

# 1 通过云简网络禁止部分用户接入 Wi-Fi

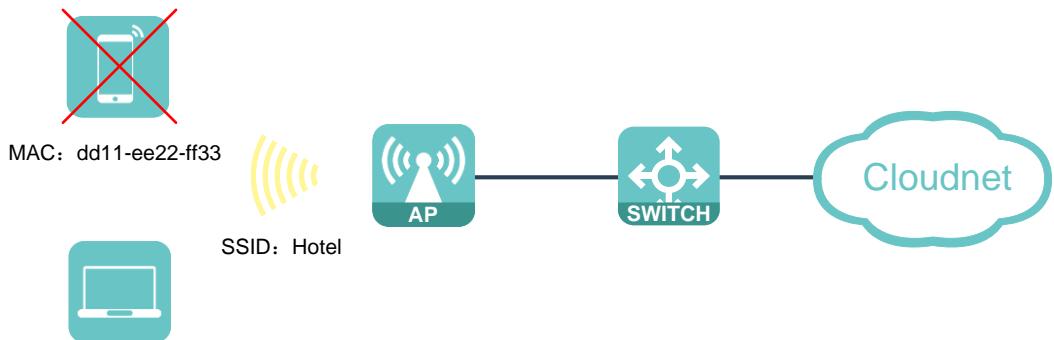
## 1.1 适用场景

云简网络的 MAC 黑名单功能，可以禁止匹配黑名单表项中 MAC 地址的用户接入 Wi-Fi，适用于安全性要求高的场景。

## 1.2 组网需求

如下图所示，交换机为云 AP 进行 PoE 供电，云 AP 直连接入交换机，并添加至云简网络，为无线客户端提供无线接入服务。现要求：检查通过 Wi-Fi 名称为 Hotel 的无线网络接入的用户，禁止 MAC 地址为 dd11-ee22-ff33 的用户接入。

图1 MAC 黑名单组网图



## 1.3 配置步骤

- (1) 在网络管理页面的左侧边栏选择[配置/云 AP/无线配置]，进入云 AP 的无线配置页面，在页面左上角选择云 AP 所在的场所。

图2 选择场所

分支：我的网络 场所：演示场景

Wi-Fi配置 | 射频配置 | 网络优化

无线服务配置 (部分云AP款型仅支持配置序号1-7的无线服务，支持情况详见《版本说明》)

自动SSID功能提示  
若当前场所的无线服务开启了自动SSID功能，在手动修改AP名称或执行了批量导入AP操作后需要执行自动SSID配置写入设备

序号	SSID	服务状态	隐藏SSID	加密状态
1	H3C_1EF704	开启	开启	关闭
2	Hotel	开启	关闭	PSK

显示第 1 ~ 2 条记录(总共 2 条记录)

- (2) 选择“Wi-Fi 配置”页签，在无线服务配置栏目中，点击 SSID 为 Hotel 的无线服务，进入 Wi-Fi 配置页面。在 Wi-Fi 配置页面开启终端 MAC 过滤功能，勾选黑名单选项，点击<配置黑名单>按钮跳转至 MAC 黑名单配置页面。

图3 开启终端 MAC 过滤功能

Wi-Fi配置

AP转发方式：Bridge模式

VLAN：14

隐藏SSID：关闭

加密状态：PSK

密码输入框（说明：密码为8~63位字符串，可以包含数字、字母、特殊字符('?'除外))

安全方式：WPA / WPA2兼容

\* Radio类型：2.4GHz, 5GHz

用户隔离：关闭

用户限速：关闭

认证：开启

认证逃生：关闭

终端MAC过滤：ON

黑名单

配置黑名单

白名单

配置白名单

确定 取消

(3) 在 MAC 黑名单配置页面，点击<增加>按钮，在弹窗中配置禁止接入的 MAC 地址，MAC 地址/掩码不区分大小写，由“-”或“:”分隔，支持如下四种格式：

- XX-XX-XX-XX-XX-XX
- XXXX-XXXX-XXXX
- XX:XX:XX:XX:XX:XX
- XX-XX-XX (识别为 00-xx-00-xx-00-xx)

本例中将 MAC 地址配置为 dd11-ee22-ff33，MAC 掩码为 ffff-ffff-ffff，然后点击<确定>按钮完成 MAC 黑名单表项添加。最后返回 Wi-Fi 配置页面，点击<确定>按钮完成配置。此时场所中所有云 AP 将禁止 MAC 地址为 dd11-ee22-ff33 的终端接入。



#### 说明

MAC 掩码用来与 MAC 地址做与运算，得到黑名单功能检查的 MAC 地址范围，掩码 f 说明进行检查，例如：检查某个 MAC 地址的前三个字节，将掩码配置为 ffff-ff00-0000。

图4 配置 MAC 黑名单表项



## 1.4 验证配置

完成配置后，MAC 地址前三字节为 dd11-ee22-ff33 的终端将无法接入名称为 Hotel 的 Wi-Fi。