

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。

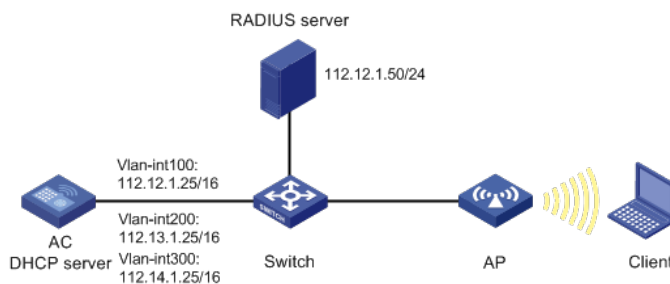
本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

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。

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。



1.1 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。

1.2 配置步骤

1.2.1 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。

```
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, 网关地址为112.12.1.25。
[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 112.12.1.25
[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, 网关地址为112.12.1.25。
[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 112.12.1.25
[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

```

1.2.2 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。
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

```

1.2.3 配置RADIUS服务器

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。

The screenshot shows the 'Add Access Device' configuration page. The configuration fields are as follows:

| | | | |
|--------|--------------|----------|-----------|
| 认证端口 * | 1812 | 计费端口 * | 1813 |
| 组网方式 | 不启用混合组网 | 业务类型 | LAN接入业务 |
| 接入设备类型 | H3C(General) | 业务分组 | 未分组 |
| 共享密钥 * | 123456789 | 确认共享密钥 * | 123456789 |
| 接入设备分组 | 无 | | |

Below the form is a table with one device entry:

| 设备名称 | 设备IP地址 | 设备型号 | 备注 | 删除 |
|------|-------------|------|----|----|
| | 112.12.1.25 | | | |

Buttons at the bottom: 确定, 取消.

(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。

The screenshot shows the 'Add Access Policy' configuration page. The configuration fields are as follows:

| | |
|---------|--------|
| 接入策略名 * | office |
| 业务分组 * | 未分组 |
| 描述 | |

Reception Information section:

| | | | |
|---|---|----------------------------------|---|
| 接入时段 | 无 | 分配IP地址 * | 否 |
| 下行速率(Kbps) | | 上行速率(Kbps) | |
| 优先级 | | <input type="checkbox"/> 启用RSA认证 | |
| 证书认证 | <input checked="" type="radio"/> 不启用 <input type="radio"/> EAP证书认证 <input type="radio"/> WAPI证书认证 | | |
| 认证证书类型 | EAP-TLS认证 | | |
| 下发VLAN | | 下发用户组 | |
| <input type="checkbox"/> 下发User Profile | | | |
| <input type="checkbox"/> 下发ACL | | | |

(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。

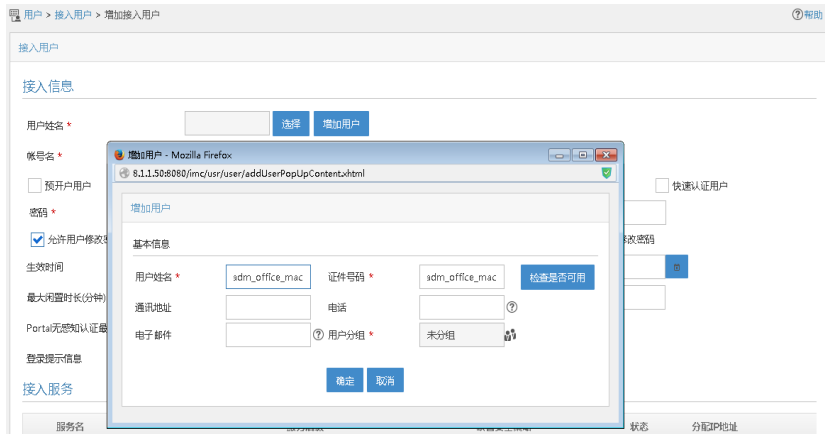
- 配置服务名为“office_mac”（这里的 service 名可以任意命名）。
- 缺省接入策略选择“office”。
- 其他采用默认配置。
- 单击<确定>按钮完成配置。



(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。

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。



1.3 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

Client Information

SSID: service

```
-----  
MAC Address  User Name      APID/RID IP Address      VLAN -----  
-----  
3ca9-f414-4c20 3ca9f4144c20      1/2  112.14.0.2      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)

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
```

1.4 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 112.12.1.25
network 112.13.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan300
gateway-list 112.12.1.25
network 112.14.0.0 mask 255.255.0.0
#
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$3$lrnigzRDMkG7Jk1FNf2+tm04+zvnCwiaJzl9TA==
key accounting cipher $c$3$ehledYNYj+vTlcYcyUEisTa+ZXvWqU1O2QISYg==
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
#
```

- 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。