REZ}|-y_]mY%^%#
capwap dtls inter-controller psk %^%#fn"&!O[*},H,}sO8]j:.7FT*XoFd\E%z`f<D]FcL%^%#
capwap dtls no-auth enable
#
hsb-service 0
service-ip-port local-ip 10.23.100.2 peer-ip 10.23.100.1 local-data-port 10241 peer-data-port 10241
service-keep-alive detect retransmit 3 interval 6
#
hsb-group 0
track vrrp vrid 1 interface Vlanif100
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
temporary-management psk %^%#PwFE@vw_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\.KXW7QH=Ogpvg'K*Y)I%^%#
traffic-profile name default
security-profile name default
security-profile name wlan-net
 security wpa-wpa2 psk pass-phrase %^%#51sYLQj@,Ph}m2@A1j:Of3n/)t5j=+!I"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}gjg1:Fn0*Z&]gVje!B>%^%#
#
return
```

# 3.4.3 SW-Core 配置

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



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

# 3.4.4 SW-Access 配置

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



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

## 3.5 思考题

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

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



# 4 云管理组网实验

# 4.1 实验介绍

## 4.1.1 关于本实验

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

## 4.1.2 实验目的

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

## 4.1.3 实验组网介绍





# 4.1.4 实验规划

设备	端口	端口类型	VLAN参数		
	MultiGE0/0/3	Trunk	PVID:1		
			Allow-pass: VLAN 100 101		
SW-Core	MultiGE0/0/4	Access	PVID: 99		
	MultiGE0/0/9	Trunk	PVID:1		
	Widtigeo, 0, 5	THUNK	Allow-pass: VLAN 100 101 200 201		
		Trunk	PVID:100		
	MulliGE0/0/1	TTUTIK	Allow-pass: VLAN 100 101		
	MultiGE0/0/2	Trunk	PVID:100		
	WIUUIGEU/U/Z	ΠΠΙΚ	Allow-pass: VLAN 100 101		
		Truck	PVID:100		
JW-ALLESS		Пинк	Allow-pass: VLAN 100 101		
		Trunk	PVID:1		
	Mutigeo/0/5	ΠΠΙΚ	PVID:100 Allow-pass: VLAN 100 101 PVID:1 Allow-pass: VLAN 200 201		
		Trunk	PVID:1		
	MulliGE0/0/9	птипк	Allow-pass: VLAN 100 101 200 201		
		Trupk	PVID:1		
WACT	GE 0/0/1	TTUTIK	Allow-pass: VLAN 100 101		

## 表4-1 VLAN 规划

## 表4-2 IP 地址规划

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



(后文简称为NCE)

## 表4-3 WAC3 业务参数规划

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

## 表4-4 AP5 业务参数规划

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





# 4.2 实验任务配置

## 4.2.1 配置思路

1.配置 SW-Core、SW-Access、WAC3 设备网络互通。

2.配置 WAC3 上云,配置 WAC3 与 NCE 网络互通。

3.配置 WAC3 上云, AP1、AP2、AP3 在 WAC3 中上线。

4.配置 WAC3 的 WLAN 业务。

5.配置 AP5 上云。

6.配置 AP5 的 WLAN 业务。

7.检查 WLAN 业务可用性。

## 4.2.2 配置步骤

### 步骤 1 配置交换机 VLAN 及 IP 地址

# 配置接入交换机 SW-Access 设备。

#在SW-Access上创建VLAN 100、101、200、201。

<Huawei> system-view

[Huawei] sysname SW-Access

[SW-Access] vlan batch 100 101 200 201

# 配置 SW-Access 下行端口类型及相应 VLAN。

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



#### # 配置 SW-Access 上行端口类型及允许通过的 VLAN。

[SW-Access] interface MultiGE 0/0/9

[SW-Access-MultiGE0/0/9] port link-type trunk

[SW-Access-MultiGE0/0/9] port trunk allow-pass vlan 100 101 200 201

[SW-Access-MultiGE0/0/9] quit

#### # 配置核心交换机 SW-Core 设备。

#### #在SW-Core上创建VLAN 100、101、200、201。

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

#### # 配置 SW-Core 下行端口类型及允许通过的 VLAN。

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

#### # 配置 SW-Core 与 WAC3 互联端口的类型及允许通过的 VLAN。

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

# 配置 SW-Core 的 IP 地址。

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

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

## 步骤 2 初始化 WAC3 设备

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



Wireless LAN	用户名:	
Access Controller	密码:	0
	确认密码:	0
	串口认证类型: 〇 AAA认证 • 密码认证	
	串口密码:	•
	串口确认密码:	0
	注册	

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

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

Wireless LAN	用户名: admin	
Access Controller	密码:	•
	确认密码:	•
	串口认证类型: 🔘 AAA认	正 💿 密码认证
	串口密码:	0
	串口确认密码:	۲
	注:	₩

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



Wireless LAN	用户名:	admin
	密 码:	·····································
	语 言:	中文 ▼
		秦登

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

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

Wireless LAN A 设备名称: AirEngine9700-	NirEngine9700-M1		「 f 维护
● 配置向导	物理接口	逻辑接[4]管理网口	
<b>2</b> • AC配置	接口名称:	MEth 0/0/1	
基本配置	接口状态:		
VLAN	IP地址:	<b>5</b> 172 . 21 . 39 . 6	5 0
3 接口管理	应用		
IP			

# 修改管理 IP, 需要重新登录, 点击"确定"。

警告		×
	修改设备当前管理IP地址将导致系统超时,需 要重新登录,是否继续?	
	确定取消	



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

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

Wireless LAN 设备名称: AirEngine9700	AirEngine9700-M1 -M1	监控	な。配置	<b>主</b> 诊断	维护
● 配置向导	物理接口	逻辑接口	管理网口		
● AC配置	按口夕秒:	N	45+b 0/0/1		
基本配置	接口(1)小·	г (			
VLAN	IP地址:		172 . 21 . 3	39 . 6	0
接口管理	应用				
IP					

# 为了实验方便,进一步修改 Web 网管的超时时间,本实验配置为 60 分钟(缺省为 10 分钟),注意,实际的生产网络中出于安全考虑,不建议将 Web 网管的超时时间配置过长。
# 选择"维护 > AC 维护 > 系统管理",选择"服务管理"选项卡,将 Web 服务的超时时间修改为 60 分钟,然后点击"应用",如下所示。

WEB服务		
HTTPS服务端源接口:	○ 所有接口 ● 指定接口	〕 〇无
	MEth0/0/1	
WEB服务器超时时间(分钟):	60	
应用		

步骤 3 配置 WAC3 设备的 VLAN 和 IP 地址

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

- # 修改 WAC1 的设备名称。
- # 选择"监控 > AC",选择"AC 概况",在"AC 基本信息"中,点击"设备名称"后面的 "更改"字样,将设备名称修改为 WAC3。



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

重命名		×
*设备名称:	WAC3 确定 取消	

## # 在 WAC3 上创建 VLAN 100、101。

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

Wireless LAN 。 设备名称: WAC3	AirEngine9700-M1	监控	<b>读</b> 配置	<b>(手)</b> 诊断	<b>    </b> 维护
● 配置向导	全局IPv6: OFF				
● AC配置	VLAN VL	ANIF V	LAN Pool		
基本配置	新建删除	批量新建	批量删除	刷新	
VLAN	VLAN ID *	VLAN 描述			VLAN 类型
接口管理	1	VLAN 0001			commonVlan
IP	10 💌 共1条				



Wireless LAN 设备名称: WAC3	AirEngine9700-M1	监控	<b>读</b> 配置	(十) 诊断	维护
● 配置向导	AC配置 > VLAN > V	LAN > 批量新建	₽VLAN		
● AC配置	*VLAN ID:	Г	100,101		(1-4094,格式: 1,3-5,7)
基本配置	确定 取消	)			
VLAN					
接口管理					
Wireless LAN A 设备名称: WAC3	AirEngine9700-M1	监控	₿	<del>[+</del> ] 诊断	また 维护
● 配置向导	全局IPv6: OFF				
● AC配置	VLAN VLA	NIF VL	AN Pool		
基本配置	新建删除	批量新建	批量删除	刷新	
VLAN	VLAN ID +	VLAN 描述 🔺			VLAN 类型
接口管理	1	VLAN 0001			commonVlan
ID	100	VLAN 0100			commonVlan
IF	101	VLAN 0101			commonVlan
PNP	10 - #2&				
● AP配置	10 ×3				

# 配置 WAC3 的 GE0/0/1 端口类型及允许通过的 VLAN。

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN Ai 设备名称: WAC3	irEngine9700-M1	- <u>~</u> 监控	な。配置	(┿) (注) (注) (注) (注) (注) (注) (注) (注) (注) (注	<b>4</b> 4 维护	
● 配置向导	物理接口	逻辑接口	管理网口			
<ul><li>● AC配置</li></ul>	接口属性 LLD	P				
基本配置	选择面板上的接     [	]进行配置 (Eth	n-Trunk接口也早	可点击紫色圆圈进行	亍选中,或 点此 进行新疆	建。)
VLAN		2 4	6 0	10 12		6
接口管理						
IP	0					
● AP配置		1 3	5 7	9 11		5
<ul> <li>安全管理</li> </ul>		Up 🗋 Do	wn 💼 Sł	nutdown		
QoS	恢复默认配置					
● 扩展业务	*接囗名称:		GigabitEtherne	et0/0/1		
• 可靠性配置	接口状态:		ON			
	链路类型:	2	Trunk	*		
	允许通过VLAN(Tagg	ed): 3	100,101			
	高级 🕑					
	4 确定 取消					

# 创建 Vlanif100 接口,并配置接口 IP 地址。

# 选择 "配置 > AC 配置 > VLAN",选择 "VLANIF" 选项卡,点击"新建"。



Wireless LAN 设备名称: WAC3	AirEngine9700-M1	监控	<b>夺</b> 配置	(┿) 诊断	<b>↓↓</b> 维护
● 配置向导	全局IPv6: OFF				
● AC配置	VLAN VL	ANIF V	LAN Pool		
基本配置	新建 删除	刷新			
VLAN	接□名称▲	连接	狀态 🔺		
接口管理	Vlanif1	• 7	下可用		
IP	10 ▼ 共1条				

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

Wireless LAN 设备名称: WAC3	AirEngine9700-M1	监控	な。配置	<del>[+]</del> 诊断	<b> </b> 维	↓↓ E护			
● 配置向导	AC配置 > VLAN > V	/LANIF > 新建\	/LANIF						
● AC配置	*VLAN ID:	Г	100						
基本配置	MTU (bytes):		1500						
VLAN	管理接口:	(	OFF	0					
接口管理	IP地址格式:		Pv4	IPv6					
IP	IPv4地址配置								_
● AP配置	主IP地址/掩码:	L	10 , 23	, 100 , 3	/ 255	. 255	. 255	. 0	
● 安全管理	从IP地址/掩码:	9	)添加						
• QoS					1				×
● 扩展业务	高级 💿								
● 可靠性配置	确定取消								



Wireless LAN # 设备名称: WAC3	AirEngine9700-M1	<u></u> 监控	<b>袋</b> 配置	(┿) ()))	维护
● 配置向导	全局IPv6: OFF				
● AC配置	VLAN VLAN	NIF VLAN	N Pool		
基本配置	新建删除	刷新			
VLAN	──接□名称 ▲	连接状态	ž 🔺	IPv4地址/掩码 🔺	
按口答理	Vlanif1	● 不可用	₿		
按口皆垤	Vlanif100	●可用		10.23.100.3/255.2	255.255.0
IP					

步骤 4 配置 NCE 与 WAC3 网络互通

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

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

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

# 配置 WAC3 的静态路由,确保 NCE 与 WAC3 之间网络互通。

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



Wireless LAN 设备名称: WAC3	AirEngine9700-M1		なる	<b>主</b> 诊断	<b>┃↓↓</b> 维护
▶ 配置向导	DHCP地址池	DHCP中继	NAT 3	路由	DNS
● AC配置	→路由表				
基本配置 4	↓ 静态路由配置表				
VLAN	新建删除	刷新			
接口管理	目的IP地址 🔺	子网掩码		下一跳。	
<b>2</b> IP					

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

AC配置 > IP > 路由 > 新建静态	拍		
*目的IP地址:	0.0.0.	*子网掩码:	0.0.0.0
下—跳:	10 . 23 . 100 . 254 🕜	出接口:	Vlanif100 X
优先级:		描述:	
確定 取消			
AC配置 > IP > 路由 > 新建静态影	語		
AC配置 > IP > 路由 > 新建静态3 *目的IP地址:	172 , 21 , 39 , 88	• 子网)电码:	255 . 255 . 255 . 255
AC配置 > IP > 路由 > 新建静态J - 目的IP地址: 下一跳:	172 . 21 . 39 . 88 10 . 23 . 100 . 254 <b>€</b>	• 子网触码: 出線口:	255 , 255 , 255 , 255 Vlanif100
AC配置 > IP > 因由 > 新建静态3 * 目的IP地址: 下一號: 优先级:	172 , 21 , 39 , 88 10 , 23 , 100 , 254	● 子闷)触码: 出缘囗: 描述:	255 . 255 . 255 Vlanif100 X

## # 配置完成后,查看静态路由如下所示。



Wireless LAN / 设备名称: WAC3	AirEngine9700-M1	监控		↓↓	
● 配置向导	DHCP地址池	DHCP中继	NAT 路	d DNS	
● AC配置	→路由表				
基本配置	↓ 静态路由配置表				
VLAN	新建删除	刷新			
接口管理	目的IP地址	子网掩码	下一跳。	出接□▲	优先级
IP	0.0.0	0.0.0.0	10.23.100.2	54 Vlanif100	60
<ul><li>● AP配置</li></ul>	172.21.39.88	255.255.255.25	5 10.23.100.2	54 Vlanif100	60
● 安全管理	10 💌 共2条				

## 步骤 5 配置 WAC3 为云模式

# 配置 WAC3 为云模式,并指定 NCE 的 IP 地址及端口。

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

$\checkmark$	-	C	7	×
Ŕ	☆			:
中文 🔻 传统模式 🔻	2 ac	lmin	G	
自动保存: 定时保存 伊 云模式	0	?	۴	

# 在弹出的对话框中点击"确定"按钮,如下所示。

确认		×
0	是否切换到云模式?	
	确定取消	



# WAC 切换为"云模式"后,AP 的认证模式会自动切换为 SN 认证,点击"确定"即可,如 下所示。

截告		×
	认证模式切换为SN认证,此类AP配置可能会丢 失。	
	确定	

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

# 配置云化管理的相关参数。

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

Wireless LAN Air 设备名称: WAC3	Engine9700-M1	「 「 监控	なる	🕂 <sub>诊断</sub> 1	<b>***</b> 维护
<b>2</b> ⊙ AC维护	控制器配置				
License管理	主动向注册中心查询:				
设备重启					
特征库升级	云管理控制器配置		-		-
Web文件更新	自动获取地址:		OFF		
日志管理	*地址形式:				
告警&事件	* IP:	4	172 . 21 .	39 , 88	
管理员	* 靖山号:		10020		
系统管理			Viaini 100		
3 云化管理					
部件电子标签					

# 测试 WAC3 与 NCE 的网络连通性。

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 。 设备名称: WAC3	AirEngine9700-M1 监控	な。配置	<b>主</b> 诊断	<b>は</b> 维护	2
智能诊断	1 通过使用Ping工具,用户可以	\检查指定IP地址或主机	名的设备是否词	可达,测试网	络连接是否出现故障。
一键信息采集	*IP地址/主机3 IPv4 1	172.21.39.88		0	
无线报文头捕获	<b>4</b> 开始				
Ping	PING 172.21.39.88: 56 da	ta bytes,			
Trace Route	Reply from 172.21.39.88: Reply from 172.21.39.88:	bytes=56 Sequence= bytes=56 Sequence=	=1 ttl=62 time =2 ttl=62 time	=1 ms =3 ms	
AAA Test	Reply from 172.21.39.88: Reply from 172.21.39.88:	bytes=56 Sequence= bvtes=56 Sequence=	=3 ttl=62 time =4 ttl=62 time	=1 ms =1 ms	
RF-Ping	Reply from 172.21.39.88:	bytes=56 Sequence=	=5 ttl=62 time	=1 ms	
AP-Ping	172.21.39.88 ping stat	istics			
空口环境检测	5 packet(s) transmitted 5 packet(s) received				
Trace Objects	0.00% packet loss round-trip min/avg/max	= 1/1/3 ms			
Station Trace					
一键配置检查					

## 步骤 6 配置 NCE 中纳管 WAC3 设备

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

		配置	准入	监控	维护	系统
iMaster NCE-Campus 此页面的仪表盘功能,洞察全网数据状态与趋势哦。	<ul> <li>读计</li> <li>益点</li> <li>送給</li> <li>设备</li> <li>● 基础</li> <li>物理</li> <li>链路</li> <li>网络</li> </ul>	新			維护	<b>系统</b>
	模板	反管理				



iMaster NCE-Camp	JS	设计	配置	准入	监控	维护	系統
/ 站点敏捷部署 / 站点管理							
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-WAC						
位置:	39.904053, 116.40412	®					
设备类型:	🗆 AP 🗆 AR 🗆 FW 🗹 LSW 🗌 N	e 🗆 olt 🗆 onu 🗹 wa	С				
更多 ~							
2 站点配置 ^							
* 配置模式:	默认 配置文件 ①						
* 配置源类型:	默认配置 从已有的站点克隆	Ł					
3 添加设备 ^							
通过型号添加	通过ESN添加 删除 选择	已有设备					
■ 名称	设备型号	ESN			设备类型	틷	
						13	2有记:

#### # 在 WAC3 上查询设备的 ESN 编号。

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

Wireless LAN A 设备名称: WAC3	irEngine9700-M1	监控	配置		<mark>≹↓</mark> 维护
● AC维护 License管理	1) 激活license文件分为 License文件信息	可以下两种情况	: 一种是新购买设备	的用户需要	同时申请购买license,
设备重启	设备ESN:		102257532207	]	
特征库升级	License文件ESN:		102257532207		
Web文件更新	License文件状态:		演示		
日志管理	License文件有效期: 撤销 加载		剩余102天		
告警&事件	查看帮助				

# 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。



iMaster NCE-Campus		设计 配置	准入 监控	维护	系统
设计 / 站点敏捷部署 / 设备管理		☐ 站点敏捷部署			
<b>设备管理</b> 管理设置		站点管理			
设备组		设备管理		☆	
		⊕ 基础网络设计			
组织: 全部 ~	● 可以在系统 > 系统管理 > License管理查看	物理拓扑			
请输入站点		链路管理			
	辺線条件 辺境	网络规划导入			
⑥ 未加入站点 0	済輸入关键字 ○	网络设置			
① 已加入站点 0		模板管理			- <del>2</del> 2 A
HCIP-WAC     0	■ 名称 ▼ ESN ▼				用巴 ↓ 没有记录。
<ul><li>1/1 - ()</li></ul>					
	更多操作    导出	切换站点	删除	设备	添加设备
角色 🗢	站点 设备型号 ♦		操作		手动添加
没有记录。					批量导入
					自动扫描

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



ne ineio		
设备组		
手动添加		
* 协议类型:	设备通过NETCONF协议向控制器发出纳管 请求	控制膨利用SNMP协议向设备发出纳管请求
	NETCONF协议	SNMP协议
<ul> <li>当设备名称符:</li> <li>站点:</li> </ul>	合设备命名规则时,控制器将下发设备名称到设	备并更新设备名称,否则不下发。(设备命名规则为英文、数 
模式:	设备型号 ESN	
*设备信息:	增加翻除	

# 在弹出的页面中,按照以下参数进行配置,点击"确定"。

* 设备信息:	增加	删除		
	类型:	WAC	型号:	AirEngine9700-M1
	数量:	1	角色:	WAC
				取消 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"。

HCIP-WAC							
设备型号 ESN							
增加 删除							
名称	ESN	角色	① 描述	类型	设备型号	性能	③ 操作
WAC3	102257532207	WAC ~	HCIP	WAC	AirEngine9700-M1		
						[	取消 确定

# 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。



组织: <b>全部</b>	$\sim$	<ul> <li>可以在系统 &gt; 系统管理</li> </ul>	里 > License管理查看设备对应Licen	se系列的使用量和状态。	
请输入站点	Q		-		
◇ 全部设备	1	文 过滤条件 过滤			
@ 未加入站点	0	凄‰ λ 关键字 ○			
▲ 已加入站点	1		ECN 🌧	<del>11×</del> ▲	<b>4</b> 4
HCIP-WAC	1		102257532207		用已

#### 步骤 7 配置 DHCP 服务器

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

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

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

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

步骤 8 配置 AP 在 WAC3 中上线

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

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 设备名称: WAC3	AirEngine9700-M1	监控	☆ 配置	<del>[]</del> 诊断	维护	
● 配置向导	AC基本信息	AC间漫游	Navi-AC			
<ul><li>● AC配置</li></ul>	*AC源地址IP类型:		● IPv4 ◯ II	Pv6 O IPv	4&IPv6	
基本配置	*AC源地址:	0	• VLANIF	DoopBack	○ IP地址	
VLAN					2 3 0	
接口管理			接口	IPv4地址	IPv6地址	×
IP		8	Vlanif100	10.23.100.3	;	
PNP	AP数据缓存:		OFF			
● AP配置	AP认证方式:	4	SN认证		添加AP	
● 安全管理	无线用户IPv6业务:		OFF			
QoS	高级 🕑					
● 扩展业务	应用					

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

高级 🕤			
↓ CAPWAP链路配置			
~ AC - AP			
AC到AP的CAPWAP管理报文优先级:	7	AP到AC的CAPWAP管理报文优先级:	7
允许AP以预置证书与AC进行DTLS会话:		允许AP以不认证方式与AC进行DTLS 会话:	
AC-AP间控制隧道DTLS加密:	自动	AC-AP间数据隧道DTLS加密:	OFF ?
*AC-AP间DTLS加密预共享密钥:	•••••	AC-AP间敏感信息加密预共享密钥:	(3)
报文完整性校验:		报文完整性预共享密钥:	•••••
_ AC - AC			
AC-AC间控制隧道DTLS加密:	自动	AC-AC间数据隧道DTLS加密:	OFF
*AC-AC间DTLS加密预共享密钥:	••••••	AC-AC间敏感信息加密预共享密钥:	
CAPWAP心跳检测时间间隔(秒):	25	CAPWAP心翻检测次数:	6

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



配置密钥	×
1 为提高系统安全性,请完成如下配置。	
AP帐号	
1为提高访问AP的安全性,请配置AP的用户名和密码,同时该配置属于全局配置,对所有AP有效。	
*用户名: admin *密码: •••••••	•
离线VAP	
↑ AP离线时会发出管理SSID,便于管理员使用无线连接AP,为保证连接的安全性,配置连接管理SSID的密钥。	
* 离线VAP密钥: ④	
确定取消	

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

● 可以在系统 > 系统管理 > License管理查看设备对应License系列的使用量和状态。								
文 过滤条件 过滤								
请输入关键字 Q								
□ 名称 ◆	ESN 🗢	状态 ◆	角色 🗢					
🗆 🔟 WAC3	102257532207	● 告答	WAC					
共1条								

## # 发现有三台未被纳管的设备,同时选中三台设备,点击"修复"。

				基本信息 位	置	工具	资源	故障告警
	AP列表							
(	<b>7</b> . A	选条件						
[	解約	將						
Þ	~	名称 ⇔	状态 ⇔	异常原因	ESN \$			型弓 🗇
	<u>~</u>	2102353VUR10N5119363		●未纳管	210235	3VUR10N511	9363	AirEngine5761-11
	~	2102353VUR10N5119339		●未纳管	210235	3VUR10N511	9339	AirEngine5761-11
	~	2102353VUR10N5119370		●未纳管	210235	3VUR10N511	9370	AirEngine5761-11
3	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	Q				
站点 🗢	描述 🗢	类型 ⇔					
HCIP-WAC		WAC,LSW					
共1条		10 🗸 条/页 🤇 🌘					
		取消	角定				

# 提示三台设备均已修复成功,正常被 NCE 纳管。



结果		×
设备名称	结果	原因
2102353VUR10N5119363	成功	
2102353VUR10N5119339	成功	
2102353VUR10N5119370	成功	
共3条		< 1/1 ↓ )> 确定

# 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"。

				基本	鶮(	立置	耳具	资源	故障告警	
	AP列	表								
	<b>7</b> , 7	<del>选条件</del>								
	解約	<b>邦</b> 修复								
Þ		名称 ⇔	状态 🗢	异常原因	ESN \$		1	型号 ◊	MAC地址	运行状态
		2102353VUR10N5119363	● 正常		2102353VU	JR10N511936	53	AirEngine5761-11	9C-B2-E8-2D-54-	10 normal
		2102353VUR10N5119339	●正常		2102353VU	JR10N511933	39	AirEngine5761-11	9C-B2-E8-2D-51-	10 normal
		2102353VUR10N5119370	●正常		2102353VU	JR10N511937	70	AirEngine5761-11	9C-B2-E8-2D-54-	F0 normal
	共3条									

# 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。


<b>第10/贝</b>	第1	07页
--------------	----	-----

输入关键字    〇				更多操作	<b>导出</b> 切换站点	删除设
名称 ⇔	ESN ¢	状态 ◊	角色 🗘	站点	设备型号 ⇔	操作
2102353VUR10N511	2102353VUR10N5119339	• 正常	AP	HCIP-WAC	AirEngine5761-11	1
2102353VUR10N511	2102353VUR10N5119363	• 正常	AP	HCIP-WAC	AirEngine5761-11	11
2102353VUR10N511	2102353VUR10N5119370	• 正常	AP	HCIP-WAC	AirEngine5761-11	1 II
🔟 WAC3	102257532207	● 告答	WAC	HCIP-WAC	AirEngine9700-M1	11
Ş						20 ~
多改设备			(	$\overline{\times}$		
名称:		AP1				
描述:		•				
资产编号:						
ESN:		2102353VUR10	N5119370			
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:		V200R021C00S	PC200			
		取消	确定			
AP1、AP2、AP	3 的名称修改	完成后,如下	所示。			

义 过路条件 过渡						
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	1
🗆 💿 AP2	2102353VUR10N5119363	● 正常	AP	HCIP-WAC	AirEngine5761-11	∥ Ш
🗆 😨 АРЗ	2102353VUR10N5119339	● 正常	AP	HCIP-WAC	AirEngine5761-11	∥ Ш
🗆 🔟 WAC3	102257532207	● 告警	WAC	HCIP-WAC	AirEngine9700-M1	∥ Ш
共4条						20 ∨ 祭/页

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



Wireless LAN 设备名称: WAC3	AirEngine9700-M1	监控	<b>谷</b> 配置	<b>(十</b> ) 诊断	<b>↓↓</b> 维护
● 配置向导	AP组 静态	<b>灸载均衡组</b>			
● AC配置	修改新建	删除	刷新		
● AP配置	□ 组名称 ▲	VAF	模板		
AP组配置	default				
AP配置	20 ▼ 共1条				
Wireless LAN 设备名称: WAC3	AirEngine9700-M1	监控	<b>谷</b> 配置	<b>王</b> 诊断	<b>   </b> 维护
● 配置向导	AP配置 > AP组配置	> AP组 > 新建	MP组		
● AC配置	* ΔD组 <i>字</i> 称·	an-	aroun1		
● AP配置	确完 取消	ap-ç	Joapi		
AP组配置	WHAT 14X/H				
AP配置					

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

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN / 设备名称: WAC3	AirEngine9700-M1	监控	ないので、	<b>(十</b> ) 诊断	<b>{ } } </b> 维护
● 配置向导	AP信息	AP白名单	AP黑名单	AP邻居关系	AP设备类型
● AC配置	↓ AP列表				
<ul><li>● AP配置</li></ul>	🕕 点击AP ID3	列可进入AP的个性们	北配置页面。		
AP组配置	修改AP配置	添加	换删除	加入黑名单	闪灯  清空所有AP
AP配置	✓ AP ID ▲	AP MAC地址 9cb2-e82d-5410	AP名称 🔺	AP组 -	IP地址 10.23.100.45
射频规划/调优	<ul><li>✓ Ø20 1</li></ul>	9cb2-e82d-54f0	AP1	default	10.23.100.174
分支AP组配置	✓ Ø 2	9cb2-e82d-5110	AP3	default	10.23.100.38
模板管理	10 - 共3	条			
Wireless LAN 设备名称: WAC3	AirEngine9700-M1	监控	<b>读</b> 配置	<b>十</b> 诊断	<b>    </b> 维护
● 配置向导	AP配置 > AP配置	置 > AP信息 > 修改	AP		
● AC配置	AP组:	ap-gro	pup1	-	
● AP配置	AC地址列表:	<table-cell-rows> 添加</table-cell-rows>			
AP组配置				×	
AP配置	已选AP列表				
射频规划/调优	AP ID + A	P MAC地址	AP名称	AP组 ▲	IP地址获取方式
分支AP组配置	0 90	cb2-e82d-5410	AP2	default	- none -
描坛答理	1 90	:b2-e82d-54f0	AP1	default	- none -
	2 90	b2-e82d-5110	AP3	default	- none -
● 安全管理					
QoS	10 ▼ 共3条	R.			
● 扩展业务	确定取	消			

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



Wireless LAN A 设备名称: WAC3	irEngine9700-M1	监控	ないので、	☐→ 诊断	<b>\$</b> } 维护
③ 配置向导	AP信息	AP白名单	AP黑名单	AP邻居关系	AP设备类型
● AC配置	<b>↓</b> AP列表				
<ul> <li>● AP配置</li> </ul>	<ol> <li>点击AP ID歹</li> </ol>	可进入AP的个性(	七配置页面。		
AP组配置	修改AP配置	添加 春	一般	加入黑名单	内灯 清空所有AP
AP配置	AP ID -	9cb2-e82d-541	AP名称 * 0 AP2	AP组 Ap细 Ap-group1	10.23.100.45
射频规划/调优	<b>(1</b> )	9cb2-e82d-54f0	) AP1	ap-group1	10.23.100.174
分支AP组配置	2	9cb2-e82d-511	0 AP3	ap-group1	10.23.100.38
模板管理	10 💌 共35	条			

#### 步骤 9 配置无线业务(WAC3)

# 此步骤的具体配置与 1.2.2 步骤 7 类似,不再赘述。

#### 步骤 10 配置 DHCP 服务器

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

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

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

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

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

