

知 V7 AC系列产品本地MAC认证配置案例（命令行版）

MAC地址认证 樊凡 2020-09-14 发表

组网及说明

1 配置需求或说明

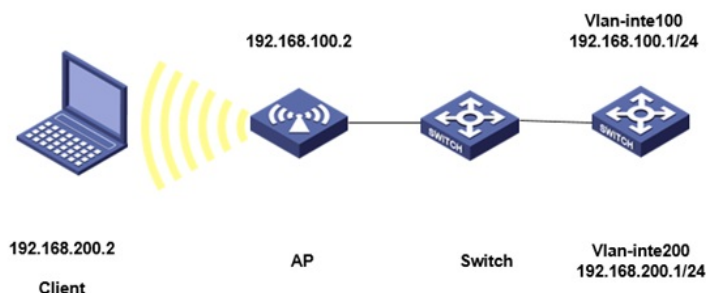
1.1 适用产品系列

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,以及WX1804H、WX2510H、WX3010H、WX3508H、WX5540H等WX18H、WX25H、WX30H、WX35H、WX55H系列的AC。。

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和认证功能。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



配置步骤

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：《2.2.14 WAC360不同SSID不同VLAN配置方法（命令行）》，此案例省略。

3.2 配置本地认证域

#新增ISP域。创建一个名称为local-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。

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。

```
[AC] domain local-mac
```

```
[AC-isp-local-mac] authentication lan-access local
```

```
[AC-isp-local-mac] accounting lan-access local
```

```
[AC-isp-local-mac] authorization lan-access local
```

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。

```
[AC-isp-local-mac] authorization-attribute idle-cut 15 1024
```

```
[AC] quit
```

3.3 配置本地用户

#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。

```
[AC] local-user b0eb57595cea class network
```

```
[AC-luser-network-3ca9f4144c20] password simple b0eb57595cea
```

```
[AC-luser-network-3ca9f4144c20] service-type lan-access
```

```
[AC-luser-network-3ca9f4144c20] quit
```

配置MAC地址认证的用户名和密码均为用户的MAC地址

默认情况下MAC地址认证的用户名格式为小写不带横杠，该配置为缺省配置。

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

3.4 配置无线服务

创建无线服务模板1，配置SSID为service，

```
[AC] wlan service-template 1
```

```
[AC-wlan-st-1] ssid service
```

#无线服务模板VLAN为200

```
[AC-wlan-st-1] vlan 200
```

#配置客户端接入认证方式为MAC地址认证，

```
[AC-wlan-st-1] client-security authentication-mode mac
```

#配置MAC地址认证用户使用的ISP域为local-mac。

```
[AC-wlan-st-1] mac-authentication domain local-mac
#配置静态PKS认证，输入wifi的密码：12345678，
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
#配置使用AES-CCMP作为加密套件，使用RSN作为安全信息元素
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
#再使能无线服务模板。
[AC-wlan-st-1] service-template enable
```

3.5 配置射频接口并绑定服务模板

```
# 创建手工AP，名称为officeap，型号名称为WA4320i-ACN。
[AC] wlan ap officeap model WA4320i-ACN
# 设置AP序列号为210235A1Q2C159000019。
[AC-wlan-ap-officeap] serial-id 210235A1Q2C159000019
# 进入AP的Radio 2视图，并将无线服务模板1绑定到Radio 2上。
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap-radio-2] service-template 1
# 开启Radio 2的射频功能。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

3.6 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
```

3.7 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	VLAN
b0eb-5759-5cea	b0eb57595cea	officeap	2	192.168.200.2	-NA-	200

#未通过认证的设备不能进行接入。

配置关键点

无