

# AC-V3200 无线控制器

## 用户手册



版权所有：深圳市中科网威科技有限公司

## 目录

版权说明	5
关于本手册	5
第1章 产品介绍	6
1.1 产品简介	6
1.2 产品特点	6
1.2.1 强大的 AP 管理、控制功能	6
1.2.2 Portal 认证、微信认证等多种认证方式	7
1.2.3 丰富的外部数据接口	8
第2章 登陆方式	9
1. 通过 Web 网页登录设备:	9
2. 通过 CLI 登录设备:	9
2.1 通过 WEB 管理界面登录设备	9
2.1.1 客户端计算机要求	9
2.1.2 设置客户端计算机的 IP 地址	9
2.1.3 确认管理计算机和设备之间的网络是否连通	10
2.1.4 登录设备 Web 设置页面	11
2.2 通过串口登录设备	12
2.2.1 必备要求	12
2.2.2 查看客户端计算机串口号	13
2.2.3 设置串口登录软件参数, 登录串口	13
2.3 远程登录设备	14
2.3.1 客户端计算机要求	14
2.3.2 设置 AC-V3200 控制器的 IP 地址	15
2.3.3 设置客户端计算机的 IP 地址	15
2.3.4 确认管理计算机和设备之间的网络是否连通	15
2.3.5 远程登录	15
第3章 系统功能配置	17
3.1 接口管理	17
3.1.1 接口简介	17
3.1.2 物理接口配置	17
3.1.3 虚接口配置	19
3.2 DHCP 服务	20
3.2.1 DHCP 服务器配置	20
3.2.2 DHCP 客户端列表	21
3.3 路由与 DNS 配置	22
3.3.1 功能简介	22
3.3.2 具体配置	23
3.4 AC 版本管理	26
3.5 配置备份与恢复	27
3.6 Web 帐号管理	28
3.6.1 简介	28
3.6.2 配置	28

第 4 章 AP 与终端配置管理 .....	29
4.1 AP 注册 AC .....	29
4.1.1 上线具体配置 (AV-V3200 与 AP-V230 举例) .....	29
4.2 射频管理 .....	31
4.3 终端管理 .....	35
4.4 SSID 管理 .....	36
4.5 AP 升级管理 .....	38
1) 升级文件命名规范 .....	38
2) 升级版本的配置 .....	39
3) 升级服务器的配置 .....	40
4) 升级操作 .....	41
4.6 MAC 黑名单 .....	41
4.7 MAC 白名单 .....	42
4.8 反向 SSH 配置 .....	43
4.9 AP 设备管理 .....	44
4.9.1 修改 AP 密码 .....	44
4.9.2 修改本地 AC .....	45
4.9.3 修改 AP 模式 .....	45
4.10 AP 录入 .....	46
第 5 章 特性功能配置管理 .....	47
5.1 漫游配置 .....	47
5.1.1 功能简介 .....	47
5.1.2 配置步骤 .....	48
5.2 弱信号管理 .....	49
5.2.1 功能简介 .....	49
5.2.2 配置步骤 .....	49
5.3 频谱导航 .....	50
5.3.1 功能简介 .....	50
5.3.2 配置步骤 .....	50
5.4 负载均衡 .....	52
5.4.1 功能简介 .....	52
5.4.2 配置步骤 .....	53
5.5 流量上报 .....	54
5.5.1 功能简介 .....	54
5.5.2 配置步骤 .....	55
5.6 流量限速 .....	57
5.6.1 功能简介 .....	57
5.6.2 配置步骤 .....	57
5.7 用户隔离 .....	59
5.7.1 功能简介 .....	59
5.7.2 配置步骤 .....	59
5.8 速率集配置 .....	60
5.8.1 功能简介 .....	60
5.8.2 配置步骤 .....	61

5.9 短信认证 .....	62
5.9.1 功能简介 .....	62
5.9.2 配置步骤 .....	62
5.10 微信认证 .....	65
5.10.1 功能简介 .....	65
5.10.2 配置步骤 .....	65
5.11 中文 SSID .....	67
5.11.1 功能简介 .....	67
5.11.2 配置步骤 .....	68
5.12 定位策略 .....	70
5.12.1 无线定位 .....	70
5.12.2 电子围栏 .....	71
5.12.3 高级设置 .....	72
5.13 vlan 接口 ID .....	72
5.14 权限管理 .....	73
5.14.1 权限策略 .....	74
5.14.2 时间策略 .....	74
5.14.3 位置策略 .....	75
5.14.4 访问策略 .....	76
第 6 章 典型组网配置举例 .....	77
6.1 典型配置举例（业务 vlan + 加密 + 限速） .....	77
6.1.1 组网需求 .....	77
6.1.2 配置注意事项 .....	78
6.1.3 配置步骤 .....	78
6.2 典型配置举例（短信认证 + 微信认证） .....	83
6.2.1 组网需求 .....	83
6.2.2 配置注意事项 .....	83
6.2.3 配置步骤 .....	84
第 7 章 故障排除 .....	88
第 8 章 缺省配置 .....	91

## 版权说明



本公司的用户手册并无任何明确或隐含的保证，包括为了特殊目的进行销售或安装的相关保证。

本公司有对手册更改或修订之权力，若有更改恕不另行通知。未经本公司的书面许可不得对本手册的任何内容进行摘录、复制或翻译等。

## 关于本手册

使用本手册的目的是为了安装及使用无线控制器和无线接入点。本手册包括配置过程及方法，可协助客户解决不可预见的问题。

为了突出一些需要注意的内容,本手册用了以下特殊文字及样式来表示

 <b>警告:</b>	表示将有潜在的 <b>危险操作</b> 会对设备造成 <b>硬件损害</b> 、 <b>数据全部丢失</b> 、 <b>设备不能正常使用</b> 等问题。
 <b>注意:</b>	表示有 <b>重要的信息提醒</b> 可以 <b>以便更好的使用设备</b> 。
<b>粗体</b>	表示有 <b>重要的功能或者设置步骤需要特别注意</b> 。

# 第 1 章 产品介绍

## 1.1 产品简介

AC-V3200 系列无线控制器 (AC, Access Controller) 是深圳中科网威科技有限公司自主研发的高性能无线控制器, 该无线控制器可集中管理所有的瘦 AP 和无线客户端, 使 WLAN 网络成为易管理、可运维的网络。

AC-V3200 系列无线控制器具有大容量、高可靠性等特点, 具备用户控制管理、智能射频管理、故障自动恢复, 快速漫游和负载均衡等功能, 可为热点覆盖、校园覆盖、大型企业园区、无线城域网覆盖等应用环境提供强大的 WLAN 接入网络。

该产品可以在任何现有的 L2/L3 网络上实现无缝、安全的无线网部署, 而无需中断当前网络的运行。AC-V3200 系列无线控制器可以与原有网络完美融合, 并且无需改变其架构, 大大简化网络的布署和管理, 节约用户投资。

该产品内置 Portal、Radius 服务器, 从用户的实际需求出发, 省去了外置 Portal 服务器和 Radius 服务器等设备, 不仅简化了整个网络的架构, 而且还大幅降低了网络建设成本, 满足了中小型无线网络建设中用户安全接入的需求。该产品同时支持与外置 Portal、Radius 服务器对接, 实现灵活的认证管理。

## 1.2 产品特点

### 1.2.1 强大的AP管理、控制功能

- 支持多种无线AP的管理

AC-V3200系列无线控制器支持对802.11a/b/g /n /ac无线AP的管理、控制, 从而提供更高的无线接入速率, 能够覆盖更大的范围, 使各种无线多媒体应用成为现实。

- 支持多种分支机构远程接入场景

当 AC 和 AP 通过广域网链路进行连接时, 用户采用本地转发模式, 提升分支机构局域网打印访问、终端互访等业务性能;

当广域网链路发生故障或 AC 发生故障时，在线用户不掉线，可以继续访问本地资源，并且可支持 AC 逃生功能；

当分支机构 AP 部署于私网内时，AC 可以穿越 NAT 与 AP 进行通信。

- 全网无缝漫游

当用户在同一AC管理的多台AP之间漫游时，用户的认证信息和授权信息不变，使得用户可以跨越整个无线网络，并保持良好的移动性和安全性，保持IP地址与认证状态 不变，从而实现快速漫游和语音的支持。

- 支持智能AP负载均衡

智能AP负载均衡可以实时地分析无线客户端的位置，动态地确定在当前时刻和当前位置下哪些AP可以彼此分担负载，通过控制无线客户端接入的AP，来实现这些AP间的负载分担。

- 支持智能频谱分析与导航

无线局域网工作的频段存在大量可能的干扰源，如雷达、微波炉，它们在网络中的出现将干扰AP的正常工作。通过信道智能导航功能，可以保证每个AP能够分配到最优的信道，尽可能地减少和避免相邻信道干扰，而且通过实时信道干扰检测，可以让AP实时避开雷达，微波炉等干扰源。

## 1.2.2 Portal认证、微信认证等多种认证方式

- Portal认证

AC-V3200 系列无线控制器提供内置的 Portal 认证服务器。该认证方式直接通过浏览器 WEB Portal 页面作为认证通道，当用户认证通过后，可以灵活跳转到指定访问首页并启动相应授权。同时也可以根据策略要求，灵活推送定制 Portal 页面，达到广告宣传、信息传递的作用，广泛使用在无线校园、无线城市、访客接入等应用场景。

- 微信认证

AC-V3200系列无线控制器提供微信认证功能。用户可以通过扫描商家公众号二维码、或者直接添加公众号方式，完成一键关注即可上网，无需借助密码。

- 丰富的Portal定制功能

AC-V3200系列无线控制器内置各种行业的Portal模板，同时支持用户Portal的自定义，从而快速、

高效完成Portal页面的定制。

- 终端智能识别

AC-V3200系列无线控制器内置的Portal服务器，能根据终端特点，智能识别终端类型，自适应弹出不同大小、页面格局的Portal认证页面。终端智能识别技术免去了用户多次拖动，调整屏幕的操作，为用户提供更加智能的无线体验，并且全面支持苹果IOS、安卓和windows等主流智能终端操作系统。

### 1.2.3 丰富的外部数据接口

- 支持外置Portal服务器

AC-V3200系列无线控制器能够与外置Portal服务器对接，第三方Portal服务器只需添加自定义的Portal属性字段，即可完成与第三方Portal服务器的对接。

- 支持外置Radius服务器

AC-V3200系列无线控制器能够与外置Radius服务器无缝对接，实现灵活的认证管理。用户数据保存在第三方的Radius服务器，保证用户数据的安全、可靠。

- 对外提供多种数据接口

第三方平台能过HTTP的GET请求方式，可从AC-V3200系列无线控制器获取多种用户数据，包括终端列表、终端流量、终端上下线时间、终端MAC-IP映射表等信息。为第三方平台提供可靠数据支持。



## 第 2 章 登陆方式

用户可以通过以下几种方式登录到交换机上，对交换机进行配置和管理：

### 1. 通过 Web 网页登录设备：

缺省情况下，用户不能直接通过 Web 登录设备。如需采用 Web 方式登录，需完成如下配置：

- 配置设备 VLAN 接口的 IP 地址，确保设备与 Web 登录用户间路由可达（缺省 IP 地址为 169.254.10.10）
- 登录 WEB 网页，输入用户名密码（缺省用户名：admin 缺省密码：password）

### 2. 通过 CLI 登录设备：

- 通过 Console 口登录设备：缺省情况下，用户可直接通过 Console 口本地登录设备。
- 通过 Telnet 登录设备：缺省情况下，用户可通过密码认证方式登录，缺省用户名：root 缺省密码：anysec。如需采用 Telnet 方式登录，需配置设备 VLAN 接口的 IP 地址，确保设备与 Web 登录用户间路由可达

## 2.1 通过 WEB 管理界面登录设备

WEB 管理提供了一个友好的用户界面，可以使用浏览器来查看和配置设备。下面以 IE 浏览器为例来示范使用 WEB 管理界面登录设备的步骤。

### 2.1.1 客户端计算机要求

- 确认计算机已安装并启用了以太网网卡。
- 确认计算机已和 AC-V3200 无线控制器的任意 LAN 口相连。

### 2.1.2 设置客户端计算机的IP地址

建议您手动为客户端计算机设置静态IP 地址。手工设置静态IP 地址时，需要将计算机的IP 地址与 AC-V3200无线控制器的IP 地址设置在同一子网中（AC-V3200无线控制器缺省IP 地址为：192.168.1.2，

子网掩码为255.255.255.0)，即输入IP 地址（在192.168.1.1 ~ 192.168.1.254 中选择除192.168.1.2 之外的任意值）、子网掩码（255.255.255.0）。

### 2.1.3 确认管理计算机和设备之间的网络是否连通

操作步骤如下（以Win7为例）：

- 从Win 7的桌面上点击“开始”，然后再点击“所有程序”。如图2-1所示



图2-1

- 用鼠标左键点击“附件”，然后再选择“命令提示符”即可打开。如图2-2所示。



图2-2

- 输入“ping 192.168.1.2（设备的IP地址，此处是缺省IP地址）”，单击<确定>按钮。如果在弹出的对话框中显示了从设备侧返回的回应，则表示网络连通；否则请检查网络连接。如图2-3所示。



图2-3

## 2.1.4 登录设备Web设置页面

- 运行Web浏览器，在地址栏中输入“http://192.168.1.2”，回车后跳转到Web登录页面，如图2-4所示。输入用户名、密码（缺省为admin，password，区分大小写）以及验证码，单击<登录>按钮或直接回车即可进入Web设置页面。



图 2-4 登录界面

- 输入用户名、密码（缺省为admin，password，区分大小写）以及验证码，单击<登录>按钮或直接回车即可进入Web设置页面。如图2-5所示



图 2-5 AC-V3200 控制器首页

## 2.2 通过串口登录设备

### 2.2.1 必备要求

- 准备一根 console 配置线。如图 2-6 所示



图 2-6 Console 配置线

- 确认 Console 配置线的 RJ45 水晶头与 AC-V3200 无线控制器的 Console 口 (如图 2-7 所示) 正确相连。



图 2-7 AC-V3200 控制器 Console 口

- 确认 Console 配置线的另外一头与客户端计算机的串口正确相连。
- 确认客户端计算机正确安装串口软件。

## 2.2.2 查看客户端计算机串口号

操作步骤如下（以Win7为例）：

- 从桌面找到“计算机”图标，单击鼠标右键，选择“管理”。
- 在管理页面里，点击“设备管理器”，在右边的页面中单击“串口”左边的小箭头，可看到当前所用的串口号。如图 2-8 所示，可看到当前的所用串口号为 com1。



图 2-8 管理页面查看串口号

## 2.2.3 设置串口登录软件参数，登录串口

操作步骤如下（以 Secure CRT）

- 打开 Secure CRT 软件，单击“快速登录”图标。如图 2-9 所示

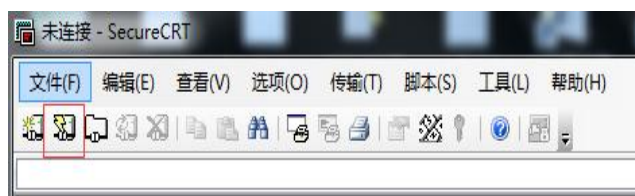


图 2-9 Secure CRT 操作界面

弹出快速连接菜单，设置连接参数。如图 2-10 所示

协议：选择 Serial。

端口：选择 COM1，此处需根据实际情况选择自己在 2.2.2 步骤中查看到的串口号。

波特率：选择 115200，AC-V3200 控制器默认波特率。

数据位：选择 8。

奇偶校验：选择 None。

停止位：选择 1。

去掉流控中 RTS/CTS 前面的选择。



图 2-10 串口参数设置

- 设置好参数后，单击连接，进入 AC-V3200 控制器的串口界面。如图 2-11 所示

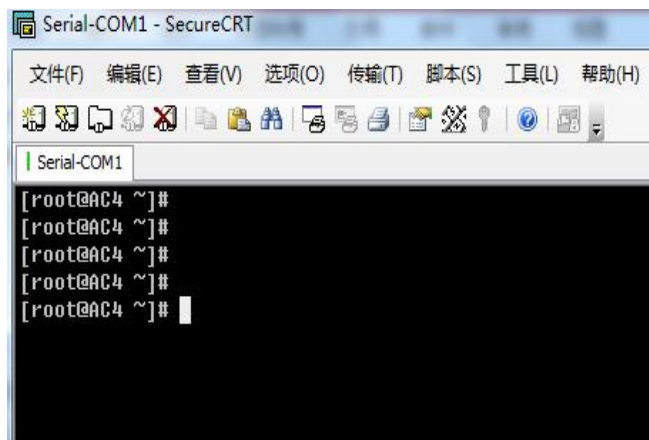


图 2-11 AC-V3200 控制器串口登录界面

## 2.3 远程登录设备

### 2.3.1 客户端计算机要求

- 确认计算机已安装并启用了以太网网卡。
- 确认计算机与 AC-V3200 控制器在同一局域网内。

### 2.3.2 设置AC-V3200控制器的IP地址

AC-V3200控制器的LAN1-LAN6口默认属于VLAN 1，所以需要进入AC-V3200控制器的管理页面设置VLAN 1的IP地址。进入管理页面的操作步骤参考2.1章节。