```
[SW-Core] display ip pool interface Vlanif200 usedPool-name: Vlanif200Pool-No: 2Lease: 1 Days 0 Hours 0 MinutesDomain-name: -Option-code: 148Option-subcode: --Option-type: ascii
```



Option-value domain=172.21.39.	: "agilemode=agile-cloud;agilemanage-mode=ip;agilemanage- 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 addres	ss 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 a	s follows:
DHCP : mac-a	ddress PPPoE : mac-address
IPSec : user-id/p	ortnumber/vrf PPP : interface index
L2TP : cpu-slot	/session-id SSL-VPN : user-id/session-id
Index	IP Client-ID Type Left Status
221 <b>10.23.2</b>	00.222 9cb2-e82d-5230 DHCP 86400 Used

## 步骤 11 配置 NCE 纳管 AP5

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



Wireless LAN Ain 设备名称: AP5	Engine5761-11	 首页	日本     日本       诊断     维护
基本信息	设备名称:		AP5
告警&事件	设备型号:		AirEngine5761-11
日志	MAC地址:		9cb2-e82d-5230
管理员记录	序列号:		2102353VUR10N5119348
恢复出厂配置	当前版本:		V200R021C00SPC200
WMI	重启后软件版本:		flash:/AirEngineX761-V200R021C00SPC200.cc
	当前配置文件:		flash:/vrpcfg.zip

# 在 NCE 主菜单中选择"设计 > 站点管理",新建站点"HCIP-AP",设备类型勾选

"AP"。添加设备选择"通过型号添加",设备类型选择"AP",设备型号选择

"AirEngine5761-11",数量为 1,角色选择"AP",点击"确定"。

	设计	配置	准入	监控	维护	系统
iMaster NCE-Campus 此页面的仪表盘功能,洞察全网数据状态与趋势哦。	<ul> <li>○ 站点</li> <li>这点</li> <li>设备</li> <li>● 基础</li> <li>物理</li> <li>链路</li> <li>网络</li> <li>横椒</li> </ul>	1994 (1994)				
	13610					



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。
● 站点基本信息 ∧
* 站点名称: HCIP-AP
位置: 39.904053, 116.40412 💿
设备类型:
更多 ~
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 角色
· 设备类型: AP · · · · · · · · · · · · · · · · · ·
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"。

6	添加设备 へ							
	通过型号添加 通过ESN添加	删除 选择已有设	<b>X</b>					
	□ 名称	设臵型号	ESN	设备类型	角色	⑦ 描述	性能	① 操作
	AP5	AirEngine5761-11	2102353VUR10N5119348	AP	AP	- HCIP-AP5	1G	~ II
							取消	应用并部署 确定

## # 选择"设计 > 设备管理",可以看到 AP5 已经被正常纳管。

<b>青输入关键字</b>	Q			
□ 名称 ♦	ESN 🗢	状态 ♦	角色 🗢	站点
🗆 💿 AP1	2102353VUR10N5119370	● 正常	AP	HCIP-WAC
🗆 🔟 AP2	2102353VUR10N5119363	●正常	AP	HCIP-WAC
🗆 💿 AP3	2102353VUR10N5119339	●正常	AP	HCIP-WAC
□	2102353VUR10N5119348	●正常	AP	HCIP-AP
🗆 🔟 WAC3	102257532207	● 告警	WAC	HCIP-WAC



#### 步骤 12 配置无线业务 (AP5)

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

🝕 iMaster NCE-Campus		设计 1 配置 准入 监	腔 维护 系统
配置 / 物理网络 / 站点配置			
■2 站点:HCIP-AP ~	组织: 站点类型: AP	站点模板: 告警设备/全部	设备: 1/1
3 站点配置 路由域编排			
站点 ▼ ◆ 快速配置 ● 投資系統配置 ● 投資系統配置 ● 投資登录配置 ● 理VLAN CLI	<u>ズAP</u> 区域 & SSID 元线安全		AP
AP 🍝	* 国家/地区: 中国 SSID名称	~ 应用	WLAN安全策略 没有记录。

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



ZAP	
区域 & SSID 无线安全	
* SSID名称:	ap5
数据转发模式:	直接转发 Soft GRE
全局DHCP获取地址:	
	去使能时,AP根据业务VLAN对终端流量进行转发,若AP上配置对应的VLANIF 址池;否则有上游设备网关为终端分配地址,需在 <b>配置 &gt; 物理网络 &gt; 站点配置</b>
VLAN:	201
安全认证	
WLAN安全策略:	• 开放网络 Open ~
	● 半开放网络 PSK/PPSK/SAE/PSK-SAE认证 ~
	• 安全网络 802.1X认证
密钥类型:	PSK PPSK SAE PSK-SAE
加密方式:	WPA2 ~
加密算法:	AES ~
*密钥:	✓ 设置
开启MAC上报:	

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

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



全局DHCP	子网 接口 IPv6业务 Mesh IPsec VPN AP安装位置 LED灯
云AP接口	中心AP接口 分布式AP接口
接口选择	
配置类型:	● 全局配置 ○ 个性化配置
● 在全局	配置的面板中对各接口配置的参数将应用于站点中匹配此面板类型的所有设备。在同一个
	+
	光口
添加面板	×
设备类型:	AirEngine5761-11 v
预览:	0
	取消 确定

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



云AP接口中心人	AP接口 分布式AP接口
接口选择	
配置类型:	● 全局配置 ○ 个性化配置
● 在全局配置的词	面板中对各接口配置的参数将应用于站点中匹配此面板类型的所有设备。在同一个面板中,
AP100EC, AP10	50DN-S, AP163, AP300EC, AP3050DE, AP310, AP330, AP363, AP365
	+
	凸 已选择 ↑ 上行口
接口配置	
接口名称:	GigabitEthernet0/0/0
接口属性:	电口
接口描述:	
LLDP:	
场景:	● WAN
* 缺省VLAN:	1
* 允许通过的VLAN:	201 每个设备最多可配置64个VLAN。

# 4.3 结果验证

# 4.3.1 在 WAC3 上检查云管理信息

# 选择"维护 > AC 维护 > 云化管理",可以查看云管理控制器配置信息。



Wireless LAN A 设备名称: WAC3	irEngine9700-M1	监控	なる	<del>[+]</del> 诊断	<b>***</b> 维护
⊙ AC维护	控制器配置				
License管理	主动向注册中心查询:				
设备重启					
特征库升级	云管理控制器配置				
Web文件更新	自动获取地址:		OFF		
日志管理	*地址形式:		🔾 URL 💿 II	P	
告警&事件	* IP:		172 . 21	, 39 , 88	
管理员	*端口号:		10020		
Z/ASTR	源接口:		Vlanif100		×
<u></u>	应用				
云化管理					
部件电子标签					

# 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> <b>ipconfig</b>
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
子网掩码
默认网关
C:\Users\admin> <b>ping 10.23.101.254</b>
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> <b>ipconfig</b>
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: <b>10.23.201.133</b>
子网掩码
默认网关
C:\Users\admin> <b>ping 10.23.201.254</b>
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。

文 过滤条件 过	过滤				
请输入关键字	Q				更多操作
□ 名称 🔷	ESN \$	状态 ⇔	角色 🗢	站点	设备型号 ≑
🗆 💿 AP1	2102353VUR10N5119370	● 正常	AP	HCIP-WAC	AirEngine5761-11
🗆 💿 AP2	2102353VUR10N5119363	● 正常	AP	HCIP-WAC	AirEngine5761-11
🗆 💿 AP3	2102353VUR10N5119339	● 正常	AP	HCIP-WAC	AirEngine5761-11
□	2102353VUR10N5119348	● 正常	AP	HCIP-AP	AirEngine5761-11
WAC3	102257532207	● 正常	WAC	HCIP-WAC	AirEngine9700-M1
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。



LAN概览			当前告警					
站点间			历史告警					
站点			事件					
终端		☆	屏蔽告警					
设备360			告警通知					
WAC组			告警设置					
终端监控								
<ul> <li>Ⅰ (VN / 终端 :</li> <li>● 终端数据通过</li> <li>用户在线时长</li> </ul>	HCIP-AI 网络设备收集	P , 默认展现1	~ 0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9	也用户。
<ul> <li><b>i</b> / VN / 终端:</li> <li>终端数据通过</li> <li>用户在线时长</li> <li>人</li> <li>3</li> </ul>	HCIP-AI	P , 默认展现1	○ 0分钟内上报的用F	〕记录, 如需查	看7天内	历史用户,	清点击 历9	也用户。
<ul> <li>b点 / VN / 终端:</li> <li>终端数据通过</li> <li>用户在线时长</li> <li>入</li> <li>2</li> <li>1</li> </ul>	HCIP-AI	P , 默认展现1	0分钟内上报的用户	⊐记录, 如需查	看7天内	历史用户,	清点击 历9	也用户。
<ul> <li>         は点 / VN / 终端:         <ul> <li></li></ul></li></ul>	HCIP-AI 网络设备收集	P , 默认展现1 <sup>()</sup> 小时	○ <	<sup>〕</sup> 记录, 如需查 4-6小时	看7天内	历史用户, 6-8小时	<b>请点击 历</b> 9	<b>也用户。</b>
<ul> <li>4. / VN / 终端:</li> <li>9. 终端数据通过</li> <li>1. (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</li></ul>	HCIP-A 网络设备收集 1-2 支持6万条数排	P , 默认展现1 <sup>2小时</sup> 器展示,导出	✓ 0分钟内上报的用户 2-4小时 列表请到 监控 > 打	□记录, 如需查 4-6小时 限表 > 统计分析	看7天内 〔 > 报表	历史用户, 5 6-8小时 定制 创建攻	请点击 历史 84 北应的报表(	<b> 日 日 一 。 </b>

# 4.4 配置参考

# 4.4.1 WAC3 配置

Software Version V200R021C00SPC100 # sysname WAC3 #



```
http secure-server ssl-policy default_policy
http secure-server server-source -i MEth0/0/1
http server enable
#
vlan batch 100 to 101
#
stp enable
#
management-port isolate enable
management-plane isolate enable
#
interface Vlanif1
ip address dhcp-alloc unicast
#
interface Vlanif100
ip address 10.23.100.3 255.255.255.0
#
interface MEth0/0/1
ip address 172.21.39.6 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif100 10.23.100.254
ip route-static 172.21.39.88 255.255.255.255 Vlanif100 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#^UY*(/s.~&jK$vHVY-Y>0lRL!``@k7w#`Y~%R]>V%^%#
capwap dtls inter-controller psk %^%#Cl;<X"Hg5BWF8dX-b{;%,~)l'W#{<.kZk2-%S%#7%^%#
capwap message-integrity psk %^%#*JU'.,fC&0;PVm8[+ur-Pfy:H(T}<)iqVr,9WM;X%^%#
capwap sensitive-info psk %^%#\MPI4+"|NH|,>g0C6_GWT=p10ACVx9YiO.YHYg>*%^%#
capwap inter-controller sensitive-info psk %^%#jcaO([qQSUSvB;Z\PJ25DWDr-qvP!O-J6z/4DSH!%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
cloud-mng controller ip-address 172.21.39.88 port 10020 source-interface Vlanif100
#
wlan
temporary-management psk %^%#NA'y2_qi*04'/tE>zQU-X5ts#{6r]"q5eUpf4GJ%^%#
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

ssid-profile name default ssid-profile name 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-profile name default

air-scan-profile name default rrm-profile name default radio-2g-profile name default radio-5g-profile name default

wids-profile name default wireless-access-specification

ap auth-mode sn-auth ap-group name default ap-group name ap-group1

radio 0

radio 1

ap-name AP3

ap-name AP1 ap-group ap-group1

ap-name AP2 ap-group ap-group1

provision-ap

# return

ap-group ap-group1

port-link-profile name default

regulatory-domain-profile domain1

ap-id 0 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339

ap-id 1 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370

ap-id 2 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363

vap-profile wlan-net wlan 1

vap-profile wlan-net wlan 1

ssid 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
mesh-handover-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
wids-spoof-profile name default
wids-whitelist-profile name default
ap-system-profile name default
wired-port-profile name default
```

第122页



#### 第123页

## 4.4.2 AP5 配置

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



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



port link-type trunk

port link-type trunk

#

#

shutdown

```
interface MultiGE0/0/3
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
interface MultiGE0/0/4
interface MultiGE0/0/5
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 切换成云模式,请思考,除了 DHCP 方式外还有什么方 式可以将 FIT AP 切换为云模式?

参考答案:

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

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

通过注册中心获取:优先级最低。

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



# **5** 802.1X 认证实验

# 5.1 实验介绍

## 5.1.1 关于本实验

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

## 5.1.2 实验目的

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

## 5.1.3 实验组网介绍





# 5.1.4 实验规划

设备	端口	端口类型	VLAN参数
	MultiGE0/0/1	Trunk	PVID:1
			Allow-pass: VLAN 100 101
SW-Core	MultiGE0/0/9	Trunk	PVID:1
	WattiGE0/0/5	Trunk	Allow-pass: VLAN 100 101
	MultiGE0/0/4	Access	PVID: 99
		<b>-</b> -	PVID:1
	MultiGE0/0/9	Trunk	Allow-pass: VLAN 100 101
		Tarada	PVID:100
	Multige0/0/1	Irunk	Allow-pass: VLAN 100 101
SW-ACCESS			PVID:100
	MultiGE0/0/2	Trunk	Allow-pass: VLAN 100 101
			PVID:100
	MultiGE0/0/3	типк	Allow-pass: VLAN 100 101
WAC1 GE		Turnel	PVID:1
	GEU/U/ I	Irunk	Allow-pass: VLAN 100 101

#### 表5-1 VLAN 规划

## 表5-2 IP 地址规划

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



#### 表5-3 WLAN 业务参数规划

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



## 5.2 实验任务配置

## 5.2.1 配置思路

1.配置基础网络,确保网络互通。

2.配置 AP 上线。

3.配置 NCE 与 WAC1 网络互通。

4.在 WAC1 上配置 802.1X 认证。

5.配置 WLAN 基本业务。

6.在 NCE 服务器上配置 802.1X 认证。

7.验证 802.1X 准入认证。

#### 5.2.2 配置步骤

- 步骤 1 配置基础网络和 AP 上线
  - # 请参考 1.2.2 步骤 1~1.2.2 步骤 6,此处不再赘述。

#### 步骤 2 配置 NCE 与 WAC1 之间网络互通

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

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

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

# 配置 WAC1 的静态路由,确保 NCE 与 WAC1 之间网络互通。

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



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	 <sup>监控</sup> 1	<b>袋</b> 配置	➡	<b>   </b> 维护
● 配置向导	DHCP地址池	DHCP中继	NAT 3	路由	DNS
● AC配置	→路由表				
基本配置 4	↓ 静态路由配置表				
VLAN 6	新建删除	刷新			
接口管理	目的IP地址 🔺			子网掩	码 -
<b>2</b> IP					

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

AC配置 > IP > 路由 > 新建静态	路由		
*目的IP地址:	0 , 0 , 0 , 0	*子网掩码:	0.0.0.0
下—跳:	10 . 23 . 100 . 254	出接口:	Vlanif100 X
优先级:		描述:	
確定 取消			
AC配置 > IP > 路由 > 新建静态	路由		
*目的IP地址:	172 . 21 . 39 . 88	*子网施码:	255 . 255 . 255 . 255
下一跳:	10 , 23 , 100 , 254 🕜	出接口:	Vlanif100 X
优先级:		描述:	
確定 取消			

#### # 配置完成后,查看静态路由如下所示。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	✿ 記置	(十) 诊断	<b>1</b> 1 维护	
● 配置向导	DHCP地址地	DHCP中继	NAT	路由	DNS	
● AC配置	→路由表					
基本配置	↓ 静态路由配置表					
VLAN	新建删除	刷新				
接口管理	目的IP地址。	子网掩码。	下一點	K ▲	出接□▲	优先级 🔺
IP	0.0.0.0	0.0.0.0	10.23	.100 <mark>.</mark> 254	Vlanif100	60
● AP配置	172.21.39.88	255.255.255.25	5 10.23	.100.254	Vlanif100	60
● 安全管理	10 🔻 共2条					



步骤 3 配置 802.1X 认证 (WAC1)

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

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

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

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

# 授权服务器模板: 点击"新建", 新建授权服务器模板, 具体细节参见下文。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1 监控	<b>谷</b> 配置		↓↓ 註沪		
● 配置向导	Portal服务器全局设置	RADIUS设置	内置EAP设置	LDAP设置	AD设置	HWTACACS设置
● AC配置	RADIUS全局配置					
● AP配置	NAS IP地址:		. 0			
⊙ 安全管理	发送报文源IP地址:		. 3			
AAA 1	*授权服务器源地址:	所有IP	•			
用户组 2	应用					
自定义应用	RADIUS服务器模板					
ACL 3	新建 删除 刷新					
SSL	模板名称 🔺			模式 ▲		
证书管理	-> 🗌 default			主备模式		
安全防护	5 💌 共1条					
攻击防御	授权服务器模板					
终端识别	新建	清空				
PPSK管理	授权服务器IP地址					

# 新建 "RADIUS 服务器模板"的具体细节请参考如下配置。



新建RADIUS服务器模板				×
*模板名称: 1	radius_huawei			
模式:	<ul> <li>主备模式</li> <li>① 负</li> </ul>	载均衡模式		
NAS IP地址:	指定IP地址	Ŧ		
2	10 , 23 , 100	), 1		
*模板默认共享密钥: 3	Huawei@123	0		
4 新建服务器 删除		IP地址		٩
IP地址 🔺	共享密钥 ▲	认证端口号▲	计费端口号 ▲	
→ 172.21.39.88	**	1812	1813	
5 🔻 共1条			< 1	>
高级 🕑				
	<b>5</b> 确定	取消		



新建服务器配置		×
*IP地址:	IPv4 ▼ 172 , 21 , 39 , 88	
共享密钥:	Huawei@123	
服务器配置 ☑ 认证		
*端口号:	1812	
权重值:	80	
Z 发送报文源IP地址:	○ LoopBack ● VLANIF ○ IP地址	
	Vlanif100 ×	
Virtual-ip:	OFF	
✓ 计费		
*端口号:	1813	
权重值:	80	
3 发送报文源IP地址:	○ LoopBack ● VLANIF ○ IP地址	
	Vlanif100 ×	
Virtual-ip:	OFF	
	4 确定 取消	

# 新建"授权服务器模板"的具体细节请参考如下配置。

新建授权服务器		×
*授权服务器IP地址:	172 . 21 . 39 . 88	
模板名称:	radius_huawei 🔻	
*密钥:	Huawei@123	
	确定取消	





# 建议在 "RADIUS 设置"全部配置完成后,进行全面检查,如下所示。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	wing Ling	な。配置	(十) 诊断	<b>  </b>   维护	-	
• 配置向导	Portal服务器全质	司设置	RADIUS设置	f 内置E/	AP设置	LDAP设置	AD设置
● AC配置	RADIUS全局配置						
● AP配置	NAS IP地址:				0		
⊙ 安全管理	发送报文源IP地址:				0		
AAA	*授权服务器源地址:		所有IP	Ŧ	]		
用户组	应用						
自定义应用	RADIUS服务器模板						
ACL	新建删除	刷新					
SSL	模板名称 🔺					模式 🔺	
	→ 🗌 default					主备模式	
业书管埋 2	→ 🗌 radius_huav	vei				主备模式	
安全防护							
攻击防御	5 🔻 共2条						
终端识别	授权服务器模板	Diter					
PPSK管理	新建    删除	刷新	清空				
0.0-0	授权服务器IP地址	*					
U QOS 3	172.21.39.88						

# 配置 AAA 认证方案模板。

# 选择 "配置 > AP 配置 > 模板管理 > AAA > 认证方案模板" ,点击"新建" ,配置模板 名称为 "radius\_huawei" ,然后点击 "确定" 。



模板管理	
⊞ ┣ 无线业务	新建认证方案模板
田 🔲 认证模板	★模板名称: radius huawei
田 🛃 802.1X模板	
田 🧧 Portal模板	确定取消
王 🛃 MAC接入模板	
🗉 📃 免认证规则模板	
🗉 📮 URL模板	
■ 日 认证方案模板	
⊞ ■授权方案模板	
田 📑 计费方案模板	
🗉 📑 业务方案模板	
田 🚦 802.1X客户端模板	

# 选择 "radius\_huawei" 认证方案模板,配置第一认证模式为 "RADIUS 认证",点击"应用"。

认证方案模板:		展示	模板引用关系		
第一认证模式:	RADIUS认证	T		第二认证模式:	不配置
第三认证模式:	不配置	Ŧ		第四认证模式:	
第五认证模式:		-		第六认证模式:	
第七认证模式:		Ŧ			
应用					

# 配置 AAA 计费方案模板。

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

模板管理	
田 🔁 无线业务	新建计费方案模板
王 📑 认证模板	* 模板名称: scheme1
田 📃 802.1X模板	
田 📮 Portal模板	确定取消
王 📮 MAC接入模板	
🗉 📒 免认证规则模板	
田 🧧 URL模板	
🗉 🚦 认证方案模板	
▶ 10 授权方案模板	
■ ■ 计费方案模板	
⊞ ■ 业务方案模板	
王 📃 802.1X客户端模板	

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



计费方案模板:	scheme1 展示模板引用关系		
计费模式:	RADIUS计费 ▼		
计费形式:	○ 按时长计赛 ● 实时计赛		
*实时计费时间间隔(分钟):	3	实时计费请求无响应最大次数:	3
实时计费失败后策略:	<ul> <li>○ 拒绝用户上线</li> <li>● 允许用户上线</li> </ul>		
开始计费后失败策略:	<ul> <li>拒绝用户上线</li> <li>允许用户上线</li> </ul>		
应用			

#### # 配置 802.1X 模板。

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

模板管理		
田 🦰 无线业务		新建802.1X模板
🗉 📃 认证模板		* 横板 2 称•
🖪 📑 802.1X模板		
🛨 📑 Portal模板		确定取消
🗄 📑 MAC接入樽	板	
🗄 📑 免认证规则	模板	
#选择名称为"。	11 "的 802.1X 模板,配置用户认	证方式为"EAP",然后点击"应用"。
802.1X模板:	d1	展示模板引用关系
● 模板介绍信	.: 通过802.1X接入模板统一管理802.1X	接入相关的所有配置。包括802.1X用户的认证方式、
用户认证方式:		IAP 🕜
高级 🕑		
应用		

# 配置认证模板。

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



模板管理	
⊞无线业务	新建认证模板
■ ■ しい正模板	*模板名称: p1
∃ 🥫 802.1X模板	
🕙 📮 Portal模板	确定取消
Ⅲ ■ MAC接入模板	
🗄 🚦 免认证规则模板	

# 选择名称为 "p1"的认证模板,在其中引用 802.1X 模板 "d1"、RADIUS 服务器模板 "radius\_huawei"、认证方案 "radius\_huawei"、计费方案 "scheme1",如下所示。





模板管理			
⊞ ┣_无线业务	认证方案模板:	2 radius huaw	ei 💌
		-	
🗆 🥫 认证模板		DADUUG) DT	
🖃 🔜 p1	第一认证模式:	RADIUSiXi	•
802.1X模板	第三认证模式:		Ŧ
■ Portal模板			
■ MAC接入模板	第五认证模式:		-
■ 免认证规则模板			
■ RADIUS模板	第七认证模式:		<b>*</b>
■二级计费RADIUS模板			
B HACA模板			
■ LDAP模板			
■ AD模板			
■ HWTACACS模板			
2 授权方案模板			
模板管理			
田   无线业务	计费方案模板: 2	scheme1	▼ (
	计费模式:	RADIUS计费	-
COLLIA (笑似 Dottol 時初	计费形式:	○ 按时长计费 (●	实时计费
		2	
■ 61派汇扣则增振	▲ 关时 日	3	
■ RADIUS模板	实时计费失败后策略:	◯ 拒绝用户上线	● 允许用户上线
I 二级计费RADIUS模板			
I HACA模板	开始计费后失败策略:	● 拒绝用尸上线	○ 允许用户上线
■ LDAP模板			
I AD模板	应用		
HWTACACS模板			
10 认证方案模板			
■ 授权方案模板			
1 日计费方案模板			
■ 业务方案模板			
■ 内置EAP服务器配置			
■ 本地用户配置			

步骤 4 配置无线业务

# 创建名为"wlan-net"的安全模板,并配置安全策略。

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



模板管理					
□ /□无线业务			新建安全模板		
🕀 📑 VAP橋	乾板				
王 📑 SSID	莫板		*模板名称:	wlan-net	
■ ■安全橋	党板				
📑 de	fault		确定 取消	)	
📃 de	fault-wds				
📃 de	fault-mesh				
# 选择 "wl	an-net"安全模板,配	置如下参数,点	、击"应用"。		
安全模板:	wlan-net	展示模板	引用关系		
● 模板介绍(	言息: 配置WLAN安全策略,可以对无线	终端进行身份验证,对用/	户的报文进行加密,保护WI	LAN网络和用户的安全。WL	AN安全策略式
基础配置	高级配置				
🚺 Openi\) 🔃	臣方式存在一定的安全风险,建议采用其	他认证方式。安全级别时	自高到低。		
*安全策略: C	WPA3 WPA2-WPA3	WAPI 💽 WPA2	WPA-WPA2 OWF	PA WEP OWE	OPEN
认证方式:	Dot1x     DPSK	○ PPSK ○ PSK			
加密方式:	• AES AES-TKI	Р 🔿 ТКІР			
应用					

# 创建名为 "wlan-net"的 SSID 模板,并配置 SSID 名称为 "wlan-net"。

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

模板管理		
	新建SSID模板	
団 VAP模板		
■ IBSSID模板	*模板名称:	wlan-net
📑 default		
∃ 🕫 安全模板	确定取消	
∃ <mark>。</mark> 流量模板		

# 选择 "wlan-net" SSID 模板,配置 SSID 名称为 "wlan-net",点击"应用"。


SSID模板:	wlan-net	展示模板引用关系
模板介绍信息: SSI	ID用来指定不同的无线网络。在STA上搜到	素可接入的无线网络时,显示出来的网络名称就是SSID。
基础配置	高级配置	
*SSID名称:	wlan-net	
最大用户数:	64	
应用		

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

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

模板管理	
	新建VAP模板
■ IEVAP使板 ④ IE default	*模板名称: wlan-net
<ul> <li>■ SSID模板</li> <li>■ go全模板</li> </ul>	确定取消

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

VAP模板:	wlan-net 展示模板引用关系		
模板介绍信息: 在VAP	模板下配置各项参数然后在AP组或AP中引用VAP模板,AP上就会生成VAP,VAP用来为STA提供无线	妾入服务。通过配置VAP模板下的	參数,使AP实现为STA
基础配置	高级配置		
使能状态:			
转发模式:	隧道转发 ▼		
指定报文直接转发:	IPv4 😧		
业务VLAN:	● 单个VLAN OVLAN Pool	业务VLAN ID:	101
应用			

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



模板管理			
		*SSID模板:	wlan-net 💌
<ul> <li>□ ■ vArtexx</li> <li>              ■ default      </li> <li>             ■ wlan-net         </li> </ul>		模板介绍信息: SSI	D用来指定不同的无线网络。在STA上搜索可打
	[default]	基础配置	高级配置
	[default]	*SSID名称:	wlan-net
<ul> <li>         •          •          •</li></ul>		最大用户数:	64
<ul> <li>智能应用控制模板</li> <li>UCC模板</li> </ul>		应用	

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



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



模板管理			
		认证模板: p1	× 展示模板引用关系
□ <mark>■</mark> VAP模板			
		模板介绍信息:通过配置认证模板下的	参数 (例如:配置认证模板下绑定的接入模板,确定认证模板的认证方:
	[wlan_ne_]	D . 1/477	其于Portal服务器的MAC性速计证
	[wlan-ne_]	Portali远坝:	2 FOLGING HUMACKEWIL
○ × 土実収	[default]	认证前授权VLAN:	0
章 目认证模板	[default]		
■ 终端黑白名单模板		认证失败授权:	● VLAN ○ 用户组
■ 智能应用控制模板			
■ UCC模板		认业失败授权VLAN:	
団 📕 Hotspot2.0模板		认证失败重认证:	OFF
王 J 攻击防御模板			
CPE隧道模板		认证服务器不可用时授权用户组权限:	×
☑ 🥫 安全模板		认业成切搅权用户组权限:	×
王 🧧 流量模板		计费开始触发时机:	<ul> <li>认证通过</li> <li>认证通过且获取IP</li> </ul>
🗄 📙 终端黑名单模板			
🗄 🧧 终端白名单模板		计费更新触发时机:	✓ 漫游触发 会话更新: OFF
∃ ■ 智能应用控制模板			( ) / 卢自雨彩钟尖
団 SoftGRE模板			
Ⅲ UCC模板			✓ IP地址更新触发
団 ■ 蜂窝网络信息模板			
□ □ 漫游联盟组织标识模板		认证成功推送页面:	- none - 🔍 🔻
☑ III NAI域模板			
田		流量统计:	OFF
■      ■      □     热点运营商域名模板     □			
		应用	
□ □ 坝段指示骗号楔板			

### # 配置 AP 组引用 VAP 模板。

# 选择 "配置 > AP 配置 > AP 组配置",选择 "AP 组"选项卡,点击 "ap-group1",进 入此 AP 组的配置界面。

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	 监控	<b>读</b> 配置	(十) 诊断	\$  } 维护
● 配置向导	AP组 静态	汤载均衡组			
● AC配置	修改新建	删除	刷新		
⊙ AP配置	组名称 ▲	VAP	模板 ▲		射频0模板▲
AP组配署	default				2.4G-default
	ap-group1				2.4G-default
AP配置					
射频规划/调优	20 🔻 共2条				

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



AP配置 > AP组配置 > AP组	
AP组配置: ap-group1 ▼ 查看成员	VAP 模板列表
型示所有模板 配置模型介绍	● 相关配置
■ <b>仁</b> VAP配置	新建 添加 移除 展示模板引用关系
☞ 肩频管理	
🐨 👝 AP	C. BERGHUD
I WIDS	

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

添加VAP模板					
🔂 添加					
* VAP模板名称:	wlan-net 🔻	*WLAN ID: 1	*射频:	0,1 🔻	
高级 🕑					
确定取消					

### # 最后查看 "VAP 模板列表"如下。

VAP 模板列表								
• 相关配置								
新建添加	移除展	宗模板引用关系						
模板名称 ▲	SSID模板 -	认证模板 🔺	安全模板 🔺	WLAN ID *	射频▲	转发模式	业务VLAN ▲	使能状态
wlan-net	wlan-net	p1	wlan-net	1	0	隧道转发	101	●开启
wlan-net	wlan-net	p1	wlan-net	1	1	隧道转发	101	●开启
10 🔻 共2条								

步骤 5 配置 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"。

🔏 iMaster NCE-Campus		设计	配置	准入	监控	维护	系
准入/准入资源/用户管理 1 用户管理 角色管理 黑名单管	查理						
用户 MAC帐号 PPSK 用户操作	印志						
请输入用户组名称    Q	创建用户组						×
2 ⊕ ⊑ ⊑ ≞ □	3 * 用户组名称:	HCIP-WLAN					
所有用户	地址:						
A Guest	邮编:						
	管理员邮箱:						
	描述:						
				取	ij <b>4</b>	确定	

# 选中 "HCIP-WLAN"用户组,单击 "创建",新增用于 802.1X 认证的用户名 "dot1xuser",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"。



of 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:	0						
过期时间:	支持除HWTACACS认证之外的所有认	正方式。					
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 2 802.1X & Portal 进行Portal2.0认证需要同时勾选Porta	2.0 日 HWTAC	ACS .0。进行H.	ACA认证需	要勾选Po	rtal.	
仅允许使用移动证书认证:							
	即EAP-TLS协议的802.1X认证,Boarc	ling场景请勿勾选该选	项。				
其他信息 <							
接入绑定信息 <							
RADIUS属性 ⑦ <							

### 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。

设计 配置	准入 监控 维护 系统	r 📀
iMaster NCE-Campus 此页面的仪表盘功能,洞察全网数据状态与趋势哦。	※ 准入资源 用户管理 访客管理 终端管理 页面管理 准入设备 ☆	<ul> <li>准入策略</li> <li>认证授权</li> <li>用户在线控制</li> <li>准入设置</li> <li>业务随行</li> <li>安全组</li> <li>溶源组</li> </ul>
レンズLAN Fabric网络 変 快速引导用户完成园区VXLAN网络的业 务规划和配置。	<ul> <li>证书认证</li> <li>冷备管理员</li> <li>HWTACACS认证授权</li> <li>☑ 增值业务</li> <li>上网行为管理</li> <li>RADIUS计费设备</li> </ul>	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。



🔏 iMaster NCE-Campus		设计	配置	准入	监控	維护	系統		ŧ	☆	0	<b>6</b> 0	<mark>!</mark> 0	<b>i</b> 0	Q	🕐 中文	1	?
准入 / 准入资源 / 准入设备																		
准入设备管理 准入区域 准入	设备模板																	
- - - - - - - - - - - - - -	第三方准入设备 请输入关键字	设备	Q								转移	- <del>9</del>	#	导入		副除	创建	
所有设备组	■ 设备名称 🗘	描述 ≎		IP地址	¢	1	备份IP ⇔	设备系列 ⇔	RADIUS认证例	数章	Port	al认证参数	8 <b>2</b> ≎	HWTA	CACSINE	E 0   操作	F	
目 准入设备组								没有记录。										

# 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。

🔏 iMaster NCE-Campus		设计配置	准入	监控	维护	系统		
准入 / 准入资源 / 准入设备								
准入设备管理 准入区域 准入	设备模板							
请输入名称    Q	第三方准入设备 云管准入设备	ž						
· / Î	创建第三方准入设备							
所有设备组	*设备名称:	WAC1						
□ 准入设备组	描述:							
	*IP地址:	10.23.100.1						
	备份IP:					0		
	设备系列:	Huawei NAC			~			
	RADIUS认证参数:							
	CoA类型:	默认CoA	No CoA	Po	ort Bound	ce	Reauth	0
	CoA端口:	3799				0		
	准入设备模板:							
	*认证计费密钥:	•••••				0		
	*确认认证计费密钥:	•••••						
	*授权密钥:	•••••				0		
	*确认授权密钥:	•••••						
	*计费周期(分钟):	3				0		

在 NCE 上创建认证规则、授权规则、授权结果。

# 选择"准入 > 准入策略 > 认证授权"。





#选择"认证规则",点击"创建",按如下参数配置认证规则。

~	iMaster NCE-Campus			设计	配置	准入	监控	维护	系统
准入		四初 如 如 如 一 寿							
1/1	近视频	反仪规则 東暗儿茶							
	创建认证规则								
	▲平信忌 *名称:	802.1X		]					
	描述:			-					
	认证方式:	用户接入认证 MAC认证	设备	管理认证	E				
	启用Portal-HACA协议:	0							
	接入方式:	WIFI 有线 蜂窝网:	洛						
	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	~ 0	
设备信息匹配:			
SSID匹配:			
终端信息匹配:	0		
终端IP范围:	通过换行符分隔IP地址, 请输入IP地址/	•	
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:	选择移除		
	□ 优先级 ⇔		名称 ≑
	□ 1 ·		本地数据源

双因子认证:	
优先识别协议:	
优先识别协议:	EAP-PEAP-MSCHAPv2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:	继续处理
身份认证失败:	拒绝接入



### #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i	证规则  授权结果	授权规则策略元素							
	l								
	创建授权规则								
	基本信息								
	*名称:	802.1X		]					
	描述:								
			10.42	dderma \ L \ra	-				
	认证方式:	用户接入认业 MAC认业	设备	官埋认证	-				
	启用Portal-HACA协议:								
	接入万式:	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	~ 0						
	设备信息匹配:								
	SSID匹配:								
	SSID:								
		wlan-net							
	终端信息匹配:	• •							
	终端IP范围:	通过换行符分隔IP地址, 请输入IP地址/掩码(如192.168.1.1/32或 2001:0DB8:0:0:0:0:1428:57AB/64)或 IP地址段(如192.168.1.1-	•						
	区域匹配:								



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

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

AP列表			
智能诊断	上线失败记录 下线记录	是 SoftGRE隧道状态	导出信息 loT插卡信息
AP ID * 🍸	AP名称 ▲ ▽	AP组▲ ▽	状态名称 ▲ ▽
0	AP1	ap-group1	normal
1	AP2	ap-group1	• normal
2	AP3	ap-group1	• normal
10 ▼ 共3条	:		
总AP数:3		normal : 3	
AirEngine5761-1	1:3		

# 5.3.2 检查 VAP 信息

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



第154页	
-------	--

AP型VAP	列表							
应用统计	清零							
AP ID +	AP名称 ▲	射频ID +	WLAN ID +	SSID +	BSSID *	认证方式 🛎	接入用户数 🔺	状态
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA2+802.1X	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA2+802.1X	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA2+802.1X	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA2+802.1X	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA2+802.1X	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA2+802.1X	0	on

## 5.3.3 STA 通过 802.1X 方式接入无线网络

- # STA 接入无线网络时,需要提前设置 802.1X 参数,本实验仅介绍 Win10 的设置方法。
- # 选择"控制面板 > 网络和 Internet > 网络和共享中心"(控制面板的"查看方式"选择 "类别"时可显示"网络和 Internet"),单击"设置新的连接或网络"。

🕎 网络和共享中心		
← → ~ ↑ 💆 > 控制面板 >	网络和 Internet > 网络和共享中心	
控制面板主页 更改适配器设置 更改高级共享设置 媒体流式处理选项	查看基本网络信息并设置连接 查看活动网络 网络 2 公用网络	访问类型: 无法连接到 Internet 连接: 🔋 以太网
	更改网络设置      设置新的连接或网络     设置新的连接或网络     设置宽带、拨号或 VPN 连接;或设置路由器或     问题疑难解答     诊断并修复网络问题,或者获得疑难解答信息。	游接入点。

# 在弹出的对话框中选择"手动连接到无线网络",然后点击"下一页"。



笡1	55页
ייהכ	22.2

	-		×
← 🚽 设置连接或网络			
选择一个连接选项			
● 连接到 Internet 设置宽带或拨号连接,连接到 Internet。			
<b>设置新网络</b> 设置新的路由器或接入点。			
手动连接到无线网络 连接到隐藏网络或创建新无线配置文件。			
连接到工作区 设置到你的工作区的拨号或 VPN 连接。			
र	一页(N)	取	肖

# 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。



			_		$\times$
←	🔮 手动连接到无线网络				
	输入你要添加的无线网	络的信息			
	网络名(E):	wlan-net			
	安全类型(S):	WPA2 - 企业 ~			
	加密类型(R):	AES ~			
	安全密钥(C):	□ 隐藏字符(H)			
	☑ 自动启动此连接(T)				
	□ 即使网络未进行广播也	连接(O)			
	警告: 如果选择此选项	则计算机的隐私信息可能存在风险。			
		- 不	·页(N)	取	肖

