H3C 无线控制器

MAC 认证+Guest VLAN 典型配置举例(V7)

资料版本：6W100-20191125

目 录

1 简介

本文档介绍当用户 MAC 地址认证失败时只能访问某一特定的 VLAN，即 Guest VLAN 内的网络资源的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的无线控制器和接入点产品，不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、MAC 地址认证、WLAN 用户接入认证和 WLAN 接入特性。

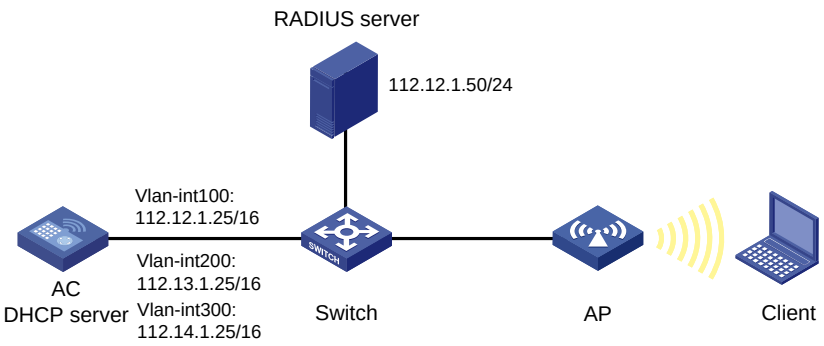
3 配置举例

3.1 组网需求

如图 1 所示，集中式转发架构下，AP 和 Client 通过 DHCP server 获取 IP 地址，设备管理员希望对 Client 进行 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 配置 VLAN 200 为 Client 的接入 VLAN，Client 通过 VLAN 200 上线并在 RADIUS server 上进行 MAC 地址认证。
- 配置 VLAN 300 为 Guest VLAN，当 Client 的 MAC 地址认证失败时进入 Guest VLAN，此时 Client 只能访问 VLAN 300 内的网络资源。

图1 MAC 地址认证＋Guest VLAN 典型配置举例组网图



3.2 配置思路

为了实现用户 MAC 地址认证失败后仅允许访问 Guest VLAN 内的资源，需要在无线服务模板下配置 Guest VLAN 功能，则认证失败的用户会被加入该 Guest VLAN，且该用户仅被授权访问 Guest VLAN 内的资源，同时设备会启动一个 30 秒的定时器，以定期对用户进行重新认证。

3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 配置 Switch 和 AP 相连的接口禁止 VLAN 1 报文通过，以防止 AC 上 VLAN 1 内的报文过多。

3.4 配置步骤

3.4.1 配置AC

(1) 配置 AC 的接口

创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AP 将获取该 IP 地址与 AC 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.12.1.25 16
[AC-Vlan-interface100] quit
```

创建 VLAN 200 及其对应的 VLAN 接口，并为该接口配置 IP 地址。Client 使用该 VLAN 接入无线网络。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.13.1.25 16
[AC-Vlan-interface200] quit
```

创建 VLAN 300 及其对应的 VLAN 接口，并为该接口配置 IP 地址。Client MAC 地址认证失败后将仅允许访问 VLAN 300（即 Guest VLAN）内的资源。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 112.14.1.25 16
[AC-Vlan-interface300] quit
```

配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100、VLAN 200 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

(2) 配置 DHCP server

开启 DHCP server 功能。

```
[AC] dhcp enable
```

配置 DHCP 地址池 vlan100，为 AP 分配的地址范围为 112.12.0.0/16，网关地址为 112.12.1.25。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
```

配置 DHCP 地址池 vlan200，为 Client 分配的地址范围为 112.13.0.0/16，为 Client 分配的 DNS 服务器地址为网关地址(实际使用过程中请根据实际网络规划配置无线客户端的 DNS 服务器地址)，网关地址为 112.13.1.25。

```
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan200] gateway-list 112.13.1.25
[AC-dhcp-pool-vlan200] dns-list 112.13.1.25
[AC-dhcp-pool-vlan200] quit
```

