

# 配置指导

## 无线控制器 · AC1000

**IP-COM**

无线网络解决方案专家

## 声明

版权所有©2017 深圳市和为顺网络技术有限公司。保留一切权利。

未经本公司书面许可，任何单位或个人不得擅自复制、摘抄及翻译本档部分或全部内容，且不得以任何形式传播。

**IP-COM** 是深圳市和为顺网络技术有限公司在中国和（或）其它国家与地区的注册商标。其它品牌和产品名称均为其相应持有人的商标或注册商标。

由于产品版本升级或其它原因，本档内容会不定期更新。除非另有约定，本档仅作为使用指导，文中的所有陈述、信息和建议均不构成任何形式的担保。

## 前言

感谢选择 IP-COM 产品。开始使用本产品前，请先阅读本说明书。

## 约定

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「开始」菜单。
按钮	边框+底纹	点击 <span style="border: 1px solid black; padding: 2px;">确定</span> 。
连续菜单选择	>	进入「状态」>「无线状态」页面。

本文可能用到的标识说明如下。

标识	含义
 注意	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
 提示	表示有助于节省时间或资源的方法。

## 缩略语

缩略语	全称
AP	Access Point
AC	Access Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SSID	Service Set Identifier
VLAN	Virtual Local Area Network

## 更多信息

如需获取更多信息，请访问 IP-COM 官方网站：<http://www.ip-com.com.cn>。

# 技术支持

如需技术支持，请通过以下方式与我们联系。



40066-50066



[ip-com@ip-com.com.cn](mailto:ip-com@ip-com.com.cn)



<http://www.ip-com.com.cn>

# 目录

<b>1 设备登录</b> .....	<b>1</b>
1.1 登录管理页面 .....	1
1.2 退出登录 .....	3
1.3 管理页面布局 .....	3
1.4 管理页面常用元素 .....	4
<b>2 典型应用</b> .....	<b>5</b>
<b>3 设备扫描</b> .....	<b>6</b>
3.1 设备扫描 .....	6
3.1.1 扫描设备 .....	6
3.1.2 导出已扫描的 AP 信息 .....	7
3.1.3 删除离线 AP 信息 .....	8
3.2 SSID 扫描 .....	8
3.2.1 扫描 SSID .....	8
3.2.2 导出已扫描的 SSID 信息 .....	9
<b>4 策略配置</b> .....	<b>10</b>
4.1 SSID 策略 .....	10
4.1.1 概述 .....	10
4.1.2 配置 SSID 策略 .....	11
4.1.3 SSID 策略配置举例 .....	14
4.2 射频策略 .....	20
4.2.1 概述 .....	20
4.2.2 配置射频策略 .....	22
4.3 VLAN 策略 .....	26
4.3.1 概述 .....	26
4.3.2 配置 VLAN 策略 .....	26
4.3.3 VLAN 策略配置举例 .....	28
4.4 高级策略 .....	32
4.4.1 概述 .....	32
4.4.2 配置高级策略 .....	33
4.4.3 高级策略配置举例 .....	38
<b>5 AP 管理</b> .....	<b>46</b>
5.1 批量维护 .....	46

5.1.1 SSID 配置.....	46
5.1.2 射频配置.....	47
5.1.3 VLAN 设置.....	47
5.1.4 高级设置.....	48
5.1.5 缺省设置.....	48
5.1.6 删除离线 AP 信息.....	48
5.2 单台维护.....	50
5.2.1 重启.....	50
5.2.2 升级.....	50
5.2.3 复位.....	51
5.2.4 修改.....	51
5.2.5 删除离线 AP 信息.....	54
<b>6 用户状态.....</b>	<b>55</b>
<b>7 系统工具.....</b>	<b>57</b>
7.1 系统状态.....	57
7.1.1 端口.....	57
7.1.2 系统状态.....	58
7.1.3 设备状态.....	58
7.2 网络设置.....	59
7.2.1 外网配置.....	60
7.2.2 内网配置.....	61
7.2.3 DHCP 配置.....	62
7.2.4 VLAN 配置.....	63
7.3 AP DHCP 列表.....	67
7.4 维护.....	68
7.4.1 授权激活.....	69
7.4.2 系统模式.....	69
7.4.3 用户管理.....	73
7.4.4 升级维护.....	74
7.5 时间与日期.....	77
7.5.1 NTP 网络校时.....	77
7.5.2 同步 PC 时间.....	78
7.6 日志显示.....	79
7.7 网络检测.....	80
7.7.1 Ping.....	80
7.7.2 Traceroute.....	81
<b>附录.....</b>	<b>82</b>

# 1 设备登录

## 1.1 登录管理页面

AC 提供了 Web 管理功能，管理员可使用 Web 页面直观地管理、维护 AC。

首次使用 AC 时，您可以使用默认登录信息通过浏览器登录到 AC 的 Web 管理页面。AC 默认的登录信息如下表：

登录信息	默认设置
IP 地址	192.168.10.1
用户名	admin
密码	admin

**登录到 AC 的 Web 管理页面**（假设 AC 的登录信息为默认设置）：

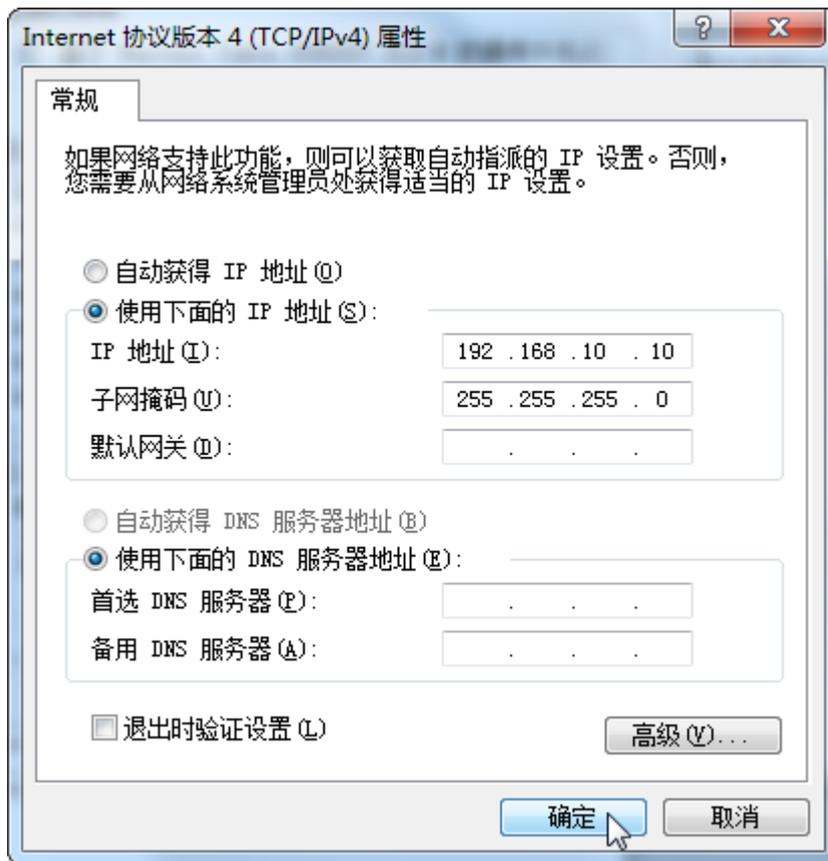
### 步骤 1：连接电脑。

确保已使用网线将电脑接到 AC 的 LAN 口（或 AC 的 LAN 口连接的交换机）。



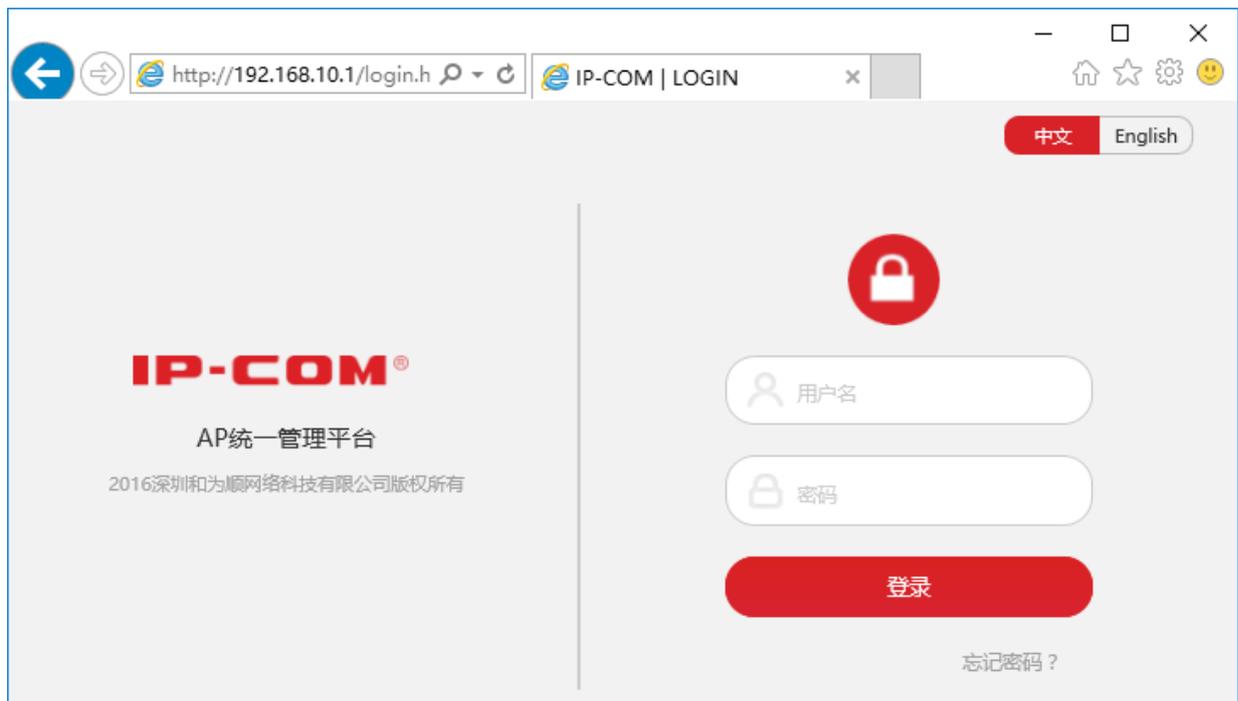
### 步骤 2：配置电脑的 IP 地址。（以 Windows 7 系统为例）

右键单击电脑桌面右下角的网络图标，点击“打开网络和共享中心>本地连接>属性”，双击“Internet 协议版本 4( TCP/IPv4 )”，选择“使用下面的 IP 地址”，设置 IP 地址为“192.168.10.X”( X 为 2~254 )，子网掩码为“255.255.255.0”，点击 。



### 步骤 3 : 登录 AC 的管理页面。

打开电脑上的浏览器，在地址栏输入 AC 的管理 IP（默认为 192.168.10.1），回车。输入用户名和密码（默认均为 admin），点击 **登录**，进入 AC 的管理页面。



成功登录到 AC 的管理页面。



## 1.2 退出登录

点击 Web 管理页面右上角的“注销”，可安全退出 AC 的 Web 管理页面。



点击可安全地退出管理页面

## 1.3 管理页面布局

Web 管理页面共分为：导航栏、页签和配置区三部分，如下图所示。



提示

管理页面上显示为灰色的功能或参数，表示 AC 不支持或在当前配置下不可修改。

序号	名称	说明
①	导航栏	以导航栏、页签的形式组织 AC 的功能菜单。用户可以根据需要选择功能菜单，
②	页签	选择结果显示在配置区。
③	配置区	用户进行配置或查看配置的区域。

## 1.4 管理页面常用元素

下表是 AC Web 管理页面中常用元素的功能介绍：

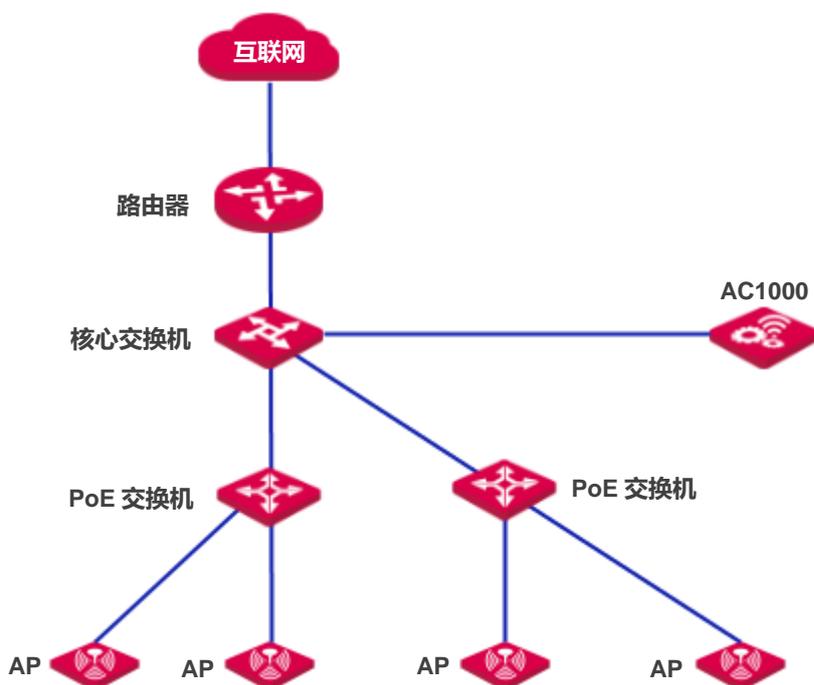
元素	说明
 	<p>点击可展开</p>
	搜索条，可输入关键字查找并定位显示信息。支持的关键字见输入框的提示。
每页条数 <input type="text" value="10"/> 	点击下拉框，选择每页显示的信息条数。
	点击可刷新显示的信息。
	点击可编辑对应的信息。
<input type="checkbox"/>	<p>单选：勾选每条信息左侧的复选框，可单独选中该条信息。</p> <p>全选：勾选列表标题栏的复选框，可选中页面显示的所有信息。</p>
	表明 AC 已经获得授权激活，可正常使用。

下表是 AC Web 管理页面常用按钮的功能介绍：

按钮	说明
	点击可删除被选中的“离线”或“未使用”状态的信息。
 	点击可保存当前页面配置，并使配置生效。

## 2 典型应用

AC 的典型应用拓扑图如下图所示。在未划分 VLAN 的环境下，参考下图连接好 AC 和其他网络设备后，无需任何设置，AC 即可管理上局域网中的 AP。



如果要修改 AP 的 SSID/射频/VLAN/高级配置，请先进行相应的[策略配置](#)，再使用[批量维护](#)功能。

如果要重启/升级/复位 AP，或者单独修改某一台 AP 的配置，请使用[单台维护](#)功能。

详情请参考后文。

# 3 设备扫描

AC 的「设备扫描」模块包括：[设备扫描](#)、[SSID 扫描](#)。

## 3.1 设备扫描

通过“设备扫描”功能，您可以了解到接入 AC 的 AP（包括在线 AP 和离线 AP）信息。

### 3.1.1 扫描设备

1. 进入「设备扫描」页面。
2. 点击 设备扫描。

----完成

扫描完成后，您可以在「设备扫描」页面查看已接入 AC 的 AP 信息。如下图示例。



The screenshot shows a web interface for device scanning. At the top, there are buttons for '设备扫描' (Device Scan), 'SSID扫描' (SSID Scan), '导出' (Export), and '删除' (Delete). A search bar contains 'MAC, 备注, IP'. Below the buttons, it says '接入AP数: 1 台' (1 device connected) and '刷新' (Refresh). On the right, '每页条数' (Items per page) is set to 10. The main table has columns: 型号 (Model), 备注 (Remarks), IP, MAC, 在线用户数 (Online users), SSID, 信道 (Channel), 软件版本 (Software version), and 状态 (Status). One AP is listed: ap325v1.0, AP325V1.0, 192.168.10.180, D8:38:0D:00:1F:70, 1, IP-COM\_AP\_0, 11, V1.0.0.3(3307), and 在线 (Online).