# 显示已成功添加了"wlan-net"无线网络,然后点击"更改连接设置"。

	_	$\times$
🔶 👱 手动连接到无线网络		
成功地添加了 wlan-net		
→ 更改连接设置(H) 打开连接属性以便更改设置。		

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



wlan-net 无线网络属性					×
连接 安全					
安全举型(F):	WPA2 - 企业	1		~	
XIXE(0)		-			
加密类型(N):	AES			$\sim$	
选择网络身份验证方法	(O):				
Microsoft: 受保护的	EAP (PEAP)	~	设置(9	S)	
☑ 每次登录时记住此道	重接的凭据(R)				
高级设置(D)					
		ł	确定	取消	

# 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"。



	這接到这些	服务器(示例:	: srv1;srv2;.*\.s	rv3\.com)(0	):	
	受信任的根证	B颁发机构(P	Q):			-
			Pv2 属性			×
	Microse	当连接时:				
	Microse	自动使	用 Windows 登	浸名和密码(	以及域,如果	有
	Micros	<sup>山</sup> 的话)(A	A).			
	Microse					
1	<		确定	取消	H.	
1	至接前週刊([					
1	如果尤法验证制	的驚點的身份	,请告知用户			~
洗	医自份验证方法	=(5)-	1			
#	+ 38 (FAD-N	ISCHAP v2)		6	10 m	7
		±19(E)		3		
		主度(F) 易供加密維定	≘AS TLV ®I₩FTT	连接(D)		
	MANNADOS HANNA	ALL OTHER STAL		213(0)		

# 在"安全"页签,单击"高级设置"。



wlan-net 无线网络属性			×
连接安全			
安全类型(E):	WPA2 - 企业	~	
加密类型(N):	AES	~	
选择网络身份验证方法	(O):		
Microsoft: 受保护的 I	EAP (PEAP) ~	设置(S)	
☑ 每次登录时记住此道	E接的凭据(R)		
	_		
高级设置(D)			
	ā	确定 )	取消

# 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"。



高级设置	×
802.1X 设置 802.11 设置	
✓ 指定身份验证模式(P):	
用户身份验证	
□ 删除所有用户的凭据(D)	
□为此网络启田单—登录(5)	
◎用户登录前立即执行(F)	
最大延迟(你)(M): 10	
✓ 允许单一登录期间显示其他对话框(L)	
□ 该网络为计算机和用户身份验证便用甲独的虚拟 LAN(V)	
确定取消	

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



wlan-net 无线网络属性		×
连接 安全		
安全类型(E):	WPA2 - 企业	~
加索米刑(N)·	AFS	
/加西关王(14).	AL3	
<u></u> 注权网络百八孙子子	\$±/0}	
远洋网络身份短亚方 Microsoft: 受保护的	法(O): 内EAP (PEAP) > 没署(S)	
「日毎次登录时记住」	上连接的凭据(R)	
	analog a samilar	
高级设置(D)		
	确定	取消
# 全部设置完成后,	选择名称为"wlan-net"的 St	SID,点击"连接"。
wlan-net		
安全		
自动道	E接	
	连接	

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



・ Wlan-net 安全 正在检查网络要求	
	取消
Windows 安全中心	×
登录	
dot1x-user	
•••••	
确定	取消

# 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
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"。

iMaster NCE-Campus	હોન	配置 准入	监控 维护	系统		🗎 🏠 🔕 🭕	)• 🕛• 🚹• Q	🛞 ¢文 👤 🤇
监控/事件日志/终端认证日志								
Portal上下线日志 RADIUS上下线	HWTACACS日志	Boarding证书申请	記志					
RADIUS认证日志 RADIUS计费日志								
● RADIUS认证日志默认只展示7天内的认	、证记录,如需要查看7天以上的记录,请	点击历史用户。						
~ 过滤条件								柳定
接入站点: 全部								
★ 认证结果: 全部	→ 失败原因:	全部		* 认证时间:		-		
认证组件: 内置认证服务								
							导出选中	导出全部
□ 用户名 用户组	终端IPv4地址 终端IPv6地址	终端MAC	接入SSID	认证规则	授权规则	认证时间 认证结果	失败原因	详情 ③
do****er ROOT\HCIP		08****B4	wlan-net	802.1X	802.1X	成功		查看详情

## 5.3.5 在 WAC1 检查终端认证情况

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

用户列表(总用户数:1,2.4G:0,5G:1)	
智能诊断 应用统计 漫游轨迹 上线失败记录 下线记录 强制	F线 导出信息
用户名 ▲ マ MAC地址 ▲ マ 协商速率(Mbps) ↓↑ ▲ マ AP名称 ▲ マ	了 IPv4地址 ▲ ▽ 频段 ▲ ▽
→ dot1x-user 081f-7153-90b4 173/24 AP1	10.23.101.136 5G
10 ▼ 共1条	
每秒关联的用户数:0 Dot1x每秒认证用户数:0 Portal每秒认证用户数:0 MAC每秒认证用户数:0	



# 5.4 配置参考

# 5.4.1 WAC1 配置

```
Software Version V200R021C00SPC100
defence engine enable
sysname WAC1
#
http timeout 10080
http secure-server ssl-policy default_policy
http secure-server server-source -i Vlanif100
http server enable
#
vlan batch 100 to 101
#
authentication-profile name p1
dot1x-access-profile d1
authentication-scheme radius_huawei
accounting-scheme scheme1
radius-server radius_huawei
#
management-port isolate enable
management-plane isolate enable
#
radius-server template radius_huawei
radius-server shared-key cipher %^%#3:KT&'SI#Fq;Rz~2dA9R2hU/&4Z8L/T{VQ4Ry(sC%^%#
radius-server authentication 172.21.39.88 1812 source Vlanif 100 weight 80
 radius-server accounting 172.21.39.88 1813 source Vlanif 100 weight 80
radius-attribute nas-ip 10.23.100.1
radius-server ip-address 172.21.39.88 shared-key cipher %^%#uz^0YJYF@Dub8K)sS9/;2k=v87NT-
Wn(lBS6A0]Q%^%#
radius-server authorization 172.21.39.88 shared-key cipher %^%#</OAY!//D0%Mn>>GL,#SJt|>3-
nx>!g58f@09>iJ%^%# server-group radius_huawei
radius-server authorization server-source all-interface
#
aaa
authentication-scheme radius_huawei
 authentication-mode radius
accounting-scheme scheme1
 accounting-mode radius
 accounting realtime 3
 local-user admin password irreversible-cipher
$1a$Z#*{";)Ik6$LUMXJS;VWR$p7mWZtx|EN3q#M`}27Bg+[8<)ELp.$
local-user admin privilege level 15
local-user admin service-type telnet ssh http
#
```



```
interface Vlanif1
ip address dhcp-alloc unicast
#
interface Vlanif100
ip address 10.23.100.1 255.255.255.0
#
interface MEth0/0/1
ip address 172.21.39.4 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif100 10.23.100.254
ip route-static 172.21.39.88 255.255.255.255 Vlanif100 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%#
capwap dtls inter-controller psk %^%#tc.5LFZ\oJ^bM8'*YYv#<te,1Oq8kAl.}J+v{puP%^%#
capwap message-integrity psk %^%#eJ&eRx\$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x*%^%#
capwap sensitive-info psk %^%#;,L1<.L'e+Ii6MX,^QxH{6z#&#z[v4Oe"pCPrFJ'%^%#
capwap inter-controller sensitive-info psk %^%#ji6gT7>2y3dm}n~Bb"%8z$0]B62~|NkD,WJF[n2U%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
wlan
calibrate enable manual
temporary-management psk %^%#PwFE@vw_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#
ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\.KXW7QH=Ogpvg'K*Y)I%^%#
traffic-profile name default
security-profile name default
security-profile name wlan-net
 security wpa2 dot1x aes
ssid-profile name default
ssid-profile name wlan-net
 ssid wlan-net
vap-profile name default
vap-profile name wlan-net
 forward-mode tunnel
 service-vlan vlan-id 101
 ssid-profile wlan-net
 security-profile wlan-net
 authentication-profile p1
 ap-group name default
ap-group name ap-group1
  radio 0
  vap-profile wlan-net wlan 1
```



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

## 5.4.2 SW-Core 配置

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



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

## 5.4.3 SW-Access 配置

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



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

# 5.5 思考题

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

参考答案:

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

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

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

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



# 6 Portal 认证实验

# 6.1 实验介绍

## 6.1.1 关于本实验

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

## 6.1.2 实验目的

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

## 6.1.3 实验组网介绍





# 6.1.4 实验规划

设备	端口	端口类型	VLAN参数	
	MultiGE0/0/1	Trunk	PVID:1	
			Allow-pass: VLAN 100 101	
SW-Core		Trupk	PVID:1	
	WulliGE0/0/9	TTUTK	Allow-pass: VLAN 100 101	
	MultiGE0/0/4	Access	PVID: 99	
SW-Access	MultiGE0/0/9	Truck	PVID:1	
		типк	Allow-pass: VLAN 100 101	
	MultiGE0/0/1	Turnel	PVID:100	
		типк	Allow-pass: VLAN 100 101	
		Turnels	PVID:100	
	MultiGE0/0/2	типк	Allow-pass: VLAN 100 101	
	MultiGE0/0/3	Turnel	PVID:100	
		типк	Allow-pass: VLAN 100 101	
		Truck	PVID:1	
WACI	GEU/U/ I	Irunk	Allow-pass: VLAN 100 101	

### 表6-1 VLAN 规划

## 表6-2 IP 地址规划

设备	端口 IP地址	
	Vlanif100	10.23.100.254/24
SW-Core	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



AP组ap-group1VAP模板Wlan-net安全模板Wlan-net安全策略OPENSSID模板Wlan-netSSIDwlan-netARADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: radius_huawei, 其中:Prb址: 172.21.39.88\u00educturduc	业务VLAN	101		
VAP模板wlan-net安全模板OPENSSID模板OPENSSID模板wlan-netSSIDwlan-netRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: scheme1RADIUS计费方案名称: scheme1RADIUS计费方案名称: scheme1RADIUS服务器模板名称: radius_huawei, 其中:IP地址: 172.21.39.88认证端口号: 1812计费端目号: 1813共享密钥: Huawei@123Portal服务器模板URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal扱人模板名称: portal1绑定的模板: Portal服务器模板abc	AP组	ap-group1		
安全模板wlan-net安全策略OPENSSID模板wlan-netSSIDwlan-netRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: 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@123Portal服务器模板URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal接入模板名称: portal1绑定的模板: Portal服务器模板abc	VAP模板	wlan-net		
安全策略OPENSSID模板wlan-netSSIDwlan-netRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: scheme1RADIUS计费方案名称: scheme1RADIUS认证方案名称: radius_huawei, 其中:IP地址: 172.21.39.88IP地址: 172.21.39.88认证端口号: 1812计费端口号: 1813共享密钥: Huawei@123Portal服务器模板URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal认证共享密钥: Huawei@123Portal接入模板名称: portal1绑定的模板: Portal服务器模板abc	安全模板	wlan-net		
SSID模板wlan-netSSIDwlan-netRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: radius_huaweiRADIUS计费方案名称: scheme1RADIUS服务器模板名称: radius_huawei, 其中:RADIUS服务器模板名称: radius_huawei, 其中:IP地址: 172.21.39.88N证端口号: 1812认证端口号: 1813共享密钥: Huawei@123日地址: 172.21.39.88Portal服务器模板IP地址: 172.21.39.88URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal设证共享密钥: Huawei@123Portal设入模板餐称: portal1绑定的模板: Portal服务器模板abc	安全策略	OPEN		
SSIDwlan-netRADIUS认证方案名称: radius_huaweiRADIUS认证方案名称: scheme1RADIUS计费方案名称: scheme1RADIUS服务器模板名称: radius_huawei,其中:IP地址: 172.21.39.88IP地址: 172.21.39.88认证端口号: 1812计费端口号: 1813共享密钥: Huawei@123Portal服务器模板URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal认证共享密钥: Huawei@123Portal投入模板名称: portal1绑定的模板: Portal服务器模板abc	SSID模板	wlan-net		
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服务器模板名称:radius_huawei,其中:           IP地址:172.21.39.88           认证端口号:1812           计表端口号:1813           共享密钥:Huawei@123           Portal服务器模板           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 接入模板           名称:portal           43称:portal           #实密钥:Huawei@123	SSID	wlan-net		
RADIUS计费方案名称: scheme1           RADIUS服务器模板名称: radius_huawei, 其中:           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           URL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设证共享密钥: Huawei@123           Portal设证共享密钥: Huawei@123		RADIUS认证方案名称:radius_huawei		
RADIUS服务器模板名称:radius_huawei,其中:           IP地址:172.21.39.88           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           Afx: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投入模板           名称:portal           #定的模板:Portal服务器模板abc		RADIUS计费方案名称:scheme1		
RADIUS认证参数         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           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           名称: portal           YAC1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		RADIUS服务器模板名称:radius_huawei,其中:		
认证端口号: 1812计费端口号: 1813共享密钥: Huawei@123A称: abcIP地址: 172.21.39.88URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal认证共享密钥: Huawei@123Portal投减板名称: portal1绑定的模板: Portal服务器模板abc	RADIUS认证参数	IP地址: 172.21.39.88		
计费端口号: 1813共享密钥: Huawei@123A称: abcIP地址: 172.21.39.88URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal认证共享密钥: Huawei@123Portal接入模板名称: portal1绑定的模板: Portal服务器模板abc		认证端口号: 1812		
共享密钥: Huawei@123名称: abcIP地址: 172.21.39.88URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal认证共享密钥: Huawei@123Portal接入模板名称: portal1绑定的模板: Portal服务器模板abc		计费端口号: 1813		
Portal服务器模板名称: abcIP地址: 172.21.39.88URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal认证共享密钥: Huawei@123Portal接入模板名称: portal1绑定的模板: Portal服务器模板abc		共享密钥:Huawei@123		
Portal服务器模板       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		名称: abc		
Portal服务器模板URL地址: https:// 172.21.39.88:19008/portalWAC1向Portal服务器主动发送报文时使用的目的端口号: 50200Portal认证共享密钥: Huawei@123Portal接入模板络称: portal1绑定的模板: Portal服务器模板abc		IP地址: 172.21.39.88		
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	Portal服务器模板	URL地址:https:// 172.21.39.88:19008/portal		
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		WAC1向Portal服务器主动发送报文时使用的目的端口号:50200		
Portal接入模板 绑定的模板: Portal服务器模板abc		Portal认证共享密钥:Huawei@123		
Portal接入模板 绑定的模板: Portal服务器模板abc		名称: portal1		
	Portal按入模板	绑定的模板: Portal服务器模板abc		
免认证规则模板 名称:free1	免认证规则模板	名称: free1		
名称: p1		名称: p1		
绑定的模板和认证方案:		绑定的模板和认证方案:		
Portal接入模板portal1		Portal接入模板portal1		
认证模板 RADIUS服务器模板radius_huawei	认证模板	RADIUS服务器模板radius_huawei		
RADIUS认证方案radius_huawei		RADIUS认证方案radius_huawei		
RADIUS计费方案scheme1		RADIUS计费方案scheme1		
免认证规则模板free1				



# 6.2 实验任务

### 6.2.1 配置思路配置

1.配置基础网络,确保网络互通。

2.配置 AP 上线。

3. 配置 iMaster NCE-Campus 与 WAC1 网络互通。

4.在 WAC1 上配置 Portal 认证。

5.配置 WLAN 基本业务。

6.在 NCE 服务器上配置 Portal 认证。

7.验证 Portal 认证。

## 6.2.2 配置步骤

步骤 1 配置基础网络和 AP 上线

# 请参考 1.2.2 步骤 1~1.2.2 步骤 6,此处不再赘述。

步骤 2 配置 NCE 与 WAC1 之间网络互通

# 请参考 5.2.2 步骤 2, 此处不再赘述。

步骤 3 配置 Portal 认证 (WAC1)

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

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

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

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

# 授权服务器模板: 点击"新建", 新建授权服务器模板, 具体细节参见下文。



### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 。 设备名称: WAC1	AirEngine9700-M1 监控	<b>谷</b> 配置	_+ 诊断	┃↓↓ 维护		
● 配置向导	Portal服务器全局设置	RADIUS设置	内置EAP设	置 LDAP设置	AD设置	HWTACACS设置
● AC配置	RADIUS全局配置					
● AP配置	NAS IP地址:		. ?			
⊙ 安全管理	发送报文源IP地址:		. 0			
AAA <b>1</b>	*授权服务器源地址:	所有IP	•			
用户组 2	应用					
自定义应用	RADIUS服务器模板					
ACL 3	新建					
SSL	模板名称 🔺			模式 🔺		
证书管理	→ 🗌 default			主备模式		
安全防护	5 🔻 共1条					
攻击防御	授权服务器模板					
4 终端识别	新建  删除  刷新	清空				
PPSK管理	──授权服务器IP地址▲					

## # 新建 "RADIUS 服务器模板"的具体细节请参考如下配置。

新建RADIUS服务器模板				×
*模板名称: 1	radius_huawei			
模式:	<ul> <li>主备模式</li> <li>① 负载</li> </ul>	载均衡模式		
NAS IP地址:	指定IP地址	The second secon		
4	10 , 23 , 100	. 1		
*模板默认共享密钥: 3	Huawei@123	0		
4 新建服务器 删除		IP地址		٩
IP地址 ▲	共享密钥 ▲	认证端口号▲	计费端□号▲	
→ 172.21.39.88	***	1812	1813	
5 🔻 共1条			< 1	>
高级 🕑				
	<b>5</b> 确定	取消		



新建服务器配置		×
*IP地址:	IPv4         ▼         172 , 21 , 39 , 88	
共享密钥:	Huawei@123	
服务器配置 ☑ 认证		
★端□号:	1812	
权重值:	80	
发送报文源IP地址:	○ LoopBack ● VLANIF ○ IP地址	
	Vlanif100 ×	
Virtual-ip:	OFF	
✓ 计费		
* 端口号:	1813	
权重值:	80	
3 发送报文源IP地址:	○ LoopBack ● VLANIF ○ IP地址	
	Vlanif100 ×	
Virtual-ip:	OFF	
	4 确定 取消	

# 新建"授权服务器模板"的具体细节请参考如下配置。

新建授权服务器		×
*授权服务器IP地址:	172 . 21 . 39 . 88	
模板名称:	radius_huawei 👻	
*密钥:	Huawei@123	
	确定取消	





# 建议在 "RADIUS 设置"全部配置完成后,进行全面检查,如下所示。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	www.	な。配置	(十) 诊断	<b>  </b>   维护	-	
• 配置向导	Portal服务器全质	司设置	RADIUS设置	置 内置E/	AP设置	LDAP设置	AD设置
● AC配置	RADIUS全局配置						
● AP配置	NAS IP地址:				0		
⊙ 安全管理	发送报文源IP地址:				0		
AAA	*授权服务器源地址:		所有IP	Ŧ	]		
用户组	应用						
自定义应用	RADIUS服务器模板						
ACL	新建删除	刷新					
SSL	模板名称 🔺					模式 🔺	
	→ 🗌 default					主备模式	
业书管埋 2	→ 🗌 radius_huav	vei				主备模式	
安全防护							
攻击防御	5 🔻 共2条						
终端识别	授权服务器模板	Ditter					
PPSK管理	新建一删除	刷新	清空				
0.0-0	授权服务器IP地址	*					
U QOS 3	172.21.39.88						

# 配置 AAA 认证方案模板。

# 选择 "配置 > AP 配置 > 模板管理 > AAA > 认证方案模板" ,点击"新建" ,配置模板 名称为 "radius\_huawei" ,然后点击 "确定" 。



模板管理	
□ ▶无线业务	新建认证方案模板
田 📙 认证模板	◆模板名称: radius huawei
田 🛃 802.1X模板	Tadius Indawer
田 📃 Portal模板	确定取消
田 📮 MAC接入模板	
田 📮 免认证规则模板	
田 📮 URL模板	
■ 日认证方案模板	
④ ■授权方案模板	
田 🚦 计费方案模板	
🕀 📕 业务方案模板	
闭 🛃 802.1X客户端模板	

# 选择 "radius\_huawei" 认证方案模板,配置第一认证模式为 "RADIUS 认证",点击"应用"。

认证方案模板:		展示	模板引用关系		
第一认证模式:	RADIUS认证	T		第二认证模式:	不配置
第三认证模式:	不配置	Ŧ		第四认证模式:	
第五认证模式:		-		第六认证模式:	
第七认证模式:		Ŧ			
应用					

# 配置 AAA 计费方案模板。

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

模板管理	
田 🔁 无线业务	新建计费方案模板
王 📑 认证模板	* 模板名称: scheme1
田 📃 802.1X模板	
田 📮 Portal模板	确定取消
王 📮 MAC接入模板	
🗉 📒 免认证规则模板	
田 🧧 URL模板	
🗉 📑 认证方案模板	
∃ 長权方案模板	
■ ■ 计费方案模板	
⊞ ■ 业务方案模板	
田 📃 802.1X客户端模板	

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



计费方案模板:	scheme1	展示模板引用关系	
计费模式:	RADIUS计费 🔻		
计费形式:	○ 按时长计费   ● 实时计费		
*实时计费时间间隔(分钟):	3	实时计费请求无响应最大次数: 3	
实时计费失败后策略:	○ 拒绝用户上线 ● 允许用户」	上线	
开始计费后失败策略:	● 拒绝用户上线 ○ 允许用户」	上线	
应用			

# 配置 Portal 服务器模板。

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

# 注意:WAC1 设备端侦听 Portal 协议报文的端口号为 2000。



### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	<u>へ</u> 協控 配置	<ul> <li>主</li> <li>诊断</li> <li>组</li> </ul>	护	
● 配置向导	Portal服务器全局设	置 RADIUS设置	内置EAP设置	LDAP设置	AD设置
● AC配置	内置Portal全局设置	外置Portal全局设置			
● AP配置	最大用户数:	32768			
⊙ 安全管理	发送报文源IP地址:		. 0		
AAA	外置Portal对接协议				
用户组	华为Portal协议				
自定义应用	Portal协议版本:	● V1 & V2	○ V2		
ACL	2 设备侦听Portal协议报文	2000			
SSL	本机网关地址:	✔ 所有地址			
证书管理	AC间漫游错误码回复:				
安全防护	HTTP协议 ?				
攻击防御	HTTP对接方式:	◎ 基于HTTPS的	Portal对接 🥚 基于H	HTTP的Portal对接	
	* SSL策略:				
终端识别	设备侦听HTTP协议报文	的端口号: 8443			
PPSK管理	本机网关地址:	所有地址	● 指定地址 ● 无		
QoS	Portal认证请求的目的II	2地址:			
<ul> <li>扩展业务</li> </ul>					
● 可靠性配置	Portal认证服务哭列表				
4	新建	山新			
	服务器名称 ▲			URL 🛎	

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

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


安全管理 > AAA > 外置Portal全局	设置 > 新建认证服务器						
*服务器名称:	abc						
*服务器IP地址:	IPv4 👻	. 0					
	服务器IP地址	×					
	172.21.39.88						
协议类型:	Portal      HTTP      HAC	CA .					
* 共享密钥:	Huawei@123						
报文端口号:	50200				发送报文源IP地址	L: 10 . 23 .	100 . 1 🔞
本机网关地址:							
URL:	https://172.21.39.88:19008/p						
URL配置结果:	https://172.21.39.88:19008/port	tal					
URL:	https://172.21.39.88:19	9008/£					
URL配置结果:	https://172.21.39.88:19	0008/portal?ac-ip=&redirect-u	rl=redirect-url&userma	c=user-mac&userip=user-ip	address&ssid=s	sid	
↓ URL选项配置							
重定向配置							
✔ AC-IP关键字/AC-IP:	ac-ip	/	×				
AC-MAC关键字/AC-MA	.C :						
系统名称关键字/系统名称	\$7 :	1					
AP-IP关键字:						AP-MAC关键字:	
✓ 用户访问URL关键字:	redirect-url					✓ 用户MAC关键字:	usermac
✓ 用户IP地址关键字:	userip					✓ SSID关键字:	ssid
AP名称关键字:						AP位置关键字:	
AP组名称关键字:							
登录URL关键字/登录UR	L:	/					
MAC地址选项							
MAC地址格式:	无分隔符	¥					
URL加密							
参数加密后名称:						加密向量名称:	
加密密钥:		۲					
→ 服务器探测配置							
确定取消							

### # 配置 Portal 模板。

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



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	<b>会</b> 配置	(➡) 诊断	<b>   </b> 维护	
● 配置向导	模板管理					
● AC配置	田 □无线业务					新建Portal模板
● AP配置						*模板名称: portal1
AP组配置	団 ■ 802.1X模板					确定取消
AP配置	<ul> <li>Ⅲ</li> <li>■ MAC接入模</li> <li>Ⅲ</li> <li>■ 免认证规则</li> </ul>	板				
射频规划/调优	<ul> <li>∃ URL模板</li> <li>田 見认证方案模様</li> </ul>	反				
分支AP组配置	<ul> <li>●授权方案模</li> <li>● 计费方案模</li> </ul>	反反				
模板管理	<ul> <li>         ∃ 业务方案模様     </li> <li>         ● 802.1X客户     </li> </ul>	扳 端模板				

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

Portal模板: portal1		展示模板引用关系				
模板介绍信息: 通过Portal 接入模板统一管理Portal 认证用户接入相关的所有配置。						
Portal认证:	○ 内置Portal服务器	小置Portal服务器				
对接使用协议:	● Portal协议 〇	HTTP协议 〇 HACA协议				
*主Portal服务器组:	abc					
备Portal服务器组:		×				
Portal服务器不可用时授权用户组权限:		×				
Portal服务器可用后用户重认证:	OFF					
高级 🕑						
应用						

# 配置免认证规则模板。

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



Wireless LAN A 设备名称: WAC1	\irEngine9700-M1	监控	いた。	(十) 诊断	Ì↓ 维护	
• 配置向导	模板管理					
● AC配置	田 🫅无线业务					新建免认证规则模板
<ul> <li>● AP配置</li> </ul>	<ul> <li>□ ► AAA</li> <li>① ■ ↓ 证模板</li> </ul>					*模板名称: free1
AP组配置	<ul> <li>団 ■ 802.1X模板</li> <li>団 ■ Portal模板</li> </ul>					确定取消
AP配置	<ul> <li>Ⅲ ■ MAC接入模板</li> <li>■ ■ 免认证规则模板</li> </ul>	ź				
射频规划/调优	<ul> <li>団 URL模板</li> <li>団 URL模板</li> </ul>					
分支AP组配置	<ul> <li>受援权方案模板</li> <li>受计费方案模板</li> </ul>					
模板管理	<ul> <li>団 ■ 业务方案模板</li> <li>団 ■ 802.1X客户端档</li> </ul>	莫板				

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

免认证规则模板:	free1	展示模板引用关系	
<ul> <li>模板介绍信息:用户认证成功</li> </ul>	力之前,为满足用户基本的网络访	i问需求,譬如下载802.1x客户端	a、更新病毒库等,需要用户免认证就能获B
控制方式:	免认证规则 O ACL		
免认证规则列表			
新建			
规则编号 · 源IP地址	上/掩码		目的IP地址/掩码
应用			暂无数据

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

新建免认证规则			
*规则编号:	1	]	
*源IP地址:	- none -		
*目的IP地址:	指定		
	172 . 21 . 39 . 88	掩码:	32(255.255.255.255)
协议类型:	- none - 🔻	目的端口号	:
确定取消			

# 配置认证模板。



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

模板管理	
🗵 🛅无线业务	新建认证模板
■ ■ 目认证模板	*模板名称: p1
田 🖥 802.1X模板	
🕙 🧧 Portal模板	确定取消
王 🚦 MAC接入模板	
🗄 🧧 免认证规则模板	

# 选择名称为 "p1"的认证模板,在其中引用 Portal 模板 "portal1"、免认证规则模板 "free1"、RADIUS 服务器模板 "radius\_huawei"、认证方案 "radius\_huawei"、计费方 案 "scheme1",如下所示。

模板管理		
🗉 🛅无线业务	Portal模板: 2 portal1	
	•	
日 🥫 认证模板	模板介绍信息:通过Portal接入模板统一	管理Portal认证用
🖂 🥃 p1		
802.1X模板	Portal认证:	○ 内置Portal删
1 Portal模板		
I MAC接入模板	对接使用协议:	<ul> <li>Portal协议</li> </ul>
🛢 免认证规则模板		(
I RADIUS模板	* 主Portal服务普组:	abc
5 二级计费RADIUS模板	备Portal服务器组:	
I HACA模板		
IDAP模板	Portal服务器不可用时授权用户组权限:	
I AD模板		
HWTACACS模板	Portal服务器可用后用户重认证:	OFF
1. 认证方案模板	<b>喜</b> 祝 (A)	
■ 授权方案模板	同权	
计费方案模板		
■ 业务方案模板		
■ 内置EAP服务器配置		
■ 本地用户配置		



模板管理	
⊞ ┣━无线业务	务认证规则模板: <b>2</b> free1
□ □ ↓ 证模板	使板介绍信息:田户认证成功之前,为满足田户基本的
🗆 📙 p1	
802.1X模板	控制方式:       免认证规则 〇 ACL
🧧 Portal模板	
MAC接入模板	免认证规则列表
● 急认证规则模板	新建删除刷新
I RADIUS模板	
I 二级计费RADIUS模板	规则编号 源IP地址/掩码
I HACA模板	□ 1
■ LDAP模板	
	10 ▼ 共1条
■ 1 1 来方安措板	
■ 州县方案模板	
■ 内罟FAP服冬器配罟	
模板管理	
田 📴 无线业务	RADIUS模板: <b>1</b> radius huawei
🗆 🧧 认证模板	昭夕思丁///
🖃 🥃 p1	版劳雷工1F模式 =
<mark>員</mark> 802.1X模板	主备模式
🧧 Portal模板	主名描式
MAC接入模板	工町1天15
■ 免认证规则模板	
① ■ RADIUS模板 3	▶
■二级计费RADIUS模板	