配置 DHCP 地址池 vlan300，为从 Guest VLAN 上线的用户分配的地址范围为 112.14.0.0/16，分配的 DNS 服务器地址为网关地址（实际使用过程中请根据实际网络规划配置无线客户端的 DNS 服务器地址）网关地址为 112.14.1.25。

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 112.14.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan300] gateway-list 112.14.1.25
[AC-dhcp-pool-vlan300] dns-list 112.14.1.25
[AC-dhcp-pool-vlan300] quit
```

(3) 配置 RADIUS 认证

创建名为 office 的 RADIUS 方案，并进入其视图。

```
[AC] radius scheme office
```

配置主认证、计费 RADIUS 服务器的 IP 地址为 112.12.1.50。

```
[AC-radius-office] primary authentication 112.12.1.50
[AC-radius-office] primary accounting 112.12.1.50
```

配置 RADIUS 认证、计费报文的共享密钥为 123456789。

```
[AC-radius-office] key authentication simple 123456789
[AC-radius-office] key accounting simple 123456789
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[AC-radius-office] user-name-format without-domain
```

配置设备发送 RADIUS 报文使用的源 IP 地址为 112.12.1.25。

```
[AC-radius-office] nas-ip 112.12.1.25
[AC-radius-office] quit
```

创建名为 office1 的 ISP 域，并进入其视图。

```
[AC] domain office1
```

为 lan-access 用户配置认证、授权、计费方案为 RADIUS 方案 office。

```
[AC-isp-office1] authentication lan-access radius-scheme office
[AC-isp-office1] authorization lan-access radius-scheme office
[AC-isp-office1] accounting lan-access radius-scheme office
```

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-office1] authorization-attribute idle-cut 15 1024
[AC-isp-office1] quit
```

配置 MAC 地址认证的用户名和密码均为用户的 MAC 地址，且不带连字符（该配置为缺省配置）。

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

(4) 配置服务模板

创建无线服务模板 1，并进入无线服务模板视图。

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

配置 SSID 为 service。

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

配置客户端从无线服务模板 1 上线后会被加入 VLAN 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 office1。

```
[AC-wlan-st-1] mac-authentication domain office1
```

(5) 配置 Guest VLAN

在无线服务模板 1 下配置 MAC 地址认证失败后可授权访问的 Guest VLAN 为 VLAN 300。

```
[AC-wlan-st-1] client-security authentication fail-vlan 300
```

开启无线服务模板。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

(6) 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 210235A1Q2C159000020。

```
[AC-wlan-ap-officeap] serial-id 210235A1Q2C159000020
```

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
```

3.4.2 配置Switch

创建 VLAN 100、VLAN 200 和 VLAN 300，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，VLAN 300 用于转发 Guest VLAN 的报文。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

配置 Switch 与 AC 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，当前 Trunk 口的 PVID 为 100。