页面向导：首页 → 网络管理 → 虚接口 进入页面后能看到如下功能配置



图 2-12 AC-V3200 控制器虚接口配置界面

点击编辑，进入配置页面，手动配置AC-V3200控制器VLAN1的IP地址与子网掩码。设置静态IP 地址时，先确认所用IP地址是否已被占用。

### 2.3.3 设置客户端计算机的IP地址

如果计算机连接的局域网内部有DHCP服务器，则设置计算机为自动获取IP地址。

如果计算机连接的局域网内部没有DHCP服务器，需手动为客户端计算机设置静态IP 地址。设置静态IP 地址时，先确认所用IP地址是否已被占用。

### 2.3.4 确认管理计算机和设备之间的网络是否连通

具体步骤与 2.1.3 相同，参考 2.1.3 章节。

### 2.3.5 远程登录

☎ 总机电话-- 0755-83658009

☎ 技术支持-- 0755-83658229

☎ 24 小时技术值班热线----135-1069-3536

🌐 <http://www.anysec.com>

📍 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

操作步骤如下 (以 Secure CRT)

- 打开 Secure CRT 软件, 单击“快速登录”图标。
- 弹出快速连接菜单, 设置连接参数, 如图 2-13 所示。

协议: 选择 SSH2。

主机名: 填入步骤 2.3.2 中设置好的 IP 地址。

用户名: 填入 root。

其它选择默认值即可。

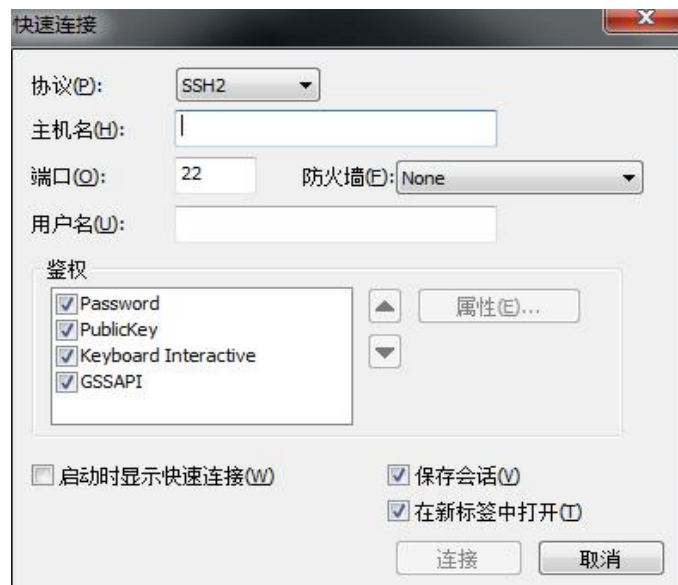


图 2-13

- 点击连接, 进入密码输入框 (如图 2-14 所示), 输入默认值 anysec。

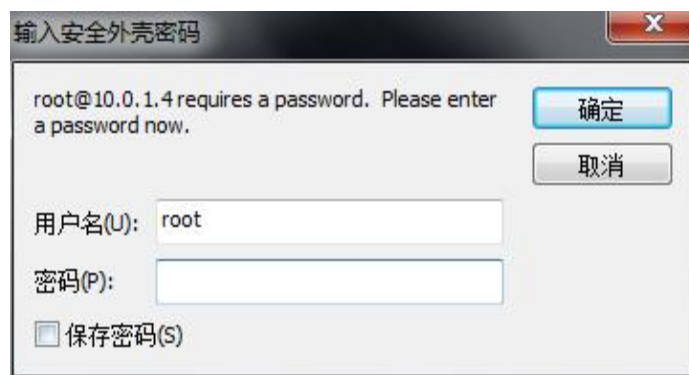


图 2-14

- 点击确定, 即可远程登录 AC-V3200 控制器。



## 第 3 章 系统功能配置

### 3.1 接口管理

#### 3.1.1 接口简介

AV-V3200 的接口包括物理接口和虚接口 2 部分，虚接口依赖于物理接口。

#### 3.1.2 物理接口配置

配置页面：网络管理→物理接口

序号	接口名称	接口开关	工作模式	接口IP	自协商	双工状态	速率	流控	MTU	操作
1	eth0	Up	交换模式	N/A	启用	Full	1000	启用	1500	<a href="#">编辑</a>
2	eth1	Up	交换模式	N/A	启用	Full	1000	启用	1500	<a href="#">编辑</a>
3	eth2	Up	交换模式	N/A	启用	Full	1000	启用	1500	<a href="#">编辑</a>
4	eth3	Up	交换模式	N/A	启用	Full	1000	启用	1500	<a href="#">编辑</a>
5	eth4	Up	交换模式	N/A	启用	Full	1000	启用	1500	<a href="#">编辑</a>
6	eth5	Up	交换模式	N/A	启用	Full	1000	启用	1500	<a href="#">编辑</a>

图 3-3

如上图，物理接口的名称依次为 eth0 ~ eth5<sup>1</sup>，需要对某接口进行配置时，可点击对应接口最右侧的“编辑”链接，出现如图 3-3 所示界面。

1 此为页面上的接口名称，AC 前面板的指示可能为 LAN1 ~ LAN6



图 3-4

其中:

- “接口开关” 用于对接口进行使能 (Up) 和禁用 (Down), 默认为 “Up” 状态。
- “工作模式” 用于配置接口工作于交换 (二层) 模式和路由 (三层) 模式, 默认为 “交换模式”。
- “自协商” 开关配置接口的工作速率和双工模式, 当 “启用” 时, 接口自动协商支持的速率和双工模式, 自协商过程遵循 IEEE 802.3 规范; 当 “禁用” 时, 会新增两条配置项 “双工状态” 和 “速率”。默认 “启用”。
- “流控” 开启时, 如果接口发生拥塞, 它将向对端设备发送消息, 通知对端设备暂时停止发送报文, 从而避免了报文丢失现象的发生。默认 “启用”。
- “MTU”, 即最大传输单元 (Maximum Transmission Unit), 表示接口能够收发的最大帧格式大小, 对于以太网接口而言, 通常最大值为 1500。默认值 “1500”。
- “端口模式” 配置端口的 VLAN 链路类型, 分别对应到 “Access” 和 “Trunk”, 详见 3.1.1 描述。
- “PVID”: 即 Port Vlan ID, 详见 3.1.1 描述。
- “Vlan 列表”: 即除 PVID 外, 该端口允许通过的 VLAN ID 列表。该配置项仅当 “端口模式” 设置为 “Trunk” 时可配。

### 3.1.3 虚接口配置

配置页面：网络管理→虚接口



序号	接口名称	状态	IP地址	子网掩码	操作
1	vlan1	Up	10.0.1.4	255.255.252.0	编辑
2	vlan5	Up	192.168.1.1	255.255.255.0	编辑   删除   设为接入接口
3	vlan168	Up	10.8.8.168	255.255.255.0	编辑   删除   设为接入接口

图 3-5

基本操作：

- “添加”，新建一个不存在的虚接口，当前 AC 最多可添加 512 个虚接口
- “编辑”，修改对应的虚接口配置参数
- “删除”，删除对应的虚接口
- “批量删除”，删除一个或多个虚接口，注意：“AP 接入接口”和 VLAN1 虚接口不可被删除。
- “设为接入接口”，选择允许 AP 连入 AC 的接口。选择后，右上角的状态将改为修改后的接口。

“新建”和“编辑”操作的视图类似，除了“编辑”时，接口名称不可更改。如图 3-6 所示：



接口名称

接口状态

IP地址

子网掩码

图 3-6

- 接口名称：仅接受类似 vlan10 这样的名称，其中数字“10”表示虚接口对应的 VLAN ID。
- 接口状态：用于对接口进行使能（Up）和禁用（Down），默认为“Up”状态
- IP 地址：接口的三层地址，主要用作三层转发。
- 子网掩码：指明“IP 地址”所在网络的大小。

**注意:**

不同的三层接口（包括三层物理接口和虚接口）的 IP/MASK 不应该在同一个网络地址中，否则将导致 AC 网络不可访问。

## 3.2 DHCP 服务

### 3.2.1 DHCP 服务器配置

配置页面：网络管理→DHCP 服务器

批量删除	添加	序号	接口名称	接口IP	起始IP地址	结束IP地址	子网掩码	网关	首选DNS	租约时间	状态	操作
<input type="checkbox"/>	<input type="checkbox"/>	1	vlan5	192.168.1.1	192.168.1.109	192.168.1.120	255.255.255.0	192.168.1.1	114.114.114.114	60	禁用	编辑   删除   启用

图 3-7

基本操作:

- “添加”：基于现有的三层接口（包括虚接口和三层物理口）创建 DHCP 服务器。每个接口只能创建一个 DHCP 地址池。每台 AC 能创建的 DHCP 最大条数不超过 128。已建立 DHCP 服务的接口
- “编辑”：修改已有的 DHCP 配置
- “删除”：删除对应接口的 DHCP 配置
- “批量删除”：删除多个选中的接口的 DHCP 配置
- “启用”：仅处于“禁用”状态的接口可用，重新开启对应接口的 DHCP 地址池
- “禁用”：仅处于“启用”状态的接口可用，类似“删除”功能，但会保留配置，以便下次使用。

“添加”和“编辑”视图如下:



接口名称: vlan5

接口IP地址: 192.168.1.1

子网掩码: 255.255.255.0

起始IP地址: 192.168.1.100

结束IP地址: 192.168.1.200

网关: 192.168.1.1

租约时间: 60 分钟(5~11520)

首选DNS: 114.114.114.114

备用DNS:

确定 取消

图 3-9

- “接口名称”：对“添加”视图可选，选择将被开启服务的接口
- “接口 IP 地址” / “子网掩码”：不可配，仅显示
- “起始 IP 地址” / “结束 IP 地址”：DHCP 可分配的地址范围，其中起始 IP 必须在结束 IP 前。
- “网关”：分配给 DHCP 客户端的网关地址，用于客户端进行路由选择，通常设置为接口 IP。该配置项为可选项。
- “租约时间”：分配给客户端 IP 地址的有效时间，详见 3.2.1。
- “首选 DNS” / “备用 DNS”：分配给客户端的 DNS 信息。该配置项为可选项。

### 3.2.2 DHCP 客户端列表

配置页面：网络管理→DHCP 服务器→DHCP 客户列表

按关键字过滤: IP地址 格式:192.168.1.1 查询 显示全部

序号	IP地址	主机名	MAC地址
<input type="checkbox"/> 1	10.0.3.133	android-d3dd6a0c90a024f1	18:dc:56:d0:1c:a4
<input type="checkbox"/> 2	10.0.3.21	android-5e7ae4277d4881e9	b4:30:52:ac:32:bb
<input type="checkbox"/> 3	10.0.2.230		00:1e:40:99:99:99
<input type="checkbox"/> 4	10.0.3.192	android-8ff3730fa5a46780	64:6c:b2:30:3d:fa
<input type="checkbox"/> 5	10.0.3.1	MI4LTE-xiaomishouji	7c:1d:d9:70:94:90
<input type="checkbox"/> 6	10.0.3.45	admin-PC	44:8a:5b:b8:a1:e3

图 3-10

该页面主要用于诊断终端状态，并查看终端的 IP-MAC 对应情况。

## 3.3 路由与 DNS 配置

### 3.3.1 功能简介

#### 3.3.1.1 静态路由

在网络中路由器根据所收到的报文的地址选择一条合适的路径，并将报文转发到下一个路由器。路径中最后一个路由器负责将报文转发给目的主机。

路由就是报文在转发过程中的路径信息，用来指导报文转发。

RIB (Routing Information Base, 路由信息库)，是一个集中管理路由信息的数据库，包含路由表信息以及路由周边信息（路由迭代信息、路由共享信息以及路由扩展信息）等。

路由表中保存了各种路由协议发现的路由，根据来源不同，通常分为以下三类：

- 直连路由：链路层协议发现的路由，也称为接口路由。该路由不可配置。
- 静态路由：网络管理员手工配置的路由。静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。其缺点是每当网络拓扑结构发生变化，都需要手工重新配置，不能自动适应。
- 动态路由：路由协议发现的路由。AC 设备不包含动态路由功能。

路由器通过对路由表进行优选，把优选路由下发到 FIB (Forwarding Information Base, 转发信息库) 表中，通过 FIB 表指导报文转发。FIB 表中每条转发项都指明了要到达某子网或某主机的报文应通过路由器的哪个物理接口发送，就可以到达该路径的下一个路由器，或者不需再经过别的路由器便可传送到直接相连的网络中的目的主机。

目的地址/子网掩码均为“0.0.0.0”的静态路由又称为默认静态路由（或缺省静态路由）。该路由通常位于 RIB 最后一项，即匹配不到其他的路由规则时，报文将被转发到默认路由指定的网关。

### 3.3.1.2 策略路由

与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件（例如根据源网段、目的网段选择）的报文，执行指定的操作（设置报文的下一跳或优先级）。

报文到达后，其后续的转发流程如下：

- 首先根据配置的策略路由转发。
- 若找不到匹配的节点或虽然找到了匹配的节点，但直到报文转发失败时，再根据路由表中除缺省路由之外的路由来转发报文。
- 若转发失败，则根据策略路由中配置的缺省下一跳和缺省出接口指导报文转发。
- 若转发失败，则再根据缺省路由来转发报文。

### 3.3.1.3 DNS

DNS（Domain Name System）提供了域名解析的功能——用于将 Internet 域名地址（如：www.szzkww.com）转换为 IP 地址（112.124.114.54）。AC 上当前的手机认证服务、微信认证服务等需要访问 Internet，因此，若需要使用这些认证功能，必须配置对 AC 可用的 DNS 服务器地址。

## 3.3.2 具体配置

### 3.3.2.1 静态路由配置

配置页面：网络管理→路由与 DNS 配置→静态路由配置

基本操作：

- “添加”：添加一条静态路由
- “删除”：删除指定的静态路由条目
- “批量删除”：删除选定的多条静态路由条目

“添加”视图：



目的地址 10.1.0.0

子网掩码 255.255.255.0

网关 10.0.0.1

接口名称 vlan1

确定 取消

图 3-11

“目的地址” / “子网掩码”：地址和掩码共同决定一个“目的网络”或“目的主机”（当“子网掩码”为“255.255.255.255”时，指向一个主机地址）。以图 3-11 为例，“目的地址”为 10.1.0.0，“子网掩码”为 255.255.255.0，其指向一个目的网络，包含的主机地址从 10.1.0.1 ~ 10.1.0.254。

