# WA系列FAT AP结合iMC EIA（V7）无线MAC认证并动态下发VLAN的配置案例

wlan接入 MAC地址认证 AAA VLAN 李树兵 2016-03-14 发表

基于MAC划分VLAN是VLAN的一种划分方法。它按照报文的源MAC地址来定义VLAN成员，将指定报文加入该VLAN的tag后发送。该功能通常会和安全（比如802.1X）技术联合使用，以实现终端的安全、灵活接入。

本案例提供了VLAN属性划分的另一种方法，并结合用户MAC认证方法，确保安全合法用户获得VLAN权限，阻止非法用户接入，有效的起到了安全隔离及授权的作用。本特性的应用场合也比较灵活，适于需要进行VLAN受限分配的场合。

目前iMC EIA（V7）使用广泛，本案例使用iMC EIA最新版本与无线AP配合实现无线MAC认证并认证通过后下发vlan，实现不同的MAC地址用户下发到不同的vlan，实现mac vlan的功能。


FAT AP型号及版本信息：WA2620E-AGN Release 1122P30
iMC EIA版本信息：7.1 E0302P18
MSR型号及版本信息：MSR920 Release 2513P59
FAT AP的管理地址是192.168.1.2，MSR920的管理地址是192.168.1.1，iMC服务器的地址是192.168.1.114，无线的SSID为macauth，本案例将基于MAC地址将iPad划分到vlan100中，并且分配192.168.100.0/24的地址，将iPhone划分到van101中，并且分配192.158.101.0/24的地址。

一.设备配置
无线AP配置：

```
port-security enable  //开启设备端口安全功能
#
 mac-authentication domain mac  //配置mac认证的domain域为mac
 mac-authentication user-name-format mac-address with-hyphen  //配置mac认证用户名的格式为XX-XX-XX-XX-XX-XX
#
 password-recovery enable
#
vlan 1
#
vlan 100 to 101   //配置vlan100和vlan101，分别用于iPad的用户和iPhone的用户
#
radius scheme mac  //配置radius方案，名字为mac
 primary authentication 192.168.1.114 key cipher $c$3$sCYBbRfLfr+n3G5W9GC98SAaPEcLXQ==  //配置进行认证的服务器，ip地址为192.168.1.114（iMC EIA地址），认证密钥为h3c
 primary accounting 192.168.1.114 key cipher $c$3$H/4OBJArNH0CwNirmMs/iwWW2nZ/rg==
 //配置进行计费的服务器，ip地址为192.168.1.114（iMCEIA的地址），计费密钥为h3c，两个密钥要保持一致，因为iMC侧只能配置一个密钥，所以认证和计费密钥要一致
```

```
 nas-ip 192.168.1.2  //配置设备发送radius报文的nas-ip地址
#
domain mac  //配置domain域，名字为mac
 authentication lan-access radius-scheme mac  //设置用户认证的radius方案为mac
 authorization lan-access radius-scheme mac //设置用户授权的radius方案为mac
 accounting lan-access radius-scheme mac //设置用户计费的radius方案为mac
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool imc   //配置用于给iMC分配IP地址的dhcp地址池
 network 192.168.1.0 mask 255.255.255.0
 gateway-list 192.168.1.1
#
dhcp server ip-pool macauth //配置用于给iPad用户分配IP地址的dhcp地址池
 network 192.168.100.0 mask 255.255.255.0
 gateway-list 192.168.100.1
 dns-list 192.168.100.1
#
dhcp server ip-pool macauth-2 //配置用于给iPhone用户分配IP地址的dhcp地址池
 network 192.168.101.0 mask 255.255.255.0
 gateway-list 192.168.101.1
 dns-list 192.168.101.1
wlan service-template 1 crypto
 ssid imc
 cipher-suite tkip
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
wlan service-template 4 clear  //配置无线mac认证的服务模板
 ssid macauth   //设置SSID为macauth
 service-template enable  //使能服务模板
interface Vlan-interface15
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface100
 ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface101
 ip address 192.168.101.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface WLAN-BSS30
 port link-type hybrid  //设置接口为hybird类型，配置mac vlan接口类型必须为hybird类型，并且
允许相应的vlanuntagged通过
 port hybrid vlan 1 100 to 101 untagged  //配置vlan100和vlan101 untagged通过
 mac-vlan enable  //使能mac vlan功能
 port-security port-mode mac-authentication  //设置端口安全默认为mac认证
 mac-authentication domain mac  //设置认证的domain域为mac
#
interface WLAN-BSS32
 port access vlan 15
 port-security port-mode psk
 port-security tx-key-type 11key
```