型号	备注	IP	MAC	在线用户数	SSID	信道	软件版本	状态
ap325v1.0	AP325V1.0	192.168.10.180	D8:38:0D:00:1F:70	1	IP-COM_AP_0	11	V1.0.0.3(3307)	在线

#### 参数说明

标题项	说明
型号	AP 的产品型号。
备注	AP 的备注信息，默认为 AP 的型号。当 AP 在线时，点击可修改。 建议将备注修改为 AP 的位置信息，如“606 房”，便于网络出现问题时，通过 AC 的日志或告警记录精确定位出现问题的 AP 的具体位置。
IP	AP 的 IP 地址。

标题项	说明
	AP 首次接入 AC 时，AC 上的 DHCP 服务器将自动给 AP 分配一个 IP 地址。
MAC	AP 的 LAN 口 MAC 地址。
在线用户数	当前连接到 AP 的 SSID 的无线客户端数量。
SSID	显示 AP 的主 SSID。如果 AP 是双频 AP，则会显示两个 SSID，即 2.4GHz 频段的主 SSID 和 5GHz 频段的主 SSID。
信道	AP 的工作信道。“自动”表示根据 AP 周围环境情况自动调整 AP 的工作信道。
软件版本	AP 的系统软件版本。
状态	<p>AP 与 AC 的连接状态。</p> <ul style="list-style-type: none"> <li>- 在线：AP 与 AC 已成功建立连接，此时 AC 可配置该 AP。</li> <li>- 离线：AP 与 AC 已断开连接，此时 AC 无法配置该 AP。</li> </ul>
	<p> <b>注意</b></p> <p>AP 离线时，它仍保留 AC 之前下发的配置，用户仍可正常使用其无线网络，除非用户重新修改了 AP 的配置。</p>

### 3.1.2 导出已扫描的 AP 信息

1. 进入「设备扫描」页面。



提示

如果您已经完成“设备扫描”，请跳过**步骤 2**。

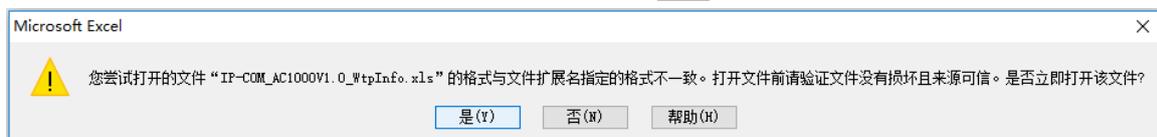
2. 点击 **设备扫描**。
3. 点击 **导出**。
4. 如果出现操作确认的对话框，请点击 **确定**，之后按页面提示将文档保存到本地电脑。

----完成



提示

在本地电脑打开文档时，如果出现类似下图的对话框，请选择 **是**。



### 3.1.3 删除离线 AP 信息

当“设备扫描”页面显示的 AP 数较多时，您可以将已离线的 AP 信息删除，便于更清晰地了解在线 AP 信息。步骤如下。

1. 进入「设备扫描」页面。
2. 选中处于“离线”状态的 AP。
3. 点击 **删除**。
4. 如果出现操作确认的对话框，请点击 **确定**。

----完成

## 3.2 SSID 扫描

使用“SSID 扫描”功能，您可以查看到 AC 下发的 SSID 策略的使用情况。**注意**：用户手动在 AP 管理页面设置的 SSID 不会显示在此处。

### 3.2.1 扫描 SSID

1. 进入「设备扫描」页面。
2. 点击 **SSID 扫描**。

----完成

扫描完成后，您可以在该页面查看到 SSID 信息。如下图示例。

The screenshot shows the SSID scanning interface. At the top, there are buttons for '设备扫描', 'SSID 扫描', and '导出'. A search bar contains 'MAC, 备注, SSID'. Below the buttons, it indicates '在线总SSID数: 1个' with a '刷新' button. On the right, there is a '每页条数' dropdown set to '10'. The main table has the following columns: 型号, 备注, SSID顺序, SSID, MAC, 终端/限制数, 信道, and 状态. One row is visible with the following data: 型号: ap325v1.0, 备注: AP325V1.0, SSID顺序: 1F:70--1, SSID: IP-COM\_AP\_0, MAC: D8:38:0D:00:1F:70, 终端/限制数: 2/64, 信道: 11, 状态: 在线.

型号	备注	SSID顺序	SSID	MAC	终端/限制数	信道	状态
ap325v1.0	AP325V1.0	1F:70--1	IP-COM_AP_0	D8:38:0D:00:1F:70	2/64	11	在线

#### 参数说明

标题项	说明
型号	AP 的产品型号。
备注	AP 的备注信息，默认为 AP 的型号。当 AP 在线时，点击可修改。 建议将备注修改为 AP 的位置信息，如“606 房”，便于网络出现问题时，通过 AC 的日志或告警记录精确定位出现问题的 AP 的具体位置。

标题项	说明
SSID 顺序	该 SSID 在 AP 中的主次顺序，格式为“MAC 地址后 4 位--序号”，如，“xx:xx--6”表示 MAC 地址为“yy:yy:yy:yy:xx:xx”的 AP 的第 6 个 SSID。
SSID	AC 下发给 AP 的对应顺序的 SSID。
MAC	AP 的 LAN 口 MAC 地址。
终端/限制数	当前连接到该 SSID 的无线客户端数量/该 SSID 最多允许连接的无线客户端数量。
信道	AP 的工作信道。“自动”表示根据 AP 周围环境情况自动调整 AP 的工作信道。
状态	<p>AP 与 AC 的连接状态。</p> <ul style="list-style-type: none"> <li>- 在线：AP 与 AC 已成功建立连接，此时 AC 可配置该 AP。</li> <li>- 离线：AP 与 AC 已断开连接，此时 AC 无法配置该 AP。</li> </ul> <p> <b>注意</b></p> <p>AP 离线时，它仍保留 AC 之前下发的配置，用户仍可正常使用其无线网络，除非用户重新修改了 AP 的配置。</p>

## 3.2.2 导出已扫描的 SSID 信息

1. 进入「设备扫描」页面。



提示

如果您已经完成“SSID 扫描”，之后并未刷新页面，可以跳过步骤 2。

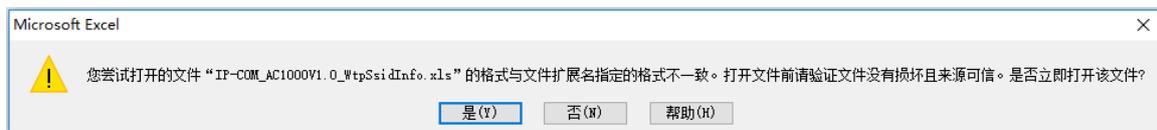
2. 点击 **SSID 扫描**。
3. 点击 **导出**。
4. 如果出现操作确认的对话框，请点击 **确定**，之后按页面提示将文档保存到本地电脑。

----完成



提示

在本地电脑打开文档时，如果出现类似下图的对话框，请选择 **是**。



# 4 策略配置

AC 的「策略配置」模块用于预置 AP 的配置信息，以便后续进行 [AP 管理](#)时引用，包括：[SSID 策略](#)、[射频策略](#)、[VLAN 策略](#)、[高级策略](#)。

## 4.1 SSID 策略

### 4.1.1 概述

无线用户要接入 AP，必须使用正确的 SSID，即与 AP 的 SSID 相同；如果不同，AP 将拒绝该无线用户接入。

SSID 策略用于配置 AP 的 SSID 相关参数。

### 加密方式

无线网络采用具有空中开放特性的无线电波作为数据传输介质，在没有采取必要措施的情况下，任何用户均可接入无线网络、使用网络资源或者窥探未经保护的数据。因此，在 WLAN 应用中必须对传输链路采取适当的加密保护手段，以确保通信安全。

针对不同应用环境需求，AC 提供以下安全模式：不加密、WPA-PSK、WPA2-PSK 供用户选择。

- **不加密**

即不加密无线网络，允许任意无线客户端接入。为了保障网络安全，不建议选择此项。

- **WPA-PSK/WPA2-PSK**

两者都采用预共享密钥认证，其设置的密钥只用来验证身份，数据加密密钥由 AP 自动生成，适合一般家庭用户用于保证无线安全。

## 最大客户端数

最大客户端数参数用于限制接入 SSID 的无线用户个数，当连上该 SSID 的无线用户数达到此值后，该 SSID 不再接受新的无线连接请求。

设置最大客户端数可以避免 AP 一些 SSID 负载过大导致用户体验不佳，而另外一些 SSID 却闲置带宽的情况。

## 客户端隔离

类似于有线网络的 VLAN，将连接到同一 SSID 的所有无线用户完全隔离，使其只能访问 AP 连接的有线网络。适用于酒店、机场等公共热点的架设，让接入的无线用户保持隔离，提供安全的互联网接入。

## 隐藏 SSID

默认情况下，AP 广播 SSID，周围的无线用户可以扫描到对应 SSID。开启“隐藏 SSID”后，AP 不广播 SSID，周围的无线用户也就扫描不到对应的 SSID，此时，如果要连接到该 SSID 的无线网络，首先必须手动设置与 AP 相同的 SSID，这在一定程度上增强了无线网络的安全性。

需要注意的是：开启“隐藏 SSID”后，如果黑客利用其他手段获得 SSID，仍然可以接入目标网络。

## VLAN ID

如果在划分了 QVLAN 的网络环境使用 AP，可以为 SSID 配置 VLAN ID，以区分不同的用户数据流。

### 4.1.2 配置 SSID 策略

默认情况下，AC 已配置了 1 条策略名称为“default”的 SSID 策略，如下图所示。AP 第 1 次上线后，AC 会自动给 AP 下发默认 SSID 策略。

SSID策略									
射频策略    VLAN策略    高级策略									
+ 添加    - 删除    策略名称, SSID									
总策略条数: 1条    刷新    每页条数 10									
<input type="checkbox"/>	策略名称	SSID	加密方式	无线密码	VLAN	客户端隔离	隐藏SSID	状态	操作
<input type="checkbox"/>	default	IP-COM_AP_0	不加密	不加密	1000	禁用	禁用	使用中	

## 添加 SSID 策略

1. 进入「策略配置」>「SSID 策略」页面。
2. 点击 **+添加**。
3. 在【SSID 策略】窗口配置各项参数。
4. 点击 **保存**。

SSID策略

策略名称

SSID

加密方式  ▼

最大客户端数

客户端隔离  开启

隐藏SSID  开启

VLAN ID

备注：需要下发VLAN策略才能生效

**保存** 取消

### 参数说明

标题项	说明
策略名称	SSID 策略的名称，注意不能和已有的 SSID 策略名称重复。
SSID	无线网络名称。 支持中文字符（采用 UTF-8 编码格式，一个汉字占 3 个字节）。
加密方式	SSID 对应的无线网络的加密方式。 支持的安全模式有： <a href="#">不加密</a> 、 <a href="#">WPA-PSK</a> 、 <a href="#">WPA2-PSK</a> 。点击超链接可以了解对应加密方式的详细说明。
最大客户端数	SSID 允许同时接入的无线设备的最大数量。 若接入该 SSID 的无线设备达到此值，除非某些设备断开连接，否则新的无线设备不能接入此 SSID。
客户端隔离	开启后，连接在该 SSID 下的设备之间不能互相通信，可增强无线网络的安全性。

标题项	说明
隐藏 SSID	开启后，AP 不广播该 SSID，无线设备连接该 SSID 的 Wi-Fi 时，需要正确输入该 SSID。
VLAN ID	<p>设置 SSID 所属的 VLAN。</p> <p> <b>注意</b></p> <p>如果要使本设置生效，还需给 AP 下发“<a href="#">VLAN 策略</a>”，启用 AP 的 VLAN 功能。之后，重启 AP 使 VLAN 相关设置生效。</p>

## ■ 不加密

允许任意无线客户端接入，为了保障网络安全，不建议选择此项。

## ■ WPA-PSK/WPA2-PSK



加密方式：不加密、WPA-PSK、WPA2-PSK

加密规则： AES  TKIP  TKIP&AES

密钥：

密钥周期： 单位：秒

## 参数说明

标题项	说明
加密方式	<p>选择加密方式：WPA-PSK、WPA2-PSK。</p> <ul style="list-style-type: none"> <li>WPA-PSK：此时，SSID 对应的无线网络采用 WPA-PSK 加密方式。</li> <li>WPA2-PSK：此时，SSID 对应的无线网络采用 WPA2-PSK 加密方式。</li> </ul>
加密规则	<p>选择 WPA 加密规则。</p> <ul style="list-style-type: none"> <li>AES：高级加密标准。</li> <li>TKIP：临时密钥完整性协议。相较于 AES，采用 TKIP 时，AP 只能使用较低的无线速率（最大 54Mbps）。</li> <li>TKIP&amp;AES：兼容 TKIP 和 AES，无线设备使用 TKIP 和 AES 均可连接。</li> </ul>
密钥	WPA 预共享密钥。
密钥周期	WPA 数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。 为 0 表示不更新。

## ----完成

设置完成后，您可以在「策略配置」>「SSID 策略」页面查看到已添加的 SSID 策略。如下图示例。

SSID策略		射频策略	VLAN策略	高级策略					
+ 添加		删除		策略名称, SSID					
总策略条数: 2条 <a href="#">刷新</a>				每页条数 10					
<input type="checkbox"/>	策略名称	SSID	加密方式	无线密码	VLAN	客户端隔离	隐藏SSID	状态	操作
<input type="checkbox"/>	default	IP-COM_AP_0	不加密	不加密	1000	禁用	禁用	使用中	
<input type="checkbox"/>	示例	IP-COM	不加密	不加密	1000	禁用	禁用	未使用	

## 修改 SSID 策略

1. 进入「策略配置」>「SSID 策略」页面。
2. 找到要修改的 SSID 策略，点击操作栏的
3. 在【SSID 策略】窗口，根据需要修改各项参数。
4. 点击 **保存**。

----完成

之后，AC 会立即自动将新的 SSID 策略更新到对应 AP。

## 删除 SSID 策略

1. 进入「策略配置」>「SSID 策略」页面。
2. 找到要删除的 SSID 策略，点击 **删除**。
3. 如果出现操作确认的对话框，请点击 **确定**。

----完成

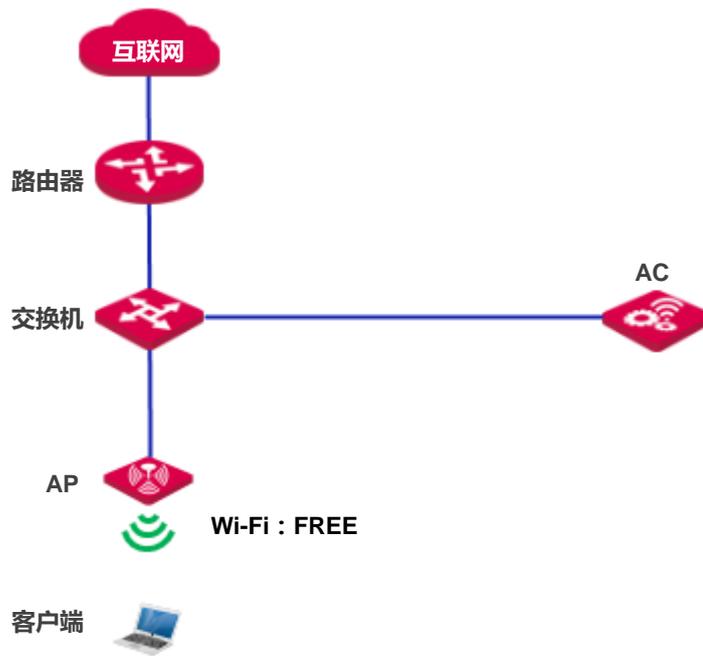
### 4.1.3 SSID 策略配置举例

#### 不加密无线网络配置举例

##### 组网需求

用户连接无线网络时，不需要输入无线密码就可以连接成功。

假设：1) 网络未划分 VLAN。2) AP 是单频 AP，工作在 2.4GHz 频段。



## 配置步骤



提示

配置步骤中，其他未提到的参数，请保持默认设置即可。

### 步骤 1：配置 SSID 策略。

1. 进入「策略配置」>「SSID 策略」页面。
2. 点击 **添加**。
3. 在【SSID 策略】窗口配置以下参数。
  - 策略名称：为所添加的 SSID 策略配置一个名称，如“OPEN”。
  - SSID：设置无线网络名称，本例中为“FREE”。
4. 点击 **保存**。

SSID策略

策略名称 OPEN

SSID FREE

加密方式 不加密

最大客户端数 30

客户端隔离  开启

隐藏SSID  开启

VLAN ID 1000

备注：需要下发VLAN策略才能生效

保存 取消

## 步骤 2：下发 SSID 策略给 AP。

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行配置的 AP，点击 **SSID 配置**。
3. 在【SSID 配置】窗口配置以下参数。
  - SSID 频段：选择要进行配置的频段，本例为“2.4G”。
  - 选择无线策略 1：选择**步骤 1**所添加的 SSID 策略，本例为“OPEN”。
4. 点击 **保存**。