“网关”：此处也叫“下一跳”（next hop），指到达上述目的网络的报文将被送达的下一个路由设备的 IP 地址。

“接口名称”：指定路由出接口。

### 3.3.2.2 策略路由配置

配置页面：网络管理→路由与 DNS 配置→策略路由配置

基本操作：

- “添加”：添加一条策略路由规则
- “编辑”：修改指定的策略路由规则
- “删除”：删除指定的策略路由规则
- “批量删除”：删除选定的多条策略路由规则

“添加” / “编辑” 视图：





图 3-12

- “策略名”：自定义的便于标识的规则名称
- “优先级”：用于确定所有规则的优先级，具有唯一性，范围为 1~252，因此，策略路由的最大规格为 252。
- “源 IP/掩码长度”：用于匹配经过 AC 的报文的来源，掩码长度即为子网掩码中二进制位“1”的个数，例如掩码长度为 24，则对应的子网掩码为“255.255.255.0”
- “目的 IP/掩码长度”：用于匹配经过 AC 的报文的目的
- “下一跳”：指匹配到上述来源和目的的报文将被送达的下一个路由设备的 IP 地址。

### 3.3.2.3 DNS 配置

配置页面：网络管理→路由与 DNS 配置→DNS 配置

基本操作：

- “添加”：添加一条 DNS 条目
- “删除”：删除指定 DNS 条目
- “批量删除”：删除选定的多条 DNS 条目

“添加”视图：

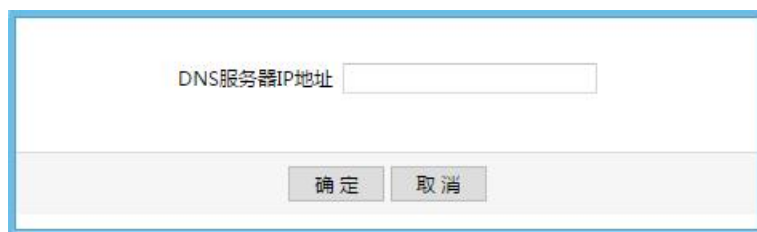


图 3-13

**注意:**

- 1、DNS 的最大条目数为 4，当存在多条 DNS 时，AC 选择 DNS 服务器的顺序从上往下；
- 2、修改 DNS 配置时（尤其是添加），需要重启设备才能生效。

## 3.4 AC 版本管理

配置页面：设备管理→AC 版本管理

AC 版本分为应用版本和内核版本，其中内核版本已经趋于稳定，当前的最新版本为 2.6.32.61-lisa-svn2341，升级必要性不大。

配置界面：



图 3-14

基本操作（以下操作对内核版本和应用版本均适用）：

- “切换”：切换到选择的版本，通常用于版本回退。
- “删除”：删除选择的版本，注：当前在使用的版本不可被删除
- “上传”：选择本地电脑的版本文件上传并升级。

 **注意：** 升级或切换后，需要重启系统（页面会提示是否立即重启）。

### 3.5 配置备份与恢复

配置页面：设备管理→备份与恢复

配置备份/恢复功能主要用于在两台或多台 AC 之间复制 AC 配置（替换现有 AC）。


操作界面：



图 3-15

基本操作：

- “导出配置”：导出 AC 现有的所有配置
- “导入配置”：选择已导出的配置文件，并执行导入操作
- “恢复默认配置”：将 AC 的配置恢复为出厂状态

 **注意：**

- 对导出的配置文件头部附有配置的校验信息，勿轻易修改文件内容，否则会导入失败。
- 恢复默认配置功能，会造成 VLAN1 的 IP 恢复为默认的“192.168.1.2”，与 AC 连接的 PC 必须配置同网段的 IP 才可重新访问 AC。

## 3.6 Web 帐号管理

### 3.6.1 简介

Web 帐号即登录 Web 管理页面的帐号，默认的用户名/密码为：admin/password。

每个 Web 用户都有特定权限：超级管理员、网络管理员、只读用户。

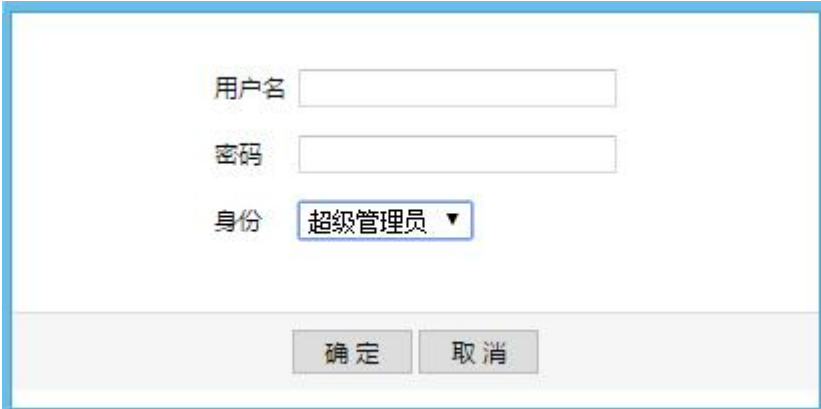
- 超级管理员:能查看并修改所有配置项
- 网络管理员：仅能查看并修改无线配置、接口配置等网络相关配置
- 只读用户：能查看所有配置，但无修改权限

### 3.6.2 配置

配置页面：设备管理→管理账户

基本操作：

- “添加”：添加一个用户
- “编辑”：修改指定的用户（可修改密码、权限）
- “删除”：删除指定的用户
- “批量删除”：删除选定的一个或多个用户



The screenshot shows a web form for user management. It contains three input fields: '用户名' (Username), '密码' (Password), and '身份' (Role). The '身份' dropdown menu is currently set to '超级管理员' (Super Administrator). At the bottom of the form, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

图 3-16

## 第 4 章 AP 与终端配置管理

### 4.1 AP 注册 AC

Capwap 中定义了标准的 AP 注册 AC 的基本业务流程，具体如下：

- AP 获取地址
- AP 发现 AC
- AP 加入 AC
- AC 与 AP 交互版本信息
- AC 下发配置
- STA 用户注册

#### 4.1.1 上线具体配置 (AV-V3200 与 AP-V230 举例)

##### 1) AP 的配置

AP 切换到集中管理模式：可切换模式的方式有两种，一种通过页面方式，在首页中切换本地模式与集中模式实现；另一种可以通过后台命令实现，配置如下：

```
AP-V230# set_ap ap_mode 1
```

##### 2) AC 上的 license 配置

License 的数目要大于或等于准备接入的 AP 的数量：一般该 license 数量发货时已经根据购买的 AP 数目导入相应的数目，但当重新增购 AP 或者接入时，需要考虑 License 的增加；

**页面向导：** 首页→设备管理→License 编辑页面后进行如下功能配置：



图 4-1

### 3) AC 上的 license 配置

升级策略中要添加对应型号的策略信息：该信息一方面用作对应型号的升级策略，一方面更重要的提供 AC 控制某种型号 AP 的准许接入规则；

**页面向导：** 首页→无线管理→AP 升级策略 编辑页面后进行如下功能配置：



图 4-2

操作	说明
设备型号	与 AP 名牌上型号一致
升级文件名	升级服务器上放置的 AP 升级文件要与该文件名一致
硬件版本	暂未区分，不需填写
软件版本	根据升级的目标版本填写，不填写时，AP 以当前版本上线

### 4) AC 上设置接入口

指定接入口信息：在 AC 的虚接口管理中，在实际组网中，可能会配置许多的接口，例如一个管理接口，多个业务接口，此时就需要指定一个接口作为 AP 上线交互的管理接口提供 AP 接入交互；

页面向导：首页→网络管理→虚接口管理，编辑页面后进行如下功能配置。

VLAN配置

批量删除
添加
➔
AP接入接口: vlan1

<input type="checkbox"/> 序号	接口名称	状态	IP地址	子网掩码	操作
<input type="checkbox"/> 1	vlan1	Up	172.20.40.102	255.255.255.0	编辑
<input type="checkbox"/> 2	vlan10	Up	172.20.60.102	255.255.255.0	编辑   删除   设为接入接口

图 4-3

**注意：**

- 二层组网中，可以不配置AC\_IPADDR信息AP通过局域网中广播发现AC，但三层组网中，必须配置AC\_IPADDR信息；
- 二层组网中，需要保证AP与AC在同一个局域网中（同一个VLAN中），三层组网中，需要保证AP与AC能够正常通信；
- 给AP分配地址的DHCP服务器，可以是AC，也可以架设为接入AP同一局域网中的核心交换机；

## 4.2 射频管理

射频(Radio Frequency)表示具有远距离传输能力、可以辐射到空间的电磁频率。在 IEEE 802.11 无线局域网协议中的 802.11b/g 工作于 2.4GHz 射频段、802.11a/ac 工作于 5GHz 射频段、802.11n 可以同时工作于 2.4GHz 和 5GHz 射频段。按照不同的工作频率可以将射频划分为信道(表示以无线信号作为传输媒体的传送通道),每个信道对应一个频率范围。

802.11ac 是 802.11n 的继承者，它借鉴了 802.11n 的各种优点并进一步优化，除了最明显的高吞吐特点外，同时还提升了多项技术。

- 更宽的通道带宽  
802.11ac 支持 80MHz 的频宽，可选择使用连续的 160MHz 频带，或者不连续的 80+80MHz 频带，频宽的提升带来了可用数据子载波的增加。80MHZ 可用的子载波数量达到 234 个，而 40MHZ 只有 108 个，这样 80MHZ 就可以带来 2.16 倍的增速。
- 更高阶的调制

802.11ac 使用了正交频分复用(OFDM)技术来调制数据比特在无线介质上传输。802.11ac 可视情况选用 256 QAM , 256 QAM 使每个子载波的数据比特数从 6 增加到了 8 个, 从而使吞吐量增加了 33%。

- 更多的空分流及 MU-MIMO

802.11ac 最多支持 8 路空间流,支持多个空间流是可选的, 但空间流数量的增加与 802.11ac 多用户多进多出 (MU-MIMO) 的新功能结合最为有效, 802.11ac 技术在单用户和多用户 MIMO 模式下, 支持最多 8 路空间流,最多 4 个用户,并且在多用户模式下, 每个无线终端不超过 4 路空间流。

**页面向导:** 首页→无线管理→分组管理→Radio 服务策略 , 若选择配置为 11ac 模式, 则进入 5G 射频射频配置, 选择<添加>按钮, 增加一条射频策略, 无线模式选择 11ac, 信道带宽可选择 80MHz, 如图所示。



图 4-4

射频设置 (服务选项) 的详细配置如表 4-1、表 4-2 所示

表 4-1

配置项	说明
-----	----



状态	分别控制射频的开与关
无线模式	选择 AP 的无线工作模式。 2.4G 射频工作模式支持 11b、11bg、11bgn、11gn、11n 5.8G 射频工作模式支持 11a、11an、11n、11ac 可选的射频模式与设备型号相关，使用中请以设备的实际情况为准
无线信道	指定射频的工作信道，信道列表由国家码和射频模式决定。信道列表与设备型号相关，使用中请以设备的实际情况为准
发射功率	射频的最大传输功率 射频的最大功率和国家码、信道、AP 型号、射频模式和天线类型相关
空间流	支持空间流的配置：1*1、2*2、3*3
信道带宽	802.11ac 通过将4个20MHz 的带宽绑定在一起组成一个80MHz 通讯带宽，在实际工作时可以作为1个80MHz 的带宽使用，这样可将速率提高一倍，提高无线网络的吞吐量 20MHz：工作带宽为20MHz 40MHz：工作带宽为40MHz 80MHz：工作带宽为80MHz 缺省情况下，802.11n(5GHz)的带宽为 40MHz，802.11n(2.4GHz)的带宽为 20MHz

表 4-2

配置项	说明
RTS 门限	启用 RTS (Request To Send, 要求发送) 机制所要求的帧的长度门限值。当帧的实际长度大于设定的门限值时，会启用 RTS 机制。RTS 用于在无线局域网中避免数据发送冲突。RTS 包的发送频率需要合理设置，设置 RTS 门限时需要进行权衡：如果将门限值设得较小，则会增加 RTS 包的发送频率，消耗更多的带宽。但 RTS 包发送得越频繁，无线网络从冲突中恢复得就越快。在高密度无线网络环境可以降低此门限值，以减少冲突发生的概率
Beacon 间隔	发送信标帧的时间间隔。信标帧按规定的時間间隔周期性发送，以允许移动用户接入网络，与其它接入点设备或其它网络控制设备进行联络

DTIM 间隔	设置信标帧的 DTIM 周期 (Delivery Traffic Indication Message, 数据待传指示信息) 当 DTIM 计数达到 0 时, AP 才会发送缓存中的多播帧或广播帧
低噪微调	默认值为 0, 可设置的范围为-20~40
CCA 门限	默认值为 10, 可设置的范围为 0~127
A-MPDU	选中“A-MPDU”前的复选框, 表示开启 A-MPDU 功能 802.11n 标准中采用 A-MPDU 聚合帧格式, 即将多个 MPDU 聚合为一个 A-MPDU, 只保留一个 PHY 头, 删除其余 MPDU 的 PHY 头, 减少了传输每个 MPDU 的 PHY 头的附加信息, 同时也减少了 ACK 帧的数目, 从而降低了协议的负荷, 有效的提高网络吞吐量
A-MSDU	选中“A-MSDU”前的复选框, 表示开启 A-MSDU 功能 802.11n 协议定义了一个新的 MAC 特性 A-MSDU, 该特性实现了将多个 MSDU 组合成一个 MSDU 发送, 通过聚合, A-MSDU 减少了传输每个 MSDU 的 MAC 头的附加信息, 提高了 MAC 层的传输效率
发包间隔	原 11a/g 的 Short GI 时长 800us, 短间隔 Short GI 时长为 400us 无线信号在空间传输会因多径等因素在接收侧形成时延, 如果后面的数据块发送的过快, 会和前一个数据块的形成干扰, GI 可以用来规避这个干扰。在使用 Short GI 的情况下, 可提高 10%的无线吞吐量
国家码	目前仅支持 CN
11nOnly	选中“只允许 11n 用户接入”前的复选框, 表示非 802.11n 的客户端将不能接入到 AP, 如果用户想要兼容 802.11a/b/g 的客户端, 同时还要接入 802.11n 的客户端, 可以取消该功能
前导码	前导码是位于数据包起始处的一组 bit 位, 接收者可以据此同步并准备接收实际的数据。 短: 短前导码。选择短前导码的能使网络同步性能更好, 一般选择短前导码 长: 长前导码。在网络中需要兼容一些比较老的客户端网卡时, 可以选择长前导码进行兼容 802.11a/an 不支持此项配置
动态频率调整	auto: 自动选择信道模式 (目前版本暂不支持)
同频功率调整	auto: 功率自动调整模式 (目前版本暂不支持)

逐包功率	开启该功能后，AP 会针对每个终端采用不同的功率发包
------	----------------------------

### 4.3 终端管理

终端接入 AP 后，所有 AP 的终端信息都会上报到 AV-V3200 上进行统计，可以提供客户进行数据分析、汇总以及后期的设备查看与维护。

**页面向导：** 首页→无线管理→设备管理→客户端设备，进入页面后进行如下功能配置。

可以统计分析如下内容：

连接的终端数	在线终端数	认证终端数
每台 AP 连接的终端数	连接终端的 IP 地址	连接终端的 MAC 地址
终端的流量信息	终端所属的 AP 信息	终端离线时间

终端管理还可以做的事情：

操作	说明
强制终端重新认证	操作后，终端需要重新就行认证才能正常上网
关闭短信用户注册通道	该功能启用后，新用户无法使用手机号注册的方式通过短信认证
设置认证时长有效时间	该功能可以设置终端多长时间需要重新认证一次



图 4-5

## 4.4 SSID 管理

SSID 是 Service Set Identifier 的缩写，意思是：服务集标识。SSID 技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。