```
[Switch] interface gigabitEthernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-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。

```
[Switch] interface gigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

开启 PoE 接口远程供电功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

3.4.3 配置RADIUS服务器

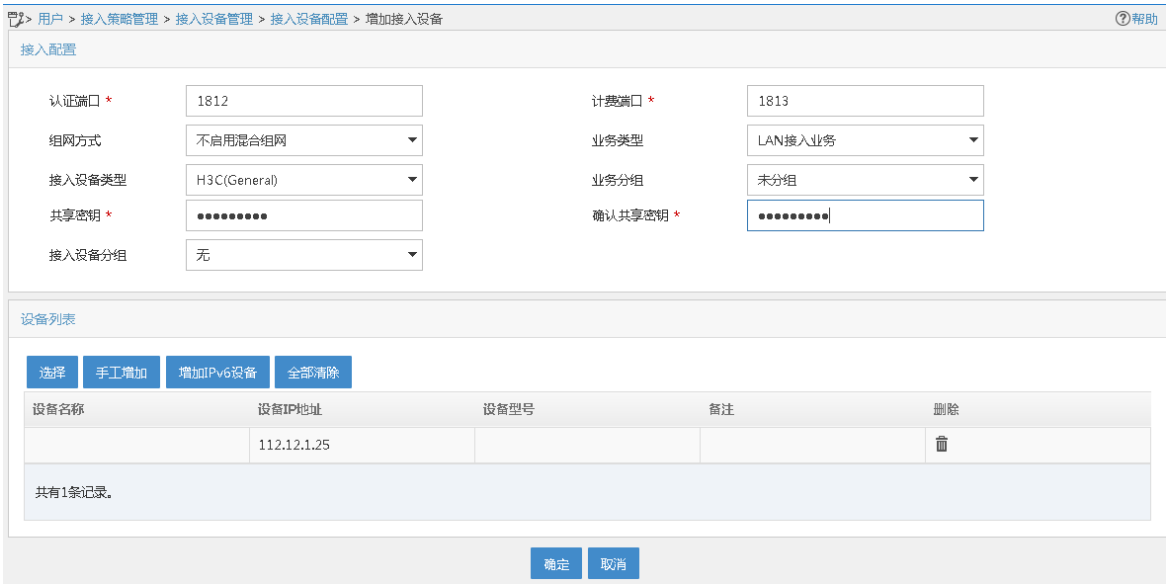
说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1(E0303P10)、iMC UAM 7.1(E0303P10)，说明 RADIUS server 的基本配置。

(1) 增加接入设备

登录进入 iMC 管理平台，“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

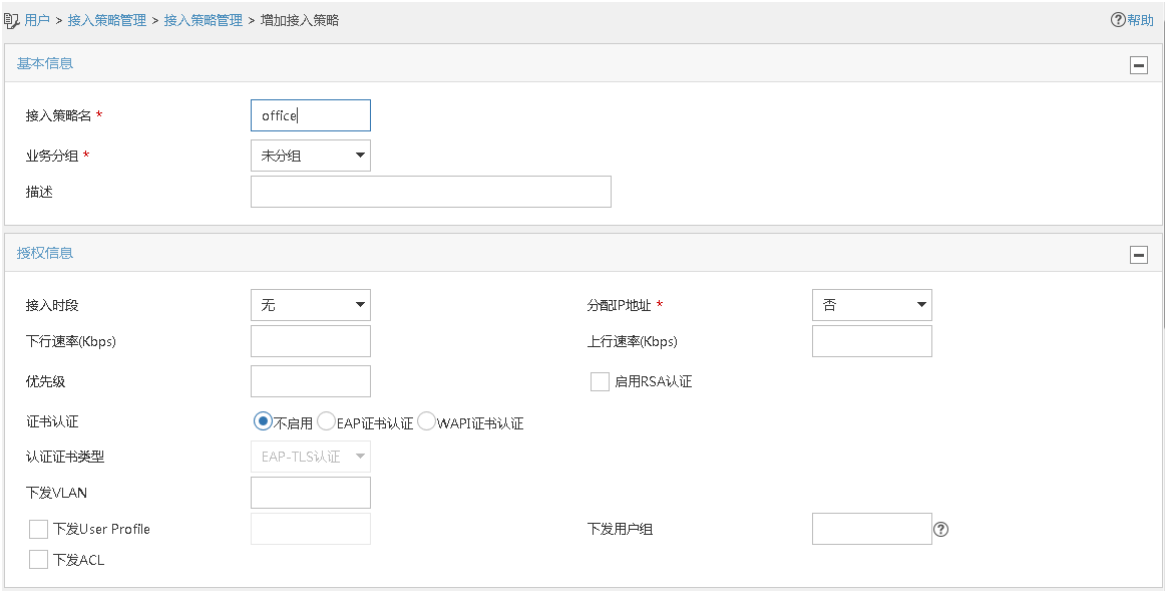
