WX系列AC结合iMC实现终端账号SSID绑定典型配置（User-Profile方式

c09467 2013-08-02 发表

WX系列AC结合iMC实现终端账号SSID绑定典型配置（User-Profile方式）

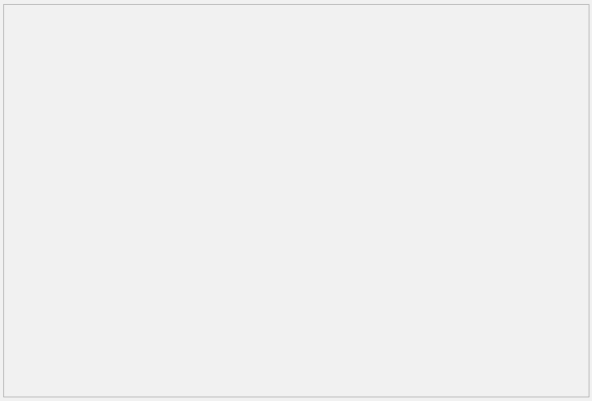
一、应用环境：

随着WLAN承载业务的日渐丰富，经常需要针对不同的接入用户制定不同的网络权限，常用的认证有802.1x和Portal，而基于这两种认证的自身特点，结合WX系列AC和iMC平台各种丰富的功能，我们提出了WX系列AC结合iMC实现终端账号SSID绑定的方案，根据用户的不同需求，对于认证用户下发user-profile实现终端的MAC地址、用户的账号、接入的无线SSID绑定的功能，实现正常网络访问和更高网络访问权限的综合需求应用，即上述三项中任何一个错误都无法认证并接入WLAN网络。

二、组网需求：

WX系列AC（无线控制器，本例中采用WX5004，版本R2308P23），Fit AP（无线接入点，本例中采用WA2612，版本为AC配套Fit版本），iMC服务器（平台版本5.2，UAM组件版本5.2），普通POE交换机，便携机（2台，需安装无线网卡）。

三、组网图：



四、配置步骤：

1. 采用Portal认证AC上的配置信息：

```
<WX5004>dis cu
#
 version 5.20, Release 2308P23
#
 sysname WX5004
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
 portal server imc ip 10.153.43.148 key cipher $c$3$xroZcZzBe8wQsioiffyMf2HvZ03zUW1M url http://10.153.43.148/portal server-type imc
 portal free-rule 0 source interface GigabitEthernet1/0/4 destination any
 portal local-server http
#
undo password-recovery enable
#
vlan 1
#
vlan 10
#
vlan 100
#
vlan 4000
#
radius scheme imc
 server-type extended
 primary authentication 10.153.43.148
```

```
 primary accounting 10.153.43.148
 key authentication cipher $c$3$szEDMyBVMO7b84qPADoC9f+L4+/L/yln
 key accounting cipher $c$3$AH6WozZlggEl39ZPYnWs84LnzP8xcPHd
 user-name-format without-domain
 nas-ip 192.168.121.154
#
domain imc
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
 accounting portal radius-scheme imc
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut enable 10 10240
 self-service-url disable
#
dhcp server ip-pool ap
 network 192.168.0.0 mask 255.255.255.0
 gateway-list 192.168.0.54
#
dhcp server ip-pool client
 network 192.168.121.0 mask 255.255.255.0
 gateway-list 192.168.121.154
 dns-list 88.8.8.8
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher $c$3$nmBMe/uKDpkC4Xtv6LT2J3/1dyLYc5D+
 authorization-attribute level 3
 service-type telnet
#
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
#
wlan service-template 1 clear
 ssid portal-mac
 bind WLAN-ESS 1
 service-template enable
#
wlan service-template 2 clear
 ssid portal-nac
 bind WLAN-ESS 2
 service-template enable
#
user-profile SSID1
 wlan permit-ssid portal-mac
user-profile SSID2
 wlan permit-ssid portal-nac
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.0.54 255.255.255.0
```

```
#
interface Vlan-interface100
 ip address 192.168.121.154 255.255.255.0
 portal server imc method direct
 portal domain imc
 portal nas-ip 192.168.121.154
#
interface Vlan-interface4000
 ip address 10.153.43.156 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
 port access vlan 4000
#
interface Ten-GigabitEthernet1/0/5
#
interface WLAN-ESS1
 port access vlan 100
#
interface WLAN-ESS2
 port access vlan 100
#
wlan ap ap2 model WA2612 id 2
 serial-id 219801A0CJC124002846
 radio 1
  service-template 1
  service-template 2
  radio enable
#
 ip route-static 10.153.43.0 255.255.255.0 10.153.43.148
#
 undo info-center logfile enable
#
 dhcp enable
#
 user-profile SSID1 enable
 user-profile SSID2 enable
#
 load xml-configuration
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

2. 采用802.1x认证AC上的配置信息：