AV-V3200 控制器上，可以将所有的 SSID 配置统一控制管理，便于后期维护，具体介绍如下：

**页面向导：首页→无线管理→分组管理→WLAN 策略管理** 进入页面后能看到如下功能配置：



组策略	RADIO服务策略	WLAN策略	定位策略	频谱导航	速率设置	数据接口																											
<div style="display: flex; justify-content: space-between;"> <span>WLAN服务策略</span> <span>WLAN安全策略</span> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <span>批量删除</span> <span>添加</span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>序号</th> <th>策略名</th> <th>ESSID</th> <th>编码</th> <th>Portal url</th> <th>Qos</th> <th>安全策略</th> <th>用户隔离</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>[Redacted]</td> <td>[Redacted]</td> <td>gb2312</td> <td>未启用</td> <td>启用</td> <td>WPA2-PSK</td> <td>隔离关闭</td> <td>编辑   删除   复制</td> </tr> <tr> <td>2</td> <td>[Redacted]</td> <td>[Redacted]</td> <td>utf8</td> <td>未启用</td> <td>启用</td> <td>WAP2-PSK</td> <td>隔离关闭</td> <td>编辑   删除   复制</td> </tr> </tbody> </table>							序号	策略名	ESSID	编码	Portal url	Qos	安全策略	用户隔离	操作	1	[Redacted]	[Redacted]	gb2312	未启用	启用	WPA2-PSK	隔离关闭	编辑   删除   复制	2	[Redacted]	[Redacted]	utf8	未启用	启用	WAP2-PSK	隔离关闭	编辑   删除   复制
序号	策略名	ESSID	编码	Portal url	Qos	安全策略	用户隔离	操作																									
1	[Redacted]	[Redacted]	gb2312	未启用	启用	WPA2-PSK	隔离关闭	编辑   删除   复制																									
2	[Redacted]	[Redacted]	utf8	未启用	启用	WAP2-PSK	隔离关闭	编辑   删除   复制																									

图 4-6

WLAN 服务策略的详细配置如表 4-3 所示。

表 4-3

操作	说明
策略名	WLAN 策略的标识名称
ESSID	定制指定的 SSID，支持中文 SSID
ESSID 编码	默认两种编码类型，该编码主要作用在中文 SSID 下，手机终端大部分默认支持 UTF8 编码，电脑大部分默认支持 GB2312 编码，组网配置时，根据实际场景进行配置
认证类型	支持免认证、短信认证、微信认证、微信+短信认证四种方式使用中请以设备的实际情况进行选择配置
安全策略	支持 wep 加密、wpa-psk、wpa2-psk 等 5 中类型的加密方式组网配置时，推荐使用 wpa2-psk，安全系数最高
隐藏 SSID	该功能开启后，终端无法搜索到 SSID
WDS 开关	该功能开启时，仅对同时开启 WDS 模式下的桥接设备才起作用

VLAN ID	可以设置终端所属的业务 VLAN 从属的 ID 值
最大用户数	可以设置该 SSID 最多允许多少用户连接
SSID 下行流控(kbps)	整个 SSID 的下行总的流量控制
STA 下行流控(kbps)	该 SSID 下，每个终端的下行带宽控制
SSID 上行流控(kbps)	整个 SSID 的上行总的流量控制
STA 上行流控(kbps)	该 SSID 下，每个终端的上行带宽控制
Qos	默认为禁用 建议组网应用时，将该功能开启，在禁用情况下，部分 Inter 网卡连接上 11n 的速率时，最高仅能协商到 54M
隧道转发模式	默认为本地转发模式（集中转发暂不支持）
用户隔离	开启隔离后，该 AP 下，用户之间的报文被隔离，无法通信

WLAN 服务策略安全策略的详细配置如表 4-4 所示。

表 4-4

操作	说明
开放式	选择此种方式，终端无需输入密码，直接可以连接 SSID
WEP	WEP 是 Wired Equivalent Privacy 的缩写，它是一种根本的加密办法 wep 加密支持三种密钥长度，5、13、16，用户可以根据实际使用对应选择配置
wpa-psk	WPA-PSK/WPA2-PSK 安全类型其实是依据同享密钥的 WPA 形式，使用加密算法为 TKIP，安全性很高，设置也对比简单，合适普通家庭用户和小型企业运用
wpa2-psk	WPA2-PSK 安全类型其实是依据同享密钥的 WPA 形式，使用加密算法为 AES，安全性很高，设置也对比简单，合适普通家庭用户和小型企业运用
wpa-eap	WPA 是一种比 WEP 强壮的加密算法，挑选这种安全类型，路由器将选用 Radius 服务器进行身份认证并得到密钥的 WPA 安全形式。因为要架

	起一台专用的认证服务器，价值对比贵重且保护也很杂乱，所以不推荐普通用户运用此安全类型
wpa2-eap	WPA2 是一种比 WEP 强壮的加密算法，挑选这种安全类型，路由器将选用 Radius 服务器进行身份认证并得到密钥的 WPA2 安全形式。因为要架起一台专用的认证服务器，价值对比贵重且保护也很杂乱，所以不推荐普通用户运用此安全类型

## 4.5 AP 升级管理

### AC 控制 AP 升级过程与原理

AP 映像文件升级可以发生在两个阶段，第一个是 CAPWAP 状态机在 Image Data 阶段，第二个是在 CAPWAP 状态机 RUN 之后手工方式让 AP 升级为新的版本。AP 在 Image Data 阶段升级映像文件的基本过程是：

AP 在 Join 阶段通过 Join Request 报文告诉 AC 自己的厂家标识 (Vendor Identifier)、AP 型号 (AP Model Number)、当前使用的软件版本号 (Active Software Version)，AC 必须随 CAPWAP 状态机保存这些信息。

AC 在回应 Join Response 之前，根据 AP 上报的厂家标识、AP 型号、硬件版本号等信息查找本地的 AP 升级策略中的一条记录，获取 AP 应该使用的映像版本号和对应的映像文件名，并和 AP 当前使用的软件版本号进行对比。如果发现一致，则 AP 不需要升级；否则需要在 Join Response 报文中携带 Image Identifier 元素，其值为 AP 应该使用的新的映像文件名，以及提供升级的服务器的地址；如果 AC 根据这些信息在 AP 升级策略中仅查看到型号，未找到对应的版本信息，则默认 AP 继续使用当前的映像版本上线。

### 升级方法与说明

通过软件升级，您可以加载最新版本的软件，以获得更多的功能和更为稳定的性能，下面简单针对升级作如下说明和注意事项介绍：

#### 1) 升级文件命名规范

### 范例：AP-V230V100R001C06B010SP0

1. AP-V230 :产品型号，由两位字母和三位数字组成。
2. V100：主版本号，数字必须三位，不够补0
3. R001：次版本号，数字必须三位，不够补0
4. C06：分支号，数字必须两位，不够补0
5. B010：变更主版本号，数字必须三位，不够补0
6. SP0：补丁版本号，数字必须三位
7. bin：升级文件后缀

### 2) 升级版本的配置

AC 对 AP 批量升级配置，首先在 AP 升级策略中填入 AP 需要跟新的版本号信息

- B021 以前的版本升级方式取到过渡版本，如 SQUASHFS-AP-V230APT140810-N110310.img，把它的名字改成 AC 可以识别的升级文件名字，如 AP-V230V100R001C06B025SP6.bin，放到 server 上面。然后配置升级策略如下：

设备型号	WA722M-E
软件版本	V100R001C06B025SP6 格式:VxxxRxxxCxxBxxx[SPx] (x为数字, []内可选)
升级文件名	WA722M-EV100R001C06B025SP6.bin
硬件版本	A

图 4-7

### 注意:

AC 新版本 SP16D 现在目前只识别后缀.bin 的升级文件，所以必须把过渡版本的名字改一下进行伪装，才能让 AP 正常进行过渡版本的升级。

- B021 及以后的版本不再需要过渡版本，直接选择后缀.bin 的文件升级。

如 WA718V100R001C06B025SP6.bin，在 AC 上配置相应的策略，并放到 server 然后即可升级。

### 3) 升级服务器的配置

AC 目前支持两种方式对瘦 AP 进行统一管理升级，如下图：



图 4-8

**FTP 方式升级：**AC 使用默认的 anonymous 的匿名用户登录，所以配置外置升级的 ftp 服务器时，需要添加用户名 anonymous 的用户，无密码。

**TFTP 方式升级：**与之前升级 AP 的方法没有改变。

#### 注意：

- a) 升级时，FTP 和 TFTP 方式同时仅支持一种
- b) 升级时，要保证 AP 与 TFTP 服务器和 FTP 服务器可达
- c) 升级推荐使用 FTP 方式升级



#### 4) 升级操作

页面向导：首页→无线管理→设备管理，进入页面后进行如下功能配置。

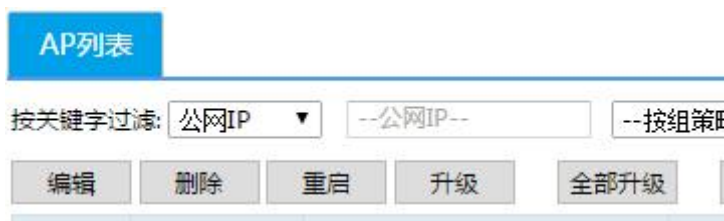


图 4-9

操作	说明
升级	该操作适合点选部分 AP 选择性升级 推荐升级方式为该种升级，针对服务器以及带宽限制，点选 10、20、30 台进行升级
全部升级	该操作适合在升级服务器性能允许、且带宽足够的情况下进行 AP 升级

## 4.6 MAC 黑名单

黑名单是在开启认证情况下，限制指定的终端不能完成认证上网。

页面向导：无线管理→设备管理→黑/白名单→黑名单，可添加、批量删除黑名单用户。配置页面如图 4-10。



图 4-10

单击<添加>按钮后，出现如图 4-11 所示页面。



图 4-11

操作	说明
用户名	配置该黑名单的名称
MAC	输入指定终端的 MAC 地址
状态	选择“启用”，则该终端需进行认证才可上网，选择“禁用”，则该终端无需认证可上网

## 4.7 MAC 白名单

白名单是在开启认证情况下，限制指定的终端不需要认证就可以直接上网，方便业务的灵活配置。

**页面向导：**无线管理→设备管理→黑/白名单→白名单，可添加、批量删除白名单用户。单击<添加>按钮后，出现如图 4-12 所示页面。



图 4-12

操作	说明
用户名	配置该白名单的名称
MAC	输入指定终端的 MAC 地址
状态	选择“启用”，则该终端无需进行认证可上网，选择“禁用”，则该终端需认证才可上网

## 4.8 反向 SSH 配置

反向连接是指主机 A（受控端）主动连接主机 B（控制端），在主机 A 和主机 B 之间建立一个远程连接，通过这个连接主机 B 可以主动的向主机 A 发送一些请求。

连接流程如下：

1. 主机 A ssh 客户端向主机 B sshd 服务端发送请求，建立远程连接。
2. 主机 B sshd 服务端创建本地连接很远程连接的映射（反向连接通道）。
3. 主机 B ssh 客户端向主机 B sshd 服务端的连接通道发送请求，建立主机 B ssh 和主机 A sshd 的连接。

页面向导：无线管理→设备管理→AP 设备→AP 列表→反向 SSH，配置页面如图 4-13。



图 4-13

选中需要设置 SSH 的 AP 设备，点击“反向 SSH”按钮后，在跳出的对话框中，勾选 SSH 开关即可，页面如图 4-14。



图 4-14

## 4.9 AP 设备管理

### 4.9.1 修改 AP 密码

页面向导: 无线管理→设备管理→AP 列表→AP 密码, 可修改配置 AP 页面登录密码以及 SSH 远程登录密码。配置页面如图 4-15、4-16 所示。



图 4-15

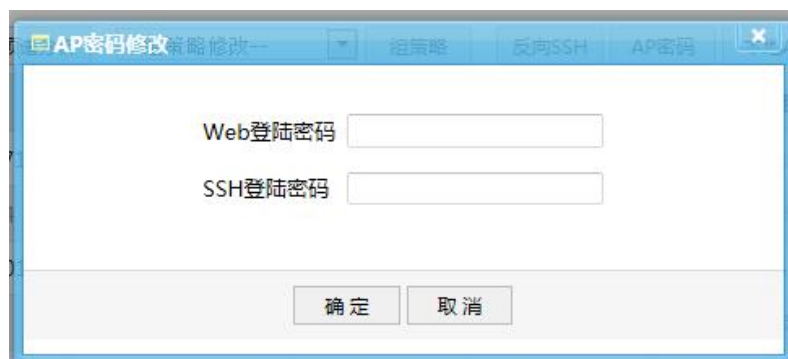


图 4-16

## 4.9.2 修改本地 AC

页面向导：无线管理→设备管理→AP 列表→本地 AC，可修改配置 AP 上线 AC 地址。配置页面如图 4-17 所示。



图 4-17

## 4.9.3 修改 AP 模式

页面向导：无线管理→设备管理→AP 列表→运行模式，配置页面如图 4-18。



图 4-18

点击“运行模式”后，在跳出的对话框中，可选择设备的工作模式，可选择路由模式、AP 模式、中继模式、STA 模式。页面如图 4-19。



图 4-19

## 4.10 AP 录入

AP 录入功能，可在 AP 未与 AC 上线时，提前录入 AP 的设备信息，如 MAC 地址、软件版本等，并可给设备配置组策略和未认证策略。当录入相关设备信息的 AP 与 AC 上线时，AP 会自动下发录入的配置。

页面向导：无线管理→设备管理→AP 列表→AP 录入，配置页面如图 4-20、4-21 所示。



图 4-20



图 4-21

## 第 5 章 特性功能配置管理

### 5.1 漫游配置

#### 5.1.1 功能简介

WLAN 漫游是指 STA 在同属于一个 ESS 内的 AP 之间移动且保持用户业务不中断。STA 从 AP1 的覆盖范围移动到 AP2 的覆盖范围的行为就叫做漫游。

WLAN 网络的最大优势就是 STA 不受物理介质所处位置的影响,可以在 WLAN 覆盖范围内四处移动,这样就需要 STA 在移动过程中能够保持业务不中断, WLAN 漫游技术因此而产生。同一个 ESS 内包含多个 AP 设备,当 STA 从一个 AP 覆盖区域移动到另外一个 AP 覆盖区域时,利用 WLAN 漫游技术可以实现 STA 用户业务的平滑过渡。

WLAN 漫游解决了以下问题:

- 避免漫游过程中用户的认证时间过长而导致数据丢包甚至业务中断。

如果 STA 接入 Internet 需要用户接入认证,认证过程(例如 802.1X 认证)时间较长。快速漫游避免 STA 重新认证的过程,保证了用户业务不中断。

- 保证用户 IP 地址不变。

应用层协议是以 IP 地址和 TCP/UDP 协议承载用户业务,漫游后的用户必须能够保持原 IP 地址不变,对应的 TCP/UDP 连接才能不中断,应用层数据才能保持正常转发。

- 说明:实现 WLAN 漫游的各 AP 必须使用相同的 SSID(例如,图 5-1 所示的 SSID 都为 anysec)和安全模板(安全模板 ID 可以不同,但是安全模板下的配置必须相同)。

漫游原理:

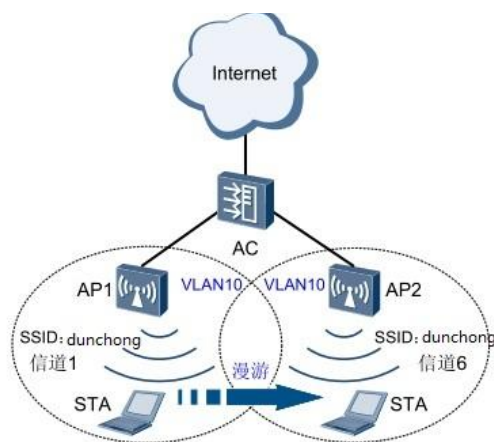


图 5-1

如图 5-1 所示，STA 已经通过 AP1 接入 Internet。此时，STA 需要从 AP1 的覆盖范围移动到 AP2 的覆盖范围，按照如下的流程实现漫游功能：

1. STA 在各个信道中发送探测请求帧，周围 AP 收到该请求帧后发送回应帧进行响应。例如，AP2 在信道 6（AP2 使用的信道）中收到请求后，通过在信道 6 中发送应答帧来进行响应。STA 收到周围各 AP 的应答帧后，根据信号强度、信号质量等信息进行评估，确定与哪个 AP 关联最合适。假设如图所示的，STA 最终确定跟 AP2 关联。