- 填写起始 IP 地址为“112.12.1.25”，该 IP 地址为 AC 上配置的 radius scheme 视图下的 nas-ip 地址。
- 单击<确定>按钮完成操作。
- 在“接入配置”区域配置共享密钥为“123456789”，该共享密钥与 AC 上配置 Radius 服务器上的密钥一致。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。



(2) 增加接入规则配置

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，单击<增加>按钮，创建一条接入策略。

- 配置接入策略名为“office”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

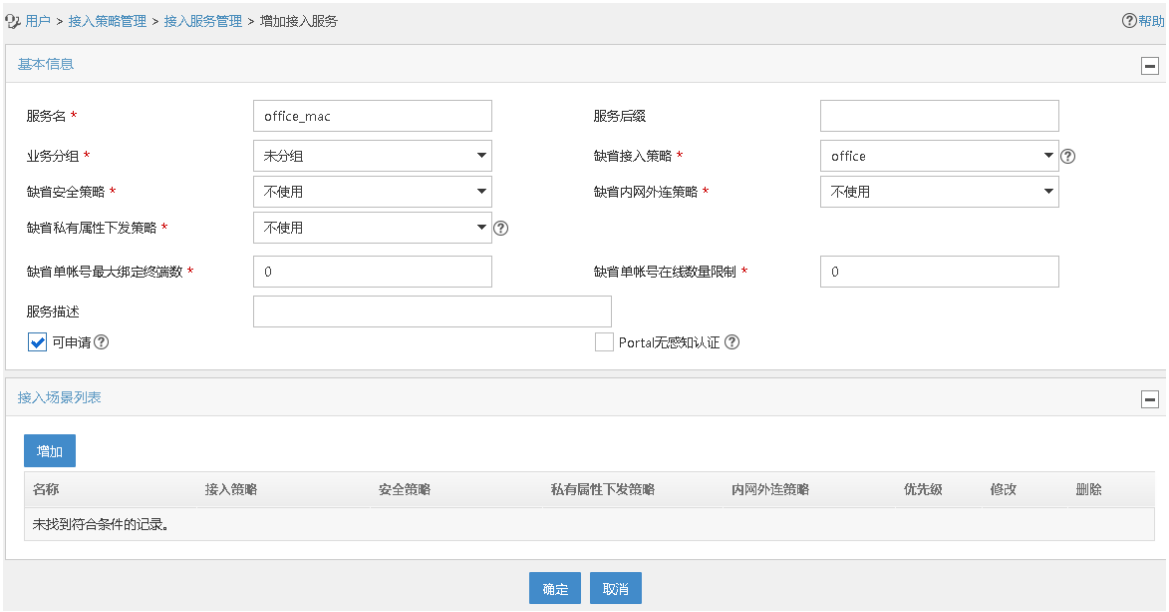


(3) 增加服务配置

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，单击<增加>按钮，创建一条服务。

- 配置服务名为“office_mac”（这里的服务名可以任意命名）。
- 缺省接入策略选择“office”。
- 其他采用默认配置。

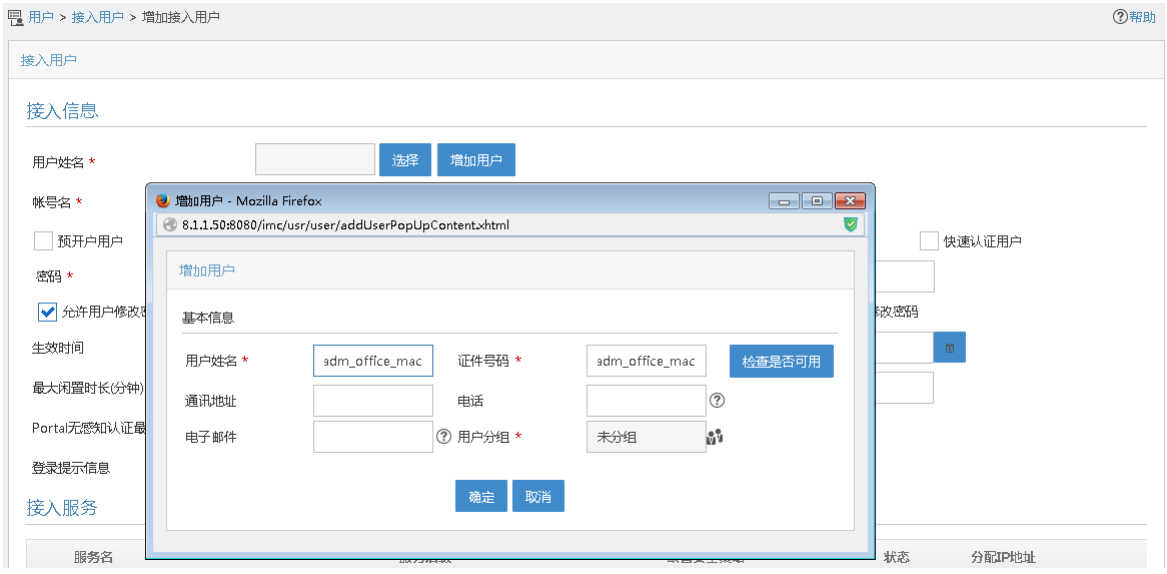