port-security preshared-key pass-phrase cipher $c$3$bzWaOZUhgl+QJtl+3jQlFp1suxykWzj1TKTSyA==

#

interface WLAN-Radio1/0/1

service-template 1 interface wlan-bss 32

service-template 4 interface wlan-bss 30

snmp-agent

snmp-agent local-engineid 800063A20380F62E18D7D0

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info version all

snmp-agent target-host trap address udp-domain 192.168.1.114 params securityname public v2c

dhcp enable  //开启设备的dhcp服务功能

二.iMC配置:

①增加接入设备

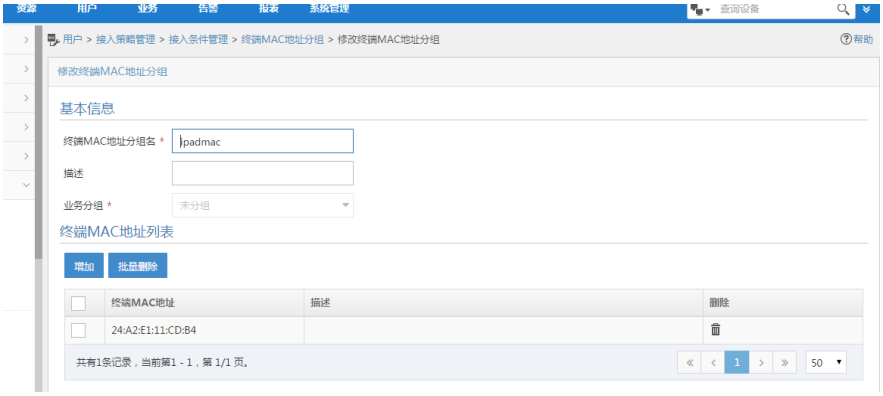