```
<WX5004>dis cu
#
 version 5.20, Release 2308P23
#
 sysname WX5004
#
 domain default enable system
#
 telnet server enable
#
```

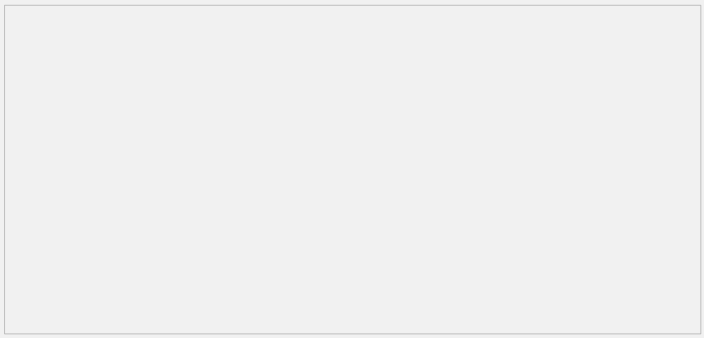
```
 port-security enable
#
 dot1x authentication-method eap
#
portal local-server http
#
undo password-recovery enable
#
vlan 1
#
vlan 10
#
vlan 100
#
vlan 4000
#
radius scheme dot1x
 primary authentication 10.153.43.148
 primary accounting 10.153.43.148
 key authentication cipher $c$3$yZomOUw3PnoJ5uV/cfY7B4WSAEtbXrNz
 key accounting cipher $c$3$e+PwLiyQet7l9In2CwzW2tYXaGHMih8H
 user-name-format without-domain
 nas-ip 192.168.121.154
#
domain dot1x
 authentication lan-access radius-scheme dot1x
 authorization lan-access radius-scheme dot1x
 accounting lan-access radius-scheme dot1x
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut enable 10 10240
 self-service-url disable
#
dhcp server ip-pool ap
 network 192.168.0.0 mask 255.255.255.0
 gateway-list 192.168.0.54
#
dhcp server ip-pool client
 network 192.168.121.0 mask 255.255.255.0
 gateway-list 192.168.121.154
 dns-list 88.8.8.8
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher $c$3$nmBMe/uKDpkC4Xtv6LT2J3/1dyLYc5D+
 authorization-attribute level 3
 service-type telnet
#
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
#
wlan service-template 3 crypto
```

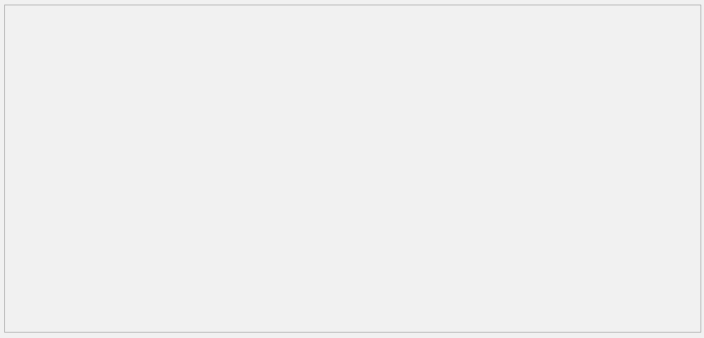
```
 ssid dot1x_mac
 bind WLAN-ESS 3
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
wlan service-template 4 crypto
 ssid dot1x_nac
 bind WLAN-ESS 4
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
user-profile SSID3
 wlan permit-ssid dot1x_mac
user-profile SSID4
 wlan permit-ssid dot1x_nac
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.0.54 255.255.255.0
#
interface Vlan-interface100
 ip address 192.168.121.154 255.255.255.0
#
interface Vlan-interface4000
 ip address 10.153.43.156 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
 port access vlan 4000
#
interface Ten-GigabitEthernet1/0/5
#
interface WLAN-ESS3
 port access vlan 100
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain dot1x
 undo dot1x multicast-trigger
#
interface WLAN-ESS4
 port access vlan 100
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain dot1x
 undo dot1x multicast-trigger
#
wlan ap ap2 model WA2612 id 2
 serial-id 219801A0CJC124002846
 radio 1
  service-template 3
  service-template 4
  radio enable
```

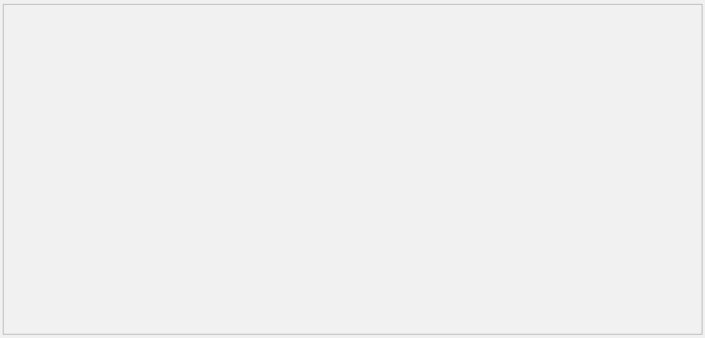
```
#
 ip route-static 10.153.43.0 255.255.255.0 10.153.43.148
#
 undo info-center logfile enable
#
 dhcp enable
#
user-profile SSID3 enable
user-profile SSID4 enable
#
 load xml-configuration
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