1天112日1王			
☞ ┣━无线业务	认证方案模板:	2 radius hua	wei 🔻
E 🔁 AAA			
□ ■ 认证模板			
🖂 📃 p1	第一认证模式:	RADIUS认证	•
■ 802.1X模板	笛三认证模式·		*
Portal模板			
■ MAC接入模板	第五认证模式:		*
■ 免认证规则模板			
■ RADIUS模板	第七认证模式:	不配置	*
二级计费RADIUS模板			
I HACA模板	3 应用		
LDAP模板			
B AD模板			
HWTACACS模板			
1 ■认证方案模板			
■ 授权方案模板			
日计费方案模板			
<ul> <li>         ① 一无线业务      <li>         □ 一 AAA      </li> </li></ul>	计费方案模板: 2	scheme1	•
<ul> <li>□ こ</li> <li>□ 二</li> <li>□ △AA</li> <li>□ □</li> <li>□ ↓ 证模板</li> </ul>	计费方案模板: 2	scheme1	•
<ul> <li>□ こ 无线业务</li> <li>□ □ AAA</li> <li>□ □ 认证模板</li> <li>□ □ □ 1</li> </ul>	计费方案模板: 2	scheme1 RADIUS计费	•
<ul> <li>● 元线业务</li> <li>● AAA</li> <li>● ● 认证模板</li> <li>● ● p1</li> <li>● 802.1X模板</li> </ul>	计费方案模板: 2	scheme1 RADIUS计费	<ul> <li>The second se</li></ul>
<ul> <li>● 元线业务</li> <li>● ▲AAA</li> <li>● ● ↓证模板</li> <li>● ● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> </ul>	<ul> <li>         ・计费方案模板:         <ul> <li></li></ul></li></ul>	scheme1 RADIUS计费 ) 按时长计费	<ul> <li>实时计费</li> </ul>
<ul> <li>● 元线业务</li> <li>● AAA</li> <li>● ● JAE</li> <li>● ● P1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>● MAC接入模板</li> </ul>	计费方案模板: 2 计费模式: 计费形式: *实时计费时间间隔(分钟):	scheme1 RADIUS计费 分技时长计费 3	<ul> <li>▼</li> <li>○ 实时计费</li> </ul>
<ul> <li>● 元线业务</li> <li>● AAA</li> <li>● ● p1</li> <li>● Bo2.1X模板</li> <li>● Portal模板</li> <li>● MAC接入模板</li> <li>■ MAC接入模板</li> </ul>	<ul> <li></li></ul>	scheme1 RADIUS计费 按时长计费 3	<ul> <li>实时计费</li> <li>① 实时计费</li> </ul>
<ul> <li>● 元线业务</li> <li>● ▲AAA</li> <li>● ● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>● Portal模板</li> <li>● ▲AAA</li> </ul>	<ul> <li>计费方案模板:</li> <li>计费模式:</li> <li>计费形式:</li> <li>* 实时计费时间间隔(分钟):</li> <li>实时计费失败后策略:</li> </ul>	scheme1 RADIUS计费 分按时长计费 3 )拒绝用户上线	<ul> <li>实时计费</li> <li>介许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● 二 AAA</li> <li>● ● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>● Portal模板</li> <li>● AAA</li> <li>● ● p1</li> <li>● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○</li></ul>	<ul> <li>计费方案模板:</li> <li>计费模式:</li> <li>计费形式:</li> <li>* 实时计费时间间隔(分钟):</li> <li>实时计费失败后策略:</li> <li>开始计费后失败策略:</li> </ul>	scheme1 RADIUS计费 按时长计费 3 拒绝用户上线 ● 拒绝用户上线	<ul> <li>实时计费</li> <li>介许用户上线</li> <li>介许用户上线</li> </ul>
<ul> <li>■ 无线业务</li> <li>■ AAA</li> <li>■ ↓证模板</li> <li>■ ₽ 1</li> <li>■ 802.1X模板</li> <li>■ Portal模板</li> <li>■ Portal模板</li> <li>■ MAC接入模板</li> <li>■ 含认证规则模板</li> <li>■ RADIUS模板</li> <li>■ 二级计费RADIUS模板</li> <li>■ HACA模板</li> </ul>	计费方案模板: 2 计费模式: 计费形式: * 实时计费时间间隔(分钟): 实时计费失败后策略: 开始计费后失败策略:	scheme1 RADIUS计费 分按时长计费 3 行拖电用户上线 ● 拒绝用户上线	<ul> <li>实时计费</li> <li>介许用户上线</li> <li>介许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● AAA</li> <li>● ↓ 证模板</li> <li>● p1</li> <li>● 802.1X模板</li> <li>■ Portal模板</li> <li>■ MAC接入模板</li> <li>■ Portal模板</li> <li>■ AAA</li> <li>● Q 1</li> <li>● Q 1</li></ul>	<ul> <li>计费方案模板:</li> <li>计费模式:</li> <li>计费形式:</li> <li>* 实时计费时间间隔(分钟):</li> <li>实时计费失败后策略:</li> <li>开始计费后失败策略:</li> <li>应用</li> </ul>	scheme1 RADIUS计费 分按时长计费 3 分拒绝用户上线 ● 拒绝用户上线	<ul> <li>实时计费</li> <li>() 实时计费</li> <li>() 允许用户上线</li> <li>() 允许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● AAA</li> <li>● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>● Portal模板</li> <li>● MAC接入模板</li> <li>● 免认证规则模板</li> <li>■ RADIUS模板</li> <li>■ RADIUS模板</li> <li>■ T级计费RADIUS模板</li> <li>■ HACA模板</li> <li>■ LDAP模板</li> <li>■ AD模板</li> </ul>	<ul> <li>计费方案模板:</li> <li>计费模式:</li> <li>计费形式:</li> <li>* 实时计费时间间隔(分钟):</li> <li>实时计费失败后策略:</li> <li>开始计费后失败策略:</li> <li>应用</li> </ul>	scheme1 RADIUS计费 按时长计费 3 拒绝用户上线 • 拒绝用户上线	<ul> <li>实时计费</li> <li>实时计费</li> <li>允许用户上线</li> <li>允许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● 二 AAA</li> <li>● ● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>● Portal模板</li> <li>● 免认证规则模板</li> <li>● RADIUS模板</li> <li>● CAA</li> <li>● ○ Portal模板</li> <li>● 日</li> <li>● ○ Portal模板</li> <li>● ○ Portal模板</li> <li>● ○ Portal模板</li> <li>● □ Portale □ Porta</li></ul>	计费方案模板: 2 计费模式: 计费形式: * 实时计费时间间隔(分钟): 实时计费失败后策略: 开始计费后失败策略: 应用	scheme1 RADIUS计费 按时长计费 3 拒绝用户上线 ● 拒绝用户上线	<ul> <li>实时计费</li> <li>实时计费</li> <li>允许用户上线</li> <li>允许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● 二 AAA</li> <li>● ● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>■ Portal模板</li> <li>■ AAA</li> <li>● ● p1</li> <li>■ 802.1X模板</li> <li>■ Portal模板</li> <li>■ AAA</li> <li>■ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○</li></ul>	计费方案模板: 2 计费模式: 计费形式: * 实时计费时间间隔(分钟): 实时计费失败后策略: 开始计费后失败策略:	scheme1 RADIUS计费 分按时长计费 3 行拒绝用户上线 ● 拒绝用户上线	<ul> <li>实时计费</li> <li>(1) 实时计费</li> <li>(1) 允许用户上线</li> <li>(1) 允许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● 二 AAA</li> <li>● ● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>■ MAC接入模板</li> <li>■ 会认证规则模板</li> <li>■ RADIUS模板</li> <li>■ RADIUS模板</li> <li>■ HACA模板</li> <li>■ LDAP模板</li> <li>■ AD模板</li> <li>■ HWTACACS模板</li> <li>■ 以证方案模板</li> <li>■ 授权方案模板</li> <li>■ 计重方案模板</li> </ul>	计费方案模板: 2 计费模式: 计费形式: *实时计费时间间隔(分钟): 实时计费失败后策略: 开始计费后失败策略: 应用	scheme1 RADIUS计费 分按时长计费 3 分拒绝用户上线 ● 拒绝用户上线	<ul> <li>实时计费</li> <li>(1) 实时计费</li> <li>(1) 允许用户上线</li> <li>(1) 允许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● AAA</li> <li>● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>● MAC接入模板</li> <li>● AAA</li> <li>● この1</li> <li>● AAA</li> <li>● 2 p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>● AAA</li> <li>● 2 p1</li> <li>● 802.1X模板</li> <li>● AAA</li> <li>● 2 p1</li> <li>● 802.1X模板</li> <li>● AAA</li> <li>● 2 p1</li> <li>● 802.1X模板</li> <li>● AAA</li> <li>● 2 p1</li> <li>● 1 ● 2 p1</li> <li>● 2 ● 2 p1</li> <li>● 1 ● 2 p1</li> <li>● 2 ● 2 ● 2 p1</li> <li>● 2 ● 2 ● 2 ● 2 ● 2 ● 2 ● 2 ● 2 ● 2 ● 2</li></ul>	计费方案模板: 2          计费模式:         计费形式:         * 实时计费时间间隔(分钟):         实时计费失败后策略:         开始计费后失败策略:         应用	scheme1 RADIUS计费 分按时长计费 3 行拒绝用户上线 ● 拒绝用户上线	<ul> <li>实时计费</li> <li>() 实时计费</li> <li>() 允许用户上线</li> <li>() 允许用户上线</li> </ul>
<ul> <li>● 元线业务</li> <li>● AAA</li> <li>● p1</li> <li>● 802.1X模板</li> <li>● Portal模板</li> <li>■ MAC接入模板</li> <li>● 免认证规则模板</li> <li>■ RADIUS模板</li> <li>■ RADIUS模板</li> <li>■ T级计费RADIUS模板</li> <li>■ HACA模板</li> <li>■ LDAP模板</li> <li>■ LDAP模板</li> <li>■ AD模板</li> <li>■ HWTACACS模板</li> <li>■ 以证方案模板</li> <li>■ 登权方案模板</li> <li>■ 如务方案模板</li> <li>■ 如常FAP服务器配置</li> </ul>	计费方案模板: 2          计费模式:	scheme1 RADIUS计费 按时长计费 3 f拒绝用户上线 • 拒绝用户上线	<ul> <li>实时计费</li> <li>文计用户上线</li> <li>允许用户上线</li> </ul>

步骤 4 配置无线业务

# 创建名为"wlan-net"的安全模板,并配置安全策略。

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



模板管理	
□ ■无线业务	新建安全模板
🗉 🥫 VAP模板	
	* 横板空段·
■ ■安全模板	wian-net
🛢 default	确定取消
default-wds	
■ default-mesh	
#选择"wlan-net"安全模板,配置安全策略为	"OPEN",点击 "应用" 。
安全模板: wlan-net 展示模板	引用关系
● 模板介绍信息: 配置WLAN安全策略,可以对无线终端进行身份验证,对用户	的报文进行加密,保护WLAN网络和用户的安全。WLAN安全策略支持
基础配置高级配置	
Open认证方式存在一定的安全风险,建议采用其他认证方式。安全级别由	高到低。
*安全策略: WPA3 WPA2-WPA3 WAPI WPA2	WPA-WPA2 WPA WEP OWE OPEN
应用	

# 创建名为 "wlan-net"的 SSID 模板,并配置 SSID 名称为 "wlan-net"。

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

模板管理		
	新建SSID模板	
∃ UAP模板		
■ ESSID模板	*模板名称;	wlan-net
📃 default		
∃ 🥫 安全模板	确定取消	
④ <mark>圓</mark> 流量模板		

# 选择 "wlan-net" SSID 模板,配置 SSID 名称为 "wlan-net",点击"应用"。



SSID模板:	wlan-net展示模板引用关系
模板介绍信息: SSII	D用来指定不同的无线网络。在STA上搜索可接入的无线网络时,显示出来的网络名称就是SSID。
基础配置	高级配置
*SSID名称:	wlan-net
最大用户数:	64
应用	

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

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

模板管理	
	新建VAP模板
■ <mark>■</mark> VAP模板	
🕀 📃 default	*模板名称: wlan-net
団 I SSID模板	
団 🥫 安全模板	确定取消
∃ <mark>  </mark> 流量模板	

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

VAP模板:	wian-net 展示模板引用关系		
模板介绍信息: 在VAP	模板下配置各项参数然后在AP组或AP中引用VAP模板,AP上就会生成VAP,VAP用来为STA提供无	线接入服务。通过配置VAP模板下的	参数,使AP实现为STA
基础配置	高级配置		
使能状态:			
转发模式:	隧道转发		
指定报文直接转发:	□ IPv4 💡		
业务VLAN:	● 单个VLAN ○ VLAN Pool	业务VLAN ID:	101
应用			

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



模板管理				
		*SSID模板:	wlan-net	r ]
□ I I VAP 模倣				
🖭 📃 default		模板介绍信息: SSI	D用来指定不同的无线网络。在STA上搜索	可
🖃 📃 wlan-net				
ISSID模板	[default]	基础配置	高级配置	
■ 安全模板	[default]			
■ 流量模板	[default]	*SSID名称:	wlan-net	
🗉 🧧 认证模板				
<mark>見</mark> 终端黑白名单模板		最大用户数:	64	
3 智能应用控制模板		(成田)		
I UCC模板				

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

模板管理	
<ul> <li>二 无线业务</li> <li>日 [] VAP 関板</li> </ul>	*安全模板: wlan-net ▼ 展示模板引用关系
🗄 🛃 default	● 模板介绍信息:配置WLAN安全策略,可以对无线终端进行身份验证,对用户的报文进行加密,保护WLAN网络和用户的安全。WLAN安全策整支
I SSID模板 [wlan-ne]	基础配置 高级配置
夏安全模板 [wlan-ne]	
□ 流量模板 [default]	Open认证方式存在一定的安全风险,建议采用其他认证方式。安全级别由高到低。
🗵 📮 认证模板	
■终端開白名单模板	*安全策略: WPA3 WPA2-WPA3 WAPI WPA2 WPA-WPA2 WPA WPA OWE OPEN
2 智能应用控制模板	
UCC模板	成田
🗉 🧧 Hotspot2.0模板	
① 및 攻击防御模板	
CPE隧道模板	

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

模板管理					
🗆 🔁无线业务			认证模板: p1		★ 展示模板引用关系
⊡ 🥫 VAP模板	Σ̄				
표 📃 defa	ult		模板介绍信息:通过配置认证模板下的	)参数 (例如: 配置认证模板下绑定	的接入模板,确定认证模板的认证方:
🖃 📃 wlan	-net				
📃 SS	SID模板	[wlan-ne]	Portal选项:	基于Portal服务器的MAC快速	ā认证
夏安	全模板	[wlan-ne]			
🧾 流	這種板	[default]	认证前授权VLAN:		0
■ 圓认	证模板		1)正开断摇刀.		
10 50	端黑白名单模板		以证大规模议.		
<mark>員</mark> 智	能应用控制模板		认证失败授权VLAN:		0
🧾 U	CC模板				
🕀 📃 H	otspot2.0模板		认证失败重认证:	OFF	
王 📃 攻	<b>Z</b> 击防御模板				
	PE隧道模板		认业服务馏个可用时投权用户组权限:		· · · · · ·
∃ SSID模相	版		认证成功授权用户组权限:		<b>X</b>
⊡ 流量模板			计费开始触发时机:	• 认证通过	认证通过且获取IP
Ⅰ ■終端黑名	3単模板				
	S单模板		计费更新触发时机:	✓ 漫游触发 会	活更新: OFF
	相控制模板			✔ 信息更新触发	
				✓ IP地址更新触发	
	合言尽快恢 8/2/01-21-21#1-1				
			认证成功推送页面:	- none -	
			法里达计,	OFF	
日 📑 网络注意	RHD/JJtW		かい重われた。		
	= 回%(ロロケロス)				
	な種板		应用		
田 国 師 時 指示	「金星檀板				

# 配置 AP 组引用 VAP 模板。



# 选择 "配置 > AP 配置 > AP 组配置",选择 "AP 组"选项卡,点击 "ap-group1",进 入此 AP 组的配置界面。

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	<u>-</u> 监控	<b>读</b> 配置	(十) 诊断	┃↓↓ 维护
● 配置向导	AP组 静态	负载均衡组			
● AC配置	修改新建	删除	刷新		
⊙ AP配置	组名称 ▲	VAP	模板 ▲		射频0模板▲
AP组配罟	default				2.4G-default
	ap-group1				2.4G-default
AP配置					
射频规划/调优	20 ▼ 共2条				

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

AP配置 > AP组配置 > AP组			
AP组配置: ap-group1 ▼ 查看成员		VAP 模板列表	
显示所有模板	配置模型介绍	● 相关配置	
■ /= VAP配置		新建添加移	除展示模板引用关系
∃ ┣射频管理		模板名称 ▲	SSID模板 ▲
⊕ 🔁 AP			

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

添加VAP模板					
🕂 添加					
<ul> <li>* VAP模板名称:&lt;</li> <li>高级 ●</li> </ul>	wlan-net 🔻	*WLAN ID: 1	*射频:	0,1 💌	×
确定取消					

# 最后查看 "VAP 模板列表"如下。



VAP 模板列表								
● 相关配置								
新建添加	移除展	示模板引用关系						
模板名称 🔺	SSID模板 -	认证模板 ▲	安全模板	WLAN ID +	射频	转发模式	业务VLAN ▲	使能状态
wlan-net	wlan-net	p1	wlan-net	1	0	隧道转发	101	●开启
wlan-net	wlan-net	p1	wlan-net	1	1	隧道转发	101	●开启
10 💌 共2条								

### 步骤 5 配置 Portal 认证 (NCE)

在 NCE 上创建 Portal 认证所用的用户名和密码。

# 在主菜单中选择"准入 > 准入资源 > 用户管理"。

设计 i	配置進入监控维护系统	☆ 📀
iMaster NCE-Campus 此页面的仪表盘功能,洞察全网数据状态与趋势哦。	※ 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	<ul> <li>准入策略</li> <li>认证授权</li> <li>用户在线控制</li> <li>准入设置</li> <li>业务随行</li> <li>安全组</li> <li>资源组</li> </ul>
	<ul> <li>证书认证</li> <li>冷 设备管理员</li> <li>HWTACACS认证授权</li> <li>ご 增值业务</li> <li>上网行为管理</li> <li>RADIUS计费设备</li> </ul>	策略控制 IP-安全组订阅 IP-安全组表项

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



🔏 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	建						
用户 MAC帐号 PPSK 用户操作	日志						
请输入用户组名称    Q	创建用户组						×
	* 用户组名称:	HCIP-WLAN					
所有用户 一 ペ ROOT	地址:						
A Guest	邮编:						
	管理员邮箱:						
	描述:						
						1. 2010	
				取	<u>я</u>	确定	

# 选中 "HCIP-WLAN"用户组,单击 "创建",新增用于 Portal 认证的用户名 "portaluser",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i	证之外的所有认证方式。						
过期时间:								
下次登录修改密码:								
1.0	仅对控制器内置Portal	以证和自助服务页面登录	影生效。					
* 允许登录方式:	Portal 802	2.1X & Portal 2.0	HWTAC	ACS	ACA:1379	同時から彼口の	rtal	
仅分许使用移动证书认证:		Stight and a straig of the straig of the straig of the straight of the straigh	TA OFFOIGH 2	We 3221111	ACA WALK	936 *31520, O	i (d) <sub>e</sub>	
PAY OF LOCAL PROPERTY AND A	即EAP-TLS协议的802.	.1X认证, Boarding场频	建黄勿勾选该选	両.				
其他信息 ~								
接入绑定信息 ~								
RADIUS属性① へ								

### 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。

设计 配置	准入 监控 维护 系统	r 📀
iMaster NCE-Campus 此页面的仪表盘功能,洞察全网数据状态与趋势哦。	ペ 准入资源 用户管理 访客管理 终端管理 页面管理 准入设备  介部数据源	<ul> <li>准入策略</li> <li>认证授权</li> <li>用户在线控制</li> <li>准入设置</li> <li>业务随行</li> <li>安全组</li> <li>资源组</li> </ul>
	<ul> <li>证书认证</li> <li>冷省管理员</li> <li>HWTACACS认证授权</li> <li>▷ 增值业务</li> <li>上网行为管理</li> <li>RADIUS计费设备</li> </ul>	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。



≼ iMaster NCE-Campus		设计	配置	准入	监控	維护	系统		ė	☆	0	<b>6</b> 0	. 0	<b>i</b> 0	Q	🕐 中文	1	?
准入 / 准入资源 / 准入设备																		
准入设备管理 准入区域 准)	入设备模板																	
请输入名称 Q ⊙ ℓ II	第三方准入设备 云管 请输入关键字	准入设备	Q								转移	9	<u>ط</u>	导入		B(14)	郞建	
所有设备组	■ 设备名称 🗘	描述 ⇔		IP地站	Φ.	1	新份IP ≑	设备系列 ≑	RADIUS认证	¢ Ω14	Port	al认证例	数 0	HWTA	CACSWE	E ♀   操作	۴	
□ 准入设备组								没有记录。										

# 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。

🔏 iMaster NCE-Campus		设计 配置	准入监	腔 维护	系统		
准入 / 准入资源 / 准入设备							
准入设备管理 准入区域 准	主入设备模板						
请输入名称     Q	第三方准入设备 云管准入设备	ž					
• / ii	创建第三方准入设备						
所有设备组	*设备名称:	WAC1					
目 准入设备组	描述:						
	*IP地址:	10.23.100.1					
	备份IP:				0		
	设备系列:	Huawei NAC		,	<		
	RADIUS认证参数:						
	CoA类型:	默认CoA	No CoA	Port Bo	unce	Reauth	0
	CoA端口:	3799			0		
	准入设备模板:				•		
	*认证计费密钥:				0		
	*确认认证计费密钥:	•••••					
	*授权密钥:				0		
	*确认授权密钥:	•••••					
	*计费周期(分钟):	3			0		
	自定义MAC认证密码:						

# 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:	0	
Portal心跳检验:	0	
*Portal密钥:	•••••	0
*确认Portal密钥:	•••••	
URL密钥:		0
确认URL密钥:		
终端IP地址列表:		
		0
*Portal认证端口:	2000	0
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"。

	设计	配置	准入	监控	维护	系统			☆	0
iMaste 此页面的仪表盘	r NCE-Campus 功能,洞察全网数据状态与趋势明	tç o	2	准入资源 用户管理 访客管理 炎端管理 页面管理 准入设备	ā		ı.	<b>准入策略</b> 认证授权 用户在线控制 准入设置 <b>业务随行</b> 安全组 浴源组		·
↓ 观 快速引导 务规划和	XLAN Fabric网络 用户完成园区VXLAN网络的业 配置。		2	证书认证 设备管理员 HWTACA 增值业务 上网行为管 RADIUS计	<b>7</b> CS认证授付 管理 十费设备	权		策略控制 IP-安全组订阅 IP-安全组表项		

#选择"认证规则",点击"创建",按如下参数配置认证规则。



🟅 iMaster NCE-Campu	S	设计	配置	准入	监控	维护	
入/准入策略/认证授权							
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	设备管理认识	Ē				
启用Portal-HACA协议:	0						
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	~ ⑦					
设备信息匹配:							
SSID匹配:							
SSID:	增加						
	wlan-net						
终端信息匹配:	0						
终端IP范围:		•					
	通过现行行分词PP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-	•					



认证信息			
RADIUS中继:			
接入参数:			
*数据源:	选择 移除		
	□ 优先级 ⇒	名称 ⇔	
		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:	继续处理		
身份认证失败:	拒绝接入		
	//////////////////////////////////////		

#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	十 配置	t 准入	监控	维护	系统
准)	(/ 准入策略 / 认证授权							
认词	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 说	设备管理	认证				
	启用Portal-HACA协议:	0						
	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	0					
	设备信息匹配:							
	SSID匹配:							
	SSID:	增加						
		wlan-net						
	<u>  彼</u> 逆  信  自  爪  嗣  ・	0						
	☆端旧心凹山.		*					
	≂ <ymui clai.<="" td=""><td>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</td><td></td><td></td><td></td><td></td><td></td><td></td></ymui>	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						
		2001.0DDo.0.0.0.0.1428:57AB/64)现 IP地址段位1192.168.1.1-	•					
	区域匹配:							



协议信息		
协议信息匹配:		
MDM信息		
MDM检查:		
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 …	

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。

设计 配置	准入 监控 维护 系统	
	🔏 准入资源	🗟 准入策略
	用户管理	认证授权
iMaster NCE-Campus	访客管理	用户在线控制
	终端管理	准入设置
山此贝面的仅表盈功能,洞察至网数据状态与趋势哦。	页面管理 🗘	2. 业务随行
	准入设备	安全组
	外部数据源	资源组
	证书认证	策略控制
	🔏 设备管理员	IP-安全组订阅
	HWTACACS认证授权	IP-安全组表项
**	☑ 増值业务	
VXLAN Fabric网络	上网行为管理	
现 快速引导用户完成园区VXLAN网络的业	RADIUS计费设备	

# 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"。



/ 准入资源 / 而而管理								
(7)在八页旅7 贝面官理								
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 ✓ Windows Phone	<ul><li>IOS</li><li>MAC OS</li></ul>	v	Andro Other	id	~	Linux/Un	inix 別新作
推送页面规则 🔨								
认证方式:	用户名密码认证 ~							ع اnix ترابی
推送页面:	请输入推送页面名称	Q 没有合适的页面	面? 跳转到;	准入 > 准〉	、资源 > 页面	面管理 > 页	面定制 规划销	Inix 別新伯
	●     ●       A = 74       ● =							
首推页面:	认证页面 注册页面	用户须知页面						

# 查看 Portal 页面推送策略,如下所示。



~	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	而定制 Portal页面推送策略 语言模板 门户管理						
	请输入关键字 Q						
	☐ 优先级 名称 认证方	र्रह				页面名称	
	□ 1 · Portal 用户	名密码认证				默认用户	户名密码认证定制页面
	N V Default 匿名	认证				默认匿名	3认证定制页面
	共2条						

# 6.3 结果验证

- 6.3.1 检查 AP 上线状态
  - # 选择"监控 > AP",选择"AP 统计"选项卡,可以查看 AP 的状态信息,其中 "normal"代表 AP 已正常上线。

AP列表			
智能诊断	上线失败记录 下线记录	是 SoftGRE隧道状态	导出信息 loT插卡信息
AP ID 🔺 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 ▲ 🍸
0	AP1	ap-group1	normal
1	AP2	ap-group1	• normal
2	AP3	ap-group1	• normal
10 🔻 共3条	ŧ		
急AP数:3		normal : 3	
AirEngine5761-1	1:3		

# 6.3.2 检查 VAP 信息

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



AP型VAP	列表							
应用统计	清零							
AP ID +	AP名称 🔺	射频ID▲	WLAN ID +	SSID *	BSSID +	认证方式 ▲	接入用户数 🗕	状态
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	Open+Portal	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	Open+Portal	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	Open+Portal	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	Open+Portal	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	Open+Portal	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	Open+Portal	0	on

# 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。

• Web Authentication Redirect	+	$\sim$	-		×
← → C ▲ 不安全   1.1.1	1	B	☆	•	:

# 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。

登录成功	× +			$\sim$			×
← → C ▲ 不安全   http	s://172.21.39.88:19008/portal	page/00000000-0000-0000-0	0000-00000000	ß	☆		:
	欢迎	使用WIFI!					
	100	$\checkmark$					
	恭喜您	,认证成功!					
	- K   S   N.	1					
	用户名:	portal-user					
	剩余流量:	无限制					
	剩余时长:	无限制					
	过期时间:	无限制					
		h Dierebarra					
	1	<sup>参</sup> 仪					
		注销					
E × SCULPTOR							
		自助服务					

## 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。



设计	配置准入	监控 维护 系统	☆ 📀	0 🔗 (
		⊗ 概览	↓ 告答	
		LAN概览	当前告警	
iMaster NCE-Campus		站点间	历史告警	
	rb	站点	事件	
1匹贝围的仅表盈功能, 洞祭至网数据状态与趋势	Ro	终端	屏蔽告警	
		设备360	告警通知	
		WAC组	告警设置	
		WLAN资源	🗐 事件日志	
		区域监控	终端认证日志	☆
		🖾 报表	设备关键事件日志	
Sector 1		统计分析	设备通道日志	
VXLAN Fabric网络		敏捷报表	📖 监控设置	
见 快速引导用户完成园区VXLAN网络的业		周期任务	应用体验设置	
务规划和配置。			性能任务管理	
			数据采集配置	
			终端隐私设置	

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

🔏 iMaster NCE	E-Campus			设计	配置	准入	监控	維护	系统			ŧ	ል 📀	<del>6</del> 0 (	<u>!</u> 0 🚺	• Q	🕐 中文	1
监控/事件日志/终端	认证日志																	
Portal上下线日志	RADIUS上下线	日志 H	IWTACACS日志	Во	arding	证书申	请日志									R	9	
<ul> <li>Portal上下台</li> </ul>	我日志默认只展示7天内的设	人证记录,如需	需要查看7天以上的记	录, 请点;	击历史日:	あ (历史	日志不包	含认证组	性记录)。									
~ 过滤条件																		确定
接入站点:																		
* 认证结果:	全部		认证组件:	内置	l认证服务	;			* 认证时间:	00	:00:00	-	23:5	9:59 🗈				
																导出选中	导出	全部
□ 用户名	用户组	<ol> <li>认证时间</li> </ol>	17 0	浅时间		下线服	原因	\$	失败原因	详细失败原因	终端IP	v4地址	终端IPv6地	址	终端MAC		接入SSID	0
Do****er	ROOT\HCIP-WLAN		09:22:								10***	*96			08****B	4	wlan-net	

# 6.3.5 在 WAC1 上检查终端认证情况

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

用户列表 (总用户数: 1, 2.4G: 0, 5G: 1)									
智能诊断 应用统计	+ 浸游轨迹	上线失败记录 下线记	录 强制下线	导出信息					
用户名 ★ 🍸	MAC地址 🔺 🍸	协商速率(Mbps) ↓↑ ▲ 🍸	AP名称 ▲ ▽	IPv4地址 ▲ ▽	频段▲♡				
→ 🗌 portal-user	081f-7153-90b4	144/156	AP2	10.23.101.136	5G				
10 ▼ 共1条									
每秒关联的用户数:0 Dot1x每秒认证用户数:0	Portal每秒认证用户	P数:0 MAC每秒认证用户	敗:0						



# 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 %^%#]qR#5-y9p=z#}}Pk4-L;WGPdIm[,VBkhjz&Wf<G%%^%#
radius-server authentication 172.21.39.88 1812 source Vlanif 100 weight 80
 radius-server accounting 172.21.39.88 1813 source Vlanif 100 weight 80
radius-server authorization 172.21.39.88 shared-key cipher %^%#5jF1YZq(*OsX-2U&P}A<]`!XH,|-
r15kUd$G}=]"%^%# server-group radius_huawei
radius-server authorization server-source all-interface
#
free-rule-template name default_free_rule
#
free-rule-template name free1
free-rule 1 destination ip 172.21.39.88 mask 255.255.255.255
#
url-template name urlTemplate_0
url https://172.21.39.88:19008/portal
url-parameter device-ip ac-ip redirect-url redirect-url ssid ssid user-ipaddress userip user-mac usermac
#
web-auth-server abc
```



