

WX系列AC支持MAC快速认证（山东模式）典型配置

一、应用环境

为了方便WLAN业务更便捷的承载于手机、ipad等移动终端，山东移动推出了有别于浙江模式的基于PORTAL重定向信息的MAC快速认证的无感知认证方案，用以简化认证操作，优化用户体验。在该方案中，MAC快速认证方式的无感知业务仍承载于SSID: CMCC上，为了继续兼容原PORTAL业务，该方案仅对原有的PORTAL架构做了扩展。和浙江模式不同，该方案中不需新增服务器，仅通过web重定向url携带用户MAC地址信息到portal server，由portal server完成绑定用户信息的查询。

认证流程：用户通过web浏览器触发认证。AC将用户的MAC地址以及首访页面等信息通过重定向url携带到portal server，server根据MAC地址信息查询有无绑定用户。如果对应MAC未绑定用户，则server直接推送portal页面给终端用户，用户输入用户名密码完成进行正常的portal交互。如果对应MAC有绑定用户，则server直接后台获取用户的帐号密码信息向AC发起认证，认证通过后，重定向到首访页面，对用户最终呈现“无需认证，直接通过web浏览器访问网络”的体验。

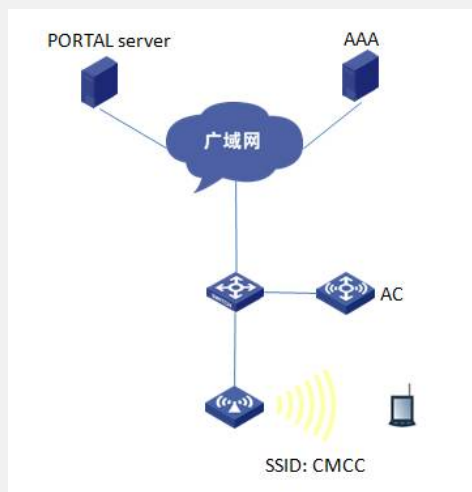
二、应用限制：

山东的MAC快速认证方案，对设备和服务器侧改动均不大，实施较方便。但认证机制决定了该MAC认证解决方案存在一定的应用限制条件。山东模式的MAC认证是通过web重定向来触发的，绑定用户在访问网络之前必须要先打开web浏览器完成认证过程，后续才能正常访问网络，尽管用户并不需要在浏览器上输入帐号、密码信息。但实际上用户的业务并不局限于web网页浏览，比如QQ、FTP、视频等业务，但这些业务流量并不能触发山东模式的MAC快速认证，必须要先借助web浏览器完整用户MAC快速认证。举个例子：绑定用户想通过QQ上网之前必须要先打开浏览器访问一个网页才行，任何一个网页都可以。

三、组网需求

按照普通的PORTAL接入进行组网。AC使用的是WX6000系列无线控制器(WX6103)。Client和AP通过DHCP服务器获取IP地址(DHCP服务器配置略)。由AC对无线用户做PORTAL认证，在原PORTAL SERVER和AAA基础上新增MAC-Trigger SERVER。

四、组网图：



五、配置方法：

1. 配置思路

- ? 在AC上配置RADIUS方案、DOMAIN等
- ? 配置Portal server
- ? 配置重定向url添加用户mac地址和首访url信息
- ? 在AC上配置无线服务，并在相关业务VLAN接口上开启portal认证