3. iMC服务器上有关Portal和802.1x的基本配置请分别参考KMS-22518和KMS-21186，这里针对接入规则、接入服务及用户账号的相关配置做详细说明：

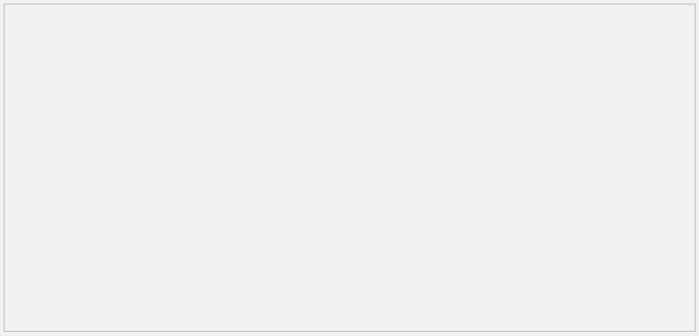
(1).Portal配置时，需要在接入规则中配置user-profile的名称以及勾选绑定用户MAC，其他配置和普通Portal相同，如下图所示：







(2).相比Portal，802.1x只需要在接入规则设置时选择相应的证书认证类型即可：



4.PC终端（Win 7操作系统）上关于802.1x配置步骤请参考KMS-21716。

五、配置关键点：

1.设备上的配置和普通portal和802.1x基本一致，只需增加user-profile的相关配置即可，必须在全局视图下使能（enable）user-profile，否则会出现认证立刻下线的问题。

2.iMC上配置和普通的也基本类似，接入设备配置和portal配置完成后，可以按照接入规则管理配置（是否启用证书认证、是否下发user-profile、是否绑定用户MAC地址）、接入服务配置（是否携带服务后缀、选择相应接入规则）、增加接入用户、增加账号（账号名、密码、绑定相应接入服务）的顺序配置，记得下发的user-profile和设备上保持一致（包括大小写），注意802.1x认证的证书类型（Eap-Peap还是Eap-TLS）。

3.所有账号第一次认证后，可以从iMC所有接入用户视图中看到各个账号绑定的MAC地址。iMC也支持账号创建时候绑定MAC，需要按照要求格式输入正确即可。

4.简单来讲，这种组网下用户账号、终端MAC地址、SSID三者是完全严格对应关系，任何一个替换后都无法认证成功。

5.需要特别注意的是，由于user-profile是在radius code 2号报文里携带的，设备收到iMC的code 2回应后，会通过下发user-profile的name在设备上查询，一旦查询发现问题（permit-SSID不匹配或者全局user-profile未enable）,会立刻把终端踢下线，设备上日志信息提示user got online failed，同时iMC无法收到设备回送的ack，因此如果是由于user-profile错误导致的认证失败在iMC上是无法看到认证失败日志、接入明细等信息的，Radius的报文也就中止在code 2，portal认证时会看到页面提示上线成功后又立刻下线的情况，dis connection和iMC上所有在线用户都看不到用户在线，但如果portal页面有弹出的计时小框，不会消失，这点需要格外注意。