```
第204页
```

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



capwap source interface vlanif100 capwap dtls psk %^%#EJVsX!hYu4YZ2 G4#DzXA@:RKv34&REZ}|-y ]mY%^%# capwap dtls inter-controller psk %^%#{9Wo7!%#BFZ<@EQ|:JG>Rp<|47s,v>YPa.#^!]A9%^%# capwap dtls no-auth enable # wlan calibrate flexible-radio auto-switch temporary-management psk %^%#PwFE@vw\_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%# ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0\*)B\.KXW7QH=Oqpvg'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





# 7.1.4 实验规划

设备	端口	端口类型	VLAN参数
		Truel	PVID:1
	MulliGE0/0/1	ттипк	Allow-pass: VLAN 100 101
SNV Core		Truel	PVID:1
SW-Core	MULLIGE0/0/2	Trunk	Allow-pass: VLAN 200 201
		Truel	PVID:1
	MULLIGEU/U/9	Trunk	Allow-pass: VLAN 100 101 200 201
		Truel	PVID:1
	MULTIGE0/0/9	Trunk	Allow-pass: VLAN 100 101 200 201
		Truel	PVID:100
	MulliGE0/0/1	тгипк	Allow-pass: VLAN 100 101
SW-Access		Truel	PVID:100
	Muttige0/0/2	Trunk	Allow-pass: VLAN 100 101
		Turnels	PVID:200
	Muttige0/0/3	Trunk	Allow-pass: VLAN 200 201
	CE0/0/1	Turnels	PVID:1
WACI	GEU/U/ I	Trunκ	Allow-pass: VLAN 100 101
	CE0/0/1	Turnels	PVID:1
WAC2	GE0/0/1	типк	Allow-pass: VLAN 200 201

### 表7-1 VLAN 规划

## 表7-2 IP 地址规划

设备	端口	IP地址
	VLANif 100	10.23.100.1/24
WACT	VLANif 101	10.23.101.254/24
	VLANif 200	10.23.200.1/24
VVAC2	VLANif 201	10.23.201.254/24
SW/ Core	VLANif 100	10.23.100.254/24
Svv-Core	VLANif 200	10.23.200.254/24



### 表7-3 WAC1 业务参数规划

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

## 表7-4 WAC2 业务参数规划

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



## 7.2 实验任务配置

## 7.2.1 配置思路

1.配置 WAC1、WAC2、SW-Access、SW-Core 之间的网络互通。

2.配置 WAC1、WAC2 为 DHCP 服务器,给 AP 及 STA 分配 IP 地址。

3.配置 AP1、AP2 在 WAC1 上线。

4.配置 AP3 在 WAC2 上线。

5.配置 WLAN 业务参数,实现 STA 访问 WLAN 网络功能。

6.配置 WAC 间漫游功能。

7.验证漫游结果。

## 7.2.2 配置步骤

### 步骤 1 配置交换机 VLAN 信息

配置接入交换机 SW-Access 设备。

#在 SW-Access 上创建 VLAN 100、101、200、201。

<Huawei> system-view

[Huawei] sysname SW-Access

[SW-Access] vlan batch 100 101 200 201

# 配置 SW-Access 下行端口类型、PVID 和允许通过的 VLAN。

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

# 配置 SW-Access 上行端口类型及允许通过的 VLAN。

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



### 配置核心交换机 SW-Core 设备。

#在SW-Core上创建VLAN 100、101、200、201。

<Huawei> system-view

[Huawei] sysname SW-Core

[SW-Core] vlan batch 100 101 200 201

# 配置 SW-Core 下行端口类型及允许通过的 VLAN。

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

# 配置 SW-Core 与 WAC1 互联端口的类型及允许通过的 VLAN。

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

# 配置 SW-Core 与 WAC2 互联端口的类型及允许通过的 VLAN。

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

步骤 2 初始化 WAC1、WAC2 设备

# 配置过程请参考 1.2.2 步骤 3, 不再赘述。

- # WAC1 的管理地址配置为 172.21.39.4/24, WAC2 的管理地址配置为 172.21.39.5/24。
- 步骤 3 配置 WAC1、WAC2 的 VLAN 信息

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

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



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

重命名		×
*设备名称:	WAC1	
	确定取消	

### # 在 WAC1 上创建 VLAN 100、101。

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

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	<u></u> 监控	<b>读</b> 配置	(十) 诊断	↓  维护		
<ul> <li>● 配置向导 全局IPv6: OFF</li> <li>● AC配置 VLAN VLANIF VLAN Pool</li> </ul>							
VLAN	VLAN ID *	VLAN 描述 🔺			VLAN 类型 ▲		
	1	VLAN 0001			commonVlan		
接口管埋							
IP	10 🔻 共1条						


Wireless LAN 。 设备名称: WAC1	AirEngine9700-M1		(+) 诊断	┃↓↓ 维护
● 配置向导	AC配置 > VLAN > VLAN	> 批 <del>量新</del> 建VLAN		
▼ AC配置	*VLAN ID:	100,101		(1-4094,格式: 1,3-5,7)
基本配置	确定取消			
VLAN				
Wireless LAN 。 设备名称: WAC1	AirEngine9700-M1	<u>へ</u> 空 空 で 置	(十) 诊断	┃↓↓ 维护
● 配置向导	全局IPv6: OF			
● AC配置	VLAN VLANIF	VLAN Pool		
基本配置	新建 删除 批	北量新建 北量删除	刷新	
VLAN	VLAN ID + VLA	AN 描述▲		VLAN 类型▲
接口管理	□ 1 VL4	N 0001		commonVlan
10	100 VLA	N 0100		commonVlan
IP	101 VLA	N 0101		commonVlan
● AP配置	10 - #20			
● 安全管理	10 ▼ 共3条			

# 配置 WAC1 的 GE0/0/1 端口类型及允许通过的 VLAN。

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



Wireless LAN A 设备名称: WAC1	irEngine9700-M1	 监控	<b>谷</b> 配置	(+) 诊断	 维护	
● 配置向导	物理接口 逻辑	目接口	管理网口			
● AC配置	接口属性 LLDP					
基本配置	() 选择面板上的接口法	±行配置 (Eth	·Trunk接口也可	「点击紫色圆圌进	行选中,或 点此 进	进行新建。)
VLAN		2 4	6 9	10 12		6
接口管理						
IP	0					
● AP配置		1 3	5 7	9 11		5
● 安全管理		Do	wn 💼 Sł	hutdown		
QoS	恢复默认配置					
● 扩展业务	*接口名称:	6	igabitEthernet	t0/0/1		
● 可靠性配置	接口状态:					
	KCHIXE.		TUTIK			
	允许通过VLAN(Tagged	): 3 1	00,101			
	高级 🕑					
	4 确定 取消					

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

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

# 在 WAC2 上创建 VLAN 200、201。

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



rEngine9700-M1	监控	<b>袋</b> 配置	<del>;</del> 诊断	↓ ↓ ↓ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	1
全局IPv6: OFF					
VLAN VLA	NIF VL	AN Pool			
新建删除	批量新建	批量删除	刷新		
VLAN ID *	VLAN 描述 🔺				VLAN 类型 🔺
1	VLAN 0001				commonVlan
10 🔻 共1条					
irEngine9700-M1	监控	<b>袋</b> 配置	<del>[]</del> 诊断	创	}
AC配置 > VLAN > VL	AN > 批量新建'	VLAN			
*VLAN ID:	2	00,201		(1-4094	,格式: 1,3-5,7)
确定取消					
AirEngine9700-M1	监控	な配記	<b>}</b>	<del>[+</del> ] 诊断	<b>   </b>   维护
全局IPv6: OF					
VLAN	VLANIF	VLAN Po	ol		
新建删除	批量新	建 批量	删除	刷新	
VLAN ID +	VLAN 描	述 -		VLAN 类型	2 *
1	VLAN 00	001		commonV	/lan
200	VLAN 02	200		common	/lan
201	VLAN 02	201		commonV	/lan
10 🔻 共3条	D.				
	irEngine9700-M1 全局IPv6: OFF VLAN VLA 新建 删除 VLAN ID - 1 10   共1条 irEngine9700-M1 AC配置 > VLAN > VL * VLAN ID: 确定 取消 AirEngine9700-M1 全局IPv6: OF VLAN 新建 删版 ① VLAN ID - 1 1 1 1 1 1 1 1 1 1 1 1 1	irEngine9700-M1	Image: Properties of the second s	IEngine9700-M1	rEngine9700-M1 监控 副理 全局IPV6: ① 「 VLAN VLANIF VLAN MB 小UAN MB MB MB MB MB MB MB MB MB MB



#### # 配置 WAC2 的 GE0/0/1 端口类型及允许通过的 VLAN。

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

Wireless LAN / 设备名称: WAC2	irEngine9700-M1 监控 酉	<ul> <li></li></ul>	<b>}}</b> 维护
● 配置向导	物理接口 逻辑接口 管理	「四日	
● AC配置	接口属性 LLDP		
基本配置	()选择面板上的接口进行配置 (Eth-Trur	k接口也可点击紫色圆圈进	行选中,或 点此 进行新建。)
VLAN	2 4 6	0 10 10	c.
接口管理			
IP	<b>1</b>		
● AP配置	1 3 5	7 9 11	5
<ul> <li>安全管理</li> </ul>	🚹 已选中 💼 Up 📋 Down	Shutdown	
QoS	恢复默认配置		
● 扩展业务	*接口名称: Gigab	itEthernet0/0/1	
可靠性配置	接口状心: 链路类型: <b>2</b> Trunk		
	允许通过VLAN(Tagged): <b>3</b> 200-2	01	
	高级 💿		
	4 确定 取消		

#### 步骤 4 配置 IP 地址信息

# 配置 SW-Core 的 IP 地址。

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

# 配置 WAC1 的 IP 地址。

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



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

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	ご         ご           监控         配置	+ 诊断	<b>↓↓↓</b> 维护	
● 配置向导	全局IPv6: OFF				
Image: AC配置	VLAN VLA	NIF VLAN Poo	ol		
基本配置	新建 删除	刷新			
VLAN	接口名称 ▲	连接状态 ▲			IPv4地址/掩码 ▲
接口管理	Vlanif1	● 不可用			
IP	10 ▼ 共1条				
Wireless LAN A 设备名称: WAC1	irEngine9700-M1 日 歴	·····································	[+] 诊断	↓↓ 维护	
● 配置向导	AC配置 > VLAN > VLANIF	- > 新建VLANIF			
● AC配置	* VLAN ID:	100			
基本配置	MTU (bytes):	1500			
VLAN	管理接口:	OFF	9		
接口管理	IP地址格式:	✓ IPv4 IP	vб		
IP	IPv4地址配置	-			
● AP配置	主IP地址/掩码:	10 . 23 .	100.1/	255 . 255 . 2	55.0
● 安全管理	从IP地址/掩码:	🔂 添加			
QoS			. /		. ×
● 扩展业务					
⑦ 可靠性配置	(明正) 取消				



Wireless LAN 设备名称: WAC1	AirEngine9700-M1 监控		┃↓↓ 维护	
▶ 配置向导	AC配置 > VLAN > VLANIF >	新建VLANIF		
<ul><li>● AC配置</li></ul>	*VLAN ID:	101		
基本配置	MTU (bytes):	1500		
VLAN	管理接口:	OFF ?		
接口管理	IP地址格式:	✓ IPv4 IPv6		
IP	IPv4地址配置			
● AP配置	主IP地址/掩码:	10 . 23 . 101 . 25	54 / 255 . 255 .	255.0
安全管理	从IP地址/掩码:	↔ 添加		
QoS			/	•
● 扩展业务	高级 🕑			
● 可靠性配置				
Wireless LA 设备名称: WAC1	N AirEngine9700-M1	上小	☐→ 诊断	<b>   </b> 维护
● 配置向导	全局IPv6: OFF			
● AC配置	VLAN V	LANIF VLAN Pool		
基本配置	新建删除	刷新		
VLAN	接口名称	连接状态 🔺	IPv4地址/掩码	} <b>*</b>
接口管理	Vlanif1	● 不可用		
	Vlanif100	●可用	10.23.100.1/2	255.255.255.0
IP	Vlanif101	● 可用	10.23.101.25	4/255.255.255.
● AP配置	10 - 40.5			
● 安全管理	10 平 共3条			

# 配置 WAC2 的 IP 地址。

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

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



Wireless LA 设备名称: WAC2	N AirEngine9700-M1	监控	な。配置	<b>(十</b> ) 诊断	┃↓↓ 维护
● 配置向导	全局IPv6: OFF				
● AC配置	VLAN	LANIF	/LAN Pool		
基本配置	新建删除	刷新			
VLAN	接□名称 ▲	连拍	妾状态 ▲	IPv4地址/排	奄码 ▲
接口管理	Vlanif1	• 7	不可用		
IP	10 🔻 共1条				
Wireless         LAN         AirEngine9700-M1					
● 配置向导	AC配置 > VLAN > VLANIF > 新	建VLANIF			
● AC配置	*VLAN ID:	200			
基本配置	MTU (bytes):	1500			
VLAN	管理接口:	OFF	3		
接口管理	IP地址格式:	✓ IPv4 IP	Рvб		
IP	IPv4地址配置				
● AP配置	主IP地址/掩码:	10 . 23 .	200.1/	255 . 255 . 255	. 0
⊙ 安全管理	从IP地址/掩码:	↔ 添加			
QoS			. /		. ×
● 扩展业务	高级 🕑				
● 可靠性配置	确定取消				



Wireless LAN / 设备名称: WAC2	AirEngine9700-M1 监控	<b> </b>		
▶ 配置向导	AC配置 > VLAN > VLANIF >	新建VLANIF		
● AC配置	*VLAN ID:	201		
基本配置	MTU (bytes):	1500		
VLAN	管理接口:	OFF ?		
接口管理	IP地址格式:	✓ IPv4 IPv6		
IP	IPv4地址配置			
● AP配置	主IP地址/掩码:	10 . 23 . 20	1 . 254 / 255 . 255	. 255 . 0
● 安全管理	从IP地址/掩码:	分添加		
QoS			. / .	^
● 扩展业务	局级し			
● 可靠性配置	明定取消			
Wireless LA 设备名称: WAC2	N AirEngine9700-M1	监控	<ul> <li></li></ul>	<b>\$</b> } 维护
● 配置向导	全局IPv6: OFF			
● AC配置	VLAN	LANIF VLAN	Pool	
基本配置	新建删除	刷新		
VLAN	接口名称	连接状态	▲ IPv4地址/描	码 -
接□管理	Vlanif1	● 不可用		
10	Vlanif200	●可用	10.23.200.1	1/255.255.255.0
IP	Vlanif201	●可用	10.23.201.2	254/255.255.255.0
● AP配置	10 = #2条			
● 安全管理	10 * 共3家			

#### 步骤 5 配置路由信息

#在 SW-Core 上配置 WLAN 业务相关路由。

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

# 在 WAC1 上配置缺省路由。



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

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	<u>上</u> 监控	<b>口</b>	☐→ 诊断	┃ ↓↓↓
● 配置向导	DHCP地址池	DHCP中继	NAT 3	路由	DNS
● AC配置	→路由表				
基本配置 4	↓ 静态路由配置表				
VLAN 5	新建删除	刷新			
接口管理	目的IP地址。			子网掩	码 🔺
<b>2</b> IP					

# 在"新建静态路由"页面,配置缺省路由如下所示,然后点击"确定"。

AC配置 > IP > 胞由 > 銅建聯志語由							
*目的IP地址:	0.0.0.0		*子网掩码:	0.0.0.0	]		
下—跳:	10 . 23 . 100 . 254	0	出接口:	Vlanif100	×		
优先级:			描述:				
確定取消							

# 在 WAC2 上配置缺省路由。

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

Wireless LAN / 设备名称: WAC2	AirEngine9700-M1	<u>上</u> 监控	<b>谷</b> 配置	<b>(十</b> ) 诊断	<b>4</b> 4 维护
● 配置向导	DHCP地址池	DHCP中继	NA	路由	DNS
● AC配置	→路由表				
基本配置	↓ 静态路由配置表	]			
VLAN	新建删除	刷新			
接口管理	目的IP地址 🔺			子网掩	码▲
<b>2</b> IP					

# 在"新建静态路由"页面,配置缺省路由如下所示,然后点击"确定"。



第224页
-------

AC配置 > IP > 路由 > 新建静态跟	洛由				
*目的IP地址:	0.0.0.0	]	*子网掩码:	0.0.0.0	
下一跳:	10 . 23 . 200 . 254	0	出接口:	Vlanif200	 ×
优先级:			描述:		
确定取消					

#### 步骤 6 配置 DHCP 服务器

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

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

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	上 监控	☆ 配置	(➡) 诊断	<b>∦↓</b> 维护
● 配置向导	DHCP地址池	DHCP中继	NAT	路由	DNS
● AC配置	DHCP状态: ON				
基本配置	DHCPv4地址池列表				
VLAN	新建删除	显示地址池信息	刷新	)	
接口管理	地址池名称 🔺			IP地址池子网	列地址 ▲
IP					
Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	✿ 配置	(➡) 诊断	<b>   </b> 维护
● 配置向导	AC配置 > IP > DHCP地	址池 > 新建DHCP\	/4地址池		
● AC配置	*地址池类型:	○ 全局:	地址池 💿	接口地址池	
基本配置	*接口选择:	Vlanif	100		🕜
VLAN	*接囗IP地址:	10	23 . 10	0.1	
接口管理	厂商自定义:	- none	e -	•	
IP	高级 💽				
● AP配置	确定取消				



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	<b>读</b> 配置	<b>王</b> 诊断	<b>省</b> 维护
● 配置向导	AC配置 > IP > DHCI	P地址池 > 新建	DHCPv4地址池		
<ul><li>● AC配置</li></ul>	*地址池类型:		全局地址池	● 接口地址池	
基本配置	*接口选择:		Vlanif101		📀
VLAN	*接口IP地址:		10 . 23 .	101 . 254	
接口管理	厂商自定义:		- none -	•	
IP	高级 💽				
● AP配置	确定取消	)			

# 检查 WAC1 的 DHCPv4 地址池列表,如下所示。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	<b>谷</b> 配置	<b>(土</b> ) 诊断	<b>∦↓</b> 维护
● 配置向导	DHCP地址池	DHCP中继	NAT	路由	DNS
● AC配置	DHCP状态: ON				
基本配置	DHCPv4地址池列表	ŧ			
VLAN	新建删除	显示地址池信息	刷新		
接口管理	- 地址池名称 -	IP地址池子	网地址。	子网排	奄码 ▲
IP	Vlanif100	10.23.100	.0	255.2	255.255.0
10 I	Vlanif101	10.23.101	.0	255.2	255.255.0
● AP配置					
● 安全管理	5 ▼ 共2条				

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

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



Wireless LAN 设备名称: WAC2	AirEngine9700-M1	<u></u> 监控	<b>☆</b> 配置	<b>(十</b> ) 诊断	<b>   </b>   维护
● 配置向导	DHCP地址池	DHCP中继	NAT	路由	DNS
● AC配置	DHCP状态: ON				
基本配置	DHCPv4地址池列表	-			
VLAN	新建    删除	显示地址池信息	刷新	)	
接口管理	地址池名称 🔺			IP地址池子网	地址 🔺
IP					
Wireless LAN A 设备名称: WAC2	AirEngine9700-M1		<b>\$</b> 置	<b>(于)</b> 诊断	<b>    </b> 维护
● 配置向导	AC配置 > IP > DHCP地	址池 > 新建DHCPv	4地址池		
● AC配置	*地址池类型:	○ 全局は	etlite 💿	接口地址池	
基本配置	*接口选择:	Vlanif2	00		📀
VLAN	*接口IP地址:	10 .	23 . 200	). 1	
接口管理	厂商自定义:	- none	: -	•	
IP	高级 💽				
● AP配置	确定 取消				



Wireless LAN 设备名称: WAC2	AirEngine9700-M1	监控	な。配置	(手) 诊断	<b>11</b> 维护
● 配置向导	AC配置 > IP > DHCI	P地址池 > 新建	DHCPv4地址池		
● AC配置	*地址池类型:		全局地址池	• 接口地址池	
基本配置	*接口选择:	0	Vlanif201		📀
VLAN	*接口IP地址:		10 . 23 .	201 , 254	
接口管理	厂商自定义:		- none -	٣	
IP	高级 💽				
● AP配置	确定 取消	)			

# 检查 WAC2 的 DHCPv4 地址池列表,如下所示。

Wireless LAN AirEngine9700-M1 设备名称: WAC2		监控	<b>袋</b> 配置	☐→ 诊断	维护
• 配置向导	DHCP地址池	DHCP中继	NAT	路由	DNS
● AC配置	DHCP状态: ON				
基本配置	DHCPv4地址池列表				
VLAN	新建删除	显示地址池信息	刷新		
接口管理	地址池名称	IP地址池子	四地址 🔺	子网	掩码 ▲
IP	Vlanif200	10.23.200	.0	255.	255.255.0
	Vlanif201	10.23.201	.0	255.	255.255.0
● AP配置					
<ul> <li>安全管理</li> </ul>	5 ▼ 共2条				

#### 步骤 7 配置 AP1、AP2 上线

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

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

步骤 8 配置 AP3 上线

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



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

步骤 9 配置无线业务(WAC1)

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

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

步骤 10 配置无线业务(WAC2)

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

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

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

步骤 11 配置 WAC 间漫游功能

# 在 WAC1 上创建漫游组,并配置 WAC1 和 WAC2 为漫游组成员。

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

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	な。配置	<b>(</b> 手) 诊断	律 护
● 配置向导	AC基本信息	AC间漫游	Navi-A0	2	
● AC配置	漫游组配置方式:	<ul> <li>本</li> </ul>	地配置	远程获取	
基本配置	新建    删除	刷新			
VLAN	漫游组名称	•			已加入AC IP地址 🔺
接口管理					
IP	3 应用				



Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	监控	<b>袋</b> 配置	<b>(王)</b> 诊断	<b>   </b> 维护		
• 配置向导	AC配置 > 基本配置 >	· AC间漫游 >	新建漫游组				
● AC配置	*漫游组名称:	Γ	mob1				
基本配置	组内成员						
VLAN	3 添加						
接口管理	组内成员AC IP地址:		IPv4 🔻	10 . 23 .	100 . 1	描述:	WAC1
IP	组内成员AC IP地址:		IPv4 *	10 . 23 . 2	200 . 1	描述:	WAC2
● AP配置	确定 取消						

# 在 WAC2 上创建漫游组,并配置 WAC1 和 WAC2 为漫游组成员。

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

Wireless L/ 设备名称: WAC2	AirEngine9700-M1	监控	<b>谷</b> 配置	<ul> <li>主</li> <li>诊断</li> </ul>	<b>\$</b> } 维护
▶ 配置向导	AC基本信息	AC间漫游	Navi-AC		
● AC配置	漫游组配置方式:	• 本	地配置 🛛 远	程获取	
基本配置	2 新建 删除	刷新			
VLAN	漫游组名称	R 🛋		已加	入AC IP地址 🔺
接口管理					
IP	3 应用				
Wireless LAN Air 设备名称: WAC2	Engine9700-M1 监控		┃↓ 维护		
● 配置向导	AC配置 > 基本配置 > AC间漫游 > 新建透	膨缩			
<ul> <li>● AC配置</li> </ul>	*漫游组名称: mob	1			
基本配置	组内成员				
VLAN	分添加				
接口管理	组内成员AC IP地址: IPv4	• • 10 . 23	. 100 . 1	描述:	WAC1
IP	组内成员AC IP地址: IPv4	▼ 10 . 23	. 200 . 1	描述:	WAC2
● AP配置	确定取消				

步骤 12 配置 WAC 间数据隧道 DTLS 加密



# 在 WAC1 和 WAC2 上同时启用 WAC 间数据隧道 DTLS 加密功能,以提高数据安全性。由于之前的步骤中,已经配置了 WAC 间 DTLS 加密的预共享密钥,此处无需重复配置密钥。
# 选择"配置 > AC 配置 > 基本配置",选择"AC 基本信息"选项卡,展开"高级"选项,在"CAPWAP 链路配置"模块中,配置"AC-AC 间数据隧道 DTLS 加密"为"ON",最后点击"应用",如下所示。

高级 •					
✓ CAPWAP提始低量					
AC - AP					
AC到AP的CAPWAP管理报文优先级:	7	·	AP到AC的CAPWAP管理报文优先级:	7	
允许AP以预置证书与AC进行DTLS会 话:			允许AP以不认证方式与AC进行DTLS 会话:	CON	
AC-AP间控制隧道DTLS加密:	自动	*	AC-AP间数据隧道DTLS加密:	OFP 🕜	
*AC-AP间DTLS加密预共享密钥:		0	AC-AP间敏感信思加密预共享密钥:		0
报文完整性校验:			报文完整性预共享密钥:	•••••	0
AC - AC					
AC-AC间控制隧道DTLS加密:	自动		AC-AC间数据隧道DTLS加密:	ON	
*AC-AC间DTLS加密预共享密钥:	•••••	0	AC-ACI同戰感信息加密预共事密钥:	•••••	6
CAPWAP心跳检测时间间隔(秒):	25		CAPWAP心就检测次数:	6	

# 7.3 结果验证

## 7.3.1 检查 AP 上线

# 在 WAC1 上选择"监控 > AP",选择"AP 统计"选项卡,可以查看 AP1 和 AP2 的状态 信息,其中"normal"代表 AP 已正常上线。

AP列表						
智能诊断	上线失败记录 下线记录	SoftGRE隧道状态	导出信息 loT插卡信息			
AP ID * 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称▲ ▽			
0	AP1	ap-group1	normal			
1	AP2	ap-group1	normal			
10 🔻 共2务	z					
总AP数:2 normal:2 AirEngine5761-11:2						

# 在 WAC2 上选择"监控 > AP",选择"AP 统计"选项卡,可以查看 AP3 的状态信息,其 中"normal"代表 AP 已正常上线。



AP列表			
智能诊断	线失败记录 下线记录	SoftGRE隧道状态	P出信息 IoT插卡信息
AP ID * 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 🔺 🍸
0	AP3	ap-group2	• normal
10 ▼ 共1条			
总AP数:1 AirEngine5761-11:1	1	normal : 1	

# 7.3.2 检查 VAP 状态

# 在 WAC1 上选择"监控 > SSID",选择"VAP"选项卡,查看 VAP 的相关信息如下。

P型VAP	列表							
应用统计	清零							
AP ID +	AP名称 -	射频ID▲	WLAN ID +	SSID -	BSSID *	认证方式 -	接入用户数	状态
)	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA/WPA2-PSK	0	on
)	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA/WPA2-PSK	0	on
Î.	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA/WPA2-PSK	0	on
l.	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA/WPA2-PSK	0	on

# 在 WAC2 上选择"监控 > SSID",选择"VAP"选项卡,查看 VAP 的相关信息如下。



SSID 自动刷新: 0	VAP							
AP型VAF	列表							
应用统计	+清零							
AP ID +	AP名称 -	射频ID▲	WLAN ID +	SSID *	BSSID *	认证方式 -	接入用户数 🔺	状态 -
0	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA/WPA2-PSK	0	on
0	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA/WPA2-PSK	0	on
5 💌	共2条 表中的VAP,查看该	VAP应用统计信	自。					

# 7.3.3 检查漫游组状态

# 在 WAC1/WAC2 上查看漫游组的状态,以 WAC1 为例进行说明。

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

Wireless LAN Air 设备名称: WAC1	Engine9700-M1	·····································	な配置	<b>(于</b> ) 诊断	┃↓↓ 维护
概览	AC概況	游用户数概况	接口流過	量统计	无线配置同步信息
网络KPI	自动刷新: OFF				
AC	基于AC的AC间)	曼游用户总数统计	t 🕜		
用户	导出				
射频	对端AC IP地址 ▲	ś.	状态 🔺		
AP	10.23.100.1		normal		
SSID	10.23.200.1		normal		
CPE隧道	10 🔻 共2条				

## 7.3.4 观察 STA 漫游轨迹

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

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



用户列表(总用户数:1,2.4G:0,5G:1)						
智能诊断 应用统计	+ 漫游轨迹	上线失败记录 下线	记录 强制下线	导出信息		
□ 用户名 ▲ 🍸	MAC地址 🔺 🍸	协商速率(Mbps) ↓↑ ▲ `		IPv4地址 ▲ ▽	频段 ▲ 🍸	认证方式 🔺 🍸
→ 🗌 081f715390b4	081f-7153-90b4	57/156	AP1	10.23.101.128	5G	WPA2-PSK
10 ▼ 共1条						
每秒关联的用户数:0						
Dot1x每秒认证用户数:0	Portal每秒认证用户	数:0 MAC每秒认证用,	⊃数:0			
# 点击对应的用户	白名,即可查礼	看用户明细信息	,如:运行指	「标、漫游轨道	迹、下线i	记录等。

运行指标	立用统计	漫游轨迹 上线	线失败记录	下线记录	AP参数明细						
刷新 导出											
时间 *	AP-AC IP地	* AP-AC IPv6 *	AC-AC IP地*	AC-AC IPv6 *	当前AP名称 *	射频ID *	BSSID *	离开速率(M *	接入RSS *	离开RSS *	二层/三层漫游。
09:55:39	9 10.23.100.1				AP1	1	9cb2-e82d-5500	/	-21		-
10 ▼ 共1条											1 >

# 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 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source interface vlanif100
capwap dtls inter-controller control-link encrypt on
capwap dtls psk %^%#GE$'=NySIMd>$B62GoO'Mkw:TmVsCChcg,Ni(--%%^%#
capwap dtls inter-controller psk %^%#ntHh31}TQ:k#NH4i%We/,E>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(IaTNN+gWg:01O1Q)ewt6V[@y>HXMJP@$
local-user admin privilege level 15
local-user admin service-type ssh http
#
interface Vlanif1
ip address dhcp-alloc unicast
#
interface Vlanif200
ip address 10.23.200.1 255.255.255.0
dhcp select interface
management-interface
#
interface Vlanif201
ip address 10.23.201.254 255.255.255.0
dhcp select interface
#
interface MEth0/0/1
ip address 172.21.39.5 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 200 to 201
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.200.254
#
capwap source interface vlanif200
capwap dtls inter-controller control-link encrypt on
capwap dtls psk %^%#vn\1=HRVL@N"+C-7e:b#I1%`PR@S60sh\SOH2r69%^%#
capwap dtls inter-controller psk %^%#ia.O&Gj]lXF|RqJut_t)$l05E-|%MH!}Y-(c.3@D%^%#
```



capwap dtls no-auth enable
# wlan
temporary-management psk %^%#6E3B'y&// <o[iyoiy(x#rgryehabisdwi o".aizt%^%#<="" th=""></o[iyoiy(x#rgryehabisdwi>
ap username admin password cipher %^%#:Te88XR+1A10tUUB1R6(lnY3=wakm> iFW9Oq: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<="" td=""></w6-fyp(p'z'iw_+w8"6zq%^%#>
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-spool-profile name default
wids-profile name default
wireless-access-specification
an-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

设备	端口	端口类型	VLAN参数
		Truck	PVID:1
SN/ Coro	MultiGE0/0/1	типк	Allow-pass: VLAN 100 101
SW-Core		Trupk	PVID:1
	MultiGE0/0/9	ттипк	Allow-pass: VLAN 100 101
		Truck	PVID:1
	MultiGE0/0/9	типк	Allow-pass: VLAN 100 101
		Truck	PVID:100
	MultiGE0/0/1	типк	Allow-pass: VLAN 100 101
SVV-ACCESS		Truck	PVID:100
	MultiGE0/0/2	типк	Allow-pass: VLAN 100 101
		Truck	PVID:100
	MultiGE0/0/3	типк	Allow-pass: VLAN 100 101
		Truck	PVID:1
WACI	GEU/U/ I	Trunk	Allow-pass: VLAN 100 101

#### 表8-1 VLAN 规划

## 表8-2 IP 地址规划

设备	端口	IP地址
SWL Corro	Vlanif100	10.23.100.254/24
Svv-Core	Vlanif101	10.23.101.254/24
	Vlanif100	10.23.100.1/24
VVACT	MEth0/0/1	172.21.39.4/24

## 表8-3 WLAN 业务参数规划

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



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

# 8.2 实验任务配置

## 8.2.1 配置思路

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

## 8.2.2 配置步骤

- 步骤 1 配置基础网络、AP上线、无线业务
  - # 请参考 1.2.2 步骤 1~1.2.2 步骤 7,此处不再赘述。
- 步骤 2 配置射频调优
  - # 配置射频调优模式为自动调优(默认已配置),并开启 DFA 功能。
  - # 选择"配置 > AP 配置 > 射频规划/调优",选择"调优配置"选项卡,按照如下参数进行 配置,然后点击"应用"。



射频规划 调优配	置		
1 WLAN网络中,AP的工作时	状态会受到周围环境的景	《响。例如,当相邻AP的工作信道存在	E重叠频段时,某个AP的功率过大会对相邻AP造
注意事项:			
• 对于配置WDS网桥或Mesh锁	推路的射频,射频调优功能	能不生效。	
• 射频调优功能不适用于AP相	互无法感知的场景,例如	: AP使用定向天线、AP相隔较远或有	皆AP间被阻隔等导致无法相互感知的情况。
• 射频调优功能不适用于高密域	杨晨、WDS/Mesh回传	场景、轨交场景和室外定向天线的暴	盖场景。
• 射频的工作模式为监控模式即	时,此射频不参与调优。		
•配置射频调优、智能漫游、V	VIDS等依赖于信道扫描	的功能后,在扫描过程中如果触发了	时频的信道切换,在信道切换的瞬间会导致用户,
调优开关:			
* 触发条件:	<ul> <li>自动</li> </ul>	*优化开始时间: 03:00:0	0 💠 调优间隔(分钟): 1440
	○ 定时		
	○手动 💡		
高级 💿			
冗余射频切换:		• 切换为5G/Monitor	○ 自动关闭
高级调优策略(可远):	入侵模式 😮	🗌 3EWi-Fi 🕜	底噪调优(noise-floor) 🥜
调优灵敏度:	<b>中</b>	v	
非法邻居干扰:			
干扰信道恶化黑名单阈值:	16		
高密抗干扰:	ON		
应用			

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

# 选择 "配置 > AP 配置 > AP 组配置",选择 "AP 组"选项卡,点击 "ap-group1",进 入此 AP 组配置界面。



Wireless LAN A 设备名称: WAC1	irEngine9700-M1	监控	<b>袋</b> 配置	<del>[]</del> 诊断	<b>    </b> 维护
● 配置向导	AP组静态	负载均衡组			
● AC配置	修改新建	删除	刷新		
⊙ AP配置	□ 组名称 →		VAP模板 ▲	射频0模板	₹ <del>^</del>
ΔP组积署	default			2.4G-def	ault
	ap-group1		wlan-net	2.4G-def	ault
AP配置					
射频规划/调优	20 💌 共2条				

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

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1 监控	な。配置	<b>(十</b> ) 诊断	り 维护
● 配置向导	AP配置 > AP组配置 > AP组			
● AC配置	AP组配置: ap-group1 ▼	查看成员		
● AP配置	显示所有模板	• 20	配置榜	輕介绍
AP组配置	団 → VAP配置			
AP配置	□ □ □ □ 前频管理 □ ↓ 域管理模板		[do	main]
射频规划/调优	<ul> <li>■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■</li></ul>			
分支AP组配置	<ul> <li>団</li></ul>			
模板管理				



射频0配置(2.4G)			
基础配置	高级配置		
工作状态:			
工作模式:	<ul> <li>正常模式</li> <li>监控模式</li> </ul>		
功率自动调优:	<ul> <li>● 跟随(全局: 开)</li> <li>○ 关</li> </ul>	发送功率(dBm):	127
信道自动调优:	<ul> <li>● 跟随(全局: 开)</li> <li>○ 关</li> </ul>	信道:	20 MI 🔻 🛛 - non 💌 😮
大数据调优:			
天线增益(dB):		WDS/Mesh桥接距离 (0.1km):	3
频谱分析:	OFF		
全信道检测:	OFF		
切换为5G:	OFF	冗余射频切换:	<ul> <li>● 跟随(全局: 开)</li> <li>○ 关</li> </ul>
$\rightarrow$ wids			
应用			

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

射频1配置(5G)			
基础配置	高级配置		
工作状态:			
工作模式:	<ul> <li>正常模式 〇 监控模式</li> </ul>		
功率自动调优:	<ul> <li>● 跟随(全局: 开)</li> <li>○ 关</li> </ul>	发送功率(dBm):	127
信道自动调优:	<ul> <li>● 跟随(全局: 开)</li> <li>○ 关</li> </ul>	信道:	20 MI 🔻 🛛 - non 🔻 🔞
大数据调优:			
天线增益(dB):		WDS/Mesh桥接距离 (0.1km):	3
频谱分析:	OFF		
全信道检测:	OFF	频宽自动调整:	
$\rightarrow$ wids			
应用			

# 手动触发射频调优。

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



	AP名称 ▲	射频ID ▲	AP组名称 ▲	频段 ▲	工作模式 ▲	射频状态 ▲	频宽/(	言道
2	AP3	0	ap-group1	2.4G	正常模式	on	自动	20M/6
2	AP3	1	ap-group1	5G	正常模式	on	自动	20M/40
I	AP2	0	ap-group1	2.4G	正常模式	on	自动	20M/11
1	AP2	1	ap-group1	5G	正常模式	on	自动	20M/64
0	AP1	0	ap-group1	2.4G	正常模式	on	自动	20M/6
D	AP1	1	ap-group1	5G	正常模式	on	自动	20M/161
2 立即调	1优一次,预计需要	更大约15min到	则达稳定状态。		^			
<ul> <li>调优范国:</li> <li>① 全部AP</li> <li>① 指定AP组</li> </ul>								

射频列表	
立即调优 导入配置 导出配置 刷新 识别冗余射频	正在调优 33%

#### 步骤 3 配置频谱导航

# 使能 VAP 的频谱导航功能。(缺省情况下已经使能)

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

√ 射频	
频谱导航:	

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



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

模板管理	
● 〒无线业务	新建RRM模板
🕀 🔚 🗛	
□ □ □ 射频管理	×描标文约· wian-rrm
∃ ■ 域管理模板	Wan-min
■ IRRM模板	确定取消
∃ ■空口扫描模板	

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

↓ 频谱导航			
i 通过频谱导航功能,AP可以控制	制STA优先接入5G,减少2.4G频段上的负责	成和干扰,提升用户体验。	
双频间负载均衡负载起始阈值(终 端数):	90	双频间负载均衡负载差值阈值(%):	80
双频间负载均衡SNR阈值 (dB):	18		
拒绝终端关联最大次数:	0	终端支持频段信息老化probe次数:	35

# 创建射频模板,并引用 RRM 模板。

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

模板管理	
<ul> <li></li></ul>	新建2G射频模板
<ul> <li>□ ■ 封频管理</li> <li>● ■ 域管理模板</li> <li>● ■ RRM模板</li> <li>● ■ QC口扫描模板</li> </ul>	*模板名称: wlan-2g 确定 取消
<ul> <li>■ 102G動频模板</li> <li>● 105G動频模板</li> </ul>	

# 在 2G 射频模板中引用 RRM 模板,配置如下。



模板管理		
<ul> <li>         Ⅲ 二元线业务     </li> <li>         ● 二AAA     </li> </ul>		RRM模板: 2 wlan-rrm ▼
<ul> <li>□ ■ 射频管理</li> <li>① ■ 域管理模板</li> </ul>		• 模板介绍信息: RRM模板主要用于保持最优的射频资源状态
<ul> <li>■ ■ RRM模板</li> <li>● ■ ■ 空口扫描模板</li> </ul>		基础配置 高级配置
□ <mark>■</mark> 2G射频模板		空口时间公平调度: OFF
<ul> <li></li></ul>		→ 强制用户下线
BRRM模板	[default]	-> 动态负载均衡
<ul> <li>■ 空口扫描模倣</li> <li>□ ■ 5G射频模板</li> </ul>	[default]	-> 智能漫游
🗄 📃 default		
<ul> <li></li></ul>	e	

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

模板管理	
	新建5G射频模板
<ul> <li>● ▲AAA</li> <li>■ ▲自频管理</li> <li>● ■ ■ ■ ■ ■ ■ ■ ■ ■ ■</li> </ul>	×模板名称: wlan-5g
Image: Back and the second secon	确定取消
<ul> <li>□ L 1</li></ul>	
■ <b>目</b> 5G射频模板	

# 在 5G 射频模板中引用 RRM 模板, 配置如下。

模板管理	
∃ = 二无线业务	RRM模板: 2 wlan-rrm マ
🗄 🦰 AAA	
🗆 🦾 射频管理	● 模板介绍信号: RRM模板主要用于保持最优的射频资源状态
∃ <mark>員</mark> 域管理模板	
王 ERM模板	其來記罢    高級記罢
🗉 🥫 空口扫描模板	
🗉 🥫 2G射频模板	空口时间公平调度: OFF
□ <mark>■</mark> 5G射频模板	
🗉 🥫 default	── 强制用户 ▶线
🖂 📃 wlan-5g	→ 动态角截均衡
RRM模板	[default]
■ 空口扫描模板	[default] -> 智能漫游
🕀 🗁 A P	
🗄 🗁 Mesh	3 应用
🗄 🫅 WDS	

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



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

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	上 监控	ない	<del>王</del> 诊断	<b>↓↓↓</b> 维护
● 配置向导	AP组静态	负载均衡组			
● AC配置	修改新建	删除	剥新		
● AP配置	□ 组名称 ▲		VAP模板 ▲	射频0模板	*
AP组配置	default			2.4G-defa	ult
	ap-group1		wlan-net	2.4G-defa	ult
AP配置					
射频规划/调优	20 🔻 共2条				

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

AP配置 > AP组配置 > AP组			
AP组配置: ap-group1 ▼ 查看成员		*2G射频模板: 2	wlan-2g
显示所有模板	配置模型介绍	基础配置 高级	及配置
<ul> <li>         ■ VAP配置      </li> <li>         ■ ■ 前频管理      </li> </ul>		射频类型:	802.11ax 🔻
国城管理模板	[domain]	射频自动关闭:	OFF
① ■ □ 2G射频模板	[default]	Wi-Fi灯闪烁信息含义:	● 信号强度 ○ 业务流量
<ul> <li></li></ul>		信道切换通告:	
		→ 802.11n配置	
		→ 802.11bg速率集	
		→ 802.11ax配置	
	(	2 应用	

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


AP配置 > AP组配置 > AP组				
AP组配置: ap-group1 ▼ 查看成员		*5G射频模板:	2 wlan-5g	<b>•</b> (
显示所有模板	配置模型介绍	基础配置	高级配置	
+ <b>一</b> VAP配置		射频类型:	802.11ax	-
🗆 🧰 射频管理				
■ 域管理模板	[domain]	射频自动关闭:	OFF	
団 ┣┓射频0				
□ ≧射频1		3 应用		
■ 1 5G射频模板	[default]			
🗄 🧀 射频2				