SSID配置

SSID 频段  2.4G  5G

选择无线策略1 OPEN

选择无线策略2 禁用

选择无线策略3 禁用

选择无线策略4 禁用

保存 取消

----完成

## 验证配置

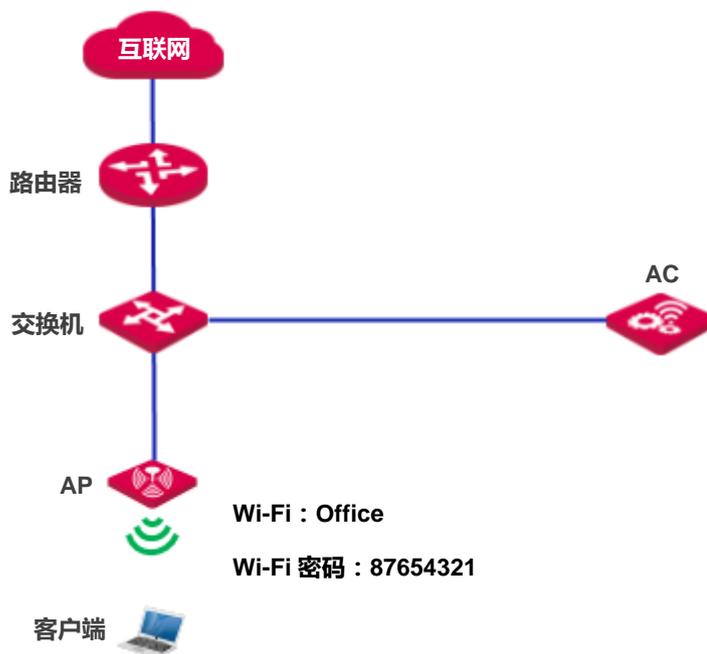
无线设备连接无线信号“FREE”时，无需输入无线密码就可以连接成功。

## WPA-PSK/WPA2-PSK 加密无线网络配置举例

### 组网需求

供企业内部员工接入的无线网络，要求有一定安全性，且配置简单。针对上述需求，建议采用 WPA-PSK 或 WPA2-PSK 安全模式。

假设：1) 网络未划分 VLAN。2) AP 是单频 AP，工作在 2.4GHz 频段。



### 配置步骤



提示

配置步骤中，其他未提到的参数，请保持默认设置即可。

#### 步骤 1：配置 SSID 策略。

1. 进入「策略配置」>「SSID 策略」页面。
2. 点击 **添加**。
3. 在【SSID 策略】窗口配置以下参数。
  - 策略名称：为所添加的 SSID 策略配置一个名称，如“PSK”。
  - SSID：设置无线网络名称，本例中为“Office”。

- 加密方式：选择“WPA-PSK”或“WPA2-PSK”。
- 密钥：本例中为“87654321”。

4. 点击 **保存**。

SSID策略

策略名称 PSK

SSID Office

加密方式 WPA2-PSK

加密规则  AES  TKIP  TKIP&AES

密钥 87654321

密钥周期 0 单位：秒

最大客户端数 30

客户端隔离  开启

隐藏SSID  开启

保存 取消

**步骤 2：下发 SSID 策略给 AP。**

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行配置的 AP，点击 **SSID 配置**。
3. 在【SSID 配置】窗口配置以下参数。
  - SSID 频段：选择要进行配置的频段，本例为“2.4G”。
  - 选择无线策略 1：选择**步骤 1**所添加的 SSID 策略，本例为“PSK”。
4. 点击 **保存**。



----完成

### 验证配置

无线设备连接无线信号“Office”时，需要输入无线密码“87654321”，才能连接成功。

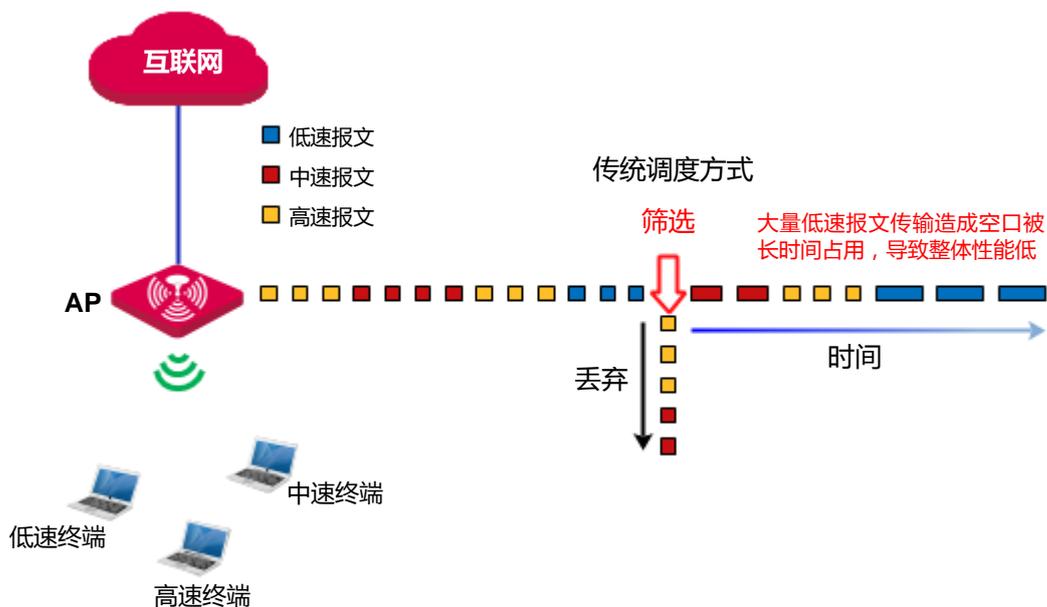
## 4.2 射频策略

### 4.2.1 概述

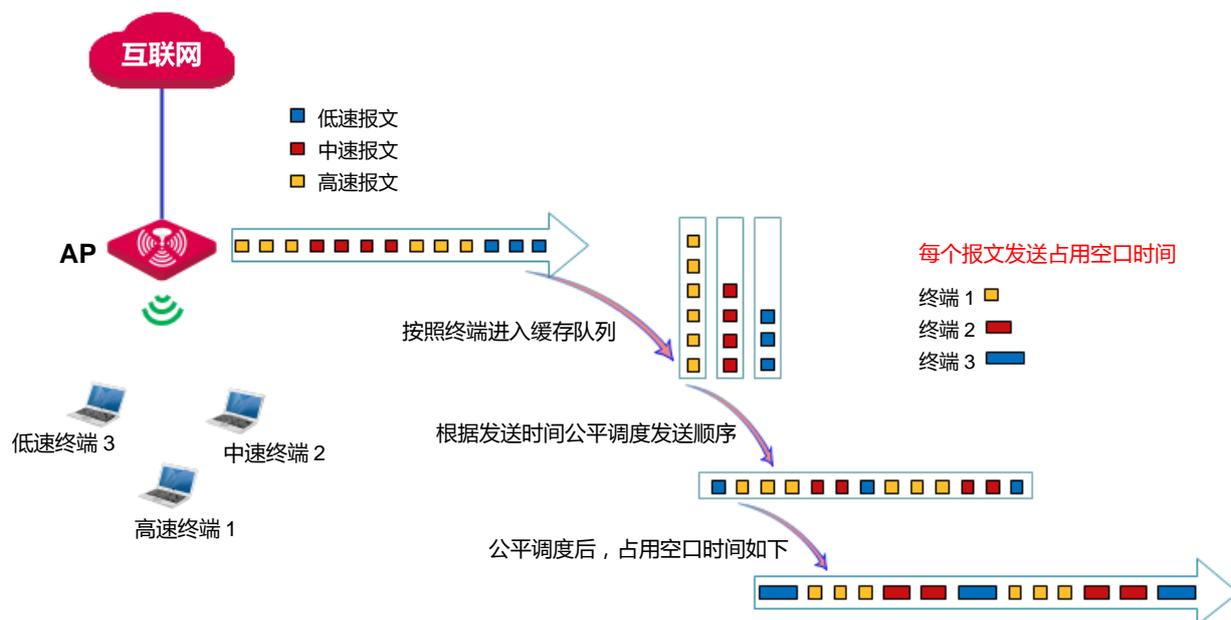
射频策略用于配置 AP 的射频相关参数。

#### 空口调度

传统的报文调度采用 FIFO 方式。在无线混合速率环境下，高速用户传送能力强，频谱效率高，却占用的空口时间更少，而低速用户传送能力弱，频谱效率低，却占用了更多的空口时间，这会降低每个 AP 的系统吞吐率，进而降低系统效率。



空口时间调度通过公平的分配下行传输时间，使得高速用户和低速用户获得相同的下行传输时间，帮助高速用户传输更多的数据，从而使 AP 实现更高的系统吞吐率和用户接入数。



## SSID 隔离

将连接到同一 AP 但不同 SSID 的无线用户隔离，如：用户 1 连上 SSID1，用户 2 连上 SSID2，则用户 1 和用户 2 之间不能相互通讯。



## 5G 策略优先

无线网络应用中，2.4GHz 频段比 5GHz 频段应用更为广泛，但 2.4GHz 频段只有 3 个不重叠的通信信道，信道相当拥挤，无线信号间的干扰也很大。实际上，5GHz 频段能提供更多不重叠的通信信道，在中国有 9 个，在有的国家更是多达二十多个。

随着无线网络的发展，越来越多的用户使用同时支持 2.4GHz 频段和 5GHz 频段的双频无线终端。然而，通常情况下，双频终端在接入无线网络的时候，默认都选择从 2.4GHz 频段接入，造成 2.4GHz 频段更加拥挤和 5GHz 频段的浪费。

5G 策略优先是指双频终端接入双频 AP 时，AP 控制终端使其优先接入 5GHz 频段，从而达到将双频

终端用户向 5GHz 频段上迁移的目的，减少 2.4GHz 频段上的负载和干扰，提升用户体验。



\* 假设 5G 频段允许的最大客户端数为 10



注意

5G 策略优先的前提是双频 AP 的 2.4GHz 和 5GHz 射频都开启，且在 2.4GHz 和 5GHz 频段配置的 SSID 相同，无线加密方式、加密规则、密码也相同。

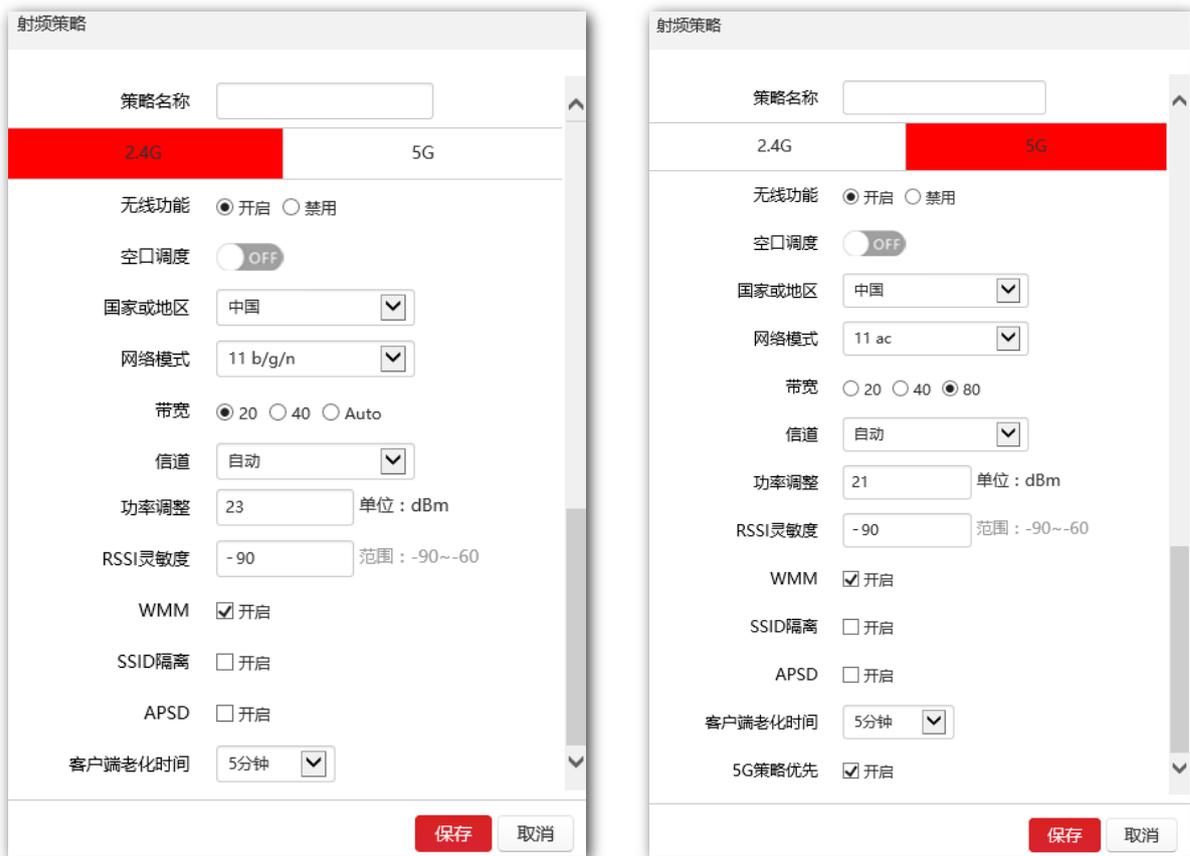
## 4.2.2 配置射频策略

默认情况下，AC 已配置了 1 条策略名称为 “default” 的射频策略，如下图所示。AP 第 1 次上线后，AC 会自动给 AP 下发默认射频策略。

SSID策略												射频策略												VLAN策略												高级策略											
+ 添加												- 删除												策略名称																							
总策略条数: 1条												刷新												每页条数												10											
策略名称	5G优先	无线频段	国家或地区	无线开关	模式	带宽	信道	功率	老化时间	状态	操作																																				
default	开启	2.4G 5G	中国 中国	开启 开启	11 b/g/n 11 ac	20MHz 80MHz	自动 自动	23dBm 21dBm	5分钟 5分钟	使用中																																					

### 添加射频策略

1. 进入「策略配置」>「射频策略」页面。
2. 点击 **+添加**。
3. 在【射频策略】窗口配置各项参数。
4. 点击 **保存**。



## 参数说明

标题项	说明
策略名称	射频策略的名称，注意不能和已有的射频策略名称重复。
2.4G、5G	选择要设置射频参数的频段。
无线功能	<ul style="list-style-type: none"> <li>- 开启：开启 AP 的无线功能。</li> <li>- 禁用：关闭 AP 的无线功能。</li> </ul>
空口调度	<p>开启/关闭 ( ON/OFF ) 空口调度功能。</p> <p>开启后，使高速用户和低速用户获得相同的下行传输时间，帮助高速用户传输更多的数据，从而使 AP 实现更高的系统吞吐率和用户接入数。</p>
国家或地区	选择当前网络所在的国家或地区，以适应不同国家或地区对信道的管制要求。
网络模式	<p>选择无线网络模式。2.4GHz 可选择 11b、11g、11b/g、11b/g/n，5GHz 可选择 11a、11ac、11a/n。</p> <ul style="list-style-type: none"> <li>- 11b：仅允许 802.11b 的无线设备连接到 AP。</li> <li>- 11g：仅允许 802.11g 的无线设备连接到 AP。</li> <li>- 11b/g：允许 802.11b、802.11g 的无线设备连接到 AP。</li> <li>- 11b/g/n：允许 802.11b、802.11g 以及工作在 2.4GHz 的 802.11n 无线设备连接到 AP。</li> <li>- 11a：仅允许 802.11a 的无线设备连接到 AP。</li> </ul>