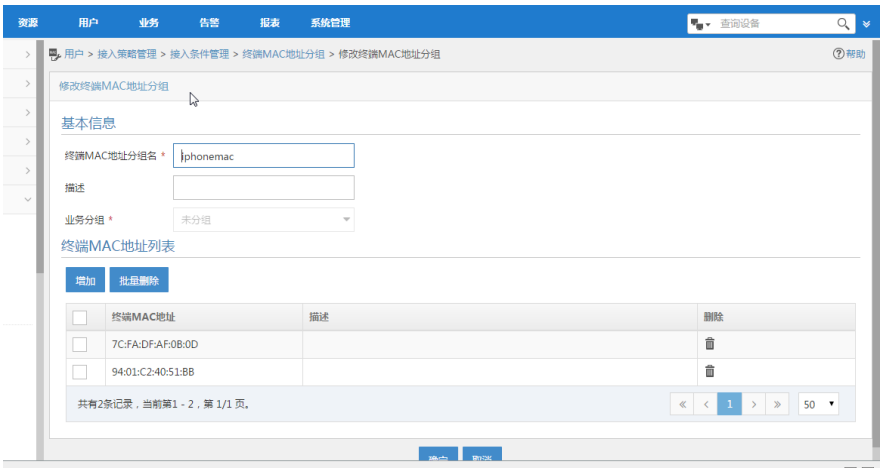

设置共享密钥，保证和设备里面radius scheme 配置的密钥一致，增加设备，保证设备的IP地址和设备上的nas-ip地址一致。

②在接入条件里面设置MAC地址分组

选择用户->接入策略管理->接入条件管理->终端MAC地址分组


点击增加，设置终端MAC地址的分组名，分别设置为ipadmac和iphonemac，并在终端MAC地址列表中添加对应的终端MAC地址

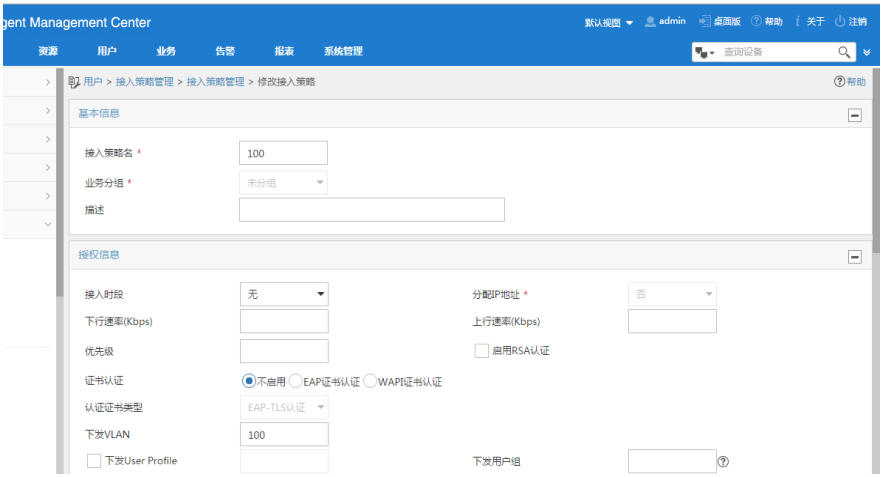


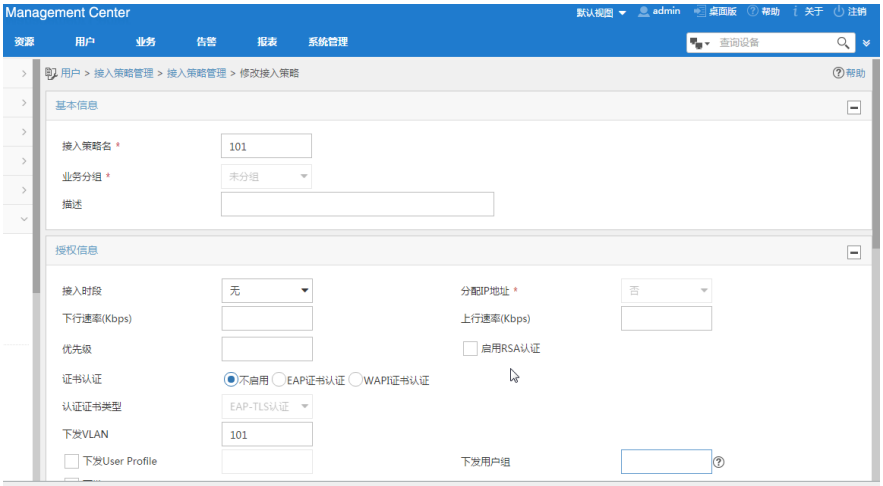




③设置终端接入策略

点击用户->接入策略管理->接入策略管理，选择增加

分别设置策略名字为100和101，并分别下发vlan 100 和vlan 101

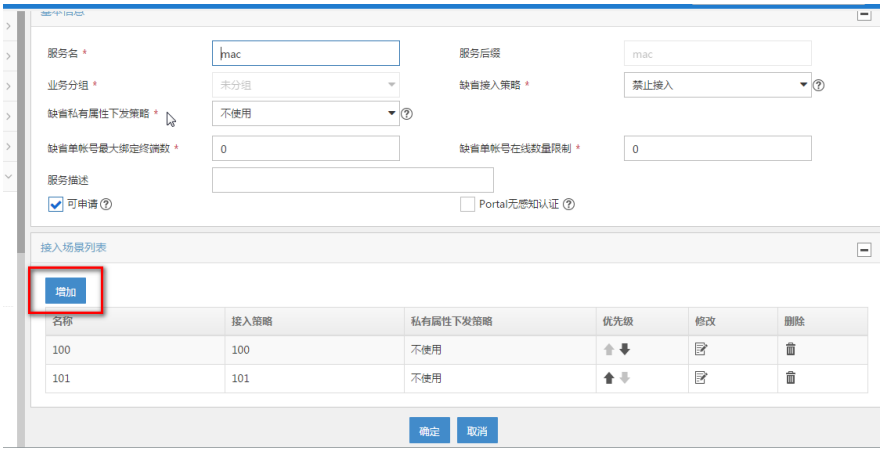




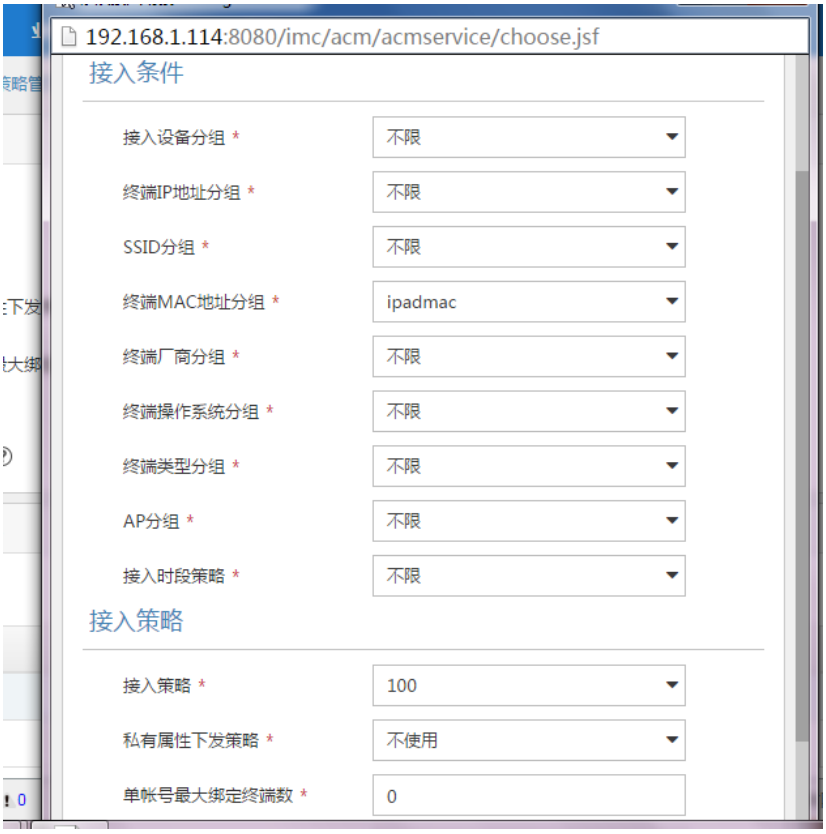

④增加接入服务mac