2. STA 向 AP2 发送重关联请求，AP2 收到后上报 AC，AC 使用重关联响应做出应答，建立 STA 与 AP2 间的关联。

3. STA 与 AP2 关联成功后，删除 STA 与 AP1 的连接。STA 通过信道 1（AP1 使用的信道）向 AP1 发送 802.11 解除关联信息，解除 STA 与 AP1 间的关联。

## 5.1.2 配置步骤

### 1) 预置条件

基本配置，即保证 AP 正常上线，配置 WLAN 基本业务

### 2) 开启漫游功能

页面向导：首页→无线管理→分组管理→组策略 进入页面后进行如下功能配置。





图 5-2

### 3) 设置漫游阈值

漫游阈值：默认配置为-75dbm，设置范围为（-60 ~ -90dbm）。如图 5-2 所示。

## 5.2 弱信号管理

### 5.2.1 功能简介

弱信号管理功能通过强制弱信号终端下线，AP 主动向低于指定信号强度或指定接入速率的 STA 发送解除关联帧，让 STA 可以重新连接或漫游。适用于高密 WLAN 网络（AP 密集布放，例如体育馆、演讲厅、图书馆、报告厅、宿舍、发布会现场等），保证用户的接入效果，提升用户体验。

### 5.2.2 配置步骤

#### 1) 预置条件

基本配置，即保证 AP 正常上线，配置 WLAN 基本业务。

#### 2) 开启弱信号管理功能

页面向导：首页→无线管理→分组管理→组策略 进入页面后进行如下功能配置。



图 5-3

### 3) 设置禁止弱信号接入值

**禁止弱信号接入：**默认配置为-80dbm，设置范围为（-60~-95dbm）。如图 5-3 所示

## 5.3 频谱导航

### 5.3.1 功能简介

目前，很多无线终端都只能工作在 2.4GHz 模式，同时，很多可以双频工作的无线终端习惯工作在 2.4GHz，这就造成 2.4G 信道资源紧张，而 5G 信道空闲造成资源浪费。频谱导航通过引导双频 STA 关联到 5GHz 的射频上，使 5GHz 和 2.4GHz 上关联用户数达到均衡，从而提高整网性能。

### 5.3.2 配置步骤

#### 1) 前置条件

基本配置，即保证 AP 正常上线，配置 WLAN 基本业务，AP 需满足以下条件。

- AP 必须为双频 AP，同时支持 2.4G 与 5.8G 频段；
- 2.4G 与 5.8G 必须下发同样的 WLAN 服务策略；

## 2) 添加频谱导航策略

页面向导：首页→无线管理→分组管理→频谱导航 进入页面后进行如下功能配置。



图 5-4

- 最大拒绝次数与老化时间一般选择默认配置，最大用户数可根据实际情况做修改。
- 导航模式分为快速导航和普通导航，推荐使用“快速导航”。

## 3) 开启频谱导航功能

页面向导：首页→无线管理→分组管理→组策略 进入页面后进行如下功能配置。



图 5-5

#### 4) 设置组策略中 2.4G 与 5.8G WLAN 服务策略一致

- 频谱导航功能要求, 2.4G 与 5.8G 广播 SSID 必须一致。如图 5-6 所示。



图 5-6

## 5.4 负载均衡

### 5.4.1 功能简介

负载均衡功能是通过配置负载均衡, 可以在 WLAN 网络中平衡 AP 的负载, 充分的保证每个 STA 的性能和带宽, 从而提高用户体验效果。

负载均衡功能原理, 如图 5-7 所示

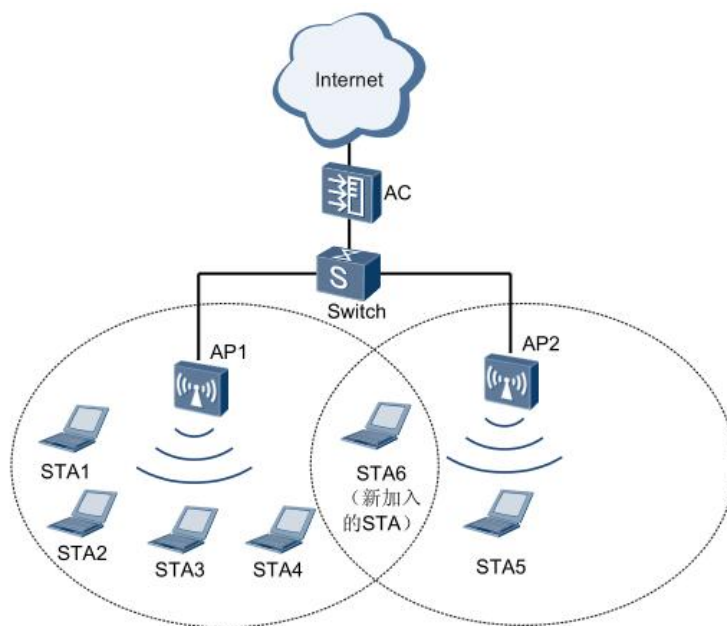


图 5-7

如图所示, AP1 和 AP2 与 AC 关联, AP1 下有 4 个在线用户(STA1 ~ STA4), AP2 上有 1 个在线用户(STA5)。如果 AP1 覆盖范围内无线用户过多,且都通过 AP1 连接 Internet,这就会导致 AP1 上负载过重,AP2 上资源空闲。使能负载均衡后,当有新的 STA (图中的 STA6) 想通过某 AP 接入 Internet 时,AC 根据负载均衡算法判断是否允许该 STA 接入此 AP。通过负载均衡,限制新关联用户接入到重负荷 AP,从而减轻其负担。

## 5.4.2 配置步骤

### 1) 预置条件

基本配置,即保证 AP 正常上线,配置 WLAN 基本业务,AP 需满足以下条件。

- 负载均衡功能的 AP 必须连接到同一 AC 上,且 STA 能够扫描到相互进行负载均衡的 AP 的 SSID 信号。

负载均衡的触发条件:

- 基本条件:连接用户达到的个数(设备设置的最大负载数\*40%)
- 信号条件:AP 扫描到终端的信号强度要高于阈值(信号强度水平-95dbm)
- 差值条件:符合以上两个条件后,两台 AP 的差值要大于该差值(设备设置的最大负载数\*负载均衡水平%)

### 2) 开启负载均衡功能

页面向导: 首页→无线管理→分组管理→组策略,进入页面后进行如下功能配置:

设备最大负载:为单台 AP 能够承担最大连接数,当此 AP 承受终端达到此数值时会自动隐藏 SSID,负载低于设置值 80%时会广播 SSID。如图 5-8 所示。



图 5-8

### 3) 设置负载均衡配置

设备最大负载：负载均衡水平根据之前设置的最大用户数而定，最大用户数为 50 则负载均衡水平推荐 20 左右，老化时间推荐 10s，信号强度水平推荐 25 左右。如图 5-9 所示。

页面向导：首页→设备管理→AP 设备→负载均衡配置 进入页面后进行如下功能配置：



图 5-9

## 5.5 流量上报

### 5.5.1 功能简介

流量上报功能分为两种：

- 基于 AP 统计实时流量上报
- 基于终端累计流量上报

流量上报功能可以了解全部管理 AP 的最新动态，每个管理 AP 对应的用户信息，时时了解 AP 负载情况和终端用户网络使用情况。

## 5.5.2 配置步骤

### 1) 预置条件

- 基本配置，即保证 AP 正常上线，配置 WLAN 基本业务，接入终端访问 internet。
- 终端流量统计功能需用户通过 portal 认证或者微信认证，所以请先完成 portal 认证环境。

### 2) 开启 AP 实时流量上报

页面向导：首页→无线管理→设备管理→AP 设备 进入页面后进行如下功能配置：

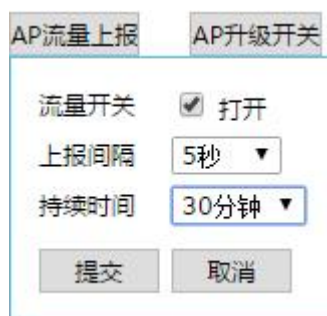


图 5-10

上报间隔为 AP 上报流量时间间隔，持续时间为 AP 上报流量的持续时间，可设置最大时间为 1 小时。

### 3) 查看 AP 实时速率

页面向导：首页→无线管理→设备管理→AP 设备 进入页面后进行查看 AP 实时速率，如图 5-11 所示。

AP列表

按关键字过滤: 公网IP --公网IP-- --按组策略名-- --按未认证策略-- --按状态-- --按升级状态-- 查询 显示全部

编辑 删除 重启 升级 全部升级 频谱分析 --组策略修改-- 修改 总上行速率: 0 总下行速率: 0

序号	设备型号	序列号	MAC地址	私网IP	公网IP	软件版本	组策略名	未认证策略	位置	上行速率	下行速率	状态
1	WA718	wadc01405120100196	a4-fb-8d-00-6f-22	172.20.40.9	172.20.40.9	B025SP6	default	N/A	N/A	21541 kbps	13384 kbps	RUN

共1条

图 5-11

#### 4) 开启终端流量统计

页面向导: 首页→无线管理→分组管理→组策略 进入页面后, 如图 5-12 所示。



图 5-12

#### 5) 查看终端流量统计

页面向导: 首页→无线管理→设备管理→客户端设备 查看终端认证后累计使用流量, 如图 5-13 所示。

客户端管理

按关键字过滤: 客户IP地址 --客户IP地址-- --按认证状态-- 在线 查询 显示全部

批量重新认证 认证间隔修改 共1条

序号	客户IP地址	客户MAC地址	所属AP信息	流量信息	认证状态	终端状态	上线时间	离线时间	操作
1	172.20.40.18	64-5a-04-c3-23-1c	序列号: wadc01405120100196 MAC: a4-fb-8d-00-6f-22	上行: 402.555MB 下行: 263.309MB	已认证	在线	2011-12-19.19:39:57		重新认证

图 5-13



## 5.6 流量限速

### 5.6.1 功能简介

流量控制用于防止在无线网络阻塞的情况下丢帧，这种方法是当发送或接收开始溢出时通过将阻塞信号发送回源地址实现的。流量控制可以有效的防止由于网络中瞬间的大量数据对网络带来的冲击，保证用户网络高效而稳定的运行。

流量控制分为如下两部分：

- 基于非 portal 用户
- 基于 portal 用户

#### 注意：

该两部分认证的配置以及实现不在同一个地方，因此需要尤其注意：

- 对于已经认证 Portal 用户的限速，该限速基于每个认证用户的帐号内部配置和实现的，与 WLAN 内部的限速无关，即使 wlan 内部不限速也没有关系
- 对于非 Portal 用户的限速，该部分的配置是在 wlan 中配置实现的，需要我们在 wlan 中进行相应的上下行的配置

### 5.6.2 配置步骤

#### 1) 预置条件

- 基本配置，即保证 AP 正常上线，配置 WLAN 基本业务。
- 终端流量限速功能需用户通过 portal 认证，所以请先完成 portal 认证环境。

#### 2) 开启基于非 portal 认证的流量控制

页面向导：首页→无线管理→WLAN 策略→组策略 进入页面后进行如下功能配置：

例：设置终端 STA 的最大上下行带宽为 2Mbps

SSID下行流控(kbps)	<input type="text" value="0"/>	<a href="#">0~100000</a>
STA下行流控(kbps)	<input type="text" value="2048"/>	<a href="#">0~100000</a>
SSID上行流控(kbps)	<input type="text" value="0"/>	<a href="#">0~100000</a>
STA上行流控(kbps)	<input type="text" value="2048"/>	<a href="#">0~100000</a>

图 5-14

### 3) 开启基于 portal 认证的流量控制

基于 portal 认证的流量控制（即基于用户的流量限速），完成设置后使用用户名密码通过 portal 认证，流量控制功能就会生效。

页面向导：首页→运营管理→权限管理→访问策略，进入页面后进行如下配置。

上行流控	<input type="text" value="基于用户"/>
	<input type="text" value="2048"/> (1~100000) kbps
下行流控	<input type="text" value="基于用户"/>
	<input type="text" value="2048"/> (1~100000) kbps

图 5-15

页面向导：首页→运营管理→用户管理→添加，进入页面后进行权限策略引用配置，如图 5-16 所示。

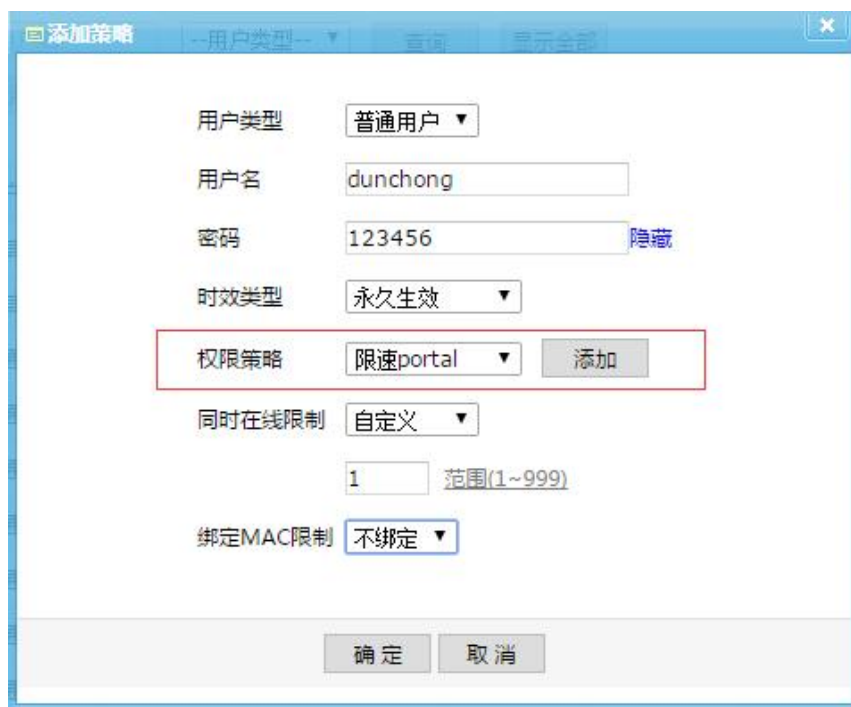


图 5-16

## 5.7 用户隔离

### 5.7.1 功能简介

用户隔离功能是指关联到同一个 VAP 上的所有无线用户之间的二层报文不能相互转发，从而使无线用户之间不能直接进行通讯，保证了用户间数据的安全性，同时也便于对用户进行管理。

由于无线网络开放性的特点，业务数据存在安全风险。用户对 WLAN 网络的安全性要求不高，可以配置 WEP 安全策略，使用共享密钥认证和 WEP 数据加密。为了对无线用户集中管理，同时为了保证 WLAN 信道资源不被占用，禁止无线用户之间通过二层转发互相通信，配置用户隔离功能。

### 5.7.2 配置步骤

#### 1) 预置条件

基本配置，即保证 AP 正常上线，配置 WLAN 基本业务。

#### 2) 开启用户隔离功能

页面向导：首页→无线管理→WLAN 策略，进入页面后进行如下功能配置。



图 5-17

## 5.8 速率集配置

### 5.8.1 功能简介

无线信号的传播受周围环境影响，多径等问题会导致无线信号在不同方向上存在非常复杂的衰减现象，所以 WLAN 网络的实施往往需要周密的网络规划。即使在成功部署无线网络后，应用阶段的参数调整仍然必不可少，这是因为无线环境是在不断变化的，移动的障碍物、正在工作的微波炉等带来的干扰等都可能对无线信号的传播造成影响，所以信道、发射功率等射频资源必须能够动态地调整以适应用户环境的变化。这样的调整过程是复杂的，需要丰富的技术经验和定期的人工检测，无疑造成非常高的管理成本。

协议标准	物理层技术	支持频段 (GHz)	支持传输速率 (Mbit/s)
802.11	FHSS/DSSS	2.4	1, 2
802.11b	DSSS	2.4	1, 2, 5.5, 11
802.11a	OFDM	5	6, 9, 12, 18, 24, 36, 48, 54
802.11g	DSSS/OFDM	2.4	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54
802.11n	OFDM/MIMO	2.4, 5.8	支持速率由调制编码方案 MCS 决定。理论支持最大速率为 600