标题项	说明
	<ul style="list-style-type: none"> <li>- 11ac：允许 802.11ac 的无线设备连接到 AP。</li> <li>- 11a/n：允许 802.11a 以及工作在 5GHz 的 802.11n 无线设备连接到 AP。</li> </ul>
带宽	<p>选择无线信道带宽。</p> <ul style="list-style-type: none"> <li>- 20：限制 AP 只能使用 20MHz 的信道带宽。</li> <li>- 40：限制 AP 只能使用 40MHz 的信道带宽。</li> <li>- Auto：AP 根据周围环境，自动调整 AP 信道带宽为 20MHz 或 40MHz。</li> <li>- 80：限制 AP 只能使用 80MHz 的信道带宽。</li> </ul>
信道	<p>给 AP 指定一个工作信道。</p> <p>选择“自动”时，会根据周围环境情况自动调整 AP 的工作信道。</p>
扩展信道	<p>在 2.4GHz 网络，用于确定 AP 在 11n 模式使用 40MHz 信道带宽时所工作的频率段。在 5GHz 网络，用于确定 AP 使用 40MHz 信道带宽时所工作的频率段。</p>
功率调整	<p>调整 AP 的无线发射功率。</p> <p>若使用本策略的 AP 不支持设置的无线发射功率，则配置下发后，以 AP 支持的最大范围为准。</p>
RSSI 灵敏度	<p>AP 可接受的无线客户端的信号强度。</p> <p>如果无线客户端信号强度小于设置的值，AP 将主动断开无线客户端，确保无线客户端主动连接到信号更强的 AP。</p>
WMM	<p>WMM 即“无线多媒体”。</p> <p>开启 WMM 后，音视频数据优先转发。如果要提高 AP 对于无线多媒体数据（如观看在线视频）的传输性能，建议开启。</p>
SSID 隔离	<p>开启/关闭 SSID 隔离功能。</p> <p>开启后，连接到 AP 的不同 SSID 的无线客户端不能互相访问。</p>
APSD	<p>APSD，Automatic Power Save Delivery，自动省电模式。是 Wi-Fi 联盟的 WMM 省电认证协议。开启 WMM 时，开启“APSD”能降低 AP 的电能消耗。默认关闭。</p>
客户端老化时间	<p>设置客户端老化时间。无线设备连接到 AP 的 Wi-Fi 后：</p> <p>如果在该时间段内与 AP 没有数据通信，AP 将主动断开该无线设备；如果在该时间段内与 AP 有数据通信，则重新开始老化计时。</p>
5G 策略优先	<p>开启后，双频终端接入双频 AP 时，AP 控制双频终端使其优先接入 5G 频段。从而达到将 2.4G 频段的双频终端用户向 5G 频段迁移的目的，减少 2.4G 频段的负载和干扰，提升用户体验。</p>

### ----完成

设置完成后，您可以在「策略配置」>「射频策略」页面查看到已添加的射频策略。如下图所示。

SSID策略		射频策略		VLAN策略		高级策略					
策略名称	5G优先	无线频段	国家或地区	无线开关	模式	带宽	信道	功率	老化时间	状态	操作
示例	开启	2.4G 5G	中国 中国	开启 开启	11 b/g/n 11 ac	20MHz 80MHz	自动 自动	23dBm 21dBm	5分钟 5分钟	未使用	
default	开启	2.4G 5G	中国 中国	开启 开启	11 b/g/n 11 ac	20MHz 80MHz	11 自动	23dBm 21dBm	5分钟 5分钟	使用中	

## 修改射频策略

1. 进入「策略配置」>「射频策略」页面。
2. 找到要修改的射频策略，点击操作栏的
3. 在【射频策略】窗口，根据需要修改各项参数。
4. 点击 **保存**。

----完成

之后，AC 会立即自动将新的射频策略更新到对应 AP。

## 删除射频策略

1. 进入「策略配置」>「射频策略」页面。
2. 找到要删除的射频策略，点击 **删除**。
3. 如果出现操作确认的对话框，请点击 **确定**。

----完成

## 4.3 VLAN 策略

### 4.3.1 概述

VLAN 策略用于配置 AP 的 VLAN 相关参数，包括 AP 的 VLAN 开启状态、管理 VLAN，Trunk 口，Trunk 口 PVID、Access 口以及 Access 口 VLAN ID。

### 4.3.2 配置 VLAN 策略

默认情况下，AC 没有配置任何 VLAN 策略。如下图所示。



### 添加 VLAN 策略

1. 进入「策略配置」>「VLAN 策略」页面。
2. 点击 **+添加**。
3. 在【VLAN 策略】窗口配置各项参数。
4. 点击 **确认**。

**VLAN策略**

策略名称

AP VLAN  开启  禁用

PVID  范围：1 - 4094

管理VLAN  范围：1 - 4094

Trunk口  LAN 0  LAN 1

有线LAN口 VLAN ID (1-4094)

LAN 0

LAN 1

## 参数说明

标题项	说明
策略名称	VLAN 策略的名称，注意不能和已有的 VLAN 策略名称重复。
AP VLAN	开启/禁用 AP 的 802.1Q VLAN 功能。 开启此功能并下发 VLAN 策略后，「策略配置」>「SSID 策略」页面配置的“VLAN ID”才会生效。
PVID	AP Trunk 口默认所属的 VLAN ID。
管理 VLAN	AP 的管理 VLAN ID。 更改管理 VLAN 后，AC 及管理电脑需要重新连接到新的管理 VLAN，才能管理 AP。
Trunk 口	选择作为 AP Trunk 口的有线 LAN 口（以太网口）。Trunk 口允许所有 VLAN 通过。 启用 802.1Q VLAN 功能时，至少要选择一个 LAN 口作为 Trunk 口。
有线 LAN 口	可以设置为 Access 口的有线 LAN 口。未被设置为 Trunk 口的 LAN 口才能被设置为 Access 口，其 VLAN ID 才可以被编辑。
VLAN ID	设置 Access 口的 VLAN ID。

----完成

## 修改 VLAN 策略

1. 进入「策略配置」>「VLAN 策略」页面。
2. 找到要修改的 VLAN 策略，点击操作栏的 .
3. 在【VLAN 策略】窗口，根据需要修改各项参数。
4. 点击 **确认**。

----完成

之后，AC 会立即自动将新的 VLAN 策略更新到对应 AP。

## 删除 VLAN 策略

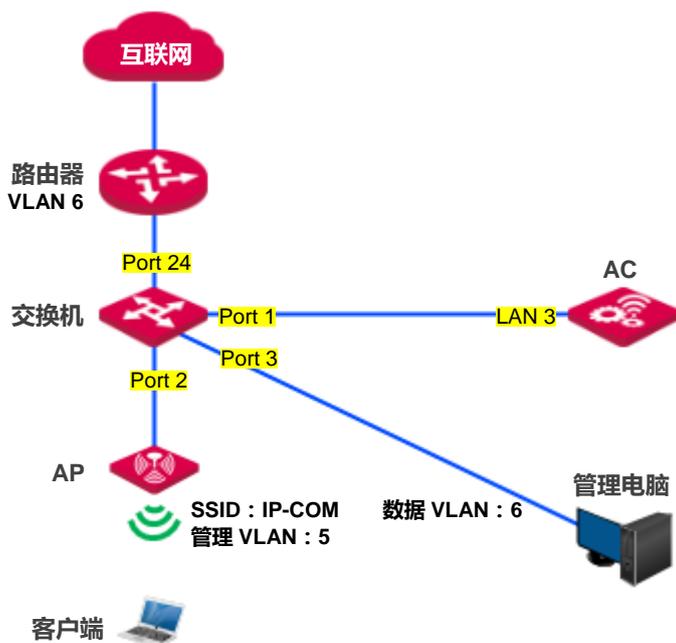
1. 进入「策略配置」>「VLAN 策略」页面。
2. 找到要删除的 VLAN 策略，点击 **删除**。
3. 如果出现操作确认的对话框，请点击 **确定**。

----完成

## 4.3.3 VLAN 策略配置举例

### 组网需求

某酒店需要实现无线覆盖,要求 AP 的管理 VLAN 与数据 VLAN 分离。其中,管理 VLAN 为 VLAN 5,数据 VLAN 为 VLAN 6。



### 配置步骤

#### 一、配置 AC



提示

配置步骤中,其他未提到的参数,请保持默认设置即可。

#### 步骤 1：配置 SSID 策略。

1. 进入「策略配置」>「SSID 策略」页面。
2. 点击 **添加**。
3. 在【SSID 策略】窗口配置以下参数。
  - 策略名称：为所添加的 SSID 策略配置一个名称,如“vlan6”。
  - SSID：设置无线网络名称,本例中为“IP-COM”。
  - VLAN ID：设置 AP 的数据 VLAN ID,本例中为“6”。

4. 点击 **保存**。

SSID策略

策略名称

SSID

加密方式

最大客户端数

客户端隔离  开启

隐藏SSID  开启

VLAN ID

备注：需要下发VLAN策略才能生效

**保存** 取消

## 步骤 2：配置 VLAN 策略。

1. 进入「策略配置」>「VLAN 策略」页面。
2. 点击 **+添加**。
3. 在【VLAN 策略】窗口配置以下参数。
  - 策略名称：为所添加的 VLAN 策略配置一个名称，如“示例”。
  - 管理 VLAN：设置 AP 的管理 VLAN ID，本例中为“5”。
4. 点击 **确认**。

VLAN策略

策略名称

AP VLAN  开启  禁用

PVID  范围：1 - 4094

管理VLAN  范围：1 - 4094

Trunk   LAN 0  LAN 1

有线LAN  VLAN ID (1-4094)

LAN 0

LAN 1

**确认** 取消

**步骤 3：下发 SSID 策略给 AP。**

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行配置的 AP，点击 **SSID 配置**。
3. 在【SSID 配置】窗口配置以下参数。
  - SSID 频段：选择要进行配置的频段，本例为“2.4G”。
  - 选择无线策略 1：选择**步骤 1**所添加的 SSID 策略，本例为“vlan6”。
4. 点击 **保存**。

**步骤 4：下发 VLAN 策略给 AP。**

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行 VLAN 配置的 AP，点击 **VLAN 设置**。
3. 在【VLAN 设置】窗口，选择**步骤 2**所添加的 VLAN 策略，本例为“示例”。
4. 点击 **保存**。

**步骤 5：配置 AC 的 VLAN。**

1. 进入「系统工具」>「网络设置」页面，找到“VLAN 配置”模块。
2. 端口隔离：选择“开启”。
3. VLAN ID：需要与 AP 的管理 VLAN ID 保持一致，本例中为“5”。
4. 端口号：选择 AC 管理 AP 所用的端口，本例中为“端口 3”。
5. 点击该模块的 **添加**，将 VLAN 配置添加并保存到下方的 VLAN 列表。

**VLAN 配置**

注：本设备最多支持48个不同VLAN。修改配置后，需要重启本设备才能生效

端口隔离  开启  关闭

VLAN ID  (例如：3-10,12)

端口号  端口 1  端口 2  端口 3  端口 4  端口 5

序号	VLAN ID	端口号	操作
1	5	3	<input type="button" value="删除"/>

6. 进入「系统工具」>「维护」页面，在“升级维护”模块，点击 **重启**。

## 二、配置交换机

在交换机上配置 802.1q VLAN，具体配置情况如下表。

交换机端口	连接到	VLAN ID(允许通过的 VLAN)	端口属性	PVID
1	AC	1,5	Trunk	1
2	AP	5,6	Trunk	1
3	管理电脑	1	Access	1
24	路由器	6	Access	6

----完成

## 验证配置

进入 AC 的「设备扫描」页面，可以看到 AP 已上线。

接入AP数：1 台  每页条数 10

<input type="checkbox"/>	型号	备注	IP	MAC	在线用户数	SSID	信道	软件版本	状态
<input type="checkbox"/>	ap325v1.0	AP325V1.0	192.168.10.180	D8:38:0D:00:1F:70	2	IP-COM	11	V1.0.0.3(3307)	在线

无线设备连接到无线信号“IP-COM”可以上网。

## 4.4 高级策略

### 4.4.1 概述

高级策略包括[维护策略](#)、[告警策略](#)、[密码策略](#)、[部署策略](#)。

#### 维护策略

WLAN 维护中，定时周期性地自动重启 AP，可以预防长时间地运行 AP 导致 WLAN 出现性能降低、不稳定等现象。

有以下两种自动重启方式可供选择：

- 定时重启：AP 周期性地在规定时间点自动重启。
- 循环重启：管理员设置好一个间隔时间，AP 每隔这个“间隔时间”就自动重启一次。

另外，您还可以通过设置维护策略来关闭/开启 AP 的指示灯。



维护策略的生效时间以 AP 的系统时间为准。

#### 告警策略

无线网络部署完成后，网络管理员还需实时监控 AP 的运行状态，以及时了解无线网络情况。借助“告警策略”，网络管理员无需亲临现场，即可实时掌握 AP 的运行情况。

支持邮件告警和 SNMP 告警两种告警方式。

##### ■ 桌面告警

AC 将告警事件信息发送到管理员指定的运行着告警客户端的电脑，管理员可以直接在该电脑上浏览历史告警信息。

##### ■ 邮件告警

AC 将告警事件信息定期通过邮件形式发送到管理员指定的邮箱，管理员打开邮箱即可浏览历史告警信息。

## 密码策略

使用“密码策略”，网络管理员可以批量地修改 AP 的管理员登录账号和密码。

## 部署策略

使用“部署策略”，您可以集中设置 AP 的这些参数：穿墙能力、部署方式、以太网模式。

### 4.4.2 配置高级策略

默认情况下，AC 没有配置任何高级策略。如下图所示。



### 添加维护策略

1. 进入「策略配置」>「高级策略」页面。
2. 点击 **+添加维护策略**。
3. 在【维护策略】窗口配置各项参数。
4. 点击 **确认**。

**维护策略**

策略名称

LED 状态  开启

重启设置  开启

重启类型  定时重启  循环重启

重启间隔设置  :

每天
  星期一
  星期二
  星期三
  星期四
  星期五
  星期六
  星期日

**参数说明**

标题项	说明
策略名称	维护策略的名称，注意不能和已有的高级策略名称重复。
LED 状态	开启/关闭 AP 的指示灯。
重启设置	开启/关闭 AP 的自动重启功能。 AP 在指定的时间点（建议为闲时）自动重启，可为 AP 始终保持高性能运行提供保障。
重启类型	选择 AP 重启的类型。 <ul style="list-style-type: none"> <li>- 定时重启：AP 在指定日期的指定时间点重启。</li> <li>- 循环重启：AP 每隔一段时间（指定的重启间隔）便自动重启一次。</li> </ul>
重启时间设置	重启类型为“定时重启”时，用于设置 AP 的重启时间点。
重启间隔设置	重启类型为“循环重启”时，用于设置 AP 的重启间隔时间。
每天、星期一、星期二、 星期三、星期四、 星期五、星期六、星期日	重启类型为“定时重启”时，用于指定 AP 重启的具体日期。

**----完成****添加告警策略**

1. 进入「策略配置」>「高级策略」页面。
2. 点击 **+添加告警策略**。
3. 在【告警设置】窗口配置各项参数。
4. 点击 **确认**。

### 告警设置

策略名称

桌面告警

---

邮件告警  测试

邮件服务器端口   SSL

邮箱密码

告警间隔  (单位：分钟)

---

AP故障告警  ON

---

AP流量告警  OFF

限制流量  (单位：MB)

---

AP接入数告警  ON

限制接入数

确认
取消

### 参数说明

标题项	说明
策略名称	告警策略的名称，注意不能和已有的高级策略名称重复。
桌面告警	<p>开启/关闭桌面告警功能。</p> <p>开启时，请输入<a href="#">接收告警信息的电脑</a>的 IP 地址。AP 使用该策略后，AC 将会把 AP 的告警信息直接发送到该电脑上的告警客户端。</p>
邮件告警	<p>开启/关闭邮件告警功能。</p> <p>开启时，请输入发送/接收 AP 告警信息的邮箱地址。AP 使用该策略后，AC 会定期把 AP 的告警信息发送到该邮箱。点击<a href="#">测试</a>可测试该邮箱是否可用。</p>
邮件服务器端口	<p>输入邮件服务器使用的发送邮件端口号。如果未勾选“SSL”，则端口号默认为 25；如果已勾选“SSL”，则端口号默认为 587。</p> <p>SSL 勾选表示使用 SMTPS (SMTP-over-SSL) 协议发送邮件。</p> <p>SMTPS 是 SMTP 协议基于 SSL 安全协议之上的一种变种协议，它继承了 SSL 安全协议的非对称加密的高度安全可靠，可防止邮件泄露。</p>
邮箱密码	开启“邮件告警”时，请输入发送 AP 告警信息的邮箱的密码。

标题项	说明
告警间隔	开启“邮件告警”时，请输入发送告警邮件的时间间隔。
AP 故障告警	开启/关闭 ( ON/OFF ) AP 故障告警功能。 开启时，若 AP 出现重启、上线、离线等情况，会发出告警。
AP 流量告警	开启/关闭 ( ON/OFF ) AP 流量告警功能。 开启时，AP 的流量若超过限定值则会发出告警。
限制流量	开启“AP 流量告警”后，若 AP 的流量超过此值，AP 会发出告警。
AP 接入数告警	开启/关闭 ( ON/OFF ) AP 接入数告警功能。 开启时，若接入 AP 的无线客户端超过限定值，AP 会发出告警。
限制接入数	开启“AP 接入数告警”后，若接入 AP 的无线客户端超过此值，AP 会发出告警。