# 最后,再次全面检查各种模板之间的相互引用关系,如下所示。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1 於 Line Constant Line Const	
• 配置向导	AP配置 > AP组配置 > AP组	
● AC配置	AP组配置: ap-group1 🔻 查看成员	
● AP配置	显示所有模板	配置模型介绍
AP组配置	∃ / VAP配置	
AP配置	■ <b>一</b> 射频管理 ■ 域管理模板	[domain]
射频规划/调优	<ul> <li>□ □ 1 □ 1 □ 1 □ 1 □</li> <li>□ □ 2 □ 2 G 射频模板</li> </ul>	[wlan-2g]
分支AP组配置	RRM模板 同空口扫描模板	[wlan-rr] [default]
模板管理	<ul> <li>□ □ 射频1</li> <li>□ □ □ 5G射频模板</li> </ul>	[wlan-5g]
● 安全管理	RRM模板 同空口扫描模板	[wlan-rr] [default]
QoS	団 ■ 射频2	
● 扩展业务	⊕ <b>i</b> WIDS	
可靠性配置		

#### 步骤 4 配置负载均衡

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



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

# "基础配置"的参数配置如下所示。

RRM模板:	wlan-rrm	展示模板引用关系	
● 模板介绍信息: R	RM模板主要用于保持最优的射频资源	原状态,通过自动检查周边无线环境、动	加态调整信道和发射功率等射频资源、
基础配置	高级配置		
空口时间公平调度:	OFF		
→ 强制用户下线			
↓ 动态负载均衡			
负载均衡:			
→ 智能漫游			
应用			

## # "高级配置"的参数配置如下所示(下图仅展示负载均衡相关参数)。

↓ 动态负载均衡	
负载均衡:	
负载均衡起始阈值(终端数):	12
负载均衡负载差值阈值:	○ 基于用户百分比   ● 基于用户实际个数
	5
RSSI阈值(dBm):	-63
高级 🕑	
→ 智能漫游	
-> SFN	
应用	

# "wlan-rrm"模板在步骤 3 中已经被引用,本步骤中无需重复引用。

步骤 5 配置用户 CAC 功能



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

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

↓ 用户CAC			
UAC策略:	○ 关闭 ● 基于用户		
新增用户用户数阈值:	40	漫游用户用户数阈值:	40
达到接入阈值:	禁止新用户接入并隐藏SSI▼		
禁止弱信号终端接入:		SNR阈值(dB):	13
→ 频谱导航			
→ 动态负载均衡			
→ 智能漫游			
→ SFN			
应用			

# "wlan-rrm"模板在步骤 3 中已经被引用,本步骤中无需重复引用。

# 8.3 结果验证

# 8.3.1 查看射频模板和 RRM 模板信息

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

# 选择 "配置 > AP 配置 > AP 组配置",选择 "AP 组"选项卡,点击 "ap-group1",进 入此 AP 组配置界面。

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



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	 监控	<b>谷</b> 配置	(┿) (注)	<mark>≹</mark> ↓ 维护
● 配置向导	AP配置 > AP组配置 > AP	组			
● AC配置	AP组配置: ap-group1	▼ 査	看成员		
⊙ AP配置	显示所有模板			配置模	國介绍
AP组配置	団 → VAP配置				
AP配置	「一」「「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」			[doi	main]
射频规划/调优	<ul> <li>□ □ 射频0</li> <li>□ □ □ 2G射频模板</li> </ul>			[wla	n-2g]
分支AP组配置	■ RRM模板	板		[w] [d	an-rr] lefault]
模板管理	<ul> <li>一 前频1</li> <li>□ 一 5G射频模板</li> </ul>			[wla	n-5g]
安全管理		眎		[w]	an-rr] lefault1
Oos	田 一 前 频 2     田 → 加 は     田 → 加 は     田	C MA		10	icidantj
● 扩展业务	⊕ <b>™</b> IDS				
可靠性配置					

# 点击 "RRM"模板,即可查看详细的配置参数,如下所示。



<b>笙</b> 255页	
わてつうひ	

↓ 用户CAC			
UAC策略:	○ 关闭 ● 基于用户		
新增用户用户数阈值:	40	漫游用户用户救阔值:	40
达到接入阈值:	禁止新用户接入并隐藏SSI 🔻		
禁止弱信号终端接入:		SNR阈值(dB):	13
↓ 频谱导航			
● 通过频谱导航功能,AP可以控制	制STA优先接入5G,减少2.4G频段上	的负载和干扰,提升用户体验。	
双频间负载均衡负载起始阈值(终 端数):	90	双频间负载均衡负载差值阈值(%):	80
双频间负载均衡SNR阈值 (dB):	18		
拒绝终端关联最大次数:	0	终端支持频段信息老化probe次数:	35
↓ 动态负载均衡			
负载均衡:			
负载均衡起始阈值(终端数):	12		
负载均衡负载差值阈值:	○ 基于用户百分比 🛛 ● 基于用	户实际个数	
	5		
RSSI阈值(dBm):	-63		
高级 🕑			

# 8.3.2 查看当前射频状态信息

# 在 WAC1 上查看 AP 当前的射频状态信息。

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

射视列表													0
類趨分析	NO NO DE F	无线报文头捕获	Mesh邻居场强信息	射频调优记录	导出信息							默认る	1 全部列 自定义列
AP ID + 7	7 AP名称	*	▲ ▽   状态 ▲ ▽	類段 ▲ ▽	射须类型 ▲ ▽	<b>频完 ▲</b> ▽	信道 + ▽	实际功率/规格功率( ▲ ▽	/ 撞入用户 ▲ ▽	嘎声强度(d▲ ♡	信道利用率▲♡	下行重传率 + 🍸	下行丢包率 + 7
→ ● 2	AP3	0	on	2.4G	802.11ax	20M	1	9/29	0	-78	99%	0%	0%
→ ● 2	AP3	1	on	5G	802.11ax	20M	161	12/30	0	-94	4% (	0%	0%
→ ●1	AP2	0	on	2.4G	802.11ax	20M	6	9/29	0	-92	88%	0%	0%
⇒ ●1	AP2	1	on	5G	802.11ax	20M	40	12/30	0	-94	4% (	<1%(89/13923)	0%
→ ● 0	AP1	0	on	2.4G	802.11ax	20M	11	9/29	0	-94	57%	0%	0%
→ ● 0	AP1	1	on	5G	802.11ax	20M	64	12/30	0	-92	2%	<1%(8/6248)	0%
10 平 共6象	ę.												< 1 >

# 8.4 配置参考

# 8.4.1 WAC1 配置

Software Version V200R021C00SPC100 # sysname WAC1 #



```
http secure-server ssl-policy default_policy
http server enable
#
vlan batch 100 to 101
#
stp enable
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name macportal_authen_profile
authentication-profile name portal_authen_profile
#
ssl policy default_policy type server
pki-realm default
version tls1.2
ciphersuite ecdhe_rsa_aes128_gcm_sha256 ecdhe_rsa_aes256_gcm_sha384
#
aaa
authentication-scheme default
  authentication-mode local
authentication-scheme radius
  authentication-mode radius
authorization-scheme default
 authorization-mode local
accounting-scheme default
 accounting-mode none
local-aaa-user password policy administrator
 domain default
 authentication-scheme default
 accounting-scheme default
 radius-server default
domain default_admin
 authentication-scheme default
 accounting-scheme default
local-user admin password irreversible-cipher
$1a$Z#*{";)Ik6$LUMXJS;VWR$p7mWZtx|EN3q#M`}27Bg+[8<)ELp.$
local-user admin privilege level 15
local-user admin service-type telnet ssh http
#
interface Vlanif100
ip address 10.23.100.1 255.255.255.0
#
interface MEth0/0/1
ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
```





interface GigabitEthernet0/0/1 port link-type trunk port trunk allow-pass vlan 100 to 101 # ip route-static 0.0.0.0 0.0.0.0 10.23.100.254 # capwap source interface vlanif100 capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%# capwap dtls inter-controller psk %^%#tc.5LFZ\oJ^bM8'\*YYv#<te,1Oq8kAl.}J+v{puP%^%# capwap message-integrity psk %^%#eJ&eRx\\$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x\*%^%# capwap sensitive-info psk %^%#;,L1<.L'e+Ii6MX,^QxH{6z#&#z[v4Oe"pCPrFJ'%^%# capwap inter-controller sensitive-info psk %^%#ji6qT7>2y3dm}n~Bb"%8z\$0]B62~|NkD,WJF[n2U%^%# capwap dtls no-auth enable capwap dtls cert-mandatory-match enable # wlan calibrate flexible-radio auto-switch temporary-management psk %^%#PwFE@vw\_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%# ap username admin password cipher %^%#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



第258页

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
	重点覆盖区域:开放办公区、办公室、会议室、经理室
覆盖区域	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
七四西北	重点区域:≥ -65 dBm
切浊安水	普通区域: > -70 dBm
	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
接入终端数	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
	开放办公区:4 Mbps;并发率:100%
****	会议室: 8 Mbps; 并发率: 100%
市克盖水	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
	外层墙体为240 mm混凝土
建筑材质及损耗	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	<ul> <li>开放办公区:终端数160台;单终端带宽需求4 Mbps;并发率:100%</li> <li>大会议室:终端数30台;单终端带宽需求8 Mbps;并发率:100%</li> <li>小会议室:终端数8台;单终端带宽需求8 Mbps;并发率:100%</li> <li>会客室:终端数24台;单终端带宽需求16 Mbps;并发率:80%</li> <li>办公室、经理室:终端数5台;16 Mbps;并发率:100%</li> </ul>
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 ( Mb	基线速率 ps)	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% ≈ 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 ≈ 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 ≈ 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 ≈ 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 ≈ 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"。

(ce	WLAN Planner 便用灾数: 317368 次 评论次数: 1146 版本: v1.0.0 发布时间:	9
Ϋ́	WLAN规划 AP布放 信号仿真	工具接口人
**** 480	室内、室外AP网络规划工具,包括现场环境规划、AP布放、网络信号仿真和生成网规报告等功能。	yangfubo@huawei.com
★★★★ 4.6分 ● 工具评价	▶ 运行	<b>8 6</b>

# 阅读客户网络数据安全管理规定后,点击确认。



客户网络数据安全管理规范V1.0	$\times$
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 据网络安全操作指导书》,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《客户网络数据安全管理规范》	
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。

项目类型:	新建项目 已有项目			
是否涉及客户网络数据	居:○ 是   ● 否			
作业凭证:	项目编码 Y TD000000323701 Q ERP-PM	客户名称: ?	HCIP-WLAN	Q
项目名称:	Huawei	* 项目经理: ʔ	请输入完整的账号或邮箱	
交付工程师: γ	请输入完整的账号或邮箱	*国家/地区:	中国	-
交付工程师: 🥐	请输入完整的账号或邮箱	* 国家/地区:	中国	

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。

辺	1 HCIP-WLAN ▼ 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	(	8	隐藏右侧面板	
工勘	B 😣 🛛	新建	×		障碍物绘制	自动识别:	۲
	å HCIP-WLAN	* 类型: ● 室内 ● 室内	<u> </u>	С	<b>手动绘制</b> ~ 形状	自动吸附	
×6×0		· 楼栋名称: 2 HCIP-WLAN室内		+		$\neg \angle$	«
Eの 验收			¥文件		<sup>矩形</sup> 类型	折线 斜坡	
(回) 设置		详细信息:			120 普通砖墙 (10dB 15dB 20dB)	240 加厚砖槽 混凝土 (15dB 25dB (25dB 30d 30dB) 35dB)	: :1B
		1.遗指文件时,推荐导入圆纸的大小在200MB以及 2.圆纸名称目前仅支持中英文、数字和部分 转落3	9. 222 .	-	<mark>8</mark> 石膏板 (3dB 4dB 9dB) (3	8 20 mm 20 泡沫板 空心木 3dB 4dB 9dB) (2dB 3dB 8	dB)
		and: Rolff			40 普通木门 (3dB 4dB 9dB)	40 mm 实大门 普通玻璃 (10dB 15dB (4dB 7dl 20dB) 12dB)	₩ B
					干扰源布放 ~		
					「「おお」		
	AP 数量(已选数/总数): 0/0 RU 数量(已选数/总数): 0/0 交换机: 0 AD: 0		查看已规划资源 设置显示项		1.000		

#选择 WLAN 场景,本项目为办公场景,点击下一步。

选择场景					>
<b>应用于:</b> ◎ 楼层	○楼栋─○工程				
4					
	酒店	をすめ	<b>(</b> ) () () () () () () () () () () () () (	商场	高密场馆
展会	合库	ズの小场	<b>日</b> 轨交	其他	
🗌 无线定位					

# 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"。



704
-----

选择场	汤景 人名英格兰人姓氏克尔 化乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基	×
	<b>应用于:</b> ◎ 楼层 ○ 楼栋 ○ 工程	
	选择子场景	
	〇 办公区-精品(100Mbps@Everywh 〇 办公区-常规(50Mbps@Everywher 〇 会议室-精品(100Mbps@Everywh	
	〇 会议室-常规(50Mbps@Everywher 〇 咖啡厅-精品(50Mbps@Everywher 〇 咖啡厅-常规(32Mbps@Everywher	
	○ 展亍-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	

## #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	:中央又、数子札部分 <u>特殊子符</u> 。	
<b>8</b> m	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:
Area-1
区域类型选择:
覆盖区域
覆盖类型:
普通覆盖(>=-65dBm) ・
并发率(%):
100
终端情况
总带宽需求 320Mbps * 100%
40 笔记本 (2*2) ~
视频教学 (4Mbps) 🖌 删除
40 智能手机 (2*2) ~
视频教学 (4Mbps) 🖌 删除
+
删除区域

# 设置小会议室(8终端)和大会议室(30终端)。



基本属性	基本属性
区域:	区域:
Area-4	Area-8
区域类型选择:	区域类型选择:
覆盖区域	覆盖区域
覆盖类型:	覆盖类型:
普通覆盖(>=-65dBm) →	 普通覆盖(>=-65dBm) ▼
并发率(%):	并发率(%):
100	100
终端情况	终端情况
总带宽需求 64Mbps * 100%	总带宽需求 240Mbps * 100%
8 笔记本 (2*2) 🗸	30 笔记本 (2*2) 🗸
720P视频 (8Mbps) > 删除	720P视频 (8Mbps) > 删除
+	+
删除区域	删除区域

# 设置会客室。



基本属性
区域:
Area-7
区域类型选择:
覆盖区域
覆盖类型:
普通覆盖(>=-65dBm) -
并发率(%):
80
终端情况
总带宽需求 384Mbps * 80%
12 笔记本 (2*2) 🗸
1080P视频 (16Mbp > 删除
12 智能手机 (2*2) 🗸
1080P视频 (16Mbp > 删除
+
删除区域

# 设置单人办公室。



基本属性
区域:
Area-9
区域类型选择:
覆盖区域
覆盖类型:
普通覆盖(>=-65dBm) -
并发率(%):
100
终端情况
总带宽需求 80Mbps * 100%
2 笔记本 (2*2) 🗸
1080P视频(16Mbp > 删除
3 智能手机 (2*2) 🗸
1080P视频(16Mbp > 删除
+
删除区域

设置普通覆盖区域。

# 设置走廊。



基本属性
区域:
Area-10 👻
区域类型选择:
覆盖区域
覆盖类型:
简单覆盖(>=-70dBm) 🔹
并发率(%):
30
终端情况
总带宽需求 40Mbps * 30%
20 智能手机 (2*2) 🗸
办公、游戏 (2Mbps > 删除
+
删除区域

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。

布放方式 ~		
自动布放AP	等三角布放	等间距布放
金制网线	信道计算	いである
设备点布放、	/	
AP/RU	AD 🕉	5换机
场景推荐		
<b>~</b>	~°	<del>?</del>
AirEngine6761-	AirEngine5761	-AirEngine5762-
21	21	12
最近使用		
<b>~</b>	((-))	<del>?</del>
AirEngine8760	AP8050DN-S	AirEngine6760
R-X1E		R-51E
选择其他人	AP款型	

# 由于该项目仅有一层建筑,选择"当前层",点击下一步。

自动布放配置			×
区域选择	AP选型	信道设置	功率设置
	<ul> <li>当前层</li> <li>多层</li> </ul>		
	上一步	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 AirEngine	5761-21 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。

<ul> <li>✓</li> <li>✓ 信道计算 (每100A)</li> </ul>	●信道计算的时间约为	<b>(</b> )	0
1G	5G		
些择信道计算方式 ○ 1/6/11信道 ● 1/5/9/13信道		HT20 36	<ul> <li>✓ 48</li> <li>✓ 52*</li> <li>✓ 149</li> <li>✓ 153</li> </ul>
主*的信道可能为雷达信道,请	尽量避开。当前国家或地区 上一步	, 室内AP和室外AP所适用	的信道不同,请正确选择信

# 设置功率。



自动布放配置				×
区域选择	AP选型	信道设置	功率设置	
			-0-	
未遵循 EIRP	0	▼ 功率调优		
频段 E	EIRP(中国)			
2.4G	20dBm			
5G(36-48)	23dBm			
5G(52-64)	23dBm			
5G(100-144)	不支持			
5G(149-165)	33dBm			
EIRP为Effective Iso EIRP≥AP单射频口 由于WiFi频段是免到	otropic Radiated Power的缩写。 发射功率+天线增益+MIMO增益 愚频段,需要控制AP的发射功率3	<b>天降</b>		
低对具他的AP或WI 国家和地区对EIRP的	LAN系统的十扰,因此也就有了4 的限制。			
	上一步	开始布放		

## # 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 吸顶部著,则安装万式保持默认"T型龙骨"即可,挂高为"2.6 m",」 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。



	名称:	AP-11	颜色:	蓝色	•
	AP类型:	AirEngine5760-51	物联网卡:	不安装	-
	安装方式:	T型龙骨	挂高:	2.60	m
	RTU License	≥升级: ○是   ◎否	工作模式:	双射频模式	-
<u>详细信息</u> <u>3D模型</u>	POE:	802.3bt(PoE++)			
<b>射频0</b> 🗸 OFF <u>ON</u>	支持协议:	WiFi6(802.11ax)	类型:	2.4G_360°_360°_2dBi	*
	信道:	5	高度:	内置天线	
类型: 2.4G	频宽:	HE20			▲会向于総
MIMO: 2*2	功率:	14 Max: 26dBn			10/02
	Guard Inter	val: 🔍 Short 🔍 Normal	{ .		下倾角:
	馈线类型:				90

## 步骤 8 交换机布放

#选择交换机型号,本项目使用 S5731-S24P4X 交换机。

设备点布放	τ~		
AP/RU	AD	交换机	
S1730S-L8P-	A S1730S-L8	P- S1730	S-
	MA	S24P4	S-A
<b>(</b>	9	6	
S5731-S24P4	XS5731-S48	P4X S5731	S-
		S24P42	X-A
=	=	- (=	
S5731S-	S5735-	\$573	5-
S48P4X-A	L12P4S-/	A L24P49	S-A
<b>(</b>	=	Ξ	) -
设备信息录	ŧ <b>λ</b> ~		
$\bigcirc$			
信息录入			

# 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"。

工具栏
<b>11开仿真图</b> 刷新仿真图 覆盖满足度
接入仿真点布放
後入仿真点
仿真图设置
频段: 🗌 2.4G 🗹 5G 🗌 6G
类型:场强仿真图
仿真图示意
信号强中弱
-20 -45 -55 -65 -70 -90
甲位: dBm

# 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。

工具栏			
<b>》</b> 关闭仿真图	同新仿真		盖满足度
接入仿真点	布放		
<b>交</b> 接入仿真点			
仿真图设置			
频段:	2.4G 🗸	5G	6G
类型: 【	易强仿真图		*
仿真图示意			
信号强		中	弱弱
	45 55	65 B	*
-20	-45 -55 -	-65 -70 #	-90 位: dBm
		4	m. aom

# 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					0
报告内容					网规检视	导出
语言	<ul> <li>● 中文</li> <li>○ 英文</li> </ul>	楼层排序方式	式 💿 升序	○ 降序		
方案设计满足度:						
目定义Logo	上传Logo	公司名称				
热图设置						
统一配色		▼ 是否包含障碍	厚物 💿 是	0 否		
频段	✓ 2.4G	<b>√</b> 5G	🗌 6G			
执图	✔ 场强仿真图	□ 信干噪比仿真图	□ 物理层吞吐率(	方真图 🗌 应用层吞吐率仿	真图	
1000	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)		



	网规自动检视
环境设置	✓障碍物设置:检查是否有图纸 (所有场景,室内室外GIS等) 没有绘制障碍物。
	✓ 障碍物类型: 检查是否有图纸 (所有场景, 室内室外GIS等) 只绘制了一种障碍物。
设备布放	✓ AP布放过近:检查AP间距,如果有小于8m (26.25英尺),并且AP间没有障碍物。
AP设置	✓ 功率调优: 以楼层/室外区域维度查询AP功率是否均为默认功率。
	✓ 信道设置: 以楼层/室外区域维度查询AP信道是否均为默认信道。
天线设置	✓ 天线款型: 查询室外外接天线的AP是否连接了非推荐的室外覆盖天线款型。
	☑角度设置: 查询单个AP维度下倾角&方位角是否是默认角度。
交付效果	☑ 覆盖满足度: 覆盖满足度是否大于95%。
	✓ 容量满足度: 容量满足度是否大于90%。
	✓ 建网标准达成度: 建网标准达成度是否大于95%。

	✓ 精品网AP选型策略: AP是否满足至少4T4R要求。	
场景化	✓ 定位场景: 1.定位AP间距是否满足小于等于15米。 3.定位AP与障碍物间距是否满足大于等于2米。	2.定位AP之间是否构成等三角形状。 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。

	网观自动位视	
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。	$\sim$
设备布放	• <b>AP布放过近:</b> 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。	$\checkmark$
	• 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%。	$\checkmark$
	• 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%。	$\checkmark$
	• 精品网AP选型策略: AP是否满足至少4T4R要求。	~
场景化	• 定位场景: 1.定位AP间距是否满足小于等于15米。 2.定位AP之间是否构成等三角形状。	~
	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。

🚰 Save archive copy as						×
← → < ↑ 🖡 < HCIP-WLAN实验手册 > HCIP-WLAN网规报告	~	Ü	9	搜索"HCIF	P-WLAN	规报告"
组织 ▼ 新建文件夹					• •	?
▲ 生産 ▲	日期			类型		大小
3D 对象 没有与搜索条件	+匹配的1	顷。				
🔢 视频						
▶ 图片						
🗎 文档						
➡ 下载						
♪ 音乐						
🐛 SystemDisk (C:)						
🥪 Data (D:) 🗸 🧹						>
文件名(N): HCIP-WLANreport.zip						~
保存类型(T): All files						~
▲ 隐藏文件夹			ť	呆存(S)	取	消

#### #查看保存的网规报告。

HCIP-WLAN_	_网规报告.docx
HCIP-WLAN_	_物料清单.xls

# 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
	重点覆盖区域:商铺中间街道、休息区
覆盖区域	普通覆盖区域:停车场
	无需覆盖区域:商铺
	重点区域:≥ -65 dBm
切蚀安水	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。

业务类型	单业务 (Mt	基线速率 ops )	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10-6 室外场景业务占比统计表

## 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 ~ 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/#/toolsummary?entityId=d59de9ac-e4ef-409e-bbdc-eff3d0346b42

# 点击"运行"。

(ce	WLAN Planner 使用次数: 317368 次 评论次数: 1146 版本: v1.0.0 发布时间:	•
Ť	WLAN规划 AP布放 信号仿真	工具接口人
**** 46分	室内、室外AP网络规划工具,包括现场环境规划、AP布放、网络信号仿真和生成网规报告等功能。	yangfubo@huawel.com
▶ 工具评价		8 0 8

# 阅读客户网络数据安全管理规定后,点击确认。



客户网络数据安全管理规范V1.0	$\times$
<ul> <li>一、目的</li> <li>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》、《客户网络数据网络安全操作指导书》,在业务活动中遵从网络安全及隐私保护的相关规定。</li> </ul>	
一、但用论国 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《客户网络数据安全管理规范》	
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。

项目类型:	新建项目 已有项目						
是否涉及客户网络数排	居:○ 是   ◎ 否						
作业凭证:	项目编码 Y TD000000323701 Q 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					

### 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"。

<u>ات</u> ا	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	8	隐藏	佑侧面板 🔀
工勘	₩ 🖪 🗞 🛛	新建	×		障碍物绘制		自动识别: 🍥
8	da Huawei	* Sic 711].	0.004	C	<b>手动绘制</b> ~ 形状	自动吸附(	$\mathcal{D}$
规划		· <sub>区域名称</sub> : <b>2</b>	) 至内 ・至外 HCIP-WLAN室外	+			<u> </u>
記验		*选择场景: 3	选择场量		垣形	折线	斜坡
6		室外类型:	平面間紙 *	<b>–</b>	120 mm	240 mm	240 mm
(5) 设置		楼层地图:	选择文件 未选择文件		普通砖墙 (10dB 15dB 20dB)	加厚砖墙 (15dB 25dB 30dB)	混凝土 (25dB 30dB 35dB)
					8 西育板 (3dB 4dB 9dB)	8 泡沫板 (3dB 4dB 9dB) (	20 空心木 (2dB 3dB 8dB)
		1.选择文件时,推荐导, 2.圆纸名称目前仅支持·	N图纸的大小在200MB以内。 中英文、数字和图约 独独主任。		40 普通木门 (3dB 4dB 9dB)	40 实木门 (10dB 15dB 20dB)	8 普通玻璃 (4dB 7dB 12dB)
					干扰源布放	/	
	AP 教養(一)清教(均数)・0/0 RI 教養(一)清教(均数)・0/0 交換用・0 AD・0		<b>泰要已初</b> 69時渡		一 一 一 式 源	國語	

# 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 HCIjpg	
预览:	X2*201/23	
	a         b         a	
1.选择文件时,推荐 2.图纸名称目前仅支持	寻入图纸的大小在200MB以内。 诗中英文、数字和部分 <u>特殊字符</u> 。	
<b>7</b> 6	<b>旋</b> 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。



#### HCIP-WLAN V2.0 实验指导手册(Web)



# 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。



						某室外步	行街	平面图					
						95	000 mm						1
	服装店	书店	쵩	¥ 饮	X	Je	宇	餐	饮	X	茶馆	珠宝店	
2													沉栗树古
				设置	比例凡	5				×			<b>反直</b> 绘品
Ę		休	包息	ച							。包区		
71000 m				9	长度:	95							
					中1立.	*		•					
					4	确定		取消					
		商	铺								甫 区		
		停	车位	_	_				_		车位		
	进出口					Ű	通道					进出口	
						停	事在位						

# 框选楼栋区域,设置障碍物高度。

设置障碍物高度	×
障碍物高度(米) 5	
确定 取消	
PAIRS PAIRS	

# 环境设置后,效果如下所示。



服装店	书店		餐	饮	X		庙宇	餐	饮	X		茶馆	珠	宝店
	休	、息区					步行街				休息	园区		
	商	鋪		-			] [			あ	鉗	R		
		и <del>н</del> з		<u> </u>			_				TH			
	停车位									ſ	亭车	位		
进出口							通道						ì	#出口
							停车位							

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。





# 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	-	^
alle.	AP类型:	AirEngine5761R-11	T	物联网卡:		*	L
and a state	安装方式:	挂墙	-	挂高:	3.00	m	L
	RTU License	評级: ○是 ◎ 召	E C	工作模式:	基础模式	Ψ.	L
详细信息 3D模型	POE:	802.3af(PoE)					I
<b>射频0</b> ∨ OFF <b>○</b> ON	支持协议:	WiFi6(802.11ax)	~	类型:	2.4G_2*2_65°_40°_10dB	i v	1
	信道:	1	-	高度:	3.00	m	L
类型: 2.4G	频宽:	HE20	-			方位角	L
MIMO: 2*2	功率:	17	Max: 17dBm	$\bigcap$		0	L
	Guard Inter	val: OShort 🔍	Normal	$\sim$		下倾角:	1
	馈线类型:		-			15	I
	支持协议:	WiFi6(802.11ax)	~	类型:	5G_2*2_65°_20°_11dBi	-	1
	信道:	157		高度:	3.00	m	L
类型: 5G	频宽:	HE40+	· ·			方位角。	L
MIMO: 2*2	功率:	23	Max: 23dBm	$\bigcap$		• 0	L
	Guard Inter	val: OShort 🔍	Normal	a	((•))	下倾角:	L
	馈线类型:	请选择	•			₹ 15	Ŧ
		确定	取消				
		POAL	-113				

# 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。



笙306	5页
2000	<u> </u>

<u>11</u> <u>11</u>	名称:	AP-1	颜色:	红色	T
14	AP类型:	AirEngine5761R-11E	物联网卡:		*
444	安装方式:	「挂墙」	挂高:	3.00	m
H H	RTU License	●升级: ○是 ◎否	工作模式:	基础模式	· ·
详细信息 <u>3D模型</u>	POE:	802.3af(PoE)			
<b>射频0</b> OFF ON	支持协议:	WiFi6(802.11ax) -	类型:	2.4G/5G_1*1_360°_30°_4	ldBi/360 🔻
	信道:	13 💌	高度:	3.00	m
类型: <b>2.4G</b> 5G	频宽:	HE20 ~			▲◆向干俅
MIMO: 2*2	功率:	16 Max: 16dBm	$\bigcap$		1 EPU/A
	Guard Inter	val: 🔍 Short 🔍 Normal	( .		下倾角:
	馈线类型:	$= - = \frac{1 - \frac{1}{2} - $		-	0
射频1 → OFF <b>●</b> ON	支持协议:	WiFi6(802.11ax) -	类型:	2.4G/5G_1*1_360°_30°_4	ldBi/360 🔻
	信道:	157 *	高度:	3.00	m
类型: 5G	频宽:	HE40+ ~			
MIMO: 2*2	功率:	26 Max: 26dBm	$\bigcap$		▼王미大戎
	Guard Inter	val: OShort ONOrmal	( .		下倾角:
	馈线类型:		~		< 0

#### 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"。

工具栏		
打开仿真图	刷新仿真图	覆盖满足度
仿真图设置		
频段:	2.4G 🗹 5G	6G
类型: 场	强仿真图	•
仿真图示意		
信号强	1	中 弱
-20 -4	5 -55 -65 -	70 -90
		单位: dBm

# 本项目只需关注商铺之间街道和休息区的信号覆盖情况。



服装店	书店		餐	饮	X		庙宇		餐	饮	X		茶馆	珠宝店
休息区					步行街					休息	〕区			
					-				<b>,</b>					
	商	铺	×	5	AP	3		2	4P-4		商	铺	X	
停车位											ſ	亭车	位	
进出口						通道							进出口	
							停空位							

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。

工具栏
仿真图设置
频段: 🗌 2.4G 🗹 5G 🗌 6G
类型: 场强仿真图 🔹
仿真图示意
信号强中弱
·
-20 -45 -55 -65 -70 -90
申心: dBm

# 本项目只需关注停车场的信号覆盖情况。



服装店	书店	餐	饮	x	庙宇		餐	饮	X		茶馆	珠宝店
休息区					步行街					休息		
				<b>^</b>							2	
	商	铺区	z	AP-3			A7-4		商	铺		
停车位									1	亭车	位	
进出口					通道							进出口
	信念位											

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。

NURCE       Warriage       遊游信       Office       NURCE       NURCE					
IBBrive					
語言       ● 中文       ● 英文       楼园排存方式       ● 升齐       ● 降齐         方案设计满足度:       □       <					
万素设计满足度:					
施商設置        是否包含障碍物       ●       星       ●         統一配色       ●       是       ●       否         频段       【 2.4G       【 5G       ● 6G         热图       【 场强仿真图       ●       信 千噪比仿真图       ●       协理层吞吐率仿真图       ●       应用层吞吐率仿真图         热图       ●       场强仿真图       ●       信 千噪比仿真图       ●       校强定位热图       ●       夏盖满足度         热图滴晰度       ●       标请(不超过0.93M)       ●       商請(不超过1.13M)       ●       越清(原图分辨率不足)					
法価収					
新正     ●     ★     ●     ●       振設     ▼     2.4G     ▼     5G     ●       振超     ●     「音干噪比仿真图     ●     ●     ●       小超     ●     毎     ●     ●     ●       振磁満断度     ●     标滴(不超过0.93M)     ●     ●     ●        ●     ●     ●     ●     ●					
热邀清晰度 ● 标清(不絕过0.93M) ○ 高清(不絕过1.13M) ○ 超清(原图分辨率不足)           网规自动检视					
Realing winde					
网规自动检视					
环境设置					
7 暗碍物米利· 於杏具不有肉斑 (所有话号、安内安外GIS等) 口经制了一种障碍物					
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。					
<b>AP设置   ☑ 功率调优:</b> 以楼层/室外区域维度查询AP功率是否均为默认功率。					
◎ 信息収重・ 以仮法/至力心域出度車川内口店追定占ろ力私以店追。					
天线设置 V 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。					
又门双未 ☑ 復霊病正長: 復ニ病正度定台入丁93℃。					
✓ 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。					
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					
♥● 开始检视 号出报告					

# 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> <li>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。</li> <li>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。</li> </ul>	<b>*</b>
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> <li>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。</li> <li>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。</li> </ul>	<ul><li></li><li></li></ul>
天线设置	<ul> <li>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。</li> <li>角度设置: 查询单个AP维度下倾角&amp;方位角是否是默认角度。</li> </ul>	× ×
交付效果	<ul> <li>覆盖满足度:覆盖满足度是否大于95%。</li> <li>容量满足度:容量满足度是否大于90%。</li> <li>建网标准达成度:建网标准达成度是否大于95%。</li> <li>精品网AP选型策略: AP是否满足至少4T4R要求。</li> </ul>	$\langle \langle \langle \langle \langle \rangle \rangle \rangle$
场景化	定位场景: 1.定位AP间距是否满足小于等于15米。     2.定位AP之间是否构成等三角形状。     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	~
	C 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。



🔤 Save archive copy as						×
← → v ↑ 📙 « HCIP-WLAN实验手机	册 > HCIP-WLAN网规报告	~ Ū	Q	搜索"HCIP	-WLANM	规报告"
组织 ▼ 新建文件夹					• • •	?
▶ 此电脑 ▲ 名称	^	修改日期		类型		大小
🧊 3D 对象	没有与搜	夏索条件匹配的项。				
视频						
■ 图片						
◆下载						
♪ 音乐						
■ 桌面						
💺 SystemDisk (C:)						
🥪 Data (D:) 🗸 🧹						>
文件名(N): HCIP-WLAN_	_report.zip					~
保存类型(T): All files						~
L						
▲ 隐藏文件夹			1	呆存(S)	取	肖