## 5.8.2 配置步骤

### 1) 预置条件

基本配置，即保证 AP 正常上线，配置 WLAN 基本业务。

### 2) 速率设置策略添加

页面向导：首页→无线管理→分组管理→速率设置 进入页面后进行如下功能配置：

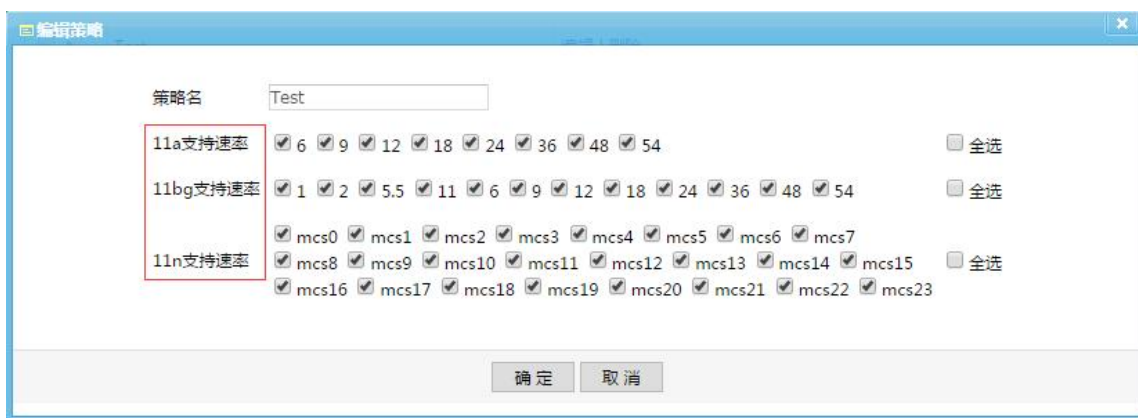


图 5-19

### 3) 组策略中引用速率设置

页面向导：首页→无线管理→分组管理→组策略 进入页面后进行速率策略引用，如图 5-20 所示。

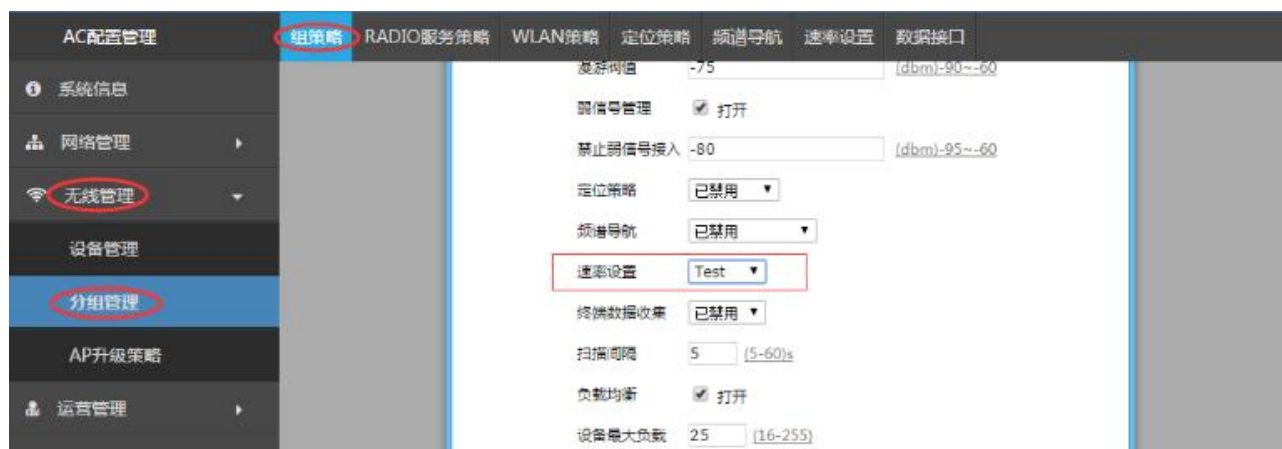


图 5-20

## 5.9 短信认证

### 5.9.1 功能简介

短信认证即在 Portal 认证的基础上，根据用户提供的手机号码动态生成登录密码，再通过短信网关将密码发送至用户手机上，用户可以通过手机号动态密码通过认证。

### 5.9.2 配置步骤

#### 1) 预置条件

基本配置，即保证 AP 正常上线，配置 WLAN 基本业务。

#### 2) Portal 页面配置

页面向导：首页→运营管理→广告页定制→定制 portal 页面 点击新建或修改“认证类型”为“账号认证”，如图 5-21 所示。



图 5-21

#### 3) WLAN 策略配置

页面向导：首页→无线管理→分组管理→WLAN 策略 点击新建或修改策略将“认证类型”修改为“账号认证”，“Portal 类型”修改为“内置 portal”，如图 5-22 所示。

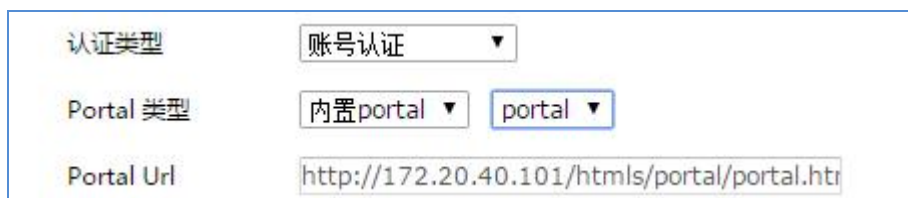


图 5-22

#### 4) 用户页面配置

页面向导：用户管理→用户→添加，页面如图 5-23 所示。



图 5-23

点击<添加>按钮，添加手机用户，跳转至添加策略页面如图 5-24 所示。



图 5-24

操作	说明
用户类型	用户类型包括普通用户和手机用户，这里需要选择手机用户
用户名	配置用户的手机号码
密码	配置手机用户的密码
时效类型	时效类型包括永久生效、定时长有效和定时间点有效 永久生效：认证后认证状态一直保存 定时长有效：认证后超过配置时长后需要重新认证 定时间点有效：在指定的时间点内用户有效，非指定时间点内不能认


	证上网
权限策略	权限策略决定了用户可访问的资源,可在“权限管理”→“权限策略”中编辑或添加权限策略。
同时在线限制	包括不限、禁止登录和自定义
绑定 MAC 限制	不绑定: 用户不限制 MAC 绑定: 只有指定的 MAC 才能完成用户认证上网

### 5) 短信网关配置

页面向导: 首页→运营管理→用户管理→短信平台 点击修改策略 “短信通”或“互亿无线”, 填写入正确的用户名和密码, 如图 5-25 所示。



图 5-25

 **注意:**

“密码提示”与“内容提示”为发送至用户手机内的短信内容提示,方便理解。用户手机收到的短信格式为:“您的验证码是: 123456。如需帮助请联系客服”。

### 6) 用户获取认证密码进行短信认证

STA 关联 SSID 后访问 Internet 推送 portal 页面,输入用户手机号获取认证密码,进行短信认证。



## 5.10 微信认证

### 5.10.1 功能简介

微信认证为用户通过认证即可上网的一种便捷的认证类型之一，微信认证实现了用户通过关注微信公众号实现认证。传统认证用户体验并不好，很多公众场合接入操作繁琐、需询问密码，同时有安全有隐患，微信认证很好的解决了此类问题，实现方便、快捷连接无线网络。

### 5.10.2 配置步骤

#### 1) 预置条件

基本配置，即在未开启 Portal 认证和微信认证的前提下，AC 与 AP 应配置达到如下要求：

- AC 能够与外网通信（保证与微信服务器与第三方微信平台的通信正常）
- 终端连接 SSID 后能够正常上网；

#### 2) 微信公众号设置

**页面向导：** 首页→运营管理→微信管理→微信公众号 进入页面后进行如下功能配置，以下以公众账号为例，如图 5-26 所示。

操作	说明
公众号名称	深圳中科网威
公众号原始 ID	gh_27677853fce4
微信号	szzkww
公众号类型	服务号
APPID	wxc98fcd063a37b770
Secret	9643f78a28a65f7a9d49c820c255b742
图文链接	<a href="http://wx.XXXX.com/Uploads/Picture/2015-01-07/54acf0f4004fb.jpg">http://wx.XXXX.com/Uploads/Picture/2015-01-07/54acf0f4004fb.jpg</a>

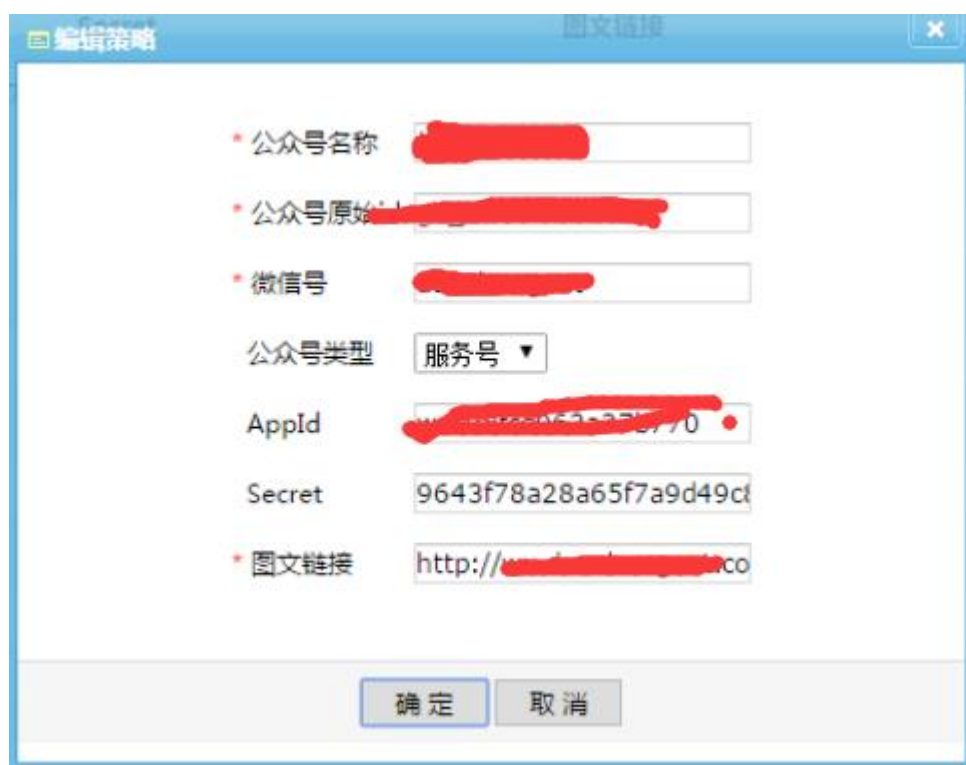


图 5-26

### 3) 定制微信 portal 页面配置

**页面向导：** 首页→运营管理→广告页定制→添加 Portal 页面 点击新建或修改定制 portal 页面将“认证类型”修改为“微信认证”，如图 5-27 所示



图 5-27

### 4) WLAN 策略配置

**页面向导：** 首页→无线管理→分组管理→WLAN 策略 点击新建或修改策略将“认证类型”修改为“微信认证”，“微信名称”选择“深圳”“Portal 类型”修改为“内置 portal”。

## 5) 设置未认证策略

**页面向导：** 首页→运营管理→未认证策略 进入页面后进行如下功能配置，以下以公众账号为例，如图 5-28 所示。

**需要添加的白名单：** qq.com; weixin.qq.com; gting.cn; weixin.com; qplic.cn; qllogo.cn



序号	策略名	允许的IP/Domain	操作
1	weixin	qllogo.cn <a href="#">编辑</a> <a href="#">删除</a> qplic.cn <a href="#">编辑</a> <a href="#">删除</a> qq.com <a href="#">编辑</a> <a href="#">删除</a> weixin.com <a href="#">编辑</a> <a href="#">删除</a> gting.cn <a href="#">编辑</a> <a href="#">删除</a>	<a href="#">添加到本组</a>   <a href="#">删除本组</a>

图 5-28

## 6) 未认证策略下发

**页面向导：** 首页→无线管理→设备管理→AP 设备 进入页面后进行如下配置。

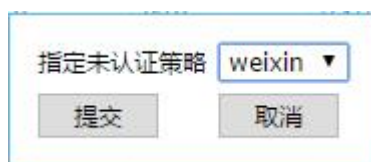


图 5-29

# 5.11 中文 SSID

## 5.11.1 功能简介

**无线网络使用中文 SSID 名** 在我们搜索到的绝大部分无线热点中，SSID 都是清一色的英文标识，甚至还有不少无线路由器使用默认的 SSID，不易区分。改成中文的 SSID 将会让你在众多的周边无线接入点中彰显个性，自然找起来更是非常方便。

目前存在部分终端扫描到中文 SSID 为乱码的情况，这是不同终端的编码解码方式不同造成的，大部分手机的编码方式为 UTF8，而大部分 PC 终端的编码方式为 GB2312，本功能就是针对此问题所设计的。

## 5.11.2 配置步骤

### 1) 预置条件

基本配置，即保证 AP 正常上线，配置 WLAN 基本业务。

### 2) 中文 SSID 配置方法

因不同的终端支持不同的编码方式，所以在配置支持中文 SSID 时，需同时支持两种编码方式，从而保证不同类型终端在搜索 SSID 时都可以搜索到。

**页面向导：** 首页→无线管理→分组管理→WLAN 策略 进入页面后进行如下功能配置，以下以 ESSID 编码为“GB2312”为例，如图 5-30 所示



The screenshot shows a configuration form with the following fields:

- 策略名 (Strategy Name): [Redacted]
- ESSID: Test\_ [Redacted]
- ESSID编码 (ESSID Encoding): gb2312

图 5-30

图 5-30

配置完成后 WLAN 策略如下。

序号	策略名	ESSID	编码	Portal url	Qos	安全策略	用户隔离	操作
1	wlan_default	Dunchong	gb2312	未启用	禁用	open	隔离关闭	编辑   删除   复制
2	[Redacted]	Test_dunchong	gb2312	未启用	禁用	open	隔离关闭	编辑   删除   复制
3	[Redacted]	Test_dunchong	utf8	未启用	禁用	open	隔离关闭	编辑   删除   复制

图 5-31

### 3) 创建多个 SSID 配置方法

**页面向导：** 首页→无线管理→分组管理→WLAN 策略→复制，此功能可配置 AP 下发多个 SSID。

选择需要创建多个 SSID 的策略，点击该条策略后的<复制>按钮，如图 5-32 所示。

WLAN服务策略		WLAN安全策略							
序号	策略名	ESSID	编码	Portal url	Qos	安全策略	用户隔离	操作	
1	11ac_test	[Redacted]	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制	
2	11ac_test	[Redacted]	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制	
3	11ac_test	[Redacted]d2	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制	
4	wlan_default	Dunchong	gb2312	未启用	启用	open	隔离关闭	编辑   删除   <b>复制</b>	

图 5-32

点击该条策略后的<复制>按钮后, 进入添加 SSID 页面, 修改 SSID 名称以及其他配置, 配置完成后, 选择<确定>按钮。即可在该条策略下新建一个 SSID。如图 5-33、5-34 所示。

**添加策略**

策略名: wlan\_default

ESSID: omg

ESSID编码: gb2312

认证类型: 免认证

安全策略: open

隐藏SSID:

WDS开关:

VLAN ID: 0 (0~4094)

WLAN ID: 1

最大用户数: 64 (1~64)

SSID下行流控(kbps): 0 (0~100000)

STA下行流控(kbps): 0 (0~100000)

SSID上行流控(kbps): 0 (0~100000)

STA上行流控(kbps): 0 (0~100000)

Qos: 启用

隧道转发模式: 本地转发

用户隔离: 隔离关闭

组播转单播开关: 关闭

图 5-33

WLAN服务策略		WLAN安全策略						
序号	策略名	ESSID	编码	Portal url	Qos	安全策略	用户隔离	操作
1	11ac_test	[redacted]d	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制
2	11ac_test	[redacted]d1	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制
3	11ac_test	[redacted]d2	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制
4	wlan_default	[redacted]	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制
5	wlan_default	omg	gb2312	未启用	启用	open	隔离关闭	编辑   删除   复制