点击用户->接入策略管理->接入服务管理，选择增加


设置服务名为mac，服务后缀为mac，缺省接入策略为禁止接入。



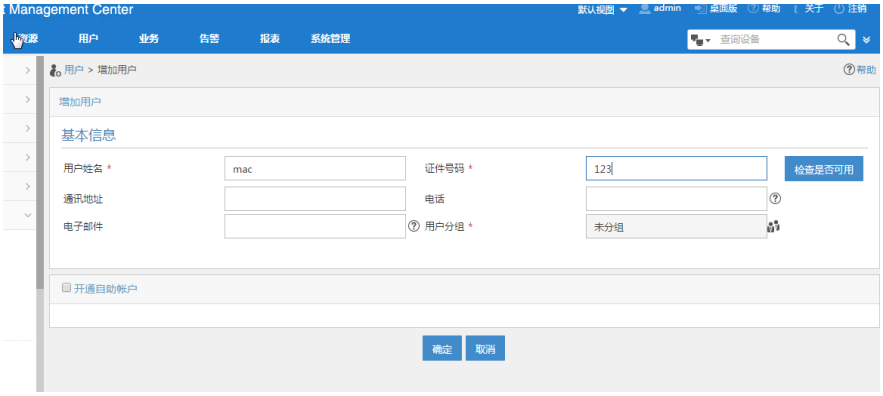

增加接入场景，设置终端MAC地址分组ipadmac对应接入策略为100，终端MAC地址分组iphonemac对应接入策略为101





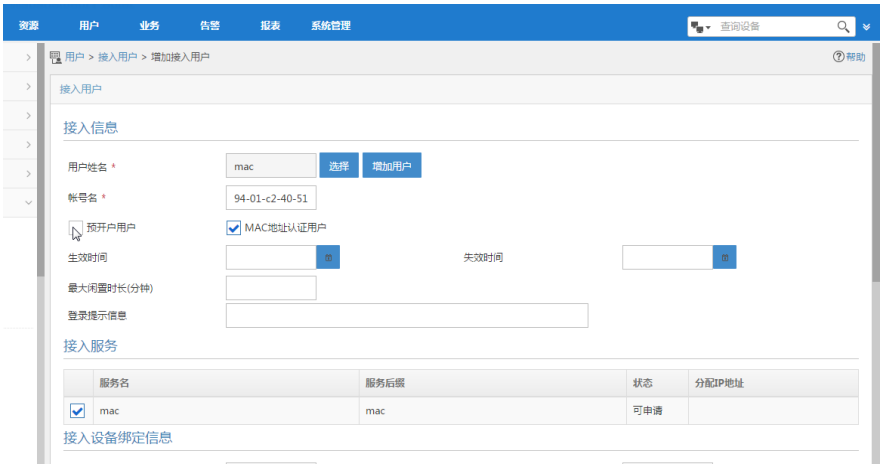
⑤增加接入用户

点击用户->增加用户，设置用户姓名为mac，证件号码随意，然后点击确定

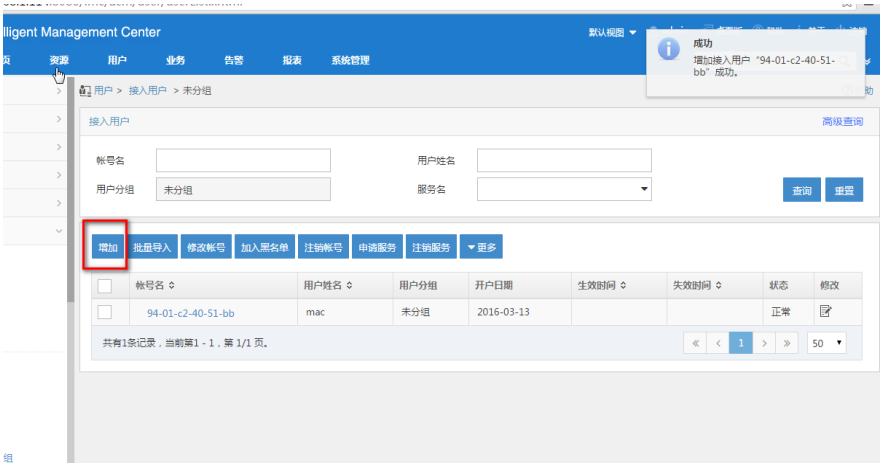


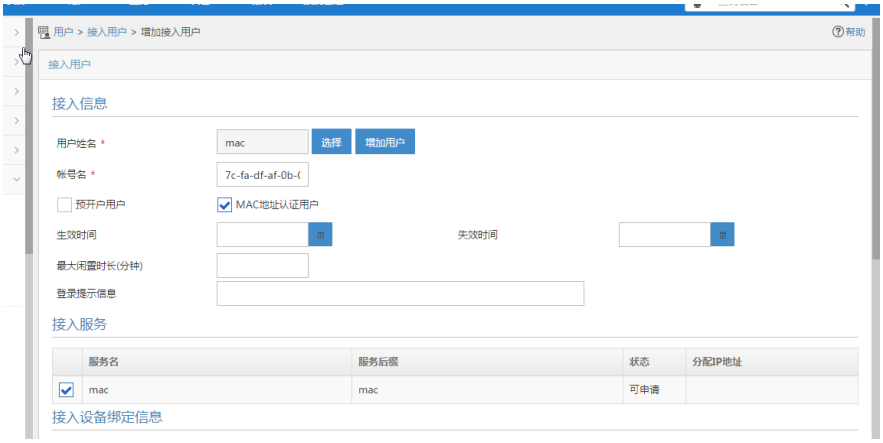

增加成功之后增加接入用户


将用户的MAC地址填写到账号名的位置，选择MAC地址认证用户，选择接入服务为mac




增加成功之后然后选择增加其他接入用户






全部增加成功之后配置完成，之后客户端可以通过联系无线信号macauth，根据不同的终端MAC地址然后划分到不同的vlan并获取不同的IP地址。
验证结果：