---完成

## 添加密码策略

1. 进入「策略配置」>「高级策略」页面。
2. 点击 **+添加密码策略**。
3. 在【密码策略】窗口配置各项参数。
4. 点击 **确认**。

密码策略

策略名称

AP统一登录账号:

AP统一登录密码:

确认登录密码:

**确认**

### 参数说明

标题项	说明
策略名称	密码策略的名称，注意不能和已有的高级策略名称重复。
AP 统一登录账号	设置 AP 管理页面的登录帐号。

标题项	说明
AP 统一登录密码	设置 AP 管理页面的登录密码。
确认登录密码	再次输入登录密码。

----完成

## 添加部署策略

1. 进入「策略配置」>「高级策略」页面。
2. 点击 **+添加部署策略**。
3. 在【部署策略】窗口配置各项参数。
4. 点击 **确认**。

部署策略

策略名称

穿墙能力  强覆盖  高密度

部署方式  默认模式  强覆盖模式  高密度模式

以太网模式  标准  10M半双工

**确认** **取消**

### 参数说明

标题项	说明
策略名称	部署策略的名称，注意不能和已有的高级策略名称重复。
穿墙能力	<p>根据实际应用场景，选择穿墙能力特性。</p> <ul style="list-style-type: none"> <li>- 强覆盖：常用于 AP 部署密度较低的场景，如办公室、仓库、医院等，使用此模式可以扩大 AP 的覆盖范围。</li> <li>- 高密度：常用于 AP 部署密度较高的场景，如会场、展厅、宴会厅、体育场馆、高校教室、候机厅等，使用此模式可以有效减少 AP 相互之间的干扰。</li> </ul>
部署方式	<p>根据实际应用场景，选择部署方式特性。</p> <ul style="list-style-type: none"> <li>- 强覆盖模式：常用于 AP 部署密度较低的场景，此方式可以尽可能地确保无线设备成功接入 AP。</li> <li>- 高密度模式：常用于 AP 部署密度较高的场景，此模式可以确保无线设备连接到信号好的 AP。</li> </ul>

标题项	说明
	<ul style="list-style-type: none"> <li>- 默认模式：介于“强覆盖”和“高密度”之间。</li> </ul>
以太网模式	<p>AP 的 PoE 口的以太网模式。</p> <ul style="list-style-type: none"> <li>- 标准：速率高，驱动距离较短。一般情况下，建议选择此模式。</li> <li>- 10M 半双工：驱动距离远，但速率较低（10Mbps）。</li> </ul> <p>当连接 AP PoE 口与对端设备的网线超过 100 米时，才建议尝试改为“10M 半双工”以提高网线驱动距离。同时，必须确保对端端口工作模式为“自协商”，否则可能导致 AP 以 PoE 口无法正常收发数据。</p>

----完成

## 修改高级策略

1. 进入「策略配置」>「高级策略」页面。
2. 找到要修改的高级策略，点击操作栏的 .
3. 在对应的高级策略窗口，根据需要修改各项参数。
4. 点击 **确认**。

----完成

之后，AC 会立即自动将新的高级策略更新到对应 AP。

## 删除高级策略

1. 进入「策略配置」>「高级策略」页面。
2. 找到要删除的高级策略，点击 **删除**。
3. 如果出现操作确认的对话框，请点击 **确定**。

----完成

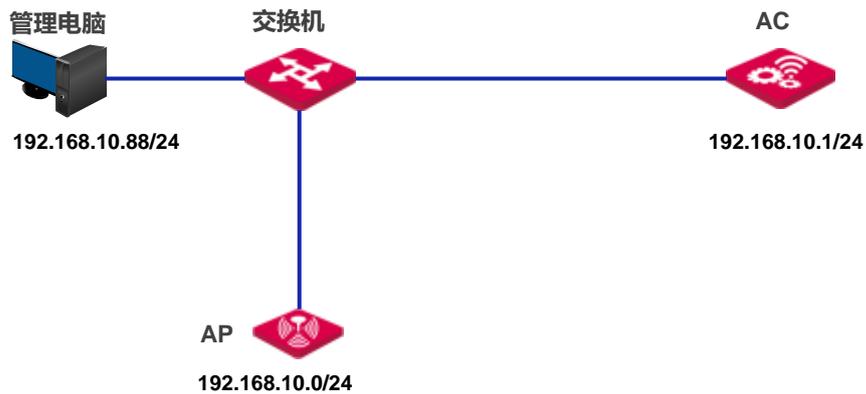
### 4.4.3 高级策略配置举例

#### 桌面告警配置举例

##### 组网需求

网络管理员电脑与 AC 通过以太网相连，该电脑的 IP 地址为 192.168.10.88/24。需求：网络管理员可以在自己的电脑上监控 AP 故障、流量、接入数情况。

假设：AP 限制流量为“80MB”，限制接入数为“15”。



## 配置步骤



提示

配置步骤中，其他未提到的参数，请保持默认设置即可。

### 步骤 1：配置 AC。

#### 1. 配置告警策略。

- (1) 进入「策略配置」>「高级策略」页面。
- (2) 点击 **+添加告警策略**。
- (3) 在【告警设置】窗口配置以下参数。
  - 策略名称：为所添加的告警策略配置一个名称，如“桌面告警”。
  - 桌面告警：勾选复选框，输入管理员电脑的 IP 地址，本例为“192.168.10.88”。
  - AP 流量告警：选择“ON”。
  - 限制流量：本例中为“80” MB。
- (4) 点击 **保存**。

告警设置

策略名称

桌面告警

邮件告警  测试

邮件服务器端口   SSL

邮箱密码

告警间隔  (单位: 分钟)

AP故障告警

AP流量告警

限制流量  (单位: MB)

AP接入数告警

限制接入数

确认 取消

## 2. 下发告警策略给 AP。

- (1) 进入「AP 管理」>「批量维护」页面。
- (2) 选中需要进行高级配置的 AP，点击 高级设置。
- (3) 在【高级设置】窗口，选择告警策略为 **步骤 1** 中配置的策略，本例为“桌面告警”。
- (4) 点击 保存。

批量维护 单台维护

SSID配置 射频配置 VLAN设置 高级: 高级设置

AP总数: 1台 刷新

<input type="checkbox"/>	型号	备注	MAC	告警策略	密码策略	部署策略	状态
<input checked="" type="checkbox"/>	ap325v1.0	AP325V...	D8:38:0D:00:1F:70	桌面告警	无策略	无策略	在线

维护策略

告警策略

密码策略

部署策略

保存 取消

## 步骤 2：配置管理员电脑。

以 Windows 7 电脑为例说明。

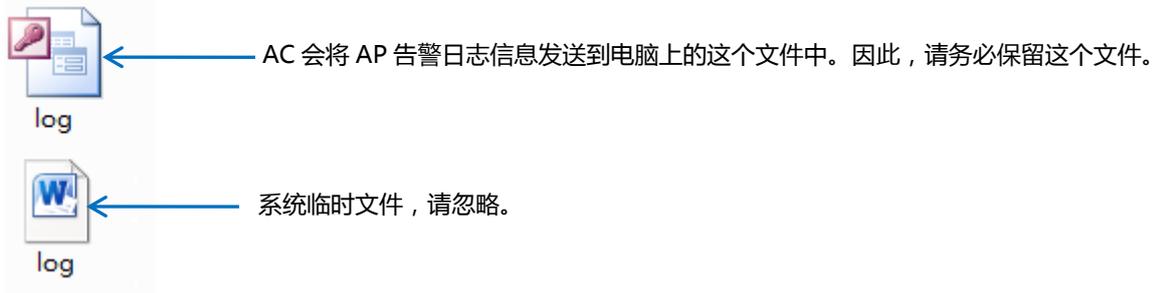
1. 联系 IP-COM 技术支持，获得告警客户端软件。
2. 将告警客户端软件存放在电脑硬盘的某个文件夹，如“D:\AP 告警”。



3. 双击告警客户端 。

若出现“您想允许来自以下未知发布者的以下程序对此计算机进行更改吗”的对话框，请选择 **是**。

运行成功后，文件夹里将生成以下两个文件：



## 验证配置

如果发生了 AP 告警事件，网络管理员可以直接在告警客户端上查看 AP 告警信息。操作过程如下：

1. 双击桌面的告警客户端。



2. 在弹出的页面查看 AP 告警信息，如下图所示。点击 **刷新**，可以查看最新的告警信息。

时间	类型	事件
2017-05-21 17:22:56	AP故障告警	AP(606 MAC = 00:b0:c6:4e:9c:2f) 上线
2017-05-21 17:20:58	AP故障告警	AP(606 MAC = 00:b0:c6:4e:9c:2f) 上线
2017-05-21 17:20:08	AP故障告警	AP(606 MAC = 00:b0:c6:4e:9c:2f) 重启离线

## 邮件告警配置举例

### 组网需求

网络管理员需要在自己的邮箱 ( zhangsan@163.com ) 里就可以查看到 AP 的所有告警信息。

假设：

- AP 限制流量为 “80MB”，限制接入数为 “15”。
- 网络管理员的发件/收件邮箱地址为 “zhangsan@163.com”，邮箱密码为 “123456”。
- 邮件服务器使用的发送邮件协议为 SMTPS，发送邮件端口为 “587”。
- 发送告警邮件的间隔为 “60 分钟”。

### 配置步骤



配置步骤中，其他未提到的参数，请保持默认设置即可。

#### 步骤 1：配置告警策略。

1. 进入「策略配置」>「高级策略」页面。
2. 点击 **+添加告警策略**。
3. 在【告警设置】窗口配置以下参数。
  - 策略名称：为所添加的告警策略配置一个名称，如 “邮件告警”。
  - 邮件告警：勾选复选框，输入发件/收件邮箱地址，本例为 “zhangsan@163.com”。
  - 邮件服务器端口：勾选 “SSL”。
  - 邮箱密码：输入邮箱密码，本例为 “123456”。
  - 告警间隔：选择 “60” 分钟。
  - AP 流量告警：选择 “ON”。
  - 限制流量：本例中为 “80” MB。
4. 点击 **确认**。

### 告警设置

策略名称

桌面告警

---

邮件告警  测试

邮件服务器端口   SSL

邮箱密码

告警间隔  (单位: 分钟)

---

AP故障告警

---

AP流量告警

限制流量  (单位: MB)

---

AP接入数告警

限制接入数

## 步骤 2：下发告警策略给 AP。

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行高级配置的 AP，点击 高级设置。
3. 在【高级设置】窗口，选择告警策略为步骤 1 中配置的策略，本例为“邮件告警”。
4. 点击 保存。

批量维护
单台维护

SSID配置
射频配置
VLAN设置
高级设置

每页条数

AP总数: 1台 刷新

<input type="checkbox"/>	型号	备注	MAC
<input checked="" type="checkbox"/>	DS-3WA2...	DS-3W...	D8:38:0D:00:1F:70

维护策略

告警策略

密码策略

部署策略

策略	密码策略	部署策略	状态
策略	无策略	无策略	在线

---完成

## 验证配置

如果发生了 AP 告警事件，网络管理员会在 1 小时之内收到 AP 告警邮件。

## 配置注意事项

确保 AC 已进行外网配置（在「系统工具」>「网络设置」页面的“外网配置”模块），使其与发件/收件邮箱路由可达，并且域名解析正常。

# 5 AP 管理

## 5.1 批量维护

借助“批量维护”功能，您可以将「策略配置」模块配置的 SSID 策略、射频策略、VLAN 策略、高级策略批量地下发到 AP，使相应配置在 AP 上生效。

### 5.1.1 SSID 配置

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行 SSID 配置的 AP，点击 **SSID 配置**。
3. 在【SSID 配置】窗口配置各项参数。
4. 点击 **保存**。



#### 参数说明

##### 标题项

##### 说明

##### SSID 频段

选择要进行 SSID 配置的频段。

可选的 SSID 频段取决于 AP，若 AP 不支持 5GHz，则 5GHz 频段不可设置。

若同时选中的 AP 所支持的频段不一致，AC 会自动以各 AP 实际支持的频段下发无线策略。

标题项

说明

选择 无线策略 1~n

选择 SSID 要匹配的 SSID 策略。

可选择的无线策略个数取决于 AP 支持的 SSID 个数。“禁用”表示禁用 AP 的该 SSID。

----完成

## 5.1.2 射频配置

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行射频配置的 AP，点击 **射频配置**。
3. 在【射频配置】窗口选择 AP 要匹配的射频策略。
4. 点击 **保存**。



----完成

## 5.1.3 VLAN 设置

1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行 VLAN 配置的 AP，点击 **VLAN 设置**。
3. 在【VLAN 设置】窗口选择 AP 要匹配的 VLAN 策略。
4. 点击 **保存**。



----完成

## 5.1.4 高级设置

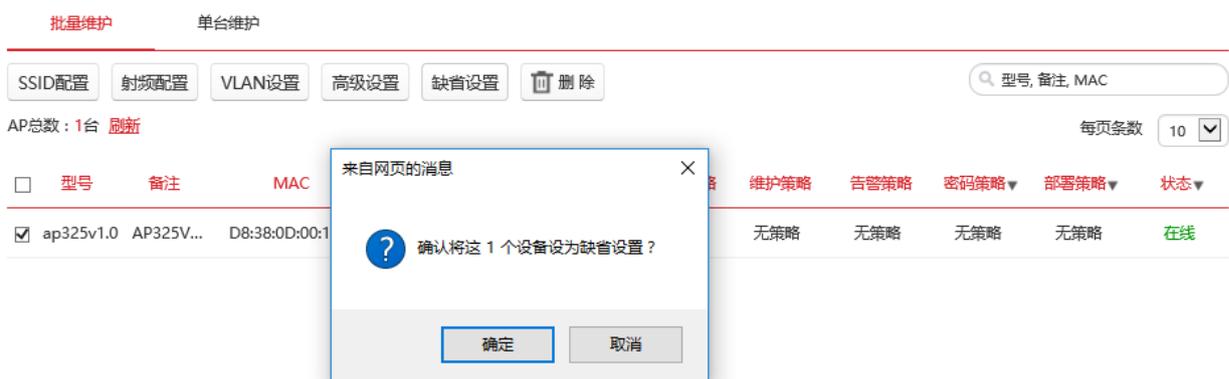
1. 进入「AP 管理」>「批量维护」页面。
2. 选中需要进行高级配置的 AP，点击 **高级设置**。
3. 在【高级设置】窗口选择 AP 要匹配的策略。
4. 点击 **保存**。



----完成

## 5.1.5 缺省设置

1. 进入「AP 管理」>「批量维护」页面。
2. 选中要取消已下发维护策略和告警策略的 AP，点击 **缺省设置**。
3. 如果出现操作确认的对话框，请点击 **确定**。



----完成

## 5.1.6 删除离线 AP 信息

当“批量维护”页面显示的 AP 数较多时，您可以将已离线的 AP 信息删除，便于更清晰地管理在线

AP。步骤如下。

1. 进入「AP 管理」>「批量维护」页面。
2. 选中处于“离线”状态的 AP。
3. 点击 **删除**。
4. 如果出现操作确认的对话框，请点击 **确定**。

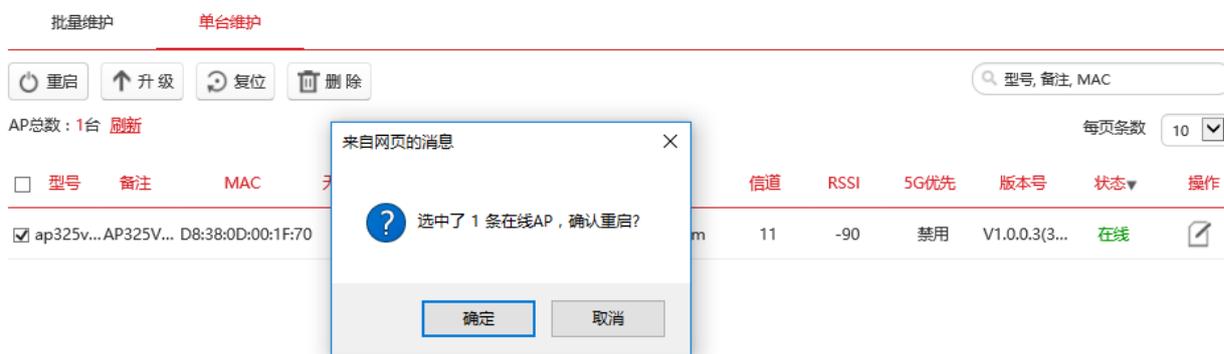
**----完成**

## 5.2 单台维护

借助“单台维护”功能，您可以批量重启/升级/复位 AP，还可以单独修改某一 AP 射频相关配置。

### 5.2.1 重启

1. 进入「AP 管理」>「单台维护」页面。
2. 选中需要进行重新启动的 AP，点击 **重启**。
3. 在操作确认的对话框中，点击 **确定**。



----完成

重启时，AP 将离线一段时间，重启完成后，AP 将自动上线。AP 从离线到重新上线的过程可能需要 1~2 分钟，请耐心等待。您可以点击页面的 **刷新** 按钮查看此过程。