六、验证结果：

1. 采用Portal认证的结果验证：

第一次认证时，PC1关联“portal-mac”采用账号“portal1”认证，PC2关联“portal-nac”采用账号“portal2”认证，这时由于iMC上这两个账号绑定的接入规则决定了这两个账号分别会和PC1和PC2的MAC地址做绑定，记录下相关绑定信息。下线后，PC1用账号“portal2”认证失败，网页提示“E63025::MAC地址绑定检查失败”,PC2用账号“portal1”认证失败，网页同样提示“E63025::MAC地址绑定检查失败”。

随后，PC1和PC2断开关联，PC1关联“portal-nac”,用“portal1”认证会被设备踢下线（user-profile检查错误），用“portal2”认证提示“E63025::MAC地址绑定检查失败”，PC2测试结果相同，不再赘述。相关截图如下：

2. 采用802.1x认证的结果验证：

第一次认证时，PC1关联“dot1x_mac”采用账号“dot1x1”认证，安卓手机（4.0版本）关联“dot1x_nac”采用账号“dot1x2”认证，这时由于iMC上这两个账号绑定的接入规则决定了这两个账号分别会和PC1和安卓手机的MAC地址做绑定，记录下相关绑定信息。下线后，PC1用账号“dot1x2”认证失败，查看iMC日志显示“E63025：：MAC地址绑定检查失败”,安卓手机用账号“dot1x1”认证失败，iMC日志同样显示“E63025：：MAC地址绑定检查失败”。

随后，PC1和PC2断开关联，PC1关联“dot1x_nac”,用“dot1x1”认证会被设备踢下线（user-profile检查错误），用“dot1x2”认证iMC日志显示“E63025：：MAC地址绑定检查失败”，安卓手机测试结果相同，不再赘述。

3. 相关认证的结果及截图：

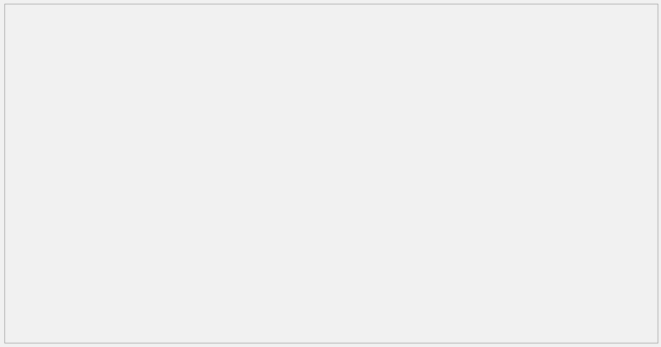
(1).Portal认证成功后，设备上的信息：

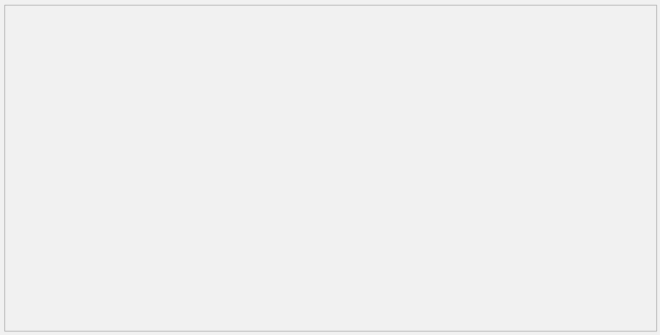
[WX5004]dis connection

Index=322 ,Username=portal1@imc
MAC=24-77-03-91-77-20
IP=192.168.121.1
IPv6=N/A
Total 1 connection(s) matched.
[WX5004]dis connection ucibindex 322
Index=322 , Username=portal1@imc

MAC=24-77-03-91-77-20
IP=192.168.121.1
IPv6=N/A
Access=PORTAL ,AuthMethod=CHAP
Port Type=Wireless-802.11,Port Name=Vlan-interface100
Initial VLAN=100, Authorization VLAN=N/A
ACL Group=Disable
User Profile=SSID1
CAR=Disable
Priority=Disable
Accounting Username=portal1
Start=2013-08-02 09:05:39 ,Current=2013-08-02 09:06:20 ,Online=00h00m41s
Total 1 connection matched.
[WX5004]

(2).认证失败的网页提示和iMC日志信息：





(3).802.1x认证类似，不再赘述。