-67 中国电信
11:30
41%
无线局域网
macauth
忽略此网络
IP 地址
DHCP
BootP
静态
IP 地址
192.168.101.4
子网掩码
255.255.255.0
路由器
192.168.101.1
DNS
192.168.101.1
搜索域
客户端 ID



在AP上查看连接用户：

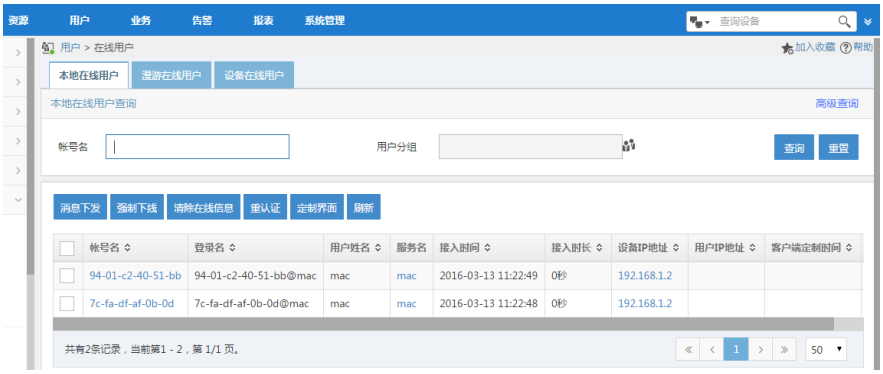
[WA2620E-AGN-WLAN-BSS30]dis wlan client
Total Number of Clients : 5
Client Information
SSID: imc

| MAC Address | User Name | APID/RID | IP Address | VLAN |
|---|---|---|---|---|
| 08ed-b9f1-8bc3 | -NA- | 1 /1 | 192.168.1.114 | 15 |
| 8019-3427-ad67 | -NA- | 1 /1 | 192.168.1.3 | 15 |

SSID: macauth

| MAC Address | User Name | APID/RID | IP Address | VLAN |
|---|---|---|---|---|
| 24a2-e111-cdb4 | 24-a2-e1-11-cd-b4 | 1 /1 | 192.168.100.2 | 100 |
| 7cfa-dfaf-0b0d | 7c-fa-df-af-0b-0d | 1 /1 | 192.168.101.4 | 101 |
| 9401-c240-51bb | 94-01-c2-40-51-bb | 1 /1 | 192.168.101.3 | 101 |

在iMC侧查看在线用户：




注意事项：

①因为是macvlan，所以wlan-bss接口下必须开启mac-vlan enable，否则会出现在iMC侧抓包显示认证通过，但是多个vlan下的用户只有一个vlan的用户才能上线。

②因为设备上radius方案模式是with-domain，所以iMC侧配置配置接入服务的时候需要配置服务后缀，并且服务后缀的名字与设备上domain域的名字一致，否则终端无法连接WiFi，在iMC侧会提示“用户不存在或没有申请该服务”