- 单击<确定>按钮完成配置。



(4) 增加接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击<增加>按钮，增加一个接入用户。

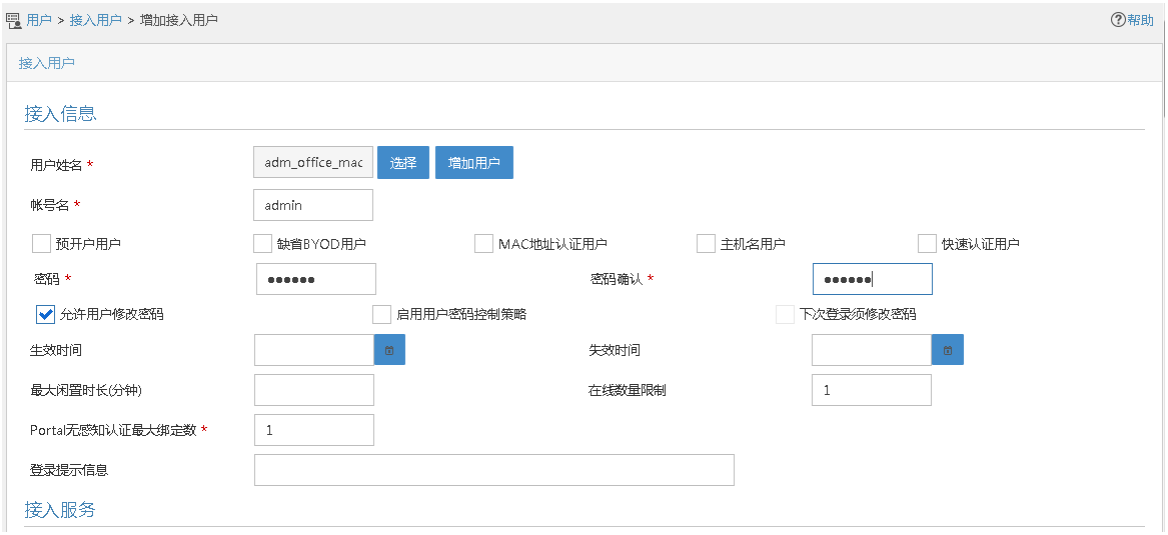
- 单击<增加用户>按钮，输入用户姓名“adm_office_mac”和证件号码“adm_office_mac”，单击<确定>按钮完成。



- 配置帐号名“admin”和密码“123456”。
- 勾选绑定服务名“office_mac”。
- 单击<确定>按钮完成。

说明

这里在 Radius 服务器上配置的用户认证账号名“admin”和密码“123456”与 AC 上配置的 MAC 地址认证的用户名和密码（Client 的 MAC 地址）不一致，所以 Client 上线后会认证不通过，从而进入 Guest VLAN。



3.5 验证配置

完成以上配置后，无线用户 Client 连接到 WLAN 网络并进行 MAC 地址认证。由于 RADIUS server 上配置的用户名和密码与 AC 上配置的 MAC 地址认证的用户名和密码不一致，因此认证失败，在 AC 上通过命令 **display wlan client** 可以看见无线用户 Client 从 Guest VLAN 300 上线。