2. 配置步骤

(1) 主AC上的配置信息：

```
dis cur
#
```

```
version 5.20, Release 2308P07
#
sysname WX6103
#
domain default enable system
#
telnet server enable
#
wlan rfid-tracking enable
#
acl number 2001
rule 0 permit source 192.168.0.0 0.0.0.255
rule 1 permit
#
portal server cmcc ip 221.176.1.140 url http://221.176.1.140:7080/index.php server-type cmcc //cmcc portal server
portal free-rule 1 source any destination ip 211.137.58.20 mask 255.255.255.255

portal free-rule 2 source any destination ip 211.136.17.107 mask 255.255.255.255
portal free-rule 11 source interface Bridge-Aggregation1 destination any
portal device-id 0344.0531.531.00 //配置AC NAME
portal url-param include user-mac des-encrypt param-name wlanparameter //配置重定向url添加用户mac地址信息并加密
portal url-param include user-url param-name wlanuserfirsturl //配置重定向url添加首访url信息
#
vlan 1
#
vlan 2
#
vlan 100 //AP关联vlan
#
vlan 200 //业务vlan
#
vlan 300 //骨干网互联vlan, nas-ip通信
#
radius scheme cmcc //配置portal的AAA策略
server-type extended
primary authentication 221.176.1.138 1645
primary accounting 221.176.1.138 1646
key authentication cipher abQuGU4cQTpZL8rzyG52eg==
key accounting cipher abQuGU4cQTpZL8rzyG52eg==
user-name-format keep-original
nas-ip 128.202.52.53
retry stop-accounting 10
#
domain cmcc //配置portal的认证域
authentication portal radius-scheme cmcc
authorization portal radius-scheme cmcc
accounting portal radius-scheme cmcc
access-limit disable
state active
idle-cut enable 15 10000
self-service-url disable
#
dhcp server ip-pool vlan100 //配置AP管理地址pool
network 192.168.0.0 mask 255.255.0.0
network ip range 192.168.0.1 192.168.0.253
gateway-list 192.168.0.254
#
dhcp server ip-pool vlan200 //配置用户业务地址pool
network 200.0.0.0 mask 255.255.255.0
gateway-list 200.0.0.1
#
local-user admin
authorization-attribute level 3
```

```
service-type ssh telnet
service-type web
#
wlan rrm
dot11a mandatory-rate 6 12 24
dot11a supported-rate 9 18 36 48 54
dot11b mandatory-rate 1 2
dot11b supported-rate 5.5 11
dot11g mandatory-rate 1 2 5.5 11
dot11g supported-rate 6 9 12 18 24 36 48 54
dot11n protection enable
#
wlan service-template 1 clear           //CMCC 服务模板
ssid CMCC
bind WLAN-ESS 1
service-template enable
#
interface NULL0
#
interface Vlan-interface100             //AP隧道三层接口
ip address 192.168.0.253 255.255.255.0
#
interface Vlan-interface200             //业务vlan三层接口
ip address 10.111.128.2 255.255.240.0
portal server cmcc method direct
portal nas-ip 128.202.52.53
portal domain cmcc
access-user detect type arp retransmit 5 interval 10
#
interface Vlan-interface300             //骨干网互联接口，作nas-ip
ip address 128.202.52.53
#
interface M-GigabitEthernet1/0/0
#
interface Ten-GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
flow-interval 5
#
interface WLAN-ESS1                     //CMCC ESS虚接口
port link-type hybrid
undo port hybrid vlan 1
mac-vlan enable
#
wlan ap testap1 model WA2610E-AGN id 2   //AP服务模板
priority level 7
serial-id 210235A35U0087000023
undo broadcast-probe reply
radio 1
service-template 1 vlan 200 nas-id 0000000000000000
radio enable
#
wlan rrm-calibration-group 1
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.100
#
dhcp enable
#
arp-snooping enable
#
user-interface con 0
user-interface vty 0 4
authentication-mode none
user privilege level 3
#
return
```

(2) RADIUS、PORTAL、MAC-Trigger服务器设置：略

3. AC配置关键点

(1) WX6103上进行配置：

创建WLAN-ESS1接口，并进入该视图。

```
[WX6103] interface WLAN-ESS 1
```

配置端口的链路类型为hybrid

```
[WX6103-WLAN-ESS1] port link-type hybrid
```

hybrid端口上使能mac-vlan功能

```
[WX6103-WLAN-ESS1] mac-vlan enable
```

配置portal server

```
[WX6103] portal server cmcc ip 221.176.1.140 url http://221.176.1.140:7080/index.php server-type cmcc
```

配置重定向url信息添加用户mac和首访url信息

```
[WX6103] portal url-param include user-mac des-encrypt param-name wlanparameter
```

```
[WX6103] portal url-param include user-url param-name wlanuserfirsturl
```

配置AAA策略和domain域，详细配置略

配置vlan接口，接口下起portal认证

```
[WX6103-vlan-interface200] portal server cmcc method direct
```

```
[WX6103-vlan-interface200] portal nas-ip 128.202.52.53
```

```
[WX6103-vlan-interface200] portal domain cmcc
```

六、验证结果：

(1) 对于初次上网的用户需在重定向页面输入完整的认证信息，完成整个的portal交互流程，最终访问网络。

(2) 该用户在web页面选择开启MAC绑定功能并下线，后续通过web浏览器上网不会弹出重定向页面，可以直接访问网络。此时，在AC上使用命令display connection查看到该MAC地址的用户在线。

```
display connection
```

```
Index=5 ,Username=client@cmcc
```

```
MAC=00-19-5B-EC-7A-E9
```

```
IP=N/A
```

```
IPv6=N/A
```

```
Total 1 connection(s) matched
```