### 5.2.2 升级

#### 注意

升级 AP 软件过程中，请勿断开 AP 电源，否则可能造成 AP 损坏！若是突发断电，请重新升级；若突发断电后无法管理 AP，请联系售后维修。

1. 访问 IP-COM 官网 <http://www.ip-com.com.cn>，下载对应型号 AP 的升级文件到本地电脑。
2. 登录 AC 的 Web 管理页面，转到「AP 管理」>「单台维护」页面。
3. 选中需要进行软件升级的 AP，点击 **升级**。
4. 在【AP 升级】窗口，点击 **浏览...**，从本地电脑选择并加载对应型号 AP 的升级软件到 AC。



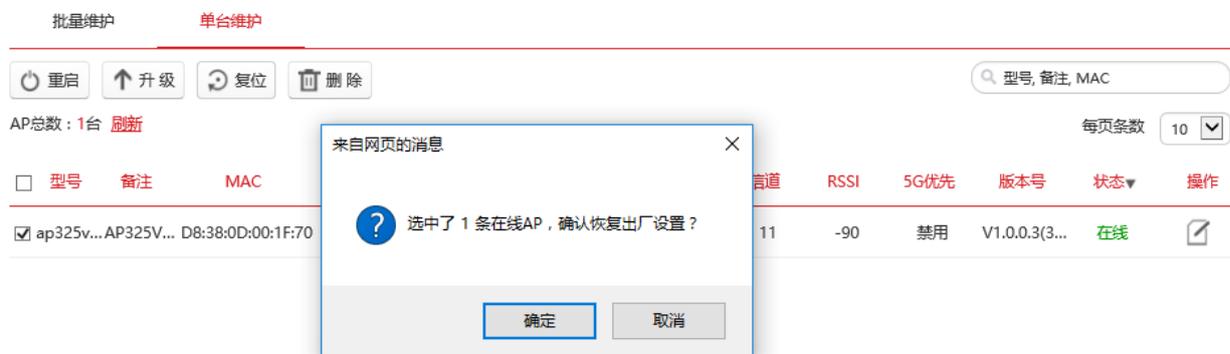
## 5. 点击 **升级**。

----完成

升级时，AP 将离线一段时间，升级完成后，AP 将自动上线。AP 从离线到重新上线的过程可能需要 1~2 分钟，请耐心等待。您可以点击页面的**刷新**按钮查看此过程。

## 5.2.3 复位

1. 进入「AP 管理」>「单台维护」页面。
2. 选中需要恢复出厂设置的 AP，点击 **复位**。
3. 在操作确认的对话框中，点击 **确定**。



----完成

AP 恢复出厂设置并重新上线后，AC 会自动给这些 AP 下发默认 SSID 策略和默认射频策略。

## 5.2.4 修改

1. 进入「AP 管理」>「单台维护」页面。
2. 找到需要修改配置的 AP，点击操作栏的 .



3. 在【单台维护】窗口，根据需要修改各参数。

4. 点击 **确认**。



## 参数说明

### 标题项

### 说明

2.4G、5G

选择要修改相关射频参数的频段。只有 AP 支持的频段才能显示和选择。

无线功能

- 开启：开启无线功能。
- 禁用：关闭无线功能。

国家或地区

选择当前网络所在的国家或地区，以适应不同国家或地区对信道的管制要求。

网络模式

选择无线网络模式。2.4GHz 可选择 11b、11g、11b/g、11b/g/n，5GHz 可选择 11a、11ac、11a/n。

- 11b：仅允许 802.11b 的无线设备连接到 AP。

标题项	说明
	<ul style="list-style-type: none"> <li>- 11g : 仅允许 802.11g 的无线设备连接到 AP。</li> <li>- 11b/g : 允许 802.11b、802.11g 的无线设备连接到 AP。</li> <li>- 11b/g/n : 允许 802.11b、802.11g 以及工作在 2.4GHz 的 802.11n 无线设备连接到 AP。</li> <li>- 11a : 仅允许 802.11a 的无线设备连接到 AP。</li> <li>- 11ac : 允许 802.11ac 的无线设备连接到 AP。</li> <li>- 11a/n : 允许 802.11a 和工作在 5GHz 的 802.11n 的无线设备连接到 AP。</li> </ul>
带宽	<p>选择无线信道带宽。</p> <ul style="list-style-type: none"> <li>- 20 : 限制 AP 只能使用 20MHz 的信道带宽。</li> <li>- 40 : 限制 AP 只能使用 40MHz 的信道带宽。</li> <li>- Auto : AP 根据周围环境, 自动调整 AP 信道带宽为 20MHz 或 40MHz。</li> <li>- 80 : 限制 AP 只能使用 80MHz 的信道带宽。</li> </ul>
信道	<p>给 AP 指定一个工作信道。</p> <p>选择“自动”时, 会根据周围环境情况自动调整 AP 的工作信道。</p>
扩展信道	<p>在 2.4GHz 网络, 用于确定 AP 在 11n 模式使用 40MHz 信道带宽时所工作的频率段, 在 5GHz 网络, 用于确定 AP 使用 40MHz 信道带宽时所工作的频率段。</p>
抗干扰模式	<p>选择 AP 的干扰抑制模式。</p> <ul style="list-style-type: none"> <li>- 0 : 禁用所有干扰抑制。</li> <li>- 1 : 启用同频段干扰抑制, 如微波炉、手机、蓝牙设备造成的同频干扰。</li> <li>- 2 : 强制启用无线电干扰抑制, 主要用在无线信号干扰源在 30 个以下的场景。</li> <li>- 3 : 自动启用无线电干扰抑制。</li> <li>- 4 : 自动启用无线电干扰抑制并降低噪声。主要用在无线信号干扰源超过 30 个的场景, 如高密场景等。</li> </ul>
功率调整	<p>调整 AP 的无线发射功率。</p> <p>若使用本策略的 AP 不支持设置的功率, 则配置下发后, 以 AP 支持的最大范围为准。</p>
RSSI	<p>AP 可接受的无线客户端的信号强度。</p> <p>如果无线客户端信号强度小于设置的值, AP 将主动断开无线客户端, 确保无线客户端主动连接到信号更强的 AP。</p>
WMM	<p>WMM 即“无线多媒体”。</p> <p>开启 WMM 后, 音视频数据优先转发。如果要提高 AP 对于无线多媒体数据 (如观看在线视频) 的传输性能, 建议开启。</p>
SSID 隔离	<p>开启/关闭 SSID 隔离功能。</p> <p>开启后, 连接到 AP 的不同 SSID 的无线客户端不能互相访问。</p>

标题项	说明
APSD	APSD, Automatic Power Save Delivery, 自动省电模式。是 Wi-Fi 联盟的 WMM 省电认证协议。开启 WMM 时, 开启“APSD”能降低 AP 的电能消耗。默认关闭。
客户端老化时间	设置客户端老化时间。无线设备连接到 AP 的 Wi-Fi 后: 如果在该时间段内与 AP 没有数据通信, AP 将主动断开该无线设备; 如果在该时间段内与 AP 有数据通信, 则重新开始老化计时。
5G 策略优先	开启后, 双频终端接入双频 AP 时, AP 控制双频终端使其优先接入 5G 频段。从而达到将 2.4G 频段的双频终端用户向 5G 频段迁移的目的, 减少 2.4G 频段的负载和干扰, 提升用户体验。

----完成

## 5.2.5 删除离线 AP 信息

当“单台维护”页面显示的 AP 数较多时, 您可以将已离线的 AP 信息删除, 便于更清晰地管理在线 AP。步骤如下。

1. 进入「AP 管理」>「单台维护」页面。
2. 选中处于“离线”状态的 AP。
3. 点击 **删除**。
4. 如果出现操作确认的对话框, 请点击 **确定**。

----完成

# 6 用户状态

点击「用户状态」进入页面。在这里，您可以了解无线网络的连接情况，包括用户 IP 地址、MAC 地址、下载总流量、信号强度、上网时长等。

用户列表

 导出 🔍 备注, IP, MAC

总人数: 1人 刷新 每页条数 10

频段:  2.4GHz  5GHz  2.4GHz+5GHz

<input type="checkbox"/>	备注	型号	SSID	频段	用户IP	用户MAC	下载总流量	信号强度	上网时长	状态
<input type="checkbox"/>	AP325V1.0	ap325v1.0	IP-COM_AP_0	2.4G	192.168.110.161	CC:08:8D:8E:9F:A6	26.77MB	-34dBm	0天00:02:48	在线

## 参数说明

标题项	说明
频段	选择要了解的无线网络所在的频段。
备注	用户连接的 AP 的备注信息。
SSID	用户连接的 SSID。
频段	用户连接的频段。
用户 IP	用户设备的 IP 地址。
用户 MAC	用户设备的 MAC 地址。
下载总流量	用户下载数据的总量。
信号强度	AP 接收到的用户设备的无线信号强度。
上网时长	用户接入网络的时长。
状态	用户连接的 AP 的状态。

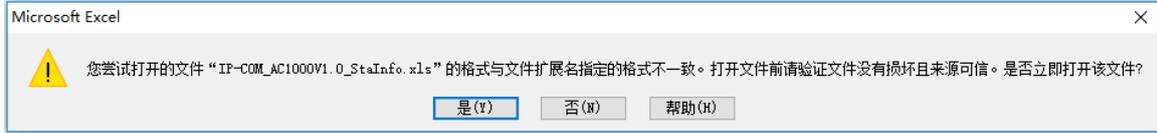
## 导出用户信息

1. 进入「用户状态」页面。
2. 点击 。
3. 如果出现操作确认的对话框，请点击 ，之后按页面提示将文档保存到本地电脑。

----完成



在本地电脑打开文档时，如果出现类似下图的对话框，请选择 **是**。



# 7 系统工具

## 7.1 系统状态

在这里，您可以了解 AC 的系统状态信息，包括[端口](#)、[系统状态](#)、[设备状态](#)。

进入页面的方法：点击「系统工具」>「系统状态」。

The screenshot displays the 'System Status' page with a navigation bar at the top containing: 系统状态 (selected), 网络设置, AP DHCP列表, 维护, 时间与日期, 日志显示, and 网络检测.

**端口 (Ports):** A row of five port status indicators: LAN1/未连接, LAN2/未连接, LAN3/已连接 (highlighted in green), LAN4/未连接, and LAN5/未连接.

**系统状态 (System Status):** A summary section showing:

- 已管理AP数量: 1
- 已离线AP数量: 0
- 已连接客户端数量: 0
- 系统运行时间: 5天 02:29:09
- CPU使用率: 15% (indicated by a gauge chart)
- 内存使用率: (indicated by a gauge chart)

**设备状态 (Device Status):** A table listing device configuration details:

IP地址	192.168.10.1
子网掩码	255.255.255.0
MAC地址	D8:38:0D:88:88:80
软件版本	V1.0.0.5(4666)

### 7.1.1 端口

在这里，您可以查看到 AC 各端口的连接情况。



## 7.1.2 系统状态

在这里，您可以查看到 AC 当前的已管理 AP 数量、已离线 AP 数量、已连接客户端数量，以及 AC 的系统运行时间、CPU/内存使用率。



## 7.1.3 设备状态

在这里，您可以查看到 AC 的 LAN 口 IP 地址、子网掩码、MAC 地址，以及软件版本号。

设备状态

IP地址	192.168.10.1
子网掩码	255.255.255.0
MAC地址	D8:38:0D:88:88:80
软件版本	V1.0.0.5(4666)

## 7.2 网络设置

在这里，您可以进行：外网配置、内网配置、DHCP 配置、VLAN 配置。

进入页面的方法：点击「系统工具」>「网络设置」。

系统状态    **网络设置**    AP DHCP列表    维护    时间与日期    日志显示    网络检测

### 外网配置

IP地址

子网掩码

网关

主DNS

备用DNS

确认

### 内网配置

IP地址

子网掩码

确认

### DHCP配置

地址池起始 IP

地址池结束 IP

网关

主DNS

备用DNS

租期  ▼

确认

### VLAN 配置

注：本设备最多支持48个不同VLAN。修改配置后，需要重启本设备才能生效

端口隔离  开启  关闭

VLAN ID  (例如：3-10,12)

端口号  端口 1  端口 2  端口 3  端口 4  端口 5

添加

序号	VLAN ID	端口号	操作
----	---------	-----	----

## 7.2.1 外网配置

### 概述

借助“外网配置”，可以将 AC 接入互联网，之后，AC 的系统时间就能同步互联网时间，从而确保 AC 上与时间相关的功能执行正确。

### 修改外网配置

1. 进入「系统工具」>「网络设置」页面。
2. 在“外网配置”模块设置各项参数。
3. 点击该模块的 **确认**。

外网配置

IP地址	<input type="text"/>
子网掩码	<input type="text"/>
网关	<input type="text"/>
主DNS	<input type="text"/>
备用DNS	<input type="text"/>

**确认**

#### 参数说明

标题项	说明
IP 地址	AC 连接互联网的 IP 地址，一般与出口路由器的 LAN 口 IP 地址在同一网段。
子网掩码	AC 连接互联网的 IP 地址的子网掩码，一般可填为 255.255.255.0。
网关	AC 的默认网关地址，一般为出口路由器的 LAN 口 IP 地址。
主 DNS	正确的 DNS 服务器或 DNS 代理服务器地址。 如果出口路由器支持 DNS 代理功能，可以为出口路由器的 LAN 口 IP 地址。否则，请咨询 ISP 获得正确的 DNS 地址。
备用 DNS	正确的 DNS 服务器或 DNS 代理服务器地址。可选项。

----完成

## 7.2.2 内网配置

### 概述

“内网配置”用于配置 AC 的 LAN 口 IP 地址/子网掩码。LAN 口 IP 是 AC 对局域网的 IP 地址，也是 AC 的管理 IP 地址。AC 默认的 LAN 口 IP 为 192.168.10.1，默认的子网掩码为 255.255.255.0。

一般情况下，您无需修改内网配置，除非遇到 IP 地址冲突，如：局域网内，有其它设备的 IP 地址也为 192.168.10.1。

### 修改内网配置

1. 进入「系统工具」>「网络设置」页面，找到“内网配置”模块。
2. IP 地址：根据需要修改。
3. 子网掩码：一般无需更改，保持为“255.255.255.0”即可。
4. 点击该模块的 **确认**。

内网配置

IP地址	<input type="text" value="192.168.10.1"/>
子网掩码	<input type="text" value="255.255.255.0"/>
<input type="button" value="确认"/>	

#### ---完成

设置完成后，如果新的 LAN 口 IP 地址与原 LAN 口 IP 地址不在同一网段，需要更改管理电脑的 IP 地址使其和新的 LAN 口 IP 在相同网段，并使用新的 LAN 口 IP 地址才能重新登录到 AC 的管理页面。



如果新的 LAN 口 IP 与原 LAN 口 IP 不在同一网段，系统将自动匹配修改 DHCP 地址池，使其和新的 LAN 口 IP 在同一网段。

## 7.2.3 DHCP 配置

### 概述

AC 提供了 DHCP 服务器，会给局域网中的 IP-COM AP 自动分配 IP 地址、子网掩码、网关、DNS 等上网信息。



注意

AC 的 DHCP 服务器只能为局域网中的 IP-COM AP 分配 IP 地址信息，不能给其他设备分配上述信息。IP-COM AP 首次上线后，AC 即会自动给 AP 分配上述信息。

### 修改 DHCP 配置

1. 进入「系统工具」>「网络设置」页面，找到“DHCP 配置”模块。
2. 根据需要修改各参数。
3. 点击该模块的 **确认**。

**DHCP配置**

地址池起始 IP	<input type="text" value="192.168.10.100"/>
地址池结束 IP	<input type="text" value="192.168.10.200"/>
网关	<input type="text"/>
主DNS	<input type="text"/>
备用DNS	<input type="text"/>
租期	<input type="text" value="一周"/> <input type="button" value="v"/>

#### 参数说明

标题项	说明
地址池起始 IP	DHCP 地址池（即 DHCP 服务器可分配的 IP 地址范围）的开始 IP 地址。默认为 192.168.10.100。
地址池结束 IP	DHCP 地址池的结束 IP 地址。默认为 192.168.10.200。

