

某局点无线控制器客户端本地MAC认证故障问题处理方法

wlan接入 [MAC地址认证](#) [AAA](#) 李洋洋 2015-10-20 发表

某局点反馈使用我司无线控制器同时开启Portal、802.1X、本地MAC认证,三种认证方式的认证域分别是portal、802.1x以及缺省的system域。如果把默认域配置成Portal认证的portal域,三种认证方式均可认证通过。

如果把默认域配置成802.1X认证的802.1x域, Portal认证、802.1X认证可以通过,但本地MAC认证无法通过。

1、现网AC使用部分配置:

```
#
domain default enable portal

#
radius scheme portal
server-type extended
primary authentication 10.16.202.216
primary accounting 10.16.202.216
key authentication cipher Ue77omzOxyQ=
key accounting cipher Ue77omzOxyQ=
security-policy-server 10.16.202.217
user-name-format without-domain
nas-ip 10.16.233.110
radius scheme 802.1x
server-type extended
primary authentication 10.16.202.216
primary accounting 10.16.202.216
key authentication cipher Ue77omzOxyQ=
key accounting cipher Ue77omzOxyQ=
security-policy-server 10.16.202.217
user-name-format without-domain
nas-ip 10.16.233.110
#
domain portal
authentication portal radius-scheme portal
authorization portal radius-scheme portal
accounting portal radius-scheme portal
access-limit disable
state active
idle-cut disable
self-service-url disable
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
domain 802.1x
authentication lan-access radius-scheme 802.1x
authorization lan-access radius-scheme 802.1x
accounting lan-access radius-scheme 802.1x
```

```
access-limit disable
state active
idle-cut disable
self-service-url disable
#
```

2、向客户了解现网信息，现网所做远程认证均与我司iMC相结合，MAC认证在本地完成。

3、针对上述现象分析，Portal、802.1X、本地MAC认证,三种认证方式的认证域分别是portal、802.1x以及设备缺省的system域。

(1) 当默认域为portal时，认证类型为portal用户到iMC侧认证，802.1X认证用户手工携带802.1x域，由于用户携带域的优先级高于设备配置域的优先级，所以802.1X认证用户也到iMC侧认证。本地MAC认证用户由于认证类型为lac-access，且默认域portal未定义此认证类型，则本地MAC认证用户在system域（缺省定义认证类型为default）本地查找认证，所以也能认证通过；

(2) 当默认域为802.1x时，认证类型为lac-access的802.1X认证用户到iMC侧认证，而Portal认证用户认证类型为portal，虽然802.1X认证未定义portal认证类型，但是Portal认证用户仍会到iMC侧认证。本地MAC认证类型也属于802.1X认证的lan-access认证类型，用户会到iMC侧认证，而iMC未定义本地MAC认证用户，所以本地MAC认证用户认证失败。

建议对Portal、802.11X用户分别强制指定认证域，而本地MAC认证用户为默认域，即可满足业务需求。