图 5-34

## 5.12 定位策略

### 5.12.1 无线定位

无线定位 (Wlan Location) 功能, 是一种利用 802.11 无线信号对终端设备进行定位的功能。可以支持所有标准的 802.11a/b/g/n 设备, 如笔记本电脑, 移动设备, 以及特殊的 WIFI 定位标签。通过对这些设备发送的 802.11 无线信号的分析 and 汇总, 可以在服务器控制端软件上实现对物资的定位, 并可以通过地图、表格或者报告的形式直观的进行表示出来。

**页面向导:** 定位策略→添加→无线定位, 配置页面如图 5-32 所示。



图 5-32

页面中关键项的含义如下表所示

操作	说明
开关	开启/关闭无线定位开关

厂商	选择将定位数据上报的厂商
协议类型	选择数据上报协议类型
上报周期	数据上报的间隔时间，可选范围为 1~120s
终端类型	设备上报给定位服务器的信息内容
服务器 IP 地址	定位服务器的网络地址
服务器端口	定位服务器的网络端口号

### 5.12.2 电子围栏

电子围栏功能可扫描到设备周围连接 WIFI 的移动终端 MAC 地址，上报给电子围栏服务器，用户可根据扫描到的终端信息进行研究分析。

**页面向导：定位策略→添加→电子围栏**，配置页面如图 5-33 所示。



图 5-33

页面中关键项的含义如下表所示

操作	说明
开关	开启/关闭电子围栏开关
厂商	选择将定位数据上报的厂商
协议类型	选择数据上报协议类型

上报周期	数据上报的间隔时间，可选范围为 1~120s
终端类型	设备上报给服务器的信息内容
服务器 IP 地址	电子围栏服务器的网络地址
服务器端口	电子围栏服务器的网络端口号

### 5.12.3 高级设置

**页面向导：**定位策略→添加→高级，高级配置页面是无线定位以及电子围栏扫描周围移动终端的参数配置，配置页面如图 5-34。

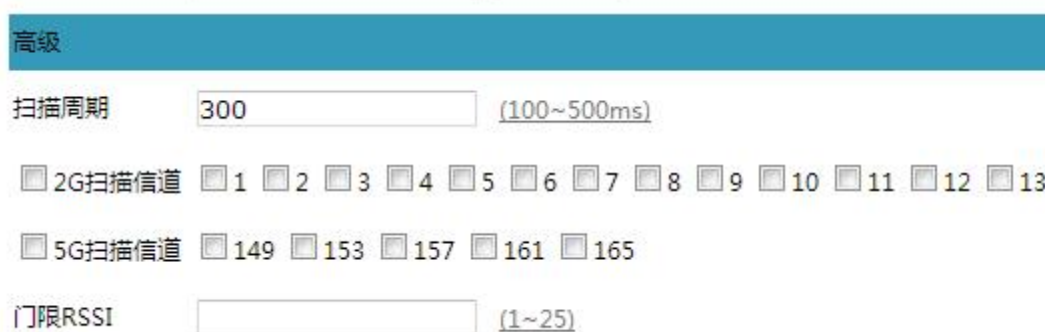


图 5-34

页面中关键项的含义如下表所示

操作	说明
扫描周期	扫描周围移动终端的间隔时间，时间范围为 100~500ms
2G 扫描信道	选择 2G 的扫描信道
5G 扫描信道	选择 5G 的扫描信道
门限 RSSI	门限是接收信号的强度指示，门限值越高，接收信号强度越好，门限值范围为 1~25

### 5.13 vlan 接口 ID

每个 vlan 是一个广播域，同一个广播域下的终端可以互通，不同广播域下的不能互通。设置 VLAN



接口 ID，杜绝了广播信息的不安全性，增强了网络安全性。此项功能主要运用于入墙式 AP，需在 AC 页面上设置 vlan ID，在 AP 设备上一层的网关或交换机设备上添加相对应的 VLAN ID 以及 IP 网段，用户在入墙式 AP 的网口上连接网线访问网络时，即可访问不同广播域，可防止信息共享，很好的解决了网络管理的问题，能实现网络监督与管理的自动化，从而更有效的进行网络监控。

页面向导：无线管理→分组管理→组策略→添加/编辑，进入页面后在圈出的红色区域进行配置，如图 5-35。

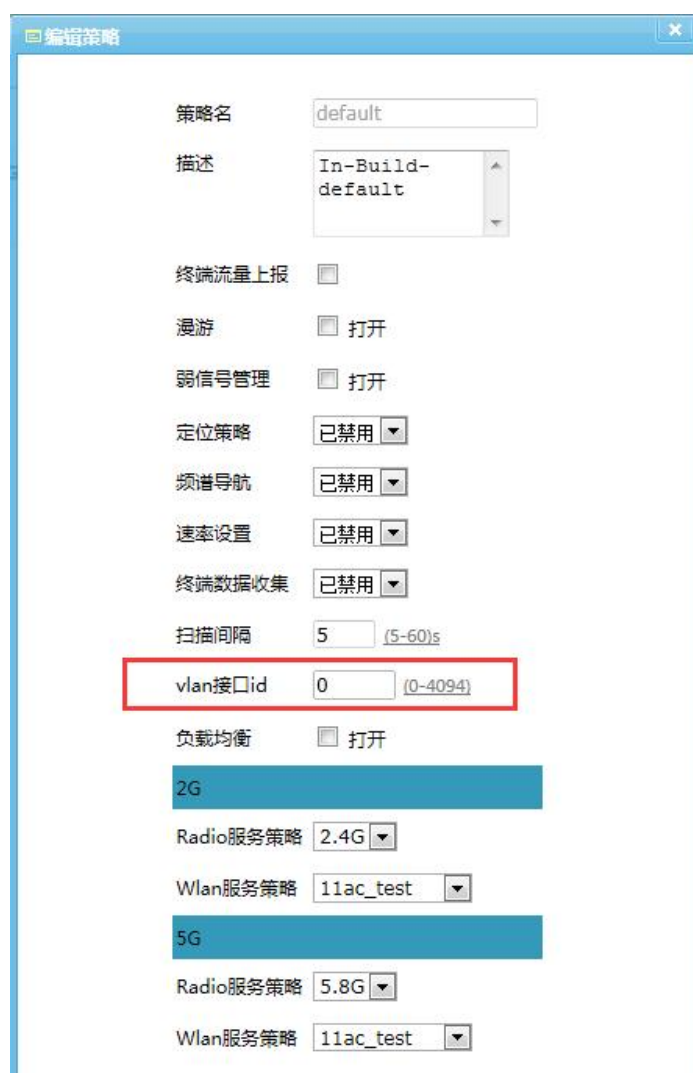


图 5-35

## 5.14 权限管理

权限管理就是基于角色访问控制技术，用户可以访问而且只能访问自己被授权的资源。

权限管理项目栏下可配置权限策略、时间策略、位置策略以及访问策略。在配置权限策略之前，需配置

时间策略、位置策略以及访问策略，才可进行权限策略的配置。

### 5.14.1 权限策略

**页面向导：**运营管理→权限管理→权限策略→添加，选择已配置好的时间策略、位置策略、访问策略，创建一条权限策略，如图 5-36 所示。

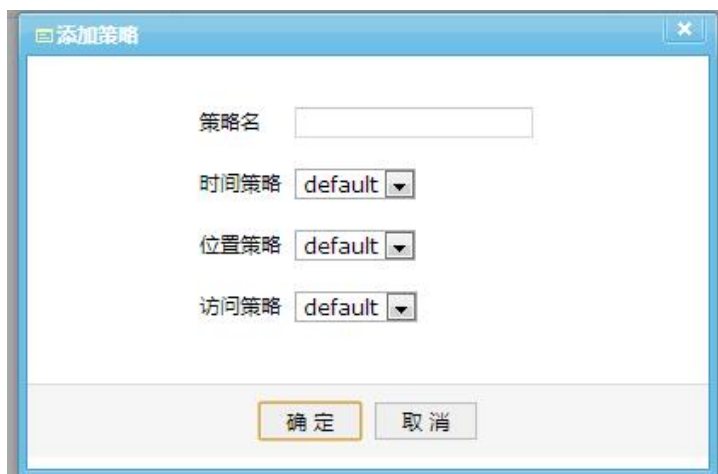


图 5-36

### 5.14.2 时间策略

**页面向导：**运营管理→权限管理→权限策略→添加，配置页面如图 5-37 所示。

选择<添加>按钮可配置指定日期指定星期指定时间，则用户只可在配置的指定时间内进行认证，系统默认时间策略为 default，可在任意日期、任意时间进行认证，没有时间限制。

**注意：**默认时间策略不可进行编辑。



图 5-37

### 5.1.4.3 位置策略

**页面向导：**运营管理→权限管理→位置策略，位置策略默认为“default”，位置为 anywhere，默认位置策略不可进行编辑。选择<添加>按钮，即可配置位置策略，如图 5-38 所示。配置指定位置，则用户需在指定位置范围内才可进行认证上网，超出位置范围内则不能进行认证上网。



图 5-38

页面中关键项的含义如下表所示。

操作	说明
策略名	输入位置策略的策略名
位置	添加多个位置需用“:”隔开，此处“:”必须为英文模式下输入。

### 5.14.4 访问策略

**页面向导:**运营管理→权限管理→访问策略, 权限策略默认为“default”, 默认选择 all ARP、all IP traffic 两种访问规则, 默认策略不可进行编辑删除。选择<添加>按钮, 即可配置访问策略, 如图 5-39 所示。可配置基于终端或用户的访问规则。



图 5-39

页面中关键项的含义如下表所示。

操作	说明
策略名	该策略配置项的名称
访问规则	可选访问规则有 ALL ARP; ALL IP traffic; HTTP; DNS UDP; ICMP Echo requ; DNS TCP; DHCP
上行流控	可选基于终端或基于用户
下行流控	可选基于终端或基于用户

## 第 6 章 典型组网配置举例

### 6.1 典型配置举例 (业务 vlan + 加密 + 限速)

#### 6.1.1 组网需求

某公司申请了运营商 WLAN 宽带，使用 AP-V230 作为企业接入设备，设备使用 AV-V3200 作为无线 WLAN 接入控制器，以下是具体需求。

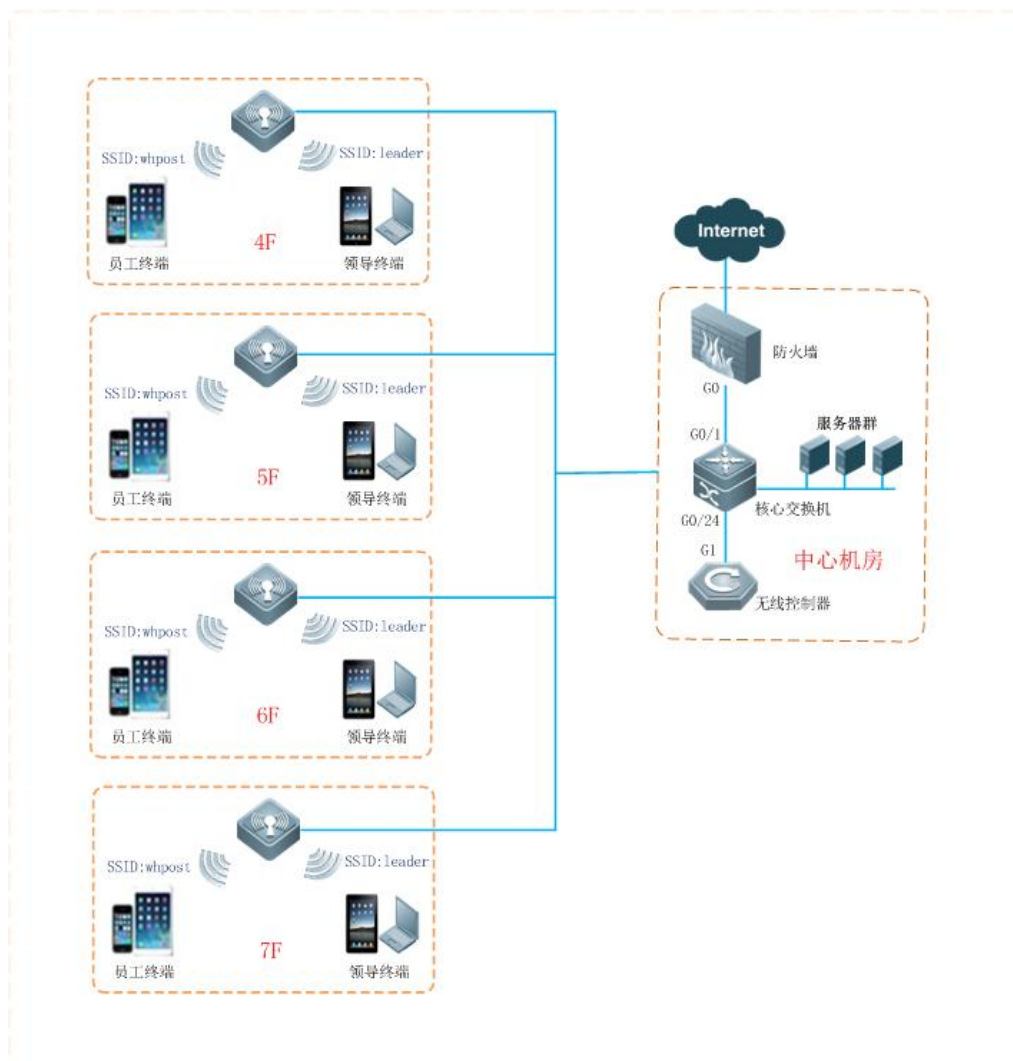



图 6-1

- 全网部署20台AP-V230，1期对4 - 7层办公楼进行无线覆盖；
- 全网采用FIT架构，AP通过POE模块供电，H3C楼层接入交换机作为AP的接入设备，再与中心机

房核心交换机连接，AC旁挂在核心交换机上；

- AP的管理地址及用户IP动态获取方式；
- AP和AC同属于一个管理VLAN1，AC的管理地址为172.20.40.101，无线终端属于vlan10，业务地址为172.20.60.101，网关地址为172.20.60.1；
- 网络建立2个SSID，whpost采用WP2-PSK认证供普通员工使用，leader采用WP2-PSK认证供领导使用。
- whpost做了带宽限制，下行256KB，leader做了带宽限制，下行2MB

## 6.1.2 配置注意事项

 注意：

- 20台AP，需要AC的license的数目不低于20个；
- AP升级接入策略中，需要将设备AP-V230添加如AV-V3200中去；
- 信道规划需根据现场无线环境进行，该手册对该部分不进行详细阐述配置；
- 需求组网需要管理VLAN与业务VLAN结合的实现，需要我们AC口和与连接AC的交换机口、所有与AP连接的POE交换机的端口均要设置为trunk口，允许vlan 10通过（vlan1为默认vlan，不需设置默认允许通过）；

## 6.1.3 配置步骤

### 1) AP 的配置

AP 切换成集中管理模式：可切换模式的方式有两种，一种通过页面方式，在首页中切换本地模式与集中模式实现；另一种可以通过后台命令实现，配置如下：

```
AP-V230# set_ap ap_mode 1
```

AP 通过 DHCP 分配地址上线：可以通过页面登录设备，在网络管理中将地址进行切换，配置如下：

## 网络设置



图 6-2

## 2) AC 的配置

物理口的设置，该配置应用与外接交换机进行的基本的物理连接，以及基本二层的 VLAN 通信，进入 AC 的首页，在网络设置中，配置如下：

**页面向导：首页→网络管理→物理接口** 编辑页面后进行如下功能配置：



图 6-3

IP 与路由的配置，该配置主要应用于配置 AC 的管理地址，业务地址，以及 AC 的出口路由网关配置，具体配置如下：

**页面向导：** 首页→网络管理→虚接口，进入页面后进行如下功能配置，如图 6-4 所示。

操作	说明
接口名称	通过 vlan+vlanid 方式命名
IP 地址	IP 地址根据组网需要任意规划
子网掩码	子网掩码根据组网需要任意规划，支持可变长的子网掩码