标题项	说明
	 <b>注意</b> 起始 IP 和结束 IP 必须与 AC 的 LAN 口 IP 地址在同一网段。
网关	DHCP 服务器分配给 AP 的默认网关 IP 地址。可以设置为出口路由器的 LAN 口 IP 地址。 留空表示 DHCP 服务器不分配网关。
主 DNS	DHCP 服务器分配给 AP 的首选 DNS 服务器 IP 地址。 如果要使 AP 能够正常上网,请务必确保 DNS 地址是正确的 DNS 服务器或 DNS 代理的 IP 地址。 留空表示 DHCP 服务器不分配主 DNS。
备用 DNS	DHCP 服务器分配给 AP 的备用 DNS 服务器 IP 地址。留空表示 DHCP 服务器不分配备用 DNS。
租期	DHCP 服务器分配给 AP 的 IP 地址信息的有效时间。 当租约到达一半时, AP 会向 DHCP 服务器发送一个 DHCP Request, 请求更新自己的租约。如果续约成功, 则在续约申请的时间基础上续租; 如果续约失败, 则到了租期的 7/8 时, 再重复一次续约过程。如果成功, 则在续约申请的时间基础上续租, 如果仍然失败, 则租约到期后, AP 需要重新申请 IP 地址信息。 当租期满后, 如果 AP 没有续约请求, 服务器会收回该 IP 地址。

----完成

## 7.2.4 VLAN 配置

### 概述

AC 支持 IEEE 802.1q VLAN, 可以在已划分 VLAN 的环境中使用, 在这种情况下, 您可以将 AC 的 LAN 口添加到 1 个或多个 VLAN, 实现跨 VLAN 管理 AP。

### 配置 VLAN



- LAN 口添加 VLAN 后, 可以接收所添加 VLAN 的数据, 也可以接收不带 VLAN 的数据。
- 每个端口只能添加 1 次。如当“端口 1”添加过一次 VLAN 后, 再添加 VLAN 时, 将不能选择“端口 1”。

## 添加 VLAN 配置

1. 进入「系统工具」>「网络设置」页面，找到“VLAN 配置”模块。
2. 端口隔离：选择“开启”。
3. VLAN ID：输入 VLAN ID。



支持设置多个 VLAN ID，VLAN ID 中用短线 (-) 表示连续的 VLAN，用英文逗号 (,) 表示间隔的 VLAN。如 3-10,12 表示从 VLAN3 到 VLAN10，和 VLAN12，共计 9 个 VLAN。

4. 端口号：选择 VLAN ID 对应的物理端口，其中端口 1 是指 LAN1 口，端口 2 是指 LAN2 口，以此类推。

**VLAN 配置**

注：本设备最多支持48个不同VLAN。修改配置后，需要重启本设备才能生效

端口隔离  开启  关闭

VLAN ID  (例如：3-10,12)

端口号  端口 1  端口 2  端口 3  端口 4  端口 5

**添加**

序号	VLAN ID	端口号	操作
----	---------	-----	----

5. 点击该模块的 **添加**，将 VLAN 配置添加并保存到下方的 VLAN 列表。

**VLAN 配置**

注：本设备最多支持48个不同VLAN。修改配置后，需要重启本设备才能生效

端口隔离  开启  关闭

VLAN ID  (例如：3-10,12)

端口号  端口 1  端口 2  端口 3  端口 4  端口 5

**添加**

序号	VLAN ID	端口号	操作
1	1,2	1	

6. 进入「系统工具」>「维护」页面，在“升级维护”模块，点击 **重启**。

### ---完成

AC 重新启动后，修改的 VLAN 配置即可生效。

## 删除 VLAN 配置

1. 进入「系统工具」>「网络设置」页面，找到“VLAN 配置”模块。
2. 找到要删除的 VLAN 配置规则，点击操作栏的.
3. 如果出现操作确认的对话框，请点击 **确定**。
4. 进入「系统工具」>「维护」页面，在“升级维护”模块，点击 **重启**。

### ---完成

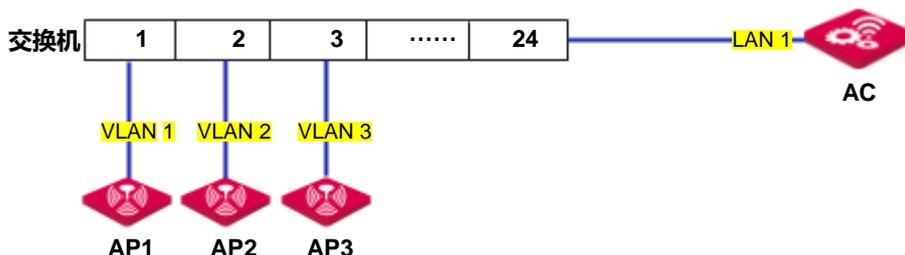
AC 重新启动后，修改的 VLAN 配置即可生效。

## VLAN 配置举例

### 组网需求

如下图，AC 要管理 3 台处于不同 VLAN 的 AP。

假设条件：1) AP 均已复位。2) AP 均连接在交换机的 Access 口。



### 配置步骤

#### 一、配置交换机

在交换机上配置 802.1q VLAN，具体配置情况如下表。

交换机端口	连接到	VLAN ID(允许通过的 VLAN)	端口属性	PVID
1	AP1	1	Access	1
2	AP2	2	Access	2
3	AP3	3	Access	3
24	AC	1,2,3	Trunk	1

#### 二、配置 AC

1. 进入「系统工具」>「网络设置」页面，找到“VLAN 配置”模块。

2. 端口隔离：选择“开启”。
3. VLAN ID：输入 VLAN ID，本例中为“1,2,3”。
4. 端口号：选择 VLAN ID 对应的物理端口，本例中 AP 接在 LAN0 口，应选择“端口 1”。
5. 点击该模块的 **添加**，将 VLAN 配置添加并保存到下方的 VLAN 列表。

**VLAN 配置**

注：本设备最多支持48个不同VLAN。修改配置后，需要重启本设备才能生效

端口隔离  开启  关闭

VLAN ID  (例如：3-10,12)

端口号  端口 1  端口 2  端口 3  端口 4  端口 5

**添加**

序号	VLAN ID	端口号	操作
1	1,2,3	1	

6. 进入「系统工具」>「维护」页面，在“升级维护”模块，点击 **重启**。

----完成

## 验证配置

AC 重新启动后，进入 AC 的「设备扫描」页面，可以看到 3 台 AP 均已被 AC 成功管理。

## 7.3 AP DHCP 列表

借助 AP DHCP 列表，您可以了解局域网中从 AC 的 DHCP 服务器获取 IP 地址的 AP 的 IP 地址、MAC 地址。

进入页面的方法：点击「系统工具」>「AP DHCP 列表」。

系统状态	网络设置	AP DHCP列表	维护	时间与日期	日志显示	网络检测
------	------	-----------	----	-------	------	------

 导出 备注, IP, MAC, 账号

用户总数1人 刷新 每页条数 10

序号	IP地址	MAC地址
1	192.168.10.180	c8:3a:35:00:1f:70

## 7.4 维护

AC 的「维护」模块包括：[授权激活](#)、[系统模式](#)、[用户管理](#)、[升级维护](#)。

进入页面的方法：点击「系统工具」>「维护」。

系统状态	网络设置	AP DHCP列表	维护	时间与日期	日志显示	网络检测
<b>授权激活</b>						
授权状态	已授权					
唯一识别码	5FA72883364B7845C61AD07AEE8CBED3		复制	如果复制无响应，请手动选取内容并复制		
可管理AP数量	128					
	当前地址池网段只能容纳101个AP，无法管理所有的AP，请修改AC的DHCP地址池大小。					
授权设备	文件导入					
<b>系统模式</b>						
设备名称	AC1000V1.0					
工作模式	<input checked="" type="radio"/> 从AC					
主AC控制器地址：	<input type="text"/> 主AC的出口路由公网地址或绑定的域名，格式为：ip/域名:端口号 (例如：http://www.ip-com.cn:8080)					
管理端口：	<input type="text"/>					
升级端口：	<input type="text"/>					
	确认					
<b>用户管理</b>						
原用户名	admin					
原密码	<input type="text"/>					
新用户名	<input type="text"/>					
新密码	<input type="text"/>					
确认新密码	<input type="text"/>					
	确认					
<b>升级维护</b>						
设备升级	选择文件					
设备重启	重启					
备份配置	备份					
恢复配置	选择文件					
恢复出厂设置	恢复					

## 7.4.1 授权激活

AC 在出厂时，IP-COM 已经对它进行了授权，使其最多可同时管理 128 台 AP。用户无需自行进行授权激活操作。

## 7.4.2 系统模式

IP-COM AC1000 的工作模式为“从 AC”，可以管理局域网中的 IP-COM AP，还可以被工作在“主 AC”模式下的 IP-COM AC2000 管理。

**系统模式**

设备名称	<input type="text" value="AC1000V1.0"/>
工作模式	<input checked="" type="radio"/> 从 AC
主 AC 控制器地址：	<input type="text"/> 主 AC 的出口路由由公网地址或绑定的域名，格式为：ip/域名：端口号（例如：http://www.ip-com.cn:8080）
管理端口：	<input type="text"/>
升级端口：	<input type="text"/>
<input type="button" value="确认"/>	

### 参数说明

标题项	说明
设备名称	该台 AC 的名称。 如果网络中有多台 AC1000，或本 AC 需要被 IP-COM AC2000 管理，建议修改本 AC 的设备名称，以便于网络管理员区分各 AC 设备。
工作模式	本 AC 的工作模式为“从 AC”，表示本 AC 既可以管理局域网中的 IP-COM AP，又可以被互联网上的“ <a href="#">主 AC</a> ”管理。
主 AC 控制器地址	仅当本 AC 需要被主 AC 管理时设置。 输入主 AC 的出口路由器公网 IP 地址（WAN 口 IP 地址）或公网 IP 地址绑定的域名。
管理端口	仅当本 AC 需要被主 AC 管理时设置。 设置为主 AC 用于管理本 AC 的端口，需要确保主 AC 与本 AC 上设置的管理端口一致。
升级端口	仅当本 AC 需要被主 AC 管理时设置。 设置为主 AC 用于升级本 AC 的端口，需要确保主 AC 与本 AC 上设置的升级端口一致。

## 主 AC+从 AC+AP 组网举例

### 组网需求

某连锁酒店进行无线组网。要求：各分店的 AP 能集中管理；总部管理人员无需亲临分店，就能了解分店的入住率情况。

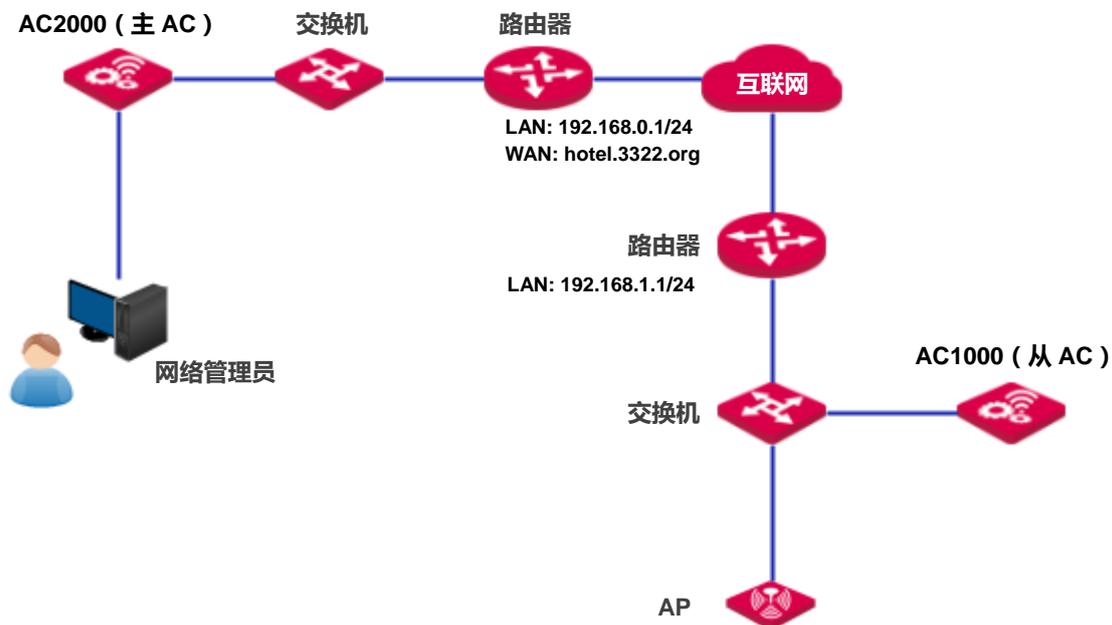
可以使用 IP-COM AC2000+AC1000+AP 实现上述需求，具体如下：

- 在各分店，部署多台 AP 作为无线接入设备。
- 在各分店，部署一台 AC1000，工作在“从 AC”模式，集中管理所在分店的 AP。
- 在总部，部署一台 AC2000，工作在“主 AC”模式，集中管理各分店的 AC1000。

假设条件：

- AC2000 连接的出口路由器的公网 IP 地址绑定的域名为“hotel.3322.org”。
- AC2000 连接的出口路由器的 LAN 口 IP 为 192.168.0.1/24，并且有 DNS 代理功能。
- AC1000 连接的出口路由器的 LAN 口 IP 为 192.168.1.1/24，并且有 DNS 代理功能。
- 管理端口为“6060”，升级端口为“9090”。

### 组网图



### 配置步骤



提示

以一个分店为例说明，其他分店类似。

## 一、配置 AP

AP 即插即用，无需进行配置。

## 二、配置 AC1000

### 步骤 1：配置系统模式。

1. 登录到 AC1000 的 Web 管理页面，进入「系统工具」>「维护」页面，找到“系统模式”模块。
2. 设备名称：为了便于总部管理员定位各从 AC，建议设置为所在分店地址。
3. 主 AC 控制器地址：输入 AC2000 的出口路由器公网 IP 绑定的域名，本例为“hotel.3322.org”。
4. 管理端口：输入 AC2000 管理 AC1000 的端口，本例为“6060”。
5. 升级端口：输入 AC2000 升级 AC1000 的端口，本例为“9090”。
6. 点击 **确认**。

**系统模式**

设备名称	<input type="text" value="深圳南山"/>
工作模式	<input checked="" type="radio"/> 从AC
主AC控制器地址：	<input type="text" value="hotel.3322.org"/> <small>主AC的出口路由公网地址或绑定的域名，格式为：ip/域名：端口号（例如：http://www.ip-com.cn:8080）</small>
管理端口：	<input type="text" value="6060"/>
升级端口：	<input type="text" value="9090"/>
<input type="button" value="确认"/>	

### 步骤 2：进行联网配置。

1. 进入「系统工具」>「网络设置」页面，找到“外网配置”模块。
2. IP 地址：与 AC1000 的出口路由器的 LAN IP 设置在同一网段，如“192.168.1.100”。
3. 子网掩码：与 AC1000 的出口路由器的 LAN IP 的子网掩码保持一致，本例为“255.255.255.0”。
4. 网关：输入 AC1000 的出口路由器的 LAN IP 地址，本例为“192.168.1.1”。
5. 主 DNS：输入正确的 DNS 服务器或 DNS 代理服务器地址，本例为“192.168.1.1”。
6. 点击 **确认**。

**外网配置**

IP地址	<input type="text" value="192.168.1.100"/>
子网掩码	<input type="text" value="255.255.255.0"/>
网关	<input type="text" value="192.168.1.1"/>
主DNS	<input type="text" value="192.168.1.1"/>
备用DNS	<input type="text"/>

### 三、配置 AC2000

#### 步骤 1：配置系统模式。

1. 登录到 AC2000 的 Web 管理页面，进入「系统工具」>「维护」页面，找到“系统模式”模块。
2. 设备名称：为了便于总部管理员定位本 AC，建议设置为总部地址。
3. 工作模式：选择“主 AC”。
4. 管理端口：输入 AC2000 用于管理 AC1000 的端口，本例为“6060”。
5. 升级端口：输入 AC2000 用于升级 AC1000 的端口，本例为“9090”。
6. 点击 **确认**。

**系统模式**

设备名称	<input type="text" value="北京"/>
工作模式	<input type="radio"/> 从AC <input checked="" type="radio"/> 主AC <input type="radio"/> 云AC
管理端口：	<input type="text" value="6060"/>
升级端口：	<input type="text" value="9090"/>