#### # 查看保存的网规报告。

HCIP-WLAN	_网规报告.docx
HCIP-WLAN_	_物料清单.xls

# 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

设备	端口	端口类型	VLAN参数
	MultiGE0/0/1	Trunk	PVID:1
			Allow-pass: VLAN 100 101
SW-Core	MultiGE0/0/9	Trunk	PVID:1
	Watticeorory	Trank	Allow-pass: VLAN 100 101
	MultiGE0/0/5	Access	PVID: 99
SW-Access	MultiGE0/0/9		PVID:1
		Trunk	Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trunk	PVID:100
			Allow-pass: VLAN 100 101
	MultiGE0/0/2	Trucelo	PVID:100
		ттипк	Allow-pass: VLAN 100 101
			PVID:100
	WIULLIGE0/0/5	Пипк	Allow-pass: VLAN 100 101
	CE0/0/1	Trupk	PVID:1
WACI	GE0/0/1		Allow-pass: VLAN 100 101

## 表11-1 VLAN 规划

#### 表11-2 IP 地址规划

设备	端口	IP地址
	Vlanif100	10.23.100.254/24
SW-Core	Vlanif101	10.23.101.254/24
	Vlanif99	172.21.39.253/17
WAC1	Vlanif100	10.23.100.1/24
CampusInsight服务器	/	172.21.39.99/17



#### 表11-3 WLAN 业务参数规划

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

# 11.2 实验任务配置

# 11.2.1 配置思路

1.配置 SW-Core、SW-Access、WAC1 设备的 VLAN 信息。

2. 配置各网络设备的 IP 地址信息,确保网络互通。

3.在核心交换机 SW-Core 上配置 DHCP 服务器,确保 AP 可以获取 IP 地址。

4.配置 WLAN 业务参数,实现 STA 接入。

5.配置 CampusInsight 相关网络,确保网络互通。

6.配置 WAC1 与 CampusInsight 服务器联动。

7.通过 Web 登录 CampusInsight 服务器实现智能运维。

## 11.2.2 配置步骤

步骤 1 配置基础网络、AP上线、无线业务

# 请参考 1.2.2 步骤 1~1.2.2 步骤 7,此处不再赘述。

#### 步骤 2 配置 CampusInsight 与 WAC1 之间网络互通

# CampusInsight 服务器的 IP 地址和网关在软件安装阶段已配置完成,本实验不再赘述。 CampusInsight 地址为 172.21.39.99/17,网关地址是 172.21.39.253(位于 SW-Core 上 )。



#### # 配置 SW-Core 的 VLAN 信息及 IP 地址。

[SW-Core] vlan 99
[SW-Core-vlan99] name Manage
[SW-Core-vlan99] quit
[SW-Core] interface MultiGE 0/0/5
[SW-Core-MultiGE0/0/5] port link-type access
[SW-Core-MultiGE0/0/5] port default vlan 99
[SW-Core-MultiGE0/0/5] quit
[SW-Core] interface Vlanif 99
[SW-Core-Vlanif99] ip address 172.21.39.253 17
[SW-Core-Vlanif99] quit

# 在 WAC1 上配置静态路由,确保 CampusInsight 与 WAC1 之间网络互通。

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

Wireless LAN A 设备名称: WAC1	<u>上</u> 监控	<b>谷</b> 配置	<b>(干)</b> 诊断	┃↓↓ 维护	
● 配置向导	DHCP地址池	DHCP中继	NAT 3	路由	DNS
<ul><li>● AC配置</li></ul>	→路由表				
基本配置 4	↓ 静态路由配置表				
VLAN 5	新建删除	刷新			
接口管理	目的IP地址・			子网掩	码 -
<b>2</b> IP					

# 在"新建静态路由"页面,依次分别配置如下两条静态路由,然后点击"确定"。其中静态路由 0.0.0.0/0 用于访问其他外部网络,静态路由 172.21.39.99/32 用于访问 CampusInsight 服务器。

AC配置 > IP > 語由 > 新建静态語由						
*目的IP地址:	0.0.0.0	*子网掏码:	0.0.0.0			
下一跳:	10 , 23 , 100 , 254	出接口:	Vlanif100 X			
优先级:		描述:				
確定 取消						
AC配置 > IP > 路由 > 新建静态	語曲					
*目的IP地址:	172 . 21 . 39 . 99	*子网掏码:	255 , 255 , 255 , 255			
下一跳:	10 , 23 , 100 , 254	出接口:	Vlanif100 X			
优先级:		描述:				
確定取消						

# 配置完成后,查看静态路由如下所示。



Wireless LAN AirEngine9700-M1 设备名称: WAC1		<u></u> 监控	<b>袋</b> 配置	(➡) 诊断	<b>    </b> 维护	
● 配置向导	DHCP地址池	DHCP中继	NAT	路由	DNS	
● AC配置	→路由表					
基本配置	↓ 静态路由配置表					
VLAN	新建					
接口管理	目的IP地址 🔺	子网掩码 🔺	下一题	K ▲	出接□▲	优先级 🔺
IP	0.0.0.0	0.0.0.0	10.23	.100.254	Vlanif100	60
● AP配置	172.21.39.99	255.255.255.25	55 10.23	.100.254	Vlanif100	60
● 安全管理	10 ▼ 共2条					

#### 步骤 3 配置 SNMP 协议

# 配置 SNMP 协议的目的是将 WAC1 添加至 CampusInsight 中进行管理。SNMPv2c 是不安 全协议,建议配置更加安全的 SNMPv3 协议。

# 选择 "维护 > AC 维护 > SNMP",选择 "全局配置"选项卡,开启 SNMP 代理功能,并 按照如下参数进行配置,然后点击"应用"。



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	いた。	<b>于</b> 诊断	<b>↓↓↓</b> 维护	
● AC维护	全局配置	团体/组管理	<b>MIB</b> 视图	Trap设	置	
License管理	SNMP代理:					
设备重启	*SNMP版本:	v1	v2c 💽 v	/3		
特征库升级	SNMP协议源接口:	○ 所有措	度口 💿 指定的	度口 〇 无		
Web文件更新		Vlanif1	00			
日志管理	本地引擎ID:			5A224		
告警&事件	设备位置:	Shenzh	ien China			
管理员	联系方式:	R&D S	henzhen, Huaw	ei Technologi	ies Co., Ltd.	
系统管理	应用					
部件电子标签						
SNMP						
WMI						
恢复出厂设置						

# 选择 "维护 > AC 维护 > SNMP",选择 "MIB 视图"选项卡,点击"新建",新建 MIB 视图。



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 设备名称: WAC1	AirEngine9700-M1     Image: Constraint of the second
<ul><li>● AC维护</li></ul>	全局配置 团体/组管理 MIB视图 Trap设置
License管理	MIB视图
设备重启	新建 删除 显示视图规则 刷新
特征库升级	视图名称 ▲
Web文件更新	ViewDefaultBasic
日志管理	10 ▼ ±2条
告警&事件	视图规则
管理员	
系统管理	
部件电子标签	
SNMP	
WMI	
恢复出厂设置	

# 在 "MIB 视图 > 新建视图规则 " 界面,配置如下参数,然后点击 "确定 "。其中视图名称 为 HCIP-test,规则包含 iso 子树。

) 排 <b>2</b> ④ 包含	* MIB子树名称: is	50	MIB子树掩码:	3 0
规则		MIB子树名称/OID	MIB子树掩码	×
		暂无数据		
	] 我见则	] 我现到	规则 MIB子树名称/OID 暂无数据	規则 MIB子树名称/OID MIB子树掩码 暫无数据

# 选择 "维护 > AC 维护 > SNMP",选择 "团体/组管理"选项卡,在"组(适用于 SNMPv3 )"中点击"新建",新建组。



全局配置	团体/组管理	MIB视图	Trap设置				
→团体(适用	→团体(适用于SNMPv1或SNMPv2c)						
↓ 组(适用于:	SNMPv3)						
新建	刷除    刷新						
_ 组名 ▲		安全级别 🔺		只读视图 🔺			
→用户(适用	→用户(适用于SNMPv3)						

# 在"团体/组管理 > 新建组"界面,配置如下参数,然后点击"确定"。其中组名为 testgroup,安全级别为认证并加密,读写视图和通知视图为 HCIP-test。

AC维护 > SNMP >	› 团体/组管理 > 新建组	
*组名:	test-group	*安全级别: 认证并加密 🔻
只读视图:	ViewDefault 👻	读写视图: HCIP-test 平
通知视图:	HCIP-test 👻	ACL编号: - none - 🔍 🔻
确定取消		

# 选择 "维护 > AC 维护 > SNMP",选择 "团体/组管理"选项卡,在 "用户(适用于 SNMPv3 )"中点击"新建",新建用户。

全局配置	团体/组管理	MIB视图	Trap设置				
→团体(适用-	→团体(适用于SNMPv1或SNMPv2c)						
→组(适用于S	SNMPv3)						
↓用户(适用=	FSNMPv3)						
新建 册	<b> 除                                    </b>						
用户名 ▲		认证算法	<u>t</u>				

# 在"团体/组管理 > 新建用户"界面,配置如下参数,然后点击"确定"。其中用户名为 test-user,认证密码为 Huawei@123,加密密码为 Huawei@456,需与 CampusInsight 侧配 置一致。



AC维护 > SNMP > 团体/	/组管理 > 新建用户			
*用户名:	test-user		]	
组名称:	test-group	Ŧ	]	
安全级别:	认证并加密	Ŧ	(推荐使用认证并加密	其他级别存在安全风险)
认证方式:	• SHA2-256			
*认证密码:	Huawei@123	0		
加密方式:	AES128 AES192	۲	AES256	
*加密密码:	Huawei@456	0		
确定取消				

# 最后,选择"维护 > AC 维护 > 系统管理",选择"管理面隔离"选项卡,按照如下步骤 添加逻辑管理口 Vlanif 100,然后点击"应用"。

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	「「」」	く 配置	(┿) 诊断	<b>↓↓↓</b> 维护	
O AC维护	服务管理1	管理面隔离	文件管理	系统时间		
License管理	管理面隔离:	C	ON			
设备重启	逻辑管理口:	1 <sup>1</sup>	影选择	2	😌 (最多添加4条数据)	
特征库升级			接口名称			×
Web文件更新		8	Vlanif100			
日志管理						
告警&事件						
管理员						
系统管理	4 应用					
部件电子标签						

#### 步骤 4 配置 SFTP 协议

# 配置 SFTP 协议的目的是使 CampusInsight 能使用 SFTP 协议从设备侧同步 AP 基本信息、端口信息、链路信息等。



# 选择"维护 > AC 维护 > 系统管理",选择"服务管理"选项卡,开启 SFTP 服务,并配置 SSH 服务端源接口为"所有接口",然后点击"应用"。

服务管理 管理面隔	离 文件管理 系统时间	
服务管理		
● FTP或者Telnet服务存在安	全风险,推荐使用STelnet和SFTP服务。	
SSH服务		
STelnet:		SFTP:
SSH服务端源接口:	<ul> <li>所有接口</li> <li>指定接口</li> <li>无</li> </ul>	
Telnet服务		
IPv4 SSH/Telnet:	OFF	IPv6 Telnet: OFF
Telnet服务端源接口:	○ 所有接口 ● 指定接口 ○ 无	
	MEth0/0/1	
FTP服务		
IPv4 FTP:	OFF	
IPv6 FTP:	OFF	
FTP服务端源接口:	○ 所有接口 ● 指定接口 ○ 无	
	MEth0/0/1	
WEB服务		
HTTPS服务端源接口:	○ 所有接口 ● 指定接口 ○ 无	
	MEth0/0/1	
WEB服务器超时时间(分钟):	1440	
应用		

#### 步骤 5 配置 LLDP 链路发现协议

# 配置 LLDP 链路发现协议的目的是使 CampusInsight 能够发现设备的 LLDP 链路。

#### # 在 WAC1 上启用全局 LLDP,确保状态为"ON",如下所示。

Wireless LAN Ain 设备名称: WAC1	Engine9700-M1	<u></u> 监控	<b>谷</b> 配置	(➡) 诊断	<b>{                                    </b>
• 配置向导	LLDP				
● AC配置	全局LLDP状态:	ON			
● AP配置	选择所有接口				
● 安全管理		2 4	68	10 12	
QoS					
⊙ 扩展业务					
mDNS		1 3	5 7	9 11	
VPN		Up 📋 C	)own 💼 S	hutdown	
LLDP	接口LLDP开启	接口LLDP关	म्र		


#### #开启AP的LLDP邻居上报功能。

# 选择 "配置 > AP 配置 > AP 组配置",选择 "AP 组"选项卡,点击 "ap-group1",进 入此 AP 组的配置界面。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1 监控 首	<ul> <li>↓</li> <li>↓</li></ul>	∲ ↓ 维护
● 配置向导	AP组 静态负载均衡组		
● AC配置	修改新建制除刷新	)	
⊙ AP配置	□ 组名称 ▲ VAP模板 ▲		射频0模板 ▲
ΔD组配罢	default		2.4G-default
	ap-group1		2.4G-default
AP配置			
射频规划/调优	20 ▼ 共2条		

# 在 AP 组配置界面中,选择 "AP > AP 系统模板",对缺省的 AP 系统模板(名称为 default )进行配置,点击"高级配置",开启 LLDP 协议的邻居上报功能,然后点击最下方 的 "应用",使配置生效。

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	<u></u> 监控	な。	(十) 诊断	<mark>は</mark> 维护
• 配置向导	AP配置 > AP组配置	> AP组			
● AC配置	AP组配置: ap-gro	oup1 ▼ ₫	语 着成员		
● AP配置	显示所有模板	27		配置樹	輕型介绍
AP组配置	I ► VAP配置				
AP配置	I ■ 「「」「」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「				
射频规划/调优	■ ■ ■ AP系统模板 田 ■ AP有线口配	置		[0	default]
分支AP组配置	<ul> <li></li></ul>	KO		[0	default]
模板管理					



* AP系统模板:	default 🔻	展示模板引用关系新建			
模板介绍信息: AP系统模板提(	共对AP系统参数的配置、引用终端鼎	黑白名单模板以及频谱分析。			
基础配置 高级配	置				
断链业务保持策略:	不保持				
MTU (bytes):	1500	0			
管理VLAN:					
AC-AP间数据隧道DTLS加密:	● 遺循全局 ○ 开 ○ 关	0			
→ 广播組播抑制					
$\rightarrow$ Mesh					
→ 双链路/N+1备份					
↓ LLDP					
LLDP使能延迟时间(秒):	2		工作模式:	接收和发送	Ŧ
报文发送延迟时间(秒):	2		报文发送间隔(秒):	30	
报文存活时间(发送时间倍数):	4				
邻居上报:			邻居上报抑制时间(秒):	30	

步骤 6 配置日志数据、WLAN 业务数据上报功能

# 数据上报功能默认支持 HTTP/2 和 UDP 两种协议通道,推荐使用 HTTP/2 协议。

# 配置 WAC1 设备的 HTTP/2 协议通道。选择"维护 > AC 维护 > WMI",选择"通道 1" 选项卡,配置如下参数,然后点击"应用"。其中服务器地址为 172.21.39.99,端口号为 27371。

通道1 通道2			
*服务翻地址:	172 , 21 , 39 , 99	*端口:	27371
上报周期(s):	60	单次数据上报最大量(KB):	5
心跳时间(min):	3	服务器重连间隔(min):	5
重连次数:	0 0		
监控数据上报:	✓ 设备 ✓ 接口 ✓ CPCAR ✓ 应用 ✓ 日志 ✓ 安全 ✓ iPCA2.0		
设备监控数据上报间隔(s):	10	接口监控数据上报间隔(s):	60
CPCAR监控数据上报间隔(s):	300	应用统计监控数据上报间隔(s):	300
日志监控数据上报间隔(s):	300	安全监控数据上报间隔(s):	300
上报的日志模块: 💙	✔ 终端上下线 ✔ 设备操作 ✔ 端口 ✔ 硬件故障 ✔ 云盒上下线 ✔ 无线射频 🗌 自定义		
应用    清空			

# 配置 AP 设备的 HTTP/2 协议通道。选择"配置 > AP 配置 > AP 组配置",进入"apgroup1"的配置界面中,选择"AP > AP 系统模板 > WMI 模板(通道 2 )",点击"新 建",新建一个 WMI 模板,配置模板名称为 test,然后点击"确定",如下所示。



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	な。配置	(十) 诊断	∲↓ 维护		
● 配置向导	AP配置 > AP组配置 >	AP组					
● AC配置	AP组配置: ap-grou	ip1 🔻 査	<b>看</b> 成员			新建WMI模板	
⊙ AP配置	显示所有模板			配置模	型介绍	*模板名称:	test
AP组配置	田 <b>一</b> VAP配置					确定取消	í
AP配置	<ul> <li>■ ■ 射频管理     <li>□ ■ ■ AP     </li> </li></ul>						
射频规划/调优	□ ■ AP系统模板 ● 终端黑白名	名单模板		[de	efault]		
分支AP组配置	I WMI模板( I WMI模板(	通道1) 通道2)					
模板管理	団 一 AP有线口配置 団 目 ETH-TRUNK(	1		[de	efault]		
● 安全管理	🗉 ┢ WIDS				-		

# 按照如下参数配置名称为 test 的 WMI 模板,然后点击"应用",使配置生效。

WMI模板:	test 🔻 展示模板引用关	系新建	
模板介绍信息: WMI模板提供对AP向	WMI服务器上报信息参数的配置。		
*服务器地址:	172 . 21 . 39 . 99	* 満口:	27371
上报周期(s):	60	单次数据上报最大量(KB):	5
心卿时间(min):	3	服务器重连间隔(min):	5
重连次数:	0		
终端识别数据上报:	DHCP Option 🗹 HTTP UA 📝 mDNS		
DHCP Option数据上报间隔(s):	300	HTTP UA数据上报间隔(s):	300
mDNS数据上报间隔(s):	300		
监控数据上报:	<ul> <li>✓ 设备</li> <li>✓ SSID</li> <li>✓ 射频</li> <li>✓ 接口</li> <li>✓ 终端</li> <li>✓ EMDI</li> <li>✓ 应用</li> <li>✓ 位置</li> <li>✓ 日志</li> <li>✓ iPC4</li> </ul>	✓ 邻居无线设备 ✓ CPCAR A2.0 ✓ DNS ✓ Non-Wi-Fi	
设备监控数据上报间隔(s):	10	SSID监控数据上报间隔(s):	60
射频监控数据上报间隔(s):	10	接口监控数据上报间隔(s):	60
终端监控数据上报间隔(s):	10	邻居无线设备监控数据上报间隔(s):	60
CPCAR监控数据上报间隔(s):	300	EMDI监控数据上报间隔(s):	10
应用统计监控数据上报间隔(s):	300	位置监控数据上报间隔(s):	60
日志监控数据上报间隔(s):	300	DNS监控数据上报间隔(s):	60
Non-Wi-Fi设备数据上报间隔(s):	60		
上报的日志模块: 😯	☑ 终端上下线 🛛 设备操作 🕢 端口 📝 音视	频应用分析 🕢 云盒上下线 📝 无线射频 🗌 自定义	
应用			

## 步骤 7 配置 CampusInsight 服务器

# 登录 CampusInsight,在主菜单中选择"资源",然后选择"站点-区域"页签,点击"添加"按钮。



iMaster NCE Campusinsight	ΰ	站点-区域				
		站点-区域	有线设备	无线设备	链路	
🕲 Global						
▶ 🕲 未选择站点	>	输入名称进行搜索		⊙ 添加	立 删除	
<b>出</b> 仪表盘		🖃 🍘 Global		□ 名称		
🚫 网络						
-♪ 用户						
🔆 资源						
③ 系統						
	为 "HCII		"Global",	然后点击"确	 定"。	

iMaster NCE Campusinsight	€ 站点-[ 	⊠域	
(Global	*类型: ● \$	站点	
◎未选择站点 >	*名称: H(	CIP-test	
	*父节点: GI		
日本の表金			
	备注:		
<b>-/.</b> 用户			
・ 資源	确定	取消 应用	
③ 系统			

# 选择"资源 > 有线设备",点击"增加设备",选择"单个添加"。



iMaster NCE CampusInsight	ΰ	有线设备				
(a) Global		站点-区域 <b>_</b>	有线设备	无线设备	链路	
♪◎未选择站点	>	⊙ 增加设备 ▼	【 设备导出 ▼	🔒 设置协议 🔻	<b>立</b> 删除设备	≭ 同步
<b>出</b> 仪表盘		<b>单个添加</b> 批量导入				
── 网络			名称 🖇	IP地址◆	MAC +	设备型号。
小,用户						
🚭 资源						

# 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"testuser",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。

基本信息					
IP地址:	10.23.100.1			★站点-区域: HCI	
设备角色:	WAC				
SNMP协议					
自动匹配SNN	MP参数模板 🔘 手动选择SNMI	参数模板 💿 手动编辑SNMP参数			
) 请根据设备例	的SNMP协议信息配置模板中的	参数。协议版本建议使用安全性较高的v3	协议。使用SNMPv3时,鉴权协	ΏHMAC_SHA、HMAC_MD5和HMAC_	_SHA2_224由于
) 请根据设备便 升安全性。建	的SNMP协议信息配置模板中的 议认证密码和加密密码不一致。	参数。协议版本建议使用安全性较高的v3	协议。使用SNMPv3时,鉴权协	汶HMAC_SHA、HMAC_MD5和HMAC_	_SHA2_224由于H
〕 请根据设备便 升安全性。 建	的SNMP协议信息配置模板中的 议认证密码和加密密码不一致。	參数。协议版本建议使用安全性较高的v3	协议。使用SNMPv3时,鉴权协	ஜнмас_sha、hmac_md5ŧ@hmac_	SHA2_224由于
〕 请根据设备像 升安全性。建	的SNMP协议信息配置模板中的 10以证金码和加密查码不一致。	参数。协议版本建议使用安全性较高的v3	协议。使用SNMPv3时,鉴权协	хнмас_sha、hmac_mds和hmac_	<u>SHA2_224由于</u> I
) 请根据设备像 升安全性。建 版本:	的SNMP协议信息配置模板中的 NX认证者码和加密者码不一致。 V3	參数。协议版本建议使用安全性较高的v3	协议。使用SNMPv3时,鉴权协	хнмас_sha、hmac_mdsяанмас_	_SHA2_224由于H
请根据设备便 升安全性。 建 版本: 安全名:	的SNMP协议信息配置模板中的 NX认证费码和加密费码不一致。 V3 test-user	參数。协议版本建议使用安全性较高的v3	协议。使用SNMPv3时,鉴权协	xhmac_sha、hmac_mdsŧihmac_	SHA2_224由于ŧ
<ul> <li>请根据设备便 升安全性。如</li> <li>版本:</li> <li>安全名:</li> <li>盗权协议:</li> </ul>	的SNMP协议信息配置模板中的 改认证密码和加密密码不一致。 v3 test-user HMAC_SHA2_256	参数。协议版本建议使用安全性较高的v3	协议、使用SNMPv3时,鉴权协 、 、 、 、	XHMAC_SHA、HMAC_MD5和HMAC_ XHMAC_SHA、HMAC_MD5和HMAC_	SHA2_224曲于ŧ
<ul> <li>清根据设备像 升安全性。如</li> <li>新安全性。如</li> <li>版本:</li> <li>安全名:</li> <li>鉴权协议:</li> <li>私有协议:</li> </ul>	的SNMP协议信息配置模板中的 议认证密码和加密密码不一致。 v3 test-user HMAC_SHA2_256 AES_256	参数。协议版本建议使用安全性较高的v3	<b>协议、使用SNMPv3时, 盗权协</b> 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	xHMAC_SHA、HMAC_MD5和HMAC_ 。认证密码: ,加密密码:	SHA2_224曲 <del>]  </del>
<ul> <li>) 请根据设备像 升安全性。如</li> <li>////////////////////////////////////</li></ul>	的SNMP协议信息配置模板中的 NX认证部码和加密部码不一致。 v3 test-user HMAC_SHA2_256 AES_256 161	參致。 协议版本建议使用安全性较高的v3	<b>协议、使用SNMPv3时, 盗权协</b> 	xHMAC_SHA、HMAC_MD5和HMAC_ - 认证密码: - 加密密码: - 超时时间(秒):	SHA2_224曲开 

# 检查有线设备上线状态,发现 WAC1 已经在线。



有线	设备							
Å	站点-区域	有线设备	无线设备	链路				
O I	曾加设备 🔻	1 设备	3出 🔻 🔀 й	置协议 ▼ 前 删除设备	香 米 同步 🕂 穆	动 🖪 设	≝License ▼	
	铤							
	状态:	名称:	IP地址 ÷	MAC +	设备型号 ÷	设备分类	厂商	站点-区域
	• 在线	WAC1	10.23.100.1	9C-B2-E8-B5-A2-24	AirEngine9700-M1	AC	Huawei	/HCIP-test
共1条								

# WAC1 添加到 CampusInsight 后,其管理的 AP 将会自动添加到 CampusInsight 的 AP 列表 当中,点击"无线设备",发现三台 AP 均已在线。

无线	设备								
\$	占点-区域	有线设	遙	无线设备	链路				
+ ;	移动 🕻	设置Licen	se 🔻	12 区域规划导入	🕻 区域规划导出 🔻				
	新选								
	状态 🕈	名称 🕴	AP分类	AP型号。	IP地址。	ESN +	MAC +	接入AC名称。	站点-区域
	● 在线		FIT AP	AirEngine5761-11	10.23.100.214	2102353VU	9c-b2-e8-2d-54-10	WAC1	Unplanned
	● 在线		FIT AP	AirEngine5761-11	10.23.100.117	2102353VU	9c-b2-e8-2d-51-10	WAC1	Unplanned
	● 在线		FIT AP	AirEngine5761-11	10.23.100.225	2102353VU	9c-b2-e8-2d-54-f0	WAC1	Unplanned
共3条									

# 在 "HCIP-test"站点中添加楼宇。选择 "资源 > 站点-区域",选中 "HCIP-test",然后 点击 "添加"。

iMaster NCE Campusinsight	Φ	站点-区域					
(B) Global		1 站点-区域	有线设备		无线设备	链路	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	>	输入名称进行搜索		Q <mark>3</mark>	④ 添加	<b>立</b> 删除	
品 仪表盘		<ul> <li>Global</li> <li>HCIP-test</li> </ul>			□ 名称		类型
── 网络							
-♪- 用户							
そ 资源							
③ 系统							

# 类型选择"楼宇",名称配置为"Building\_01",点击"确定"。



iMaster NCE CampusInsight	© 站点-区域
(a) Global	<b>∗</b> 类型: ○区域 ● 楼宇
♪◎未选择站点 >	▲名称: Building_01
田 (V表盘	★父节点: HCIP-test 备注:
<ul> <li>← 資源</li> <li>○ 系统</li> </ul>	确定 取消 应用

# 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"。

iMaster NCE CampusInsight	ΰ	站点-区域	
) Global		1 站点-区域 有线设备 无线设备 链路	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	>	输入名称进行搜索 ○ 3 ⊙ 添加 谊 删除	
<b>日日</b> 仪表盘		<ul> <li>□ Global</li> <li>□ Structure</li> <li>□ A称</li> <li>□ A</li> <li>□ A</li> </ul>	类型
₩ 网络			
小,用户			
ぞ 资源			
◎ 系統			

# 类型选择"楼层",名称配置为"First floor",点击"确定"。



iMaster NCE CampusInsight	<sup>⑥</sup> 站点-区域
() Global	▲类型: ● 楼层
◎□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	★名称: First floor
田 (V表盘)	▲父节点: Building_01 备注:
<b>-/-</b> 用户	
そ 资源	确定 取消 应用
③ 系统	

# 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。

	无约	设备					
		站点-区域	有线设备	无线设备	·		
2	÷	移动	设置License 🔻	山区域	2. 図域规划导出 ▼		
					移动至站点-区域	×	
1		状态 🗧	名称 =	AP分类			接入AC
1		• 在线		FIT AP	● AP只能移动至楼层中。		WAC1
		• 在线		FIT AP	输入名称进行搜索 Q		WAC1
		● 在线		FIT AP	🖃 🖨 Global		WAC1
	共3条				<ul> <li>Unplanned</li> <li>HCIP-test</li> <li>Ill Building_01</li> <li>Ill S First floor</li> </ul>		

# 发现三台 AP 的"站点-区域"已经变更为"/HCIP-test/Building\_01/First floor"。

站点-区域	有线	设备 	无线设备	链路				
<b>+</b> 移动	🖪 设置Lice	nse 🔻	2 区域规划导		观划导出 🔻			
7 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		FIT AP	AirEngin	10.23.100.214	21023	9c-b2-e8	WAC1	/HCIP-test/Building_01/First floor
] • 在线		FIT AP	AirEngin	10.23.100.117	21023	9c-b2-e8	WAC1	/HCIP-test/Building_01/First floor
● 在线		FIT AP	AirEngin	10.23.100.225	21023	9c-b2-e8	WAC1	HCIP-test/Building 01/First floor

#### 步骤 8 配置 CampusInsight 运维功能

#### # 查看整网状态。

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





		iMast	er NCE-Ca	mpusInsi	ght 智能运维	•.).	ä	
		D	Ĩ	流量 75.85 <sub>MB</sub>		<b>②</b> 1	急-区域数	
接入用户统计 <sup>①</sup> 2 ————							接入类型 射频 S	SSID
1								
00:00 00:20 AP速率/流量	00:40 01:00 01:20 01:40	0 02:00 02:20 02:40 (	03:00 03:20 03:40 04	:00 04:20 04:40 05	:00 05:20 05:40 06:00 06:2	0 06:40 07:00 07:20	07:40 08:00 08:20 蔬入	流出
Kbps 30 25			盘显最大值 (5分钟) : 	1,100.48KB 总流量: 建率 II 流量	106,343.42KB			KB 1,431 1,200
20 15 10 5 0 00:00	01:00 0.	2:00 03:00	0 04:00	05:00	06:00	07:00	08:00 09:	900 600 300 0 500

# 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。

健康度	健康度趋势	7				
100% 接入成功率	%			平均值 94.70%	最大值 95.83%	最小值 93.42%
音吐 接入耗时 94	80 60					
展游 达标率 65.33%						
99.02% 信号与干扰	0 00:00	02:00	04:00	06:00	08:00	

# 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。



接入成功率 1 文	伊 100 %	关联成功率 认证成功率 DHCP成功率	=% =% <b>=</b> 100%	% 100 75 50 25 0 00:00	01:00
接入耗时	(作) 5 ms	关联耗时 认证耗时 DHCP耗时	=ms =ms = 5ms	ms 5 4 3 2 1 0 00:00	01:00

漫游达标率		漫游成功率 漫游耗时 漫游前信号强度	% ms dBm	% 100 75 50 25 0 00:00	01:00
信号与干扰 1 文	伊 99.02 %	信号强度达标率 干扰达标率	<b>-</b> 100% - 98.03%	% 100 75 50 25 0 00:00	01:00



容量健康度				%	
		信道利用率达标率		100	
	R		65.33%	75	
	65.33	用户数达标率		50 25	
	%		<b>100%</b>		
				00:00	01:00
吞吐达标率					
$\sim$		非5G优先占比		% 100	
			0%	75	
		空口拥塞达标率	1000/	50	
-	100		<b>-</b> 100%		
	%	市克	172Mbps	0	01-00
				00:00	01:00

- # 查看用户旅程。
- #选择"用户 > 用户旅程",在"常规视图"页签中可以查看接入用户的基本信息。

2个结果, 耗时: 260ms										
常规视图 VIP	视图 当前用	户								
▽ 筛选										
用户MAC	用户名	质差时长。	VIP 用户	接入类型	总体验时长。	平均RSSI(dBm) °	平均下行速率。	总流量。	时延(窒秒)。	丢包率(%)
08-1f-71-53-90-6f	081f7153906f				9小时14分钟		<1bps	12.37KB	0.23	0
08-1f-71-53-90-b4	081f715390b4				9小时14分钟		1.2Kbps	77.66MB		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。

网络管理员保障用户体验; 通益时间范围内用户接入	入所有区域、极非、极层等产生的数据。			
新時間で 100.00% Solbin 2.4G/SGbbM	・・・ 1.36ms <sup>平均通道</sup> (い) -30dBm 平均面句編成	(Ť) 11小时17分钟 回日体粉95 (ア) 172.64 Mbps 平均研究	レー 94.93MB 近意 く1% 平均売価単	
0000 01.00	02:00 03:00 04:5	90 05.00 05.00 07.00	<b>ම දුඩුවාදී ම රැදුවාදී ම DHC</b> 08:00 09:00 10:00	P供敷
03:00 04:00	05:00 06:00	07:00 08:00	09:00 10:00 11:00	
Abps) 📕 1844(Mbps)	Mbps % 180 100 135 75	■ @\$\$\$\$\$\$ \M\^\N\^\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	REECONS) 22 In MWM OIL MANAGAN W 15	
	Rest 28.600 00000 04448: 28.800 00000000000000000000000000000000	000000000000000000000000000000000000	Rest         Rest         Rest         Rest         Rest         Important           Important         Impo	PRETERENDER         State         State



# 11.3 结果验证

# 11.3.1 查看 WAC1 的 SNMP 协议

# 查看 SNMP 协议的全局配置。选择"维护 > AC 维护 > SNMP",选择"全局配置"选项卡 即可查看,如下所示。

Wireless LAN 。 设备名称: WAC1	AirEngine9700-M1	<u>上</u> 监控	なる	(➡) 诊断	<b>11</b> 维护
<ul><li>● AC维护</li></ul>	全局配置	团体/组管理	MIB视图	Trap设置	2
License管理	SNMP代理:				
设备重启	*SNMP版本:	v1	v2c 🗸	/3	
特征库升级	SNMP协议源接口:	○ 所有接	印 💿 指定	g口 ○ 无	
Web文件更新		Vlanif1	00		
日志管理	本地引擎ID:			5A224	
告警&事件	设备位置:	Shenzh	en China		
管理员	联系方式:	R&D Sł	nenzhen, Huaw	ei Technologie	s Co., Ltd.
系统管理	应用				
部件电子标签					
SNMP					



# 查看 SNMP 协议的组信息和用户信息。选择"维护 > AC 维护 > SNMP",选择"团体/组管理"选项卡即可查看,如下所示。

Wireless LAN A 设备名称: WAC1	AirEngine9700-M1	监控	<b>会</b> 配置	(➡) 诊断	<b>↓↓↓</b> 维护	
<ul><li>● AC维护</li></ul>	全局配置	团体/组管理	MIB视图	Trap设置	2	
License管理	→团体(适用于9	SNMPv1或SNM	Pv2c)			
设备重启	√组(适用于SN	IMPv3)				
特征库升级	新建 删除	刷新				
Web文件面新	组名 ▲		安全级别 🔺	只读视图	读写视图 🔺	通知视图 🔺
	test-group		认证并加密	ViewDefau	ult HCIP-test	HCIP-test
日志管理						
告警&事件	10 ▼ 共1条					
管理员	→用户(适用于5	SNMPv3)				
安広禁囲	新建删除	1 刷新				
杀死官庄	用户名 🔺		认证算	法 🔺	加密算法	组名称
部件电子标签	test-user		SHA2-	256	AES256	test-group
SNMP	10 🔻 共1条					
WMI						



