

## 403 Forbidden

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。注册版本不会显示该信息。[删除广告](#)

# V7 AC从54xx版本后支持基于SSID或AP的黑白名单功能（命令行版）

## 目录

### [V7 AC从54xx版本后支持基于SSID或AP的黑白名单功能（命令行版）](#)

#### [1 配置需求或说明](#)

##### [1.1 适用产品系列](#)

##### [1.2 配置需求及实现的效果](#)

#### [2 组网图](#)

#### [3 配置步骤](#)

##### [3.1 创建一个二层acl4000，仅允许MAC地址为000e-35b2-000e的客户端接入](#)

##### [3.2 在无线服务模板或者AP视图下调用该acl](#)

#### [4 注意事项](#)

# 1 配置需求或说明

## 1.1 适用产品系列

本手册适用于如下产品：V7 平台54xx版本以后的无线控制器产品，包含：WX2500H系列、WX3000H系列、WX3500H 系列、WX5500E(V7) 系列、WX5500H系列、AC插卡(V7)系列、WAC380系列等。

## 1.2 配置需求及实现的效果

V7平台54xx以前的版本，可以通过针对该ssid做mac认证实现限制只能某些mac终端接入该ssid，但无法做到限制某些mac地址终端不能接入该ssid。

V7平台54xx以后的版本，可以通过在服务模板视图或者AP视图下调用二层acl实现限制部分mac无法上网的功能。

# 2 组网图



## 3 配置步骤

### 3.1 创建一个二层acl4000，仅允许MAC地址为000e-35b2-000e的客户端接入

```
<H3C>system-view
[H3C] acl mac 4000
[H3C-acl-mac-4000] rule 0 permit source-mac 000e-35b2-000e ffff-ffff-ffff
[H3C-acl-mac-4000] rule 2 deny
[H3C-acl-mac-4000] quit
```

### 3.2 在无线服务模板或者AP视图下调用该acl

方法一：在服务模板下调用

```
[H3C] wlan service-template 1
[H3C-wlan-st-1] access-control acl 4000
[H3C-wlan-st-1]quit
```

方法二：在AP视图下调用

```
[H3C] wlan ap 1
[H3C-wlan-ap-1] access-control acl 4000
[H3C-wlan-ap-1]quit
```

## 4 注意事项

- 1、基于ACL的接入控制的优先级高于基于名单的接入控制的优先级，建议两种接入控制**单独使用**。  
如果同时配置了两种接入控制，当设备上没有配置无线客户端访问控制规则时，按照基于名单的接入控制规则对无线客户端进行访问控制。
- 2、在ACL中配置deny规则来拒绝指定客户端接入时，请在deny规则之后配置允许所有客户端接入的permit规则，否则会导致所有客户端无法接入。
- 3、AP视图下配置的优先级高于无线服务模板视图下的配置。
- 4、基于ACL的接入控制只匹配source mac地址二层ACL规则。