#### 步骤 2：进行联网配置。

1. 待 AC2000 重新启动后，重新登录到 AC2000 的管理页面，进入「系统工具」>「网络设置」页面。
2. IP 地址：与 AC2000 的出口路由器的 LAN IP 设置在同一网段，如“192.168.0.100”。
3. 子网掩码：与 AC2000 的出口路由器的 LAN IP 的子网掩码保持一致，本例为“255.255.255.0”。
4. 网关：输入 AC2000 的出口路由器的 LAN 口 IP 地址，本例为“192.168.0.1”。
5. 主 DNS：输入正确的 DNS 服务器或 DNS 代理服务器地址，本例为“192.168.0.1”。

## 6. 点击 **确认**。

[网络设置](#)[设备维护](#)[用户管理](#)[时间与日期](#)[日志显示](#)[网络检测](#)

### 内网配置

IP地址

子网掩码

网关

主DNS

备用DNS

## 四、配置 AC2000 的出口路由器

在 AC2000 侧的出口路由器上进行端口映射，分别将 TCP 端口 6060（管理端口）和 9090（升级端口）映射到 AC2000。

具体配置方法请参考出口路由器的说明书。

## 验证配置

完成上述设置后，登录到 AC2000 的管理页面，转到「设备管理」>「AC 列表」页面，点击**刷新**，可以看到该 AC1000 已经成功被 AC2000 管理。

## 7.4.3 用户管理

您可以修改 AC 管理页面的登录账号信息，防止非授权用户进入 AC 的管理页面更改设置，影响无线网络正常使用。

### 用户管理

原用户名

原密码

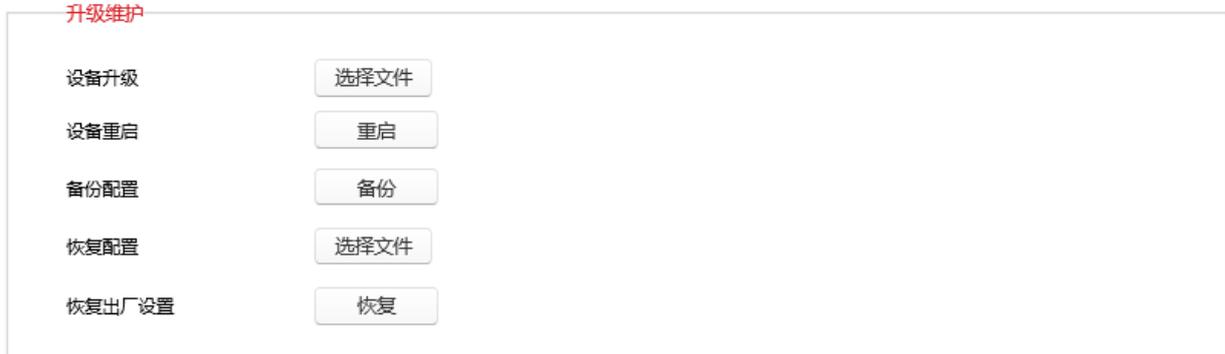
新用户名

新密码

确认新密码

## 7.4.4 升级维护

在这里，您可以对 AC 进行软件升级、重启、备份/恢复配置、恢复出厂设置。



### 设备升级

如果 AC 在某些特殊环境下使用不正常，建议您访问 IP-COM 官网 <http://www.ip-com.com.cn>，搜索是否有针对该问题发布的软件，对 AC 软件进行升级，以完善产品对某些特殊环境、应用的支持。



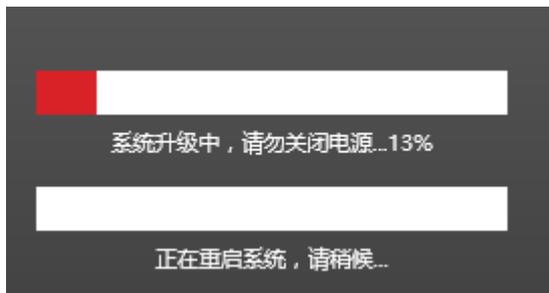
升级过程中，请勿断开 AC 电源，否则可能造成 AC 损坏！若是突发断电，请重新进行升级；若突发断电后无法进入 AC 的 Web 管理页面，请联系售后维修。

#### 设备升级步骤：

1. 访问 IP-COM 官网 <http://www.ip-com.com.cn>，下载本 AC 的升级文件到本地电脑。
2. 登录 AC 的 Web 管理页面，转到「系统工具」>「维护」页面的“升级维护”模块。
3. 设备升级：点击 **选择文件**，从本地电脑选择并加载 AC 的升级软件。
4. 如果出现操作确认的对话框，请点击 **确定**。

#### ---完成

会出现升级/重启进度条，如下图所示，请等待进度条走完即可。



## 设备重启

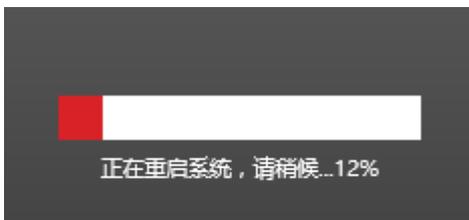
当您设置的某项参数不能正常生效时，可以尝试重启 AC 解决。

### 设置步骤：

1. 进入「系统工具」>「维护」页面，找到“升级维护”模块。
2. 设备重启：点击 **重启**。
3. 如果出现操作确认的对话框，请点击 **确定**。

----完成

会出现进度条，如下图所示，请等待进度条走完即可。



AC 重启时，会自动断开所有连接。请在网络相对空闲的时候进行重启操作。

## 备份配置

如果您对 AC 进行了大量的配置，使其在运行时拥有较好的状态/性能，或更符合对应环境的需求，此时建议对该配置进行备份。

### 备份步骤：

1. 进入「系统工具」>「维护」页面，找到“升级维护”模块。
2. 备份配置：点击 **备份**，之后按页面提示操作。

----完成

## 恢复配置

如果您需要对多台 AC 进行相同的配置；或您不经意进行了某些操作，导致 AC 性能下降，此时，可以使用恢复配置功能，将 AC 配置还原到之前备份的配置。

### 恢复步骤：

1. 进入「系统工具」>「维护」页面，找到“升级维护”模块。

2. 恢复配置：点击 **选择文件**，选择并加载之前备份的配置文件。
3. 如果出现操作确认的对话框，请点击 **确定**。

#### ---完成

会出现进度条，如下图所示，请等待进度条走完即可。



## 恢复出厂设置

如果您需要将 AC 的配置恢复至出厂状态，可以使用本功能。

#### 设置步骤：

1. 进入「系统工具」>「维护」页面，找到“升级维护”模块。
2. 恢复出厂设置：点击“恢复”。
3. 如果出现操作确认的对话框，请点击 **确定**。

#### ---完成

会出现进度条，如下图所示，请等待进度条走完即可。



## 7.5 时间与日期

在这里，您可以设置 AC 的系统时间，以保证 AC 的日志记录等功能时间执行准确。您还可以设置 AC 的 Web 登录超时时间。

进入页面的方法：点击「系统工具」>「时间与日期」。

系统状态	网络设置	AP DHCP列表	维护	时间与日期	日志显示	网络检测
系统时间	2017-06-13 15:07:31		同步PC时间			
时区	( GMT+08:00 ) 北京, 重庆, 香港					
NTP 网络校时	<input checked="" type="checkbox"/> 开启					
校时周期	30分钟					
超时时间	5 分钟					
<input type="button" value="确认"/>						

### 参数说明

标题项	说明
系统时间	显示 AC 当前的系统时间。
同步时间	点击后，将当前正在管理 AC 的电脑的时间同步到 AC。 登录时，若 AC 的系统时间与本地电脑时间不一致，AC 将自动同步本地电脑时间。
时区	选择 AC 当前所在地区的 GMT 标准时区。
NTP 网络校时	开启/关闭 NTP 网络校时功能。 开启后，AC 将每隔校时周期所设置的时间段，自动向互联网上的时间服务器校对其系统时间。
校时周期	NTP 网络校时的校时间隔，默认为 30 分钟。
超时时间	如果用户登录到 AC 的 Web 管理页面，在所设置的超时时间内没有任何操作，系统将自动退出登录。 默认值为 5 分钟。

### 7.5.1 NTP 网络校时

系统时间自动同步互联网上的时间服务器。使用此方式时，只要 AC 成功连接至互联网就能自动校准其系统时间，即使 AC 经历重启，也能自行校准，无需网络管理员重新设置。

AC 联网方法：进入「系统工具」>「网络校时」页面，在“外网配置”模块进行配置。

**NTP 网络校时设置步骤：**

1. 进入「系统工具」>「时间与日期」页面。
2. 时区：选择 AC 当前所在地区的 GMT 标准时区，如中国需选择“(GMT+08:00)北京, 重庆, , 香港特别行政区, 乌鲁木齐”。
3. NTP 网络校时：勾选“开启”。
4. 校时周期：建议保持默认“30 分钟”。
5. 点击 **确认**。

系统状态	网络设置	AP DHCP列表	维护	时间与日期	日志显示	网络检测
------	------	-----------	----	-------	------	------

系统时间	2017-07-13 15:44:19	同步PC时间
时区	(GMT+08:00) 北京, 重庆, 香港	
NTP 网络校时	<input checked="" type="checkbox"/> 开启	
校时周期	30分钟	
超时时间	5	分钟
<b>确认</b>		

----完成

## 7.5.2 同步 PC 时间

1. 进入「系统工具」>「时间与日期」页面。
2. 点击 **同步 PC 时间**。

系统状态	网络设置	AP DHCP列表	维护	时间与日期	日志显示	网络检测
------	------	-----------	----	-------	------	------

系统时间	2017-07-13 15:47:13	同步PC时间
时区	(GMT+08:00) 北京, 重庆, 香港	
NTP 网络校时	<input checked="" type="checkbox"/> 开启	
校时周期	30分钟	
超时时间	5	分钟
<b>确认</b>		

----完成

## 7.6 日志显示

本 AC 提供的日志系统能够对 AP 连接及告警等信息进行记录和分类，为网络管理员监控网络运行情况和诊断网络故障提供了强有力的支持。

进入页面的方法：点击「系统工具」>「日志显示」。

系统状态	网络设置	AP DHCP列表	维护	时间与日期	日志显示	网络检测
日志总条数：12条 <a href="#">刷新</a> <a href="#">导出日志</a> <a href="#">清空日志</a>						每页条数 <input type="text" value="10"/>
序号	时间	类型	内容			
12	2017-06-30 10:27:17	事件日志	管理员登陆			
11	2017-06-30 10:01:50	事件日志	管理超时退出			
10	2017-06-30 09:34:08	事件日志	管理员登陆			
9	2017-06-30 09:08:50	事件日志	管理超时退出			
8	2017-06-30 09:03:28	事件日志	管理员登陆			
7	2017-06-30 09:02:50	事件日志	管理超时退出			
6	2017-06-30 08:50:49	事件日志	管理员登陆			
5	2017-06-29 18:02:50	事件日志	管理超时退出			
4	2017-06-29 17:46:27	事件日志	管理员登陆			
3	2011-05-01 00:01:05	告警日志	AP状态: AP(AP325V1.0 MAC = D8:38:0D:00:1f:70)加入AC的管理列表			
<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> 跳转至: <input type="text" value="1"/> <input type="button" value="Go"/>						

如果需要查看最新的日志信息，请点击[刷新](#)；如果需要把 AC 的日志导出到本地电脑并保存，请点击[导出日志](#)；如果需要清空当前所有的日志信息，请点击[清空日志](#)。



注意

- 重启 AC 会丢失已记录的（重启之前的）日志信息。
- 断电后重新通电、恢复出厂设置、软件升级等操作都会导致 AC 重启。

## 7.7 网络检测

AC 提供了网络检测功能，包含了 Ping 和 Traceroute 两个工具，用于检测网络故障。

进入页面的方法：点击「系统工具」>「网络检测」。

系统状态    网络设置    AP DHCP列表    维护    时间与日期    日志显示    **网络检测**

网络工具：

目标IP/域名：

Ping包数量： 1-32

Ping包大小： 32-1464 单位：字节

### 7.7.1 Ping

当网络出现故障时，借助 Ping 工具，您可以快速地定位出网络具体是在哪个节点出现了故障。

#### 执行诊断：

假设要检测局域网主机“192.168.10.168”是否畅通。

1. 进入「系统工具」>「网络检测」页面。
2. 网络工具：选择“Ping”。
3. 目标 IP/域名：输入目的主机的 IP 地址或域名，本例为“192.168.10.168”。
4. Ping 包数量：建议保持默认“4”。
5. Ping 包大小：建议保持默认“32”。
6. 点击 **开始**。

稍后，诊断结果将显示在本页面的方框中。如下图示例。

系统状态

网络设置

AP DHCP列表

维护

时间与日期

日志显示

网络检测

网络工具：

目标IP/域名：

Ping包数量： 1-32

Ping包大小： 32-1464 单位：字节

```
32 bytes from 192.168.10.168: ttl=128 time=0.799
32 bytes from 192.168.10.168: ttl=128 time=0.813
32 bytes from 192.168.10.168: ttl=128 time=0.917
32 bytes from 192.168.10.168: ttl=128 time=1.323
---192.168.10.168 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.799/0.963/1.323ms
```

## 7.7.2 Traceroute

借助 Traceroute 工具，您可以了解数据包从 AC 走到目的主机所采取的路径。

### 执行诊断：

假设要检测数据从 AC 到百度“www.baidu.com”所采取的路径。

1. 进入「系统工具」>「网络检测」页面。
2. 网络工具：选择“Traceroute”。
3. 目标 IP/域名：输入目的主机的 IP 地址或域名，本例为“www.baidu.com”。
4. 点击 **开始**。

稍后，诊断结果将显示在本页面的方框中。如下图示例。

系统状态

网络设置

AP DHCP列表

维护

时间与日期

日志显示

网络检测

网络工具：

目标IP/域名：

```
traceroute to www.baidu.com (163.177.151.110), 3 hops
max, 38 byte packets
 1 192.168.110.100 (192.168.110.100) 0.323 ms 0.207 ms
0.180 ms
 2 172.16.200.1 (172.16.200.1) 0.479 ms 0.423 ms 0.403 ms
 3 192.168.20.1 (192.168.20.1) 1.507 ms 2.698 ms 2.433 ms
```

# 附录

## 常见问题解答

**问 1：输入“192.168.10.1”登录不了 AC 的管理页面，怎么办？**

答：请从以下方面检查。

- 确保网线连接正确，且网线无松动现象。
- 确认电脑的本地连接 IP 地址为 192.168.10.X ( X 为 2~254 )。
- 清空浏览器的缓存或使用别的浏览器进行尝试。
- 关闭电脑的防火墙或使用别的电脑进行尝试。
- 确认局域网内没有 IP 地址也为 192.168.10.1 的其他设备。
- 若经过上述操作仍无法登录，请将 AC 恢复出厂设置再重新操作。

**问 2：在无法进入 AC 管理页面的情况下，怎么将 AC 恢复出厂设置？**

答：AC 启动完成的状态下，用针状物按住机身前面板的“RESET”按钮 7 秒后松开，等待约 2 分钟即可。

**问 3：AC 扫描不到 AP，怎么办？**

答：请从以下方面检查。

- 确认设备连接正确，AP 已正常启动。
- 若网络已划分 VLAN，确认 AC 已添加了对应的 VLAN。
- 重启 AP 或将 AP 恢复出厂设置再尝试扫描。

**问 4：无线设备连接 AP 时，连接不上或连接上后显示“受限制或无连接”，此时查看其 IP 地址，发现为 169.254.X.X，怎么办？**

答：本 AC 提供的 DHCP 服务器只给 IP-COM AP 分配 IP 地址，不会给其他无线设备分配 IP 地址。如果无线设备需要自动获取 IP 地址上网，请在网络中另外架设一台 DHCP 服务器，给其分配 IP 地址。

## 默认参数

出厂时，AC 的各项参数默认设置如下：

参数	默认设置		
设备登录	登录 IP	192.168.10.1	
	用户名	admin	
	密码	admin	
策略配置	SSID 策略	1 条	
	射频策略	1 条	
	VLAN 策略	无	
	高级策略	无	
外网配置	无		
网络设置	内网配置	IP 地址	192.168.10.1
		子网掩码	255.255.255.0
	DHCP 配置	地址池起始 IP	192.168.10.100
		地址池结束 IP	192.168.10.200
		网关	无
		主 DNS	无
		备用 DNS	无
		租期	一周
VLAN 配置	关闭		
时间与日期	时区	( GMT+08:00 ) 北京, 重庆, 香港特别行政区, 乌鲁木齐	
	NTP 网络校时	开启	
	校时周期	30 分钟	
	超时时间	5 分钟	