# 查看 SNMP 协议的 MIB 视图。选择 "维护 > AC 维护 > SNMP",选择 "MIB 视图"选项卡即可查看,如下所示。

Wireless LAN A 设备名称: WAC1	irEngine9700-M1	监控	<b>☆</b> 配置	(手) 诊断	<b>♀↓↓</b> 维护
● AC维护	全局配置	团体/组管理	MIB视图	Trap设置	
License管理	MIB视图				
设备重启	新建删除	显示视图规则	刷新		
特征库升级	<ul><li>● 视图名称 ▲</li><li>HCIP-test</li></ul>				
Web文件更新	ViewDefault				
日志管理	ViewDefaultB	asic			
告警&事件	10 🔻 共3条				
管理员	视图规则				
系统管理					
部件电子标签					
SNMP					

## 11.3.2 查看 WAC1 的 AP 状态和 VAP 信息

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



AP列表						
智能诊断	上线失败记录 下线记	品录 SoftGRE隧道状态	导出信息 loT插卡信息			
AP ID * 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 ▲ ▽			
0	AP1	ap-group1	normal			
1	AP2	ap-group1	normal			
2	AP3	ap-group1	• normal			
10 🔻 共3筹	N.					
总AP数:3 normal:3						
AirEngine5761-1	11:3					

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

AP型VAP列	康							
应用统计源	青零							
AP ID 🔺	AP名称 ▲	射频ID▲	WLAN ID 🔺	SSID 🔺	BSSID -	认证方式 ▲	接入用户数 🔺	状态 ▲
0	AP1	0	1	wlan-net	9cb2-e82d-54f0	WPA/WPA2-PSK	0	on
0	AP1	1	1	wlan-net	9cb2-e82d-5500	WPA/WPA2-PSK	0	on
1	AP2	0	1	wlan-net	9cb2-e82d-5410	WPA/WPA2-PSK	0	on
1	AP2	1	1	wlan-net	9cb2-e82d-5420	WPA/WPA2-PSK	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	WPA/WPA2-PSK	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	WPA/WPA2-PSK	0	on
10 💌 🛓	共6条							
注: 选择列表。	中的VAP,查看该	VAP应用统计信	自。					

# 11.4 配置参考

# 11.4.1 WAC1 配置

Software Version V200R021C00SPC100

#



#

#

#

#

#

#

#

#

#

#

#

#

stp enable

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 management-port isolate enable management-plane isolate enable mgmt isolate disable interface Vlanif1 ip address dhcp-alloc unicast interface Vlanif100 ip address 10.23.100.1 255.255.255.0 management-interface interface MEth0/0/1 ip address 172.21.39.4 255.255.255.0 interface Ethernet0/0/47 ip address 169.254.3.1 255.255.255.0 interface GigabitEthernet0/0/1 port link-type trunk port trunk allow-pass vlan 100 to 101 interface NULL0 snmp-agent local-engineid 800007DB039CB2E8B5A224 snmp-agent group v3 test-group privacy write-view HCIP-test notify-view HCIP-test snmp-agent mib-view HCIP-test include iso snmp-agent usm-user version v3 test-user snmp-agent usm-user version v3 test-user group test-group snmp-agent usm-user version v3 test-user authentication-mode sha2-256 %^%#FuNM(|kva(w1dtRftXo#jiNM&VK`F7+0:q4pgdO\$%^%#

```
snmp-agent
#
```

snmp-agent usm-user version v3 test-user privacy-mode

snmp-agent protocol source-interface Vlanif100

aes256 %^%#88a5+3fR\_HZ%+\$U&6[3W!,{6V{#@8!/e(uKgo%MD%^%#



```
ssh server-source -i all
sftp server enable
stelnet server enable
undo telnet server enable
undo telnet ipv6 server enable
telnet server-source -i MEth0/0/1
ssh server secure-algorithms cipher aes256_ctr aes128_ctr
ssh server secure-algorithms hmac sha2_256
ssh server key-exchange dh_group16_sha512 dh_group15_sha512 dh_group_exchange_sha256
ssh client secure-algorithms cipher aes256_ctr aes128_ctr
ssh client secure-algorithms hmac sha2_256
ssh client key-exchange dh_group16_sha512 dh_group15_sha512 dh_group_exchange_sha256
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif100 10.23.100.254
ip route-static 172.21.39.99 255.255.255.255 Vlanif100 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#oG(.YIRAzU23F-8q]VL"~+1TE6-L)4wP,#=p8IBK%^%#
capwap dtls inter-controller psk %^%#tc.5LFZ\oJ^bM8'*YYv#<te,1Oq8kAl.}J+v{puP%^%#
capwap message-integrity psk %^%#eJ&eRx\$KYW0b\U%h`05<XvTO|"R@N%Z+J:[<}x*%^%#
capwap sensitive-info psk %^%#;,L1<.L'e+Ii6MX,^QxH{6z#&#z[v4Oe"pCPrFJ'%^%#
capwap inter-controller sensitive-info psk %^%#ji6gT7>2y3dm}n~Bb"%8z$0]B62~|NkD,WJF[n2U%^%#
capwap dtls no-auth enable
capwap dtls cert-mandatory-match enable
#
wmi-server
server ip-address 172.21.39.99 port 27371
log module mid fe030000 name WMP_RFM
 log module mid ffee0000 name WCWP
log module mid ffc10000 name CLOUD_MNG
log module mid ff8c0000 name ENTITYTRAP
log module mid ff050000 name IFPDT
 log module mid ffd10000 name VCON
log module mid d0410000 name SHELL
log module mid fff30000 name WLAN
log module mid fe050000 name WSTA
 log module mid ffa30000 name WEBS
 log module mid ff760000 name WEB
log module mid ff630000 name CM
log module mid ff620000 name DHCP
 log module mid ff600000 name PORTAL
log module mid ff5f0000 name DOT1X
log module mid ff5b0000 name RDS
log module mid ff5a0000 name AAA
log module mid c1480000 name TACACS
#
wmi-server2
#
```



## wlan calibrate flexible-radio auto-switch temporary-management psk %^%#PwFE@vw\_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%# ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0\*)B\.KXW7QH=Ogpvg'K\*Y)I%^%# traffic-profile name default security-profile name default security-profile name wlan-net security wpa-wpa2 psk pass-phrase %^%#914c;d4z)+#\$JD3kxgr@w>\*(.lMo~Sf}H8U2\c[E%^%# aes security-profile name default-wds security-profile name default-mesh ssid-profile name default ssid-profile name wlan-net ssid wlan-net vap-profile name default vap-profile name wlan-net service-vlan vlan-id 101 ssid-profile wlan-net security-profile wlan-net wds-profile name default mesh-handover-profile name default mesh-profile name default regulatory-domain-profile name default regulatory-domain-profile name domain1 air-scan-profile name default rrm-profile name default radio-2g-profile name default radio-5g-profile name default wids-spoof-profile name default wids-whitelist-profile name default wids-profile name default wireless-access-specification wmi-server name test server ip-address 172.21.39.99 port 27371 collect-item location-data enable collect-item terminal-dhcp-option-data enable collect-item terminal-http-ua-data enable collect-item terminal-mdns-data enable collect-item dns-data enable collect-item non-wifi-data enable ap log module mid C1480000 name TACACS ap log module mid FF600000 name PORTAL ap log module mid FF620000 name DHCP ap log module mid FE050000 name WSTA ap log module mid FFEF0000 name WSRV ap log module mid FFF30000 name WLAN ap log module mid D0410000 name SHELL ap log module mid FF050000 name IFPDT ap log module mid FFED0000 name SEA



```
ap log module mid FFEE0000 name WCWP
  ap log module mid FE030000 name WMP_RFM
 ap-system-profile name default
 lldp report enable
 wmi-server test index 2
 port-link-profile name default
 wired-port-profile name default
 ap-group name default
 ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
  vap-profile wlan-net wlan 1
  wids device detect enable
   spectrum-analysis enable
   channel-monitor enable
  radio 1
  vap-profile wlan-net wlan 1
  wids device detect enable
  spectrum-analysis enable
   channel-monitor enable
 ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370
  ap-name AP1
  ap-group ap-group1
 ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363
 ap-name AP2
  ap-group ap-group1
 ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339
 ap-name AP3
 ap-group ap-group1
 provision-ap
#
return
```

## 11.4.2 SW-Core 配置

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101
#
dhcp enable
#
vlan 99
name Manage
#
interface Vlanif1
#
```





```
第343页
```

```
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
#
vlan batch 100 to 101
#
interface Vlanif1
#
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





# 12.1.4 实验规划

设备	端口	端口类型	VLAN参数
	MultiGE0/0/1	Trunk	PVID:1
			Allow-pass: VLAN 100 101
SW-Core		Trunk	PVID:1
	MulliGE0/0/9	ттипк	Allow-pass: VLAN 100 101
	MultiGE0/0/4	Access	PVID: 99
		Trupk	PVID:1
	MultiGE0/0/9	ПППК	Allow-pass: VLAN 100 101
	MultiGE0/0/1	Trupk	PVID:100
		ПППК	Allow-pass: VLAN 100 101
SW-ALLESS		Trupk	PVID:100
	MulliGE0/0/2	ПППК	Allow-pass: VLAN 100 101
		Trupk	PVID:100
	MulliGE0/0/5	ПППК	Allow-pass: VLAN 100 101
	CE0/0/1	Truch	PVID:1
WAC1	GE0/0/1	ттипк	Allow-pass: VLAN 100 101

## 表12-1 VLAN 规划

## 表12-2 IP 地址规划

设备	端口	IP地址
	Vlanif100	10.23.100.254/24
SW-Core	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认证参数	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
	名称: abc
Portal服务器模板	IP地址: 172.21.39.88
	Portal认证共享密钥:Huawei@123
	名称: portal1
Portal按入惧恢	绑定的模板: Portal服务器模板abc
免认证规则模板	名称: default_free_rule
	名称: p1
	绑定的模板和认证方案:
	Portal接入模板portal1
认证模板	RADIUS服务器模板radius_huawei
	RADIUS认证方案radius_huawei
	RADIUS计费方案scheme1
	免认证规则模板default_free_rule



# 12.2 实验任务配置

## 12.2.1 配置思路

```
1.导入预配置。
```

2.依据故障现象进行排错。

## 12.2.2 配置步骤

#### 步骤1 导入预配置

#### # 导入 WAC1 的预配置。

```
Software Version V200R021C00SPC100
#
defence engine enable
sysname WAC1
#
vlan batch 100
#
authentication-profile name p1
authentication-scheme radius_huawei
accounting-scheme scheme1
radius-server radius_huawei
#
web-auth-server server-source all-interface
#
management-port isolate enable
management-plane isolate enable
#
radius-server template default
radius-server template radius_huawei
radius-server shared-key cipher Huawei@123
radius-server authentication 172.21.39.88 1812 source Vlanif 100 weight 80
radius-server accounting 172.21.39.88 1813 source Vlanif 100 weight 80
radius-server authorization 172.21.39.88 shared-key cipher Huawei@123 server-group radius_huawei
radius-server authorization server-source all-interface
#
url-template name url1
url https://172.21.39.88:8445/portal
url-parameter redirect-url redirect-url ssid ssid user-ipaddress userip user-mac usermac device-ip ac-ip
#
web-auth-server abc
server-ip 172.21.39.89
port 50100
shared-key cipher Huawei@456
url-template url1
```



```
source-ip 10.23.100.1
 server-detect
#
portal-access-profile name portal1
web-auth-server abc direct
#
portal-access-profile name portal_access_profile
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 accounting-scheme scheme1
 accounting-mode radius
 accounting realtime 3
 local-aaa-user password policy administrator
 domain default
  authentication-scheme default
 accounting-scheme default
 radius-server default
 domain default_admin
  authentication-scheme default
  accounting-scheme default
#
interface Vlanif1
 ip address dhcp-alloc unicast
#
interface Vlanif100
ip address 10.23.100.1 255.255.255.0
 management-interface
#
interface MEth0/0/1
ip address 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk a1234567
capwap dtls inter-controller psk a1234567
capwap dtls no-auth enable
```





## # wlan calibrate flexible-radio auto-switch temporary-management psk a1234567 ap username admin password cipher %^%#\4Y\*HdY5jU={"Q,)V{2J[=sNPG-eG\$TI\_.P'>AvM%^%# traffic-profile name default security-profile name default security-profile name wlan-net security open security-profile name default-wds security-profile name default-mesh ssid-profile name default ssid-profile name wlan-net ssid wlan-net vap-profile name default vap-profile name wlan-net forward-mode tunnel service-vlan vlan-id 101 ssid-profile wlan-net security-profile wlan-net authentication-profile p1 wds-profile name default mesh-handover-profile name default mesh-profile name default regulatory-domain-profile name default regulatory-domain-profile name domain1 air-scan-profile name default rrm-profile name default radio-2g-profile name default radio-5g-profile name default wids-spoof-profile name default wids-whitelist-profile name default wids-profile name default wireless-access-specification ap-system-profile name default port-link-profile name default wired-port-profile name default ap-group name default ap-group name ap-group1 regulatory-domain-profile domain1 radio 1 radio disable ap-id 0 type-id 144 ap-mac 9cb2-e82d-54f0 ap-sn 2102353VUR10N5119370 ap-name AP1 ap-group ap-group1 ap-id 1 type-id 144 ap-mac 9cb2-e82d-5410 ap-sn 2102353VUR10N5119363 ap-name AP2 ap-group ap-group1



ap-id 2 type-id 144 ap-mac 9cb2-e82d-5110 ap-sn 2102353VUR10N5119339 ap-name AP3 #

return

#导入SW-Core的预配置。

```
!Software Version V200R021C00SPC100
#
sysname SW-Core
#
vlan batch 99 to 101
#
dhcp enable
#
vlan 99
name Manage
#
interface Vlanif1
#
interface Vlanif99
ip address 172.21.39.253 255.255.128.0
#
interface Vlanif100
ip address 10.23.100.254 255.255.255.0
dhcp select interface
#
interface Vlanif101
ip address 10.23.101.254 255.255.255.0
dhcp select interface
#
interface MEth0/0/1
ip address 192.168.1.253 255.255.255.0
#
interface MultiGE0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface MultiGE0/0/4
port link-type access
port default vlan 99
#
interface MultiGE0/0/5
#
interface MultiGE0/0/6
#
interface MultiGE0/0/7
#
interface MultiGE0/0/8
```



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

#### #导入SW-Access的预配置。

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

# 认证服务器 NCE 的预配置与 6.2.2 步骤 5 配置一致,本实验不再赘述。

#### 步骤 2 排查故障:终端无法搜索到无线信号

# 在 STA 上搜索 SSID 信号,发现并未搜索到"wlan-net"的无线信号,此时需要排查 AP 是 否已经上线,在 WAC1 上选择"监控 > AP",选择"AP 统计"选项卡,查看 AP 列表如下 所示:



AP列表						
智能诊断	上线失败记录	下线记录S	oftGRE隧道状态	导出信息 IoT插卡信息		
AP ID * 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 🔺 🍸	用户数 🔺 🍸		
0	AP1	ap-group1	• normal	0		
1	AP2	ap-group1	• normal	0		
2	AP3	default	• normal	0		
10 ▼ 共3条						
总AP数:3 normal:3						
AirEngine5761-	11:3					

- # 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:
- # 选择 "配置 > AP 配置 > AP 配置",在 "AP 信息"选项卡中,点击 AP3 对应的 AP 组 "default",即可修改 AP 组。

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1	监控	な。	<b>(十)</b> 诊断	维护
• 配置向导	AP信息	AP白名单	AP黑名单	AP邻居关系	AP设备类型
● AC配置	↓ AP列表				
● AP配置	i 点击AP ID列	列可进入AP的个性	化配置页面。		
AP组配置	修改AP配置	添加	替换 删除	加入黑名单	闪灯    清空所有AP
	AP ID +	AP MAC地址	AP名称 🔺	AP组 -	IP地址
AP配置	0	9cb2-e82d-54f	0 AP1	ap-group1	10.23.100.226
射频规划/调优	🔲 <u>00</u> 1	9cb2-e82d-541	10 AP2	ap-group1	10.23.100.218
分支AP组配置	<b>(10)</b> 2	9cb2-e82d-511	10 AP3	default	10.23.100.73
模板管理	10 🔻 共3	条			

# 然后将 AP3 归属的 AP 组修改为 "ap-group1",最后点击"确定"。



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	<b>袋</b> 配置	(➡) 诊断	<b>\$</b> \$ 维护
● 配置向导	AP配置 > AP配置 > A	AP信息 > 修改AP			
● AC配置	AP组:	ap-group	1	T	
● AP配置	AC地址列表:	<table-cell-rows> 添加</table-cell-rows>			
AP组配置				×	
AP配置	已选AP列表				
射频规划/调优	AP ID 🔺 🛛 AP MA	C地址	AP名称	AP组 ▲	IP地址获取方式
分支AP组配置	2 9cb2-e	82d-5110	AP3	default	- none - 🔻
模板管理	10 ▼ 共1条				
● 安全管理	确定取消				

# 再次查看,发现三台 AP 均属于 "ap-group1"组,并且已正常上线。

智能诊断	上线失败记录 下线记录	SoftGRE隧道状态	导出信息 loT插卡信
AP ID + 🍸	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 ▲ 🍸
0	AP1	ap-group1	normal
1	AP2	ap-group1	normal
2	AP3	ap-group1	normal

# 由于当前 STA 仍然无法搜索到 SSID,所以继续查看 VAP 的状态信息,选择"监控 > SSID > VAP",查看 VAP 信息如下:



Wireless LAN A 设备名称: WAC1	irEngine9700-M1 🙀 🔅 🔂 讨 🕌 🙀
概览	SSID VAP
网络KPI	自动刷新: OFF
AC	AP型VAP列表
用户	应用统计清零
射频	AP ID ▲ AP名称 ▲ 射频ID ▲ WLAN ID ▲ SSID ▲ BSSID ▲
AP	
SSID	注:选择列表中的VAP,查看该VAP应用统计信息。

# 发现所有 AP 均没有关联任何 VAP 信息,所以进一步查看 AP 组中是否引用了 VAP 模板, 选择"配置 > AP 配置 > AP 组配置",在"AP 组"选项卡中发现"ap-group1"并未引用任 何 VAP 模板,如下所示。

Wireless LAN / 设备名称: WAC1	AirEngine9700-M1		<b>读</b> 配置	➡ 诊断	<b>┃↓↓</b> 维护
● 配置向导	AP组静态	负载均衡组			
● AC配置	修改新建	删除	刷新		
⊙ AP配置	组名称	VAP;	摸板 ▲		射频0模板 ▲
AP组配置	default				2.4G-default
	ap-group1				2.4G-default
AP配直					
射频规划/调优	20 ▼ 共2条				

# 然后在当前页面中,点击"ap-group1",进入 AP 组配置页面。选择"VAP 配置",点击 "添加",添加已经预配的 VAP 模板"wlan-net",最后点击"确定",如下所示。



AP配置 > AP组配置 :	> AP组		
AP组配置: ap-gro	oup1 T 查看成员		VAP 模板列表
显示所有模板		配置模型介绍	● 相关配置
E FVAP配置			新建 添加 移除
団 □ 射频管理			模板名称 🔺
± /⊇AP ⊕ /⊇WIDS			
添加VAP模板			
③ 添加			
*VAP模板名称:	wlan-net 💌 *WLAN ID:	1	*射频: 0,1 💌
高级 🕑			Î
确定取消			

# 再次查看 VAP 信息,发现三台 AP 均已释放名称为"wlan-net"的 SSID,但是 AP 的 Radio 1 的状态为"OFF",说明 5G 射频被关闭,需要手动打开。

Wireless LAN Airf 设备名称: WAC1	Engine9700-M1	监控	<b>4</b> 配		₽ ) )断	<b>↓↓</b> 维护			
概览	SSID V	AP							
网络KPI	自动刷新: OFF								
AC	AP型VAP列表	ŧ							
用户	应用统计清晰	ş.							
射频	AP ID 🔺 🗌 A	P名称 ▲	射频ID▲	WLAN ID *	SSID +	BSSID *	认证方式 ▲	接入用户数 🔺	状态 ▲
4.0	0 A	P1	0	1	wlan-net	9cb2-e82d-54f0	Open	0	on
AP	0 A	P1	1	1	wlan-net	9cb2-e82d-5500	Open	0	off
SSID	1 A	P2	0	1	wlan-net	9cb2-e82d-5410	Open	0	on
CPE隧道	1 A	P2	1	1	wlan-net	9cb2-e82d-5420	Open	0	off
Mesh&WDS	2 A	P3	0	1	wlan-net	9cb2-e82d-5110	Open	0	on
潜在问题	2 A	VP3	1	1	wlan-net	9cb2-e82d-5120	Open	0	off
WIDS	10 ▼ 共6	5条							
频谱分析	注: 选择列表中的	的VAP,查看该	VAP应用统计	信息。					

# 手动开启 5G 射频,选择"配置 > AP 配置 > AP 组配置",选中"ap-group1"AP 组,选择"射频管理 > 射频 1",将射频 1 的工作状态配置为"ON",然后点击"应用",如下所示。



AP配置 > AP组配置 > AP组		
AP组配置: ap-group1 ▼ 查看成员		模板介绍信息: 射频模板主要用于优化射频的参数以及配置信道切换业务不中断功能
显示所有模板	配置模型介绍	射频1配置(5G)
<ul> <li>② VAP配置</li> <li>○ ● 射频管理</li> </ul>		基础配置 高级配置
「」「城管理模板	[domain]	
● 「一」射频0     □		工作模式:
<ul> <li></li></ul>		功率自动调优:
		信道目动调优:
		大数据调优: 🕜
		天线増益(dB):
		频谱分析: OFF
		全信道检测: OFF
		ightarrow wids
		应用

## # 查看 VAP 状态信息,均已正常,如下所示:

Wireless LAN Air 设备名称: WAC1	rEngine9700-N	11 些	w 陸	なる		<b>↓↓</b> 维护			
概览	SSID	VAP							
网络KPI	自动刷新: 01	F							
AC	AP型VAP	列表							
用户	应用统计	清零							
射频	AP ID *	AP名称 ▲	射频ID▲	WLAN ID +	SSID *	BSSID *	认证方式 ▲	接入用户数 🔺	状态▲
10	0	AP1	0	1	wlan-net	9cb2-e82d-54f0	Open	0	on
АР	0	AP1	1	1	wlan-net	9cb2-e82d-5500	Open	0	on
SSID	1	AP2	0	1	wlan-net	9cb2-e82d-5410	Open	0	on
CPE隧道	1	AP2	1	1	wlan-net	9cb2-e82d-5420	Open	0	on
Mesh&WDS	2	AP3	0	1	wlan-net	9cb2-e82d-5110	Open	0	on
潜在问题	2	AP3	1	1	wlan-net	9cb2-e82d-5120	Open	0	on
WIDS	10 💌	共6条							
频谱分析	注:选择列表	長中的VAP,查看	该VAP应用编	充计信息。					

## 步骤 3 排查故障:终端关联无线信号,无法获取地址

# STA 连接"wlan-net"信号后,无法获取 IP 地址,检查发现 VAP 的数据转发方式为隧道转发,但是 WAC1 上缺少业务 VLAN 信息(即缺少 VLAN 101),如下所示。



Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	な記室	(十) 诊断	\$   维护
• 配置向导	全局IPv6: OFF				
O AC配置	VLAN V	'LANIF V	LAN Pool		
基本配置	新建 删除	批量新建	批量删除	刷新	
VLAN	VLAN ID *	VLAN 描述		VLAN	类型▲
接口管理	1	VLAN 0001		comm	ionVlan
IP	100	VLAN 0100		comn	ionVlan
● AP配置	10 🔻 共2条				

# 在 WAC1 上手动创建 VLAN 101,创建成功后,检查 VLAN 信息如下所示。(创建 VLAN 的步骤请参考 1.2.2 步骤 4,此处不再赘述 )

Wireless LAN 设备名称: WAC1	AirEngine9700-M1	监控	な配置		
<ul> <li>配置向导</li> </ul>	全局IPv6: OFF				
● AC配置	VLAN V	L <mark>ANIF V</mark>	LAN Pool		
基本配置	新建制除	批量新建	批量删除	刷新	
VLAN	VLAN ID *	VLAN 描述 -	l.	VL	AN 类型 🔺
接口管理	1	VLAN 0001		co	mmonVlan
	100	VLAN 0100		co	mmonVlan
IP	101	VLAN 0101		co	mmonVlan
● AP配置					
安全管理     安全管理	10 ▼ 共3条				

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


无线局域网适	₽₽	R R	ΨI	LA1	V:						
连接特定的	j_D	NS		卮	双双				:		
- 本地链接 -	IPv	6	봬	圳	Ľ.				1	fe80::3ce1:b4f7:546e:45a1%12	
IPv4 地址									:	10. 23. 101. 196	
子网掩码									:	255. 255. 255. 0	
默认网关.									:	10. 23. 101. 254	

步骤 4 排查故障: Portal 认证无法弹出 Portal 认证页面

# STA 搜索到"wlan-net"信号后,进行连接,然后打开浏览器,输入任意 IP 地址,发现无 法弹出 Portal 认证页面 。



# 无法弹出 Portal 认证页面的原因较多,大多数情况下都是由于认证模板配置错误导致,所以首 先检查 VAP 模板是否正确引用了认证模板。

# 选择 "配置 > AP 配置 > 模板管理 > 无线业务 > VAP 模板 ",发现 VAP 模板 "wlan-net" 中引用了认证模板 "p1 ",但是认证模板 "p1 "中没有引用 Portal 模板,如下所示。



#### HCIP-WLAN V2.0 实验指导手册(Web )

Wireless LAN A 设备名称: WAC1	irEngine9700 <mark>-</mark> M1	」 监控	なる問題	<ul><li>主</li><li>诊断</li></ul>	 (北)
① 配置向导	模板管理				
● AC配置	日 二元线业务				
● AP配置	⊡ 🥫 VAP模板 団 📑 default				
AP组配置	🖂 📑 wlan-ne 📑 SSID	et 模板		[wla	an-ne]
AP配置	■ 安全 <sup>1</sup> ■ 流量	模板 模板		[wla [d	an-ne] default]
射频规划/调优	■ ■ 认证	模板 02.1X模板			(p1)
分支AP组配置	Pe Pe	ortal模板 IAC接入模板			
模板管理	■ <del>見</del> 免 ■ R	i认证规则模板 ADIUS模板		ſra	dius]
安全管理	8 = 8 H	级计费RADIUS ACA模板	模板		
QoS		DAP模板 D模板			
● 扩展业务	BH	WTACACS模板			
<ul> <li>可靠性配置</li> </ul>	■ 认 ■ 授	wir方案模板 权方案模板		[ra	dius]
	<mark>모</mark> 버	费方案模板		[scl	neme]
	<b>1</b>	务方案模板			
	■ 内 ■ 本	i重EAP服务器配 地用户配置	适		

# 手动引用已经预配的 Portal 模板 "portal1"后,如下所示。



模板管理						
□ ┣无线业务		Portal模板:	portal1		×	影示模糊
□ □ VAP模板						
🗈 📃 default		模板介绍信息: 通过Portal接	6入模板统一管理Portal认证用户接	私 相 关 的 所 有	配置。	
🖃 📃 wlan-net						
SSID模板	[wlan-ne]	Portal认证:	○ 内置Portal服务	醫 💿 外置P	ortal服务	
10 安全模板	[wlan-ne]					
■ 流量模板	[default]	对接使用协议:	● Portal协议	HTTP协议	O HAC	A协议
🖂 📒 认证模板	[p1]					
■ 802.1X模板		*王Portal服务器组:	abc			
■ Portal模板	[portal1]	备Portal服务器组。				×
■ MAC接入模板		ELL OF GRACES HEAD				-
●免认证规则模板		Portal服务器不可用时授权用	用户组权限:			×
■ RADIUS模板	[radius]					
■ 二级计费RADIUS模板		Portal服务器可用后用户重识	从证: OFF			
HACA模板						
IDAP模板		高坂 🕑				
■ AD模板		them 1				
HWTACACS模板						
10000000000000000000000000000000000000	[radius]					
■ 授权方案模板						
10000000000000000000000000000000000000	[scheme]					
3 业务方案模板						
■ 内置EAP服务器配置						
■ 本地用户配置						

# 同时检查 Portal 模板 "portal1"中引用的 Portal 服务器组 "abc"的配置是否正确,选择 "配置 > 安全管理 > AAA > Portal 服务器全局设置 > 外置 Portal 全局设置",点击 Portal 认证服务器列表中的"abc",检查其配置,发现如下配置错误:

- Portal 服务器的 IP 地址配置错误,正确地址应该是 172.21.39.88;
- Portal 服务器的端口号配置错误,正确端口号应该是 50200;
- 为确保共享密钥与 NCE 一致,重新配置共享密钥为 Huawei@123;
- URL 中的端口号配置错误,正确端口应该是 19008 (NCE 默认端口);
- 需要关闭 Portal 服务器探测功能 (因为 NCE 默认未开启探测功能 )。



섩	ž٦	6	7ī	Ħ
স	ີ	U.	ر ک	べ

安全管理 > AAA > 外置Portal全局	设置 > 修改认证服务器
*服务器名称:	
★服务器IP地址:	IPv4 💌 🗘
	□ I 服务器IP地址 ×
1	172.21.39.89
4九2073年7月。	
//////////////////////////////////////	
*共享密钥: 2	
报文端口号: 3	50100
本机网关地址:	
URL:	https://172.21.39.88:8445/pc
URL配置结果:	https://172.21.39.88:8445/portal?ac-ip=&redirect-url=redirect-url&usermac=user-mac8
↓ 服务器探测配置	
Portal服务器探测:	5
探测周期(秒):	60
状态为UP的Portal服务器最少	小数目: 0
探测失败超过最大次数后动作	E: 发送日志信息 发送告警信息
确定取消	

# 手动修改以上五处配置错误后,正确的配置如下所示:



安全管理 > AAA > 外置Portal全局	设置 > 修改认证服务器
*服务器名称:	
*服务器IP地址:	IPv4 ▼ •
1	□ 服务器IP地址 ×
协议类型:	Portal HTTP HACA
*共享密钥: 2	Huawei@123
报文端口号: 3	50200
本机网关地址:	
URL:	https://172.21.39.88:19008/F
URL配置结果:	https://172.21.39.88:19008/portal?ac-ip=&redirect-url=redirect-url&usermac=user-mac&
↓ 服务器探测配置	
Portal服务器探测: 5	OFF
确定取消	

# 最后在 STA 上断开无线连接,然后重新连接"wlan-net",发现已经可以弹出 Portal 认证 页面,输入用户名/密码,Portal 认证成功。

## 12.3 结果验证

12.3.1 检查 AP 上线状态

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

# 同时可以看到所有 AP 均属于 AP 组 "ap-group1"。



智能诊断	上线失败记录	SoftGRE隧道状态	导出信息 loT插卡信息
AP ID + 7	AP名称 ▲ ▽	AP组 ▲ ▽	状态名称 🔺 🍸
D	AP1	ap-group1	normal
1	AP2	ap-group1	normal
2	AP3	ap-group1	normal

## 12.3.2 检查 VAP 信息

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

P型VAP	列表							
应用统计	清零							
AP ID *	AP名称 ▲	射频ID▲	WLAN ID +	SSID *	BSSID +	认证方式 🔺	接入用户数 🔺	状态
)	AP1	0	1	wlan-net	9cb2-e82d-54f0	Open+Portal	0	on
)	AP1	1	1	wlan-net	9cb2-e82d-5500	Open+Portal	0	on
	AP2	0	1	wlan-net	9cb2-e82d-5410	Open+Portal	0	on
	AP2	1	1	wlan-n <mark>e</mark> t	9cb2-e82d-5420	Open+Portal	0	on
2	AP3	0	1	wlan-net	9cb2-e82d-5110	Open+Portal	0	on
2	AP3	1	1	wlan-net	9cb2-e82d-5120	Open+Portal	0	on



# 12.3.3 STA 关联无线信号,认证通过



# 12.4 配置参考

## 12.4.1 WAC1 配置

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 172.21.39.4 255.255.255.0
#
interface Ethernet0/0/47
ip address 169.254.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.23.100.254
#
capwap source interface vlanif100
capwap dtls psk %^%#EJVsX!hYu4YZ2_G4#DzXA@:RKv34&REZ}|-y_]mY%^%#
capwap dtls inter-controller psk %^%#{9Wo7!%#BFZ<@EQ|:JG>Rp<|47s,v>YPa.#^!]A9%^%#
capwap dtls no-auth enable
#
wlan
calibrate flexible-radio auto-switch
```



temporary-management psk %^%#PwFE@vw_"@\n9{>}k<,-;9CD7K;0/%e,LB)9,^FX%^%#	
ap username admin password cipher %^%#PBMhAQ{@}1q,vb:X0*)B\.KXW7QH=Ogpvg'K*Y)I%^%#	
traffic-profile name default	
security-profile name default	
security-profile name wlan-net	
security open	
security-profile name default-wds	
security-profile name default-mesh	
ssid-profile name default	
ssid-profile name wlan-net	
ssid wlan-net	
vap-profile name default	
vap-profile name wlan-net	
forward-mode tunnel	
service-vlan vlan-id 101	
ssid-profile wlan-net	
security-profile wlan-net	
authentication-profile p1	
wds-profile name default	
mesh-handover-profile name default	
mesh-profile name default	
regulatory-domain-profile name default	
regulatory-domain-profile name domain1	
air-scan-profile name default	
rrm-profile name default	
radio-2g-profile name default	
radio-5g-profile name default	
wids-spoof-profile name default	
wids-whitelist-profile name default	
wids-profile name default	
wireless-access-specification	
ap-system-profile name default	
port-link-profile name default	
wired-port-profile name default	
ap-group name default	
ap-group name ap-group1	
regulatory-domain-profile domain1	
radio 0	
van-profile wlan-net wlan 1	
radio 1	
van profile wan net wan 1	
$a_{\rm P}$ in the main net main is a second state of the second st	
ap-lu $0$ type-lu 144 ap-lilac $3$ cb2-eo2u-3410 ap-sil $2$ 102333300K10N3113370	
ap-name Ar i	
$a_{1}$ -group $a_{1}$ -group 1 ap id 1 type id 144 ap mac 0cb2 e82d 5410 ap sp 2102252\/UP10\\5110262	
ap-iu 1 type-iu 144 ap-iiiat 9t02-eo2u-3410 ap-sil 210233380K10N3119303	
ap-name Arz	
ap-group $ap$ -group 1	
ap-iu 2 type-iu 144 ap-mac 9cb2-e820-5110 ap-sh 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。