```
[AC] display wlan client
 Total Number of Clients          : 1

MAC address     Username      AP name         RID  IP address      IPv6 address   VLAN
3ca9-f414-4c20  3ca9f4144c20  officeap        2    112.14.0.2      N/A            300
```

Guest VLAN 中的无线用户 Client 在通过 MAC 地址认证之前只能访问 VLAN 300 的网络资源。

Guest VLAN 中的无线用户 Client 通过 MAC 地址认证后，可以通过命令 **display mac-authentication** 查看 MAC 认证信息。

```
[AC] display mac-authentication
Global MAC authentication parameters:
 MAC authentication     : Enabled
 User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username       : 3ca9f4144c20
           Password       : $c$3$KWMkvq/FnQ2opPqBnpSTs3NPhVKrSOvqFPLAECSiDQ==
   Offline detect period  : 180 s
 Quiet period           : 180 s
 Server timeout         : 100 s
 Authentication domain  : office1
```

```
Online MAC-auth users    : 1

Silent MAC users:
          MAC address       VLAN ID  From port               Port index
          3ca9-f414-4c20    300      GE1/0/1                 1
GigabitEthernet1/0/1 is link-up
MAC authentication          : Enabled
 Carry User-IP              : Disabled
 Authentication domain      : Not configured
 Auth-delay timer           : Disabled
 Re-auth server-unreachable : Logoff
 Guest VLAN                 : 300
 Guest VLAN auth-period     : 30 s
 Critical VLAN              : Not configured
 Host mode                  : Single VLAN
 Offline detection          : Enabled
 Max online users           : 4294967295
 Authentication attempts    : successful 1, failed 0
Current online users       : 1
 MAC address       Auth state
3ca9-f414-4c20    Authenticated
```

3.6 配置文件

- AC

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
 gateway-list 112.12.1.25
 network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
 gateway-list 112.13.1.25
 network 112.13.0.0 mask 255.255.0.0
 dns-list 112.13.1.25
#
dhcp server ip-pool vlan300
 gateway-list 112.14.1.25
 network 112.14.0.0 mask 255.255.0.0
```

```
 dns-list 112.14.1.25
#
wlan service-template 1
 ssid service
 vlan 200
 client-security authentication-mode mac
 client-security authentication fail-vlan 300
 mac-authentication domain office1
 service-template enable
#
interface Vlan-interface100
 ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
 ip address 112.13.1.25 255.255.0.0
#
interface Vlan-interface300
 ip address 112.14.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200 300
 port trunk pvid vlan 100
#
radius scheme office
 primary authentication 112.12.1.50
 primary accounting 112.12.1.50
 key authentication cipher $c$3$IrnigzRDMkG7Jk1FNf2+tm04+zvnCwiaJzI9TA==
 key accounting cipher $c$3$ehledYNyJ+vTlcYcyUEisTa+ZXvWqU1O2QlSYg==
 user-name-format without-domain
 nas-ip 112.12.1.25
#
domain office1
 authorization-attribute idle-cut 15 1024
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access radius-scheme office
#
wlan ap officeap model WA4320i-ACN
 serial-id 210235A1Q2C159000020
 radio 1
 radio 2
  radio enable
  service-template 1
#
```

- Switch

```
#
```

```
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
poe enable
#
```

4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“网络互通配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“网络互通命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“用户接入与认证配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“用户接入与认证命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 接入配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 接入命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“AP 管理配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“AP 管理命令参考”。