图 6-4

## 管理与业务 IP

**默认静态路由：** 默认路由添加的规则为目的地址与子网掩码均为 0.0.0.0，网关设置为组网规划的网关地址，该地址必须与 AC 的某个虚接口属于同一个网段，否则添加失败。如图 6-5 所示



图 6-5

## 默认路由的配置



SSID 等的配置与下发, 包含员工的需求与领导的需求, 不同的需求需要创建的不同的策略进行实现, 具体配置如下:

**页面向导:** 首页→无线管理→分组管理→WLAN 策略配置 添加进入页面后进行如下功能配置:

员工的配置要求如图 6-6 所示:

策略名	企业SSID
ESSID	whpost → 员工SSID配置
ESSID编码	gb2312 ▼
认证类型	免认证 ▼
安全策略	WPA2-PSK ▼ → 加密配置
隐藏SSID	<input type="checkbox"/>
WDS开关	<input type="checkbox"/>
VLAN ID	10 0~4094 → 业务VLAN10配置
WLAN ID	0
最大用户数	64 1~64
SSID下行流控(kbps)	0 → 限速配置 0~100000
STA下行流控(kbps)	2000 0~100000
SSID上行流控(kbps)	0 0~100000
STA上行流控(kbps)	2000 0~100000
Qos	启用 ▼
隧道转发模式	本地转发 ▼
用户隔离	隔离关闭 ▼

图 6-6

领导的配置要求如图 6-7 所示:

策略名	企业SSID	
ESSID	leader	→ 领导SSID配置
ESSID编码	gb2312 ▼	
认证类型	免认证 ▼	
安全策略	WPA2-PSK ▼	→ 加密配置
隐藏SSID	<input type="checkbox"/>	
WDS开关	<input type="checkbox"/>	
VLAN ID	10	→ 业务VLAN配置
	0~4094	
WLAN ID	0	
最大用户数	64	1~64
SSID下行流控(kbps)	0	→ 限速配置
		0~100000
STA下行流控(kbps)	20480	0~100000
SSID上行流控(kbps)	0	0~100000
STA上行流控(kbps)	20480	0~100000
Qos	启用 ▼	
隧道转发模式	本地转发 ▼	
用户隔离	隔离关闭 ▼	

图 6-7

AP 的配置下发，该部分应用于将配置好的无线 radio 配置与 SSID 等相关的配置下发到 AP 中去，具体配置在设备管理中，将设备对应的策略名进行修改实现，如下图。

**页面向导：首页→无线管理→设备管理** 进入页面后进行如下功能配置。

指定组策略名 WA722M-E ▼

default

WA722M-E

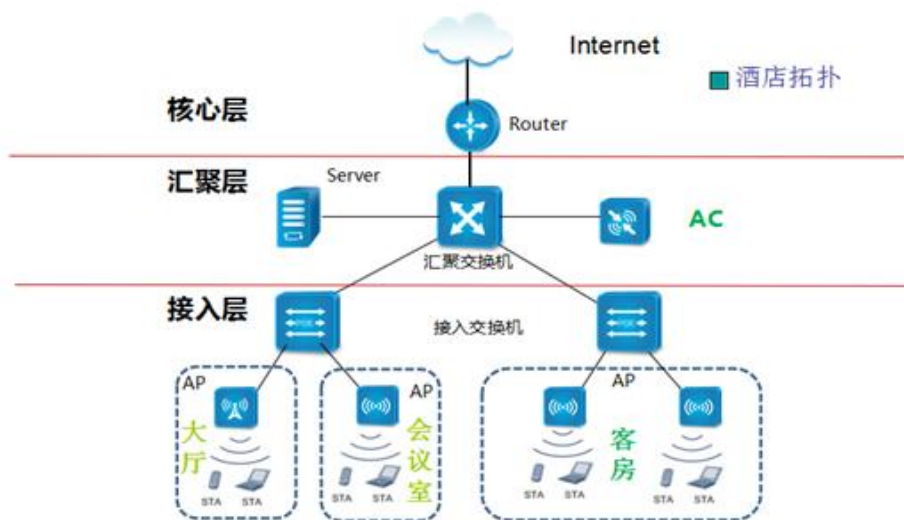
图 6-8

## 6.2 典型配置举例（短信认证 + 微信认证）

### 6.2.1 组网需求

某酒店使用我们入墙式的 WA512 面板 AP 作为接入设备，提出了以下两个组网需求：

- 无线系统支持 Portal 认证方式，portal 认证时，可结合后台在认证界面推送自由定义的广告内容，比如推送酒店自己的酒店装修设计、房间布局以及预定酒店用的联系方式、地址、网址、电话等。
- 无线系统支持微信，微信认证后，酒店可每周或定期推送酒店的二次入住优惠信息、会员卡办理优惠信息等内容给自己的微信粉丝圈，增加二次入住率，提升酒店利润价值。



### 6.2.2 配置注意事项

#### 注意：

- WA512的室内入墙AP，功率小，比吸顶以及放装AP覆盖范围要小一些；
- 开启微信认证时，需要对微信以及腾讯的部分网址域名进行放行，即配置未认证策略；
- 信道规划需根据现场无线环境进行，该手册对该部分不进行详细阐述配置；

## 6.2.3 配置步骤

### 1) 预置条件

基本配置，即在未开启 Portal 认证和微信认证的前提下，AC 与 AP 应配置达到如下要求：

AC 能够与外网通信（保证与微信服务器与第三方微信平台的通信正常）

- 终端连接 SSID 后能够正常上网；

### 2) Portal 服务器配置

Portal 服务器配置，在该配置页面，可以进行如下配置：

**页面向导：首页→运营管理→广告页定制** 进入页面后进行如下功能配置，如图 6-10 所示。

操作	说明
表单标题	设置个性化欢迎语
Banner 广告区	根据需要，定制多彩的宣传图片展示
文本介绍标题	设置文本介绍标题
文本介绍内容	可以输入酒店的公司简介情况
推送网址	根据酒店需要，设置终端认证成功后，链接的网址

编辑Portal页面

表单标题	欢迎使用xxx酒店免费
获取密码按钮	<input checked="" type="radio"/> 显示 <input type="radio"/> 隐藏
免责声明	<input type="radio"/> 显示 <input checked="" type="radio"/> 隐藏
认证类型	帐号+微信认证 ▾
Logo *250x80px(jpg.png.bmp)	<input type="button" value="选择文件"/> 未选择任何文件
行业模板图	自定义 ▾
Banner广告 1 *570x300px 链接	<input type="button" value="选择文件"/> 未选择任何文件
Banner广告 2 *570x300px 链接	<input type="button" value="选择文件"/> 未选择任何文件
Banner广告 3 *570x300px 链接	<input type="button" value="选择文件"/> 未选择任何文件
Banner广告 4 *570x300px 链接	<input type="button" value="选择文件"/> 未选择任何文件
Banner广告 5 *570x300px 链接	<input type="button" value="选择文件"/> 未选择任何文件
文本介绍标题	欢迎光临xxx酒店
文本介绍内容	xxx酒店集团，是国内第一家全品牌的连锁酒店
版权信息	xx酒店集团版权所有 2013沪 ICP 备 120号
背景色	#ffffff
登陆成功推送页面	www.abc.hotal.com

图 6-10

### 3) 微信服务器配置

微信服务器配置，在该配置页面，可以进行如下配置：

**页面向导：** 首页→运营管理→微信管理→微信公众号 进入页面后进行如下功能配置，以下以公众账号为例。如图 6-11 所示

操作	说明
公众号名称	深圳
公众号原始 id	gh_27677853fce4
微信号	szzkww
公众号类型	服务号
AppId	wxc98fcd063a37b770
Secret	9643f78a28a65f7a9d49c820c255b742
图文链接	<a href="http://wx.szzkww.com/Uploads/Picture/2015-01-07/54acf0f4004fb.jpg">http://wx.szzkww.com/Uploads/Picture/2015-01-07/54acf0f4004fb.jpg</a>



图 6-11

SSID 中开启 Portal 和微信认证，该页面配置参考如下。

**页面向导：**首页→无线管理→分组管理→WLAN 策略配置 编辑对应策略进入页面后进行如下功能配置，以下以公众账号为例。如图 6-12 所示

操作	说明
帐号类型	选择“帐号+微信”（可以根据实际需要单独开启 portal 认证或者微信认证）
微信名称	下拉选择在微信公共号里添加的微信的名称
Portal 类型	类型选择内部 Portal，Portal 内容选择新建的 Portal 策略名称

策略名

ESSID

ESSID编码

认证类型

微信名称

Portal 类型

Portal Url   
格式:http://foo.com/bar.html

图 6-12

#### 4) 未认证策略配置

微信未认证策略配置与下发，该配置容易遗漏，但是也是很关键的一步，设置该未认证策略的目的就是为了终端在未认证前可以直接访问微信认证需要的相关域名进行关注公众号等一些列的操作，达到顺利进行微信认证的目的，具体配置如下：

**页面向导：**首页→运营管理→未认证策略 进入页面后进行如下功能配置，以下以公众账号为例：

**需要添加的白名单：**qq.com; weixin.qq.com; gting.cn; weixin.com; qplic.cn; qllogo.cn

未认证策略			
批量删除		添加	
序号	策略名	允许的IP/Domain	操作
1	weixin	xiaomi.net <a href="#">编辑</a> <a href="#">删除</a>	<a href="#">添加到本组</a>   <a href="#">删除本组</a>
		qq.com <a href="#">编辑</a> <a href="#">删除</a>	
		weixin.qq.com <a href="#">编辑</a> <a href="#">删除</a>	
		gtimg.cn <a href="#">编辑</a> <a href="#">删除</a>	
		weixin.com <a href="#">编辑</a> <a href="#">删除</a>	
		qpic.cn <a href="#">编辑</a> <a href="#">删除</a>	
		qlogo.cn <a href="#">编辑</a> <a href="#">删除</a>	

图 6-13

**未认证策略的下发：** 首页→无线管理→设备管理中，对应开启的设备列表的未认证策略一栏，设置为配置的白名单策略即可，如下图：

指定未认证策略 weixin ▼

提交
取消

图 6-14

## 第 7 章 故障排除

Q1: AC 部署完毕后, 如何确认是否可用?

部署完毕后, 将 AC 上电, 连接 PC 和 AC 所在的网络, 将 PC 的有线网卡地址配置为与 AC 同网段 (192.168.1.x, 注意不要与 AC 地址相同), 然后在浏览器地址栏中输入 AC 的 IP: “192.168.1.2”, 若能打开 AC 的 Web 管理登录界面, 表明 AC 可用, 否则, 可能需要检查 AC 与 PC 之间的网络连接情况。

Q2: AP 无法注册上 AC

根据之前排查经验, 列举了如下几点排查手段供定位排查:

- 1、license 没有安装, 或者 license 已经超现
- 2、升级策略没有正确配置, 尤其对 WA718 和 WA718AP 两款硬件型号进行区分
- 3、DHCP 地址池没有建立, AP 没有获取到地址 (AC 分配或者核心交换机分配)
- 4、三层情况下 AP 的 option 43 地址没有指派
- 5、架设的网络不正确, 即使 AP 从核心交换机获取到地址, 但是仍 ping 不通 AC
- 6、设置的 AP 接入接口不正确, 目前 AC 仅支持一个 AP 接入口供 AP 注册使用, 所以在组网开局

过程中, 尤其注意

- 7、AP 的序列号存在冲突, 与设备列表中的存在相同的 (概率较小)
- 8、AP 的升级策略填写与实际 AP 版本不匹配, 造成 AP 反复上线下线

Q3: Portal 认证 portal 页面无法推出

管理 vlan 和业务 vlan 的 portal 地址混淆

目前 portal 配置策略还不够完善, 管理 vlan 和业务 vlan 的 portal 策略地址均为统一的地址, 没有相应的区分对应的 vlan 虚接口进行对应 portal 配置, 因此在组网配置时容易混淆, 容易将所有业务 vlan 中的 portal 服务器配置成管理 vlan 的 portal, 如下图: 在以后开局中, 尤其要注意, 在业务 vlan 开启的状态下, 对应的 wlan 接口开启的 Portal 服务器地址要修改成对应虚接口的 Portal 服务器的地址。

gb2312	http://172.20.40.16/htmls/portal/123.html
gb2312	http://172.20.60.16/htmls/portal/123.html

图 7-1



#### Q4: Qos 开启功能

在平时组网测试中，经常遇到有反馈下发的是 11n 的 144M 带宽模式，但是终端连接上后，部分网卡协商速率始终是 54M，此时需要我们在 AC 中，将 WLAN 策略中的 Qos 功能打开，此时这些网卡的协商速率就会变为 144M。

#### Q5: portal 手机号注册

一个手机号默认只能绑定三个终端的 MAC，当第四个终端再进行注册登录时，认证就会被拒绝，在现网测试过程中，要注意，在一台 AC 下，避免因为该机制造成的认证失败。

#### Q6: 用户的带宽控制

带宽控制分为如下两部分：

- 1、非 portal 用户
- 2、portal 用户

该两部分认证的配置以及实现不在同一个地方，因此需要尤其注意：

对于已经认证 Portal 用户的限速，该限速基于每个认证用户的帐号内部配置和实现的，与 WLAN 内部的限速无关，即使 wlan 内部不限速也没有关系

对于非 Portal 用户的限速，该部分的配置是在 wlan 中配置实现的，需要我们在 wlan 中进行相应的上下行的配置

#### Q7: 过滤和搜索功能

过滤和搜索目前该版本在 AP 列表和终端列表中部分属性支持，但仍需要注意以下事项：

- 1、搜索 MAC 地址的格式问题：注意区分 “:” 和 “-”
- 2、搜索 MAC 地址时注意区分大小写，该版本暂时只能完全匹配
- 3、过滤目前不支持模糊匹配，因此搜索时尽量完全输入进行过滤
- 4、过滤过的内容在进行页面更改切换回来后不会保存，需要重新输入过滤条件进行过滤

#### Q8: DHCP 服务器的租约时间过长

无论 DHCP 服务器开在 AC 上还是外置的核心交换机上，给终端分配的地址的租约设置不应太长，建议在一小时左右，尤其是商业区人口流动性大的场所，核心交换机默认不配置租约时间时，默认的租约一般是 8 小时或者是一天，所以使用核心交换机作为 DHCP 服务器分配地址时，注意修改租约时间，避免因租约地址长时间没有释放导致地址池耗光。

## 第 8 章 缺省配置

接口设置	LAN 口 IP 地址		192.168.1.2
	子网掩码		255.255.255.0
	物理接口 (eth0-eth5)		VLAN1, 交换模式
	DHCP		关闭
	路由		关闭
登录账号	WEB 登录	用户名	admin
		密码	password
	SSH 登录	用户名	root
		密码	anysec
AP 射频参数	2G	无线信道	6 信道 (2437MHz)
		无线模式	11bgn
		发射功率	12dbm
		信道带宽	20MHz
		空间流	2*2
		RTS 门限	2346
		Beacon 帧间隔	100ms
		发包间隔	400ns
		动态频率调节	禁用
		同频功率调整	禁用
		逐包功率控制	禁用
	5G	无线信道	149 信道 (5745Mhz)
		无线模式	11an
		发射功率	12dbm
		信道带宽	20MHz
		空间流	2*2
		RTS 门限	2346
		Beacon 帧间隔	100ms
		发包间隔	400ns
动态频率调节	禁用		

	同频功率调整	禁用
	逐包功率控制	禁用
AP WLAN 参数	SSID	anysec
	SSID 编码	GB2312
	Portal 认证	关闭
	微信认证	关闭
	最大用户数	64
	VLAN ID	0
	流控	关闭
	Qos	关闭
	安全策略	open
	转发模式	本地转发
	隐藏 SSID	关闭
	WDS	关闭
	用户隔离	关闭
AP 其它参数	终端流量上报	关闭
	弱信号管理	关闭
	频谱导航	关闭
	负载均衡	关闭
	AP 心跳间隔	10s
	AP 心跳超时次数	3 次
	AP 流量上报	关闭
	AP 升级开关	关闭
终端认证	认证有效时长	12 小时
	广告推送间隔	12 小时
	认证超时立即生效	开启
用户注册	注册通道	开启
	短信平台	互忆无线
	同时在线数	不限
	绑定 MAC 数	3
	时效	永久有效