

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](#)

WAC380系列产品本地MAC认证配置案例（WEB版）

目录

[WAC380系列产品本地MAC认证配置案例（WEB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 在无线控制器上配置相关VLAN及对应虚接口的地址](#)

[3.2 配置本地认证域](#)

[3.3 配置本地用户](#)

[3.4 配置无线服务](#)

[3.5 配置Switch](#)

[3.6 实验结果验证](#)

1 配置需求或说明

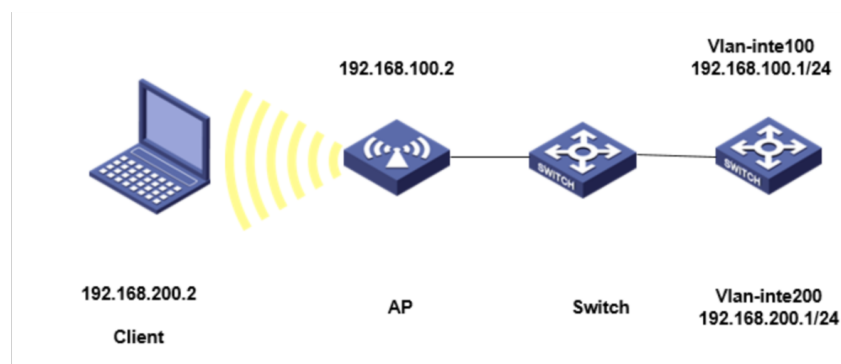
1.1 适用产品系列

本手册适用于如下产品：WAC380、WAC381系列产品：WAC380-30、WAC380-60、WAC380-90、WAC380-120、WAC381。

1.2 配置需求及实现的效果

组网中，注册VLAN是VLAN100，业务VLAN是VLAN200，无线电脑连接SSID: service后，无线电脑终端通过设备的MAC认证之后，获取到网关vlan200的IP地址：192.168.200.0/24，实现对无线用户的统一管理 and 认证功能。现使用WAC380作为无线网络的网关设备。通过对终端设备的MAC进行认证，达到对用户访问进行控制的目的。

2 组网图



3 配置步骤

3.1 在无线控制器上配置相关VLAN及对应虚接口的地址

提示：AP注册、相关VLAN及对应虚接口的地址、DHCP服务器配置、放通对应接口详细步骤参考：《2.2.11 WAC380不同SSID不同VLAN配置方法（WEB版）》，此案例省略。

3.2 配置本地认证域

#点击“系统”>“网络安全”>“认证”>“ISP域”，新增ISP域。创建一个名称为mac的认证域，为lan-access用户配置认证、授权、计费方法为本地认证。

包过滤

流策略

访问控制

认证

BYOD

用户管理

来宾管理

接入管理

系统

工具

全部网络 > 网络安全 > 认证 > ISP域 > 添加ISP域

域名 *

mac

状态

活动

接入方式

☐ 登录用户

☒ LAN接入

☐ Portal

LAN接入AAA方案

认证

☐ RADIUS

☒ 本地认证

☐ 不认证

授权

☐ RADIUS

☒ 本地授权

☐ 不授权

计费

☐ RADIUS

☒ 本地计费

☐ 不计费

#配置用户闲置切断时间为15分钟，闲置切断时间内产生的流量为1024字节。

点击菜单：显示高级设置

全部网络 > 网络安全 > 认证 > ISP域 > 添加ISP域

授权

☐ RADIUS

☐ 本地授权

☒ 不授权

计费

☐ RADIUS

☐ 本地计费

☒ 不计费

用户闲置切断时间

15

分钟 (1-600)

用户在闲置切断时间内产生的数据流量

1024

字节 (1-10240000, 缺省为10240)

为PPP用户分配IP地址的地址池

(1-63字符)

隐藏高级设置...

确定

取消

3.3 配置本地用户

#点击“系统”>“网络安全”>“用户管理”>“添加用户”，配置一个网络接入类的本地用户，名称为客户端的MAC地址b0eb57595cea，密码为明文密码b0eb57595cea(同账号)，并指定用户可以使用lan-access服务。

说明：默认情况下MAC地址认证的用户名格式为小写不带横杠。

The screenshot displays the 'Add User' configuration page. The breadcrumb path is '系统 > 网络安全 > 用户管理 > 本地用户 > 添加用户'. The left sidebar shows the navigation menu with '用户管理' (User Management) selected. The main form contains the following fields:

- 用户名 *** (Username): b0eb57595cea (1-55 characters)
- 密码** (Password): Masked with dots (1-63 characters)
- 确认密码** (Confirm Password): Masked with dots (1-63 characters)
- 描述** (Description): (1-127 characters)
- 授权用户组** (Authorization User Group): 请选择... (Please select...)
- 可用服务** (Available Services): ☐ ADVPN ☐ IKE ☐ IPsec ☒ LAN接入 ☐ Portal ☐ PPP ☐ SSL VPN
- 同时在线最大用户数** (Concurrent Maximum Users): (1-1024)
- 授权属性** (Authorization Attributes): 授权ACL (Authorization ACL)

3.4 配置无线服务

#点击“全部网络”>“无线配置”>“无线网络”>“无线服务”，创建无线服务模板service，配置SSID为service，无线服务模板VLAN为200，配置客户端接入认证方式为MAC地址认证，配置MAC地址认证用户使用的ISP域为mac。配置静态PKS认证，输入wifi的密码：12345678，和输入确认密码：12345678，再使能无线服务模板。点击：确认并进入高级设置。

点击绑定菜单，将服务模板与ap绑定，将ap选择到右侧已选择。最后点击确定。

3.5 配置Switch

#创建VLAN 100，其中VLAN 100用于转发AC和AP间CAPWAP隧道内的流量，VLAN 200用于转发Client无线报文。

<H3C> system-view

[H3C] vlan 100

[H3C-vlan200] quit

#配置Switch与WAC380相连的GigabitEthernet1/0/1接口的属性为

Trunk，禁止VLAN 1报文通过，允许VLAN 100通过，配置当前Trunk口的PVID为100。

```
[H3C] interface gigabitethernet1/0/1
```

```
[H3C-GigabitEthernet1/0/1] port link-type trunk
```

```
[H3C-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[H3C-GigabitEthernet1/0/1] port trunk permit vlan 100
```

```
[H3C-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[H3C-GigabitEthernet1/0/1] quit
```

#配置Switch与AP相连的GigabitEthernet1/0/2接口属性为Access，并允许VLAN 100通过

```
[H3C] interface gigabitethernet1/0/2
```

```
[H3C-GigabitEthernet1/0/2] port link-type access
```

```
[H3C-GigabitEthernet1/0/2] port access vlan 100
```

#开启PoE接口远程供电功能

```
[H3C-GigabitEthernet1/0/2] poe enable
```

```
[H3C-GigabitEthernet1/0/2] quit
```

3.6 实验结果验证

#无线用户Client通过连接到WLAN网络并进行本地MAC认证，用户在通过认证后。

通过执行以下显示命令查看WAC上生成的无线在线用户信息。Web界面点击监控-客户端进行查看。

```
<H3C> display wlan client
```

```
Total Number of Clients : 1
```

MAC address	User name	AP name	RID	IP address	IPv6 address
b0eb-5759-5cea	b0eb57595cea	officeap	2	192.168.200.2	-
NA-	200				

#未通过认证的设备不能不能进行接入。