iMC UAM BYOD功能与AC结合实现8021x快速接入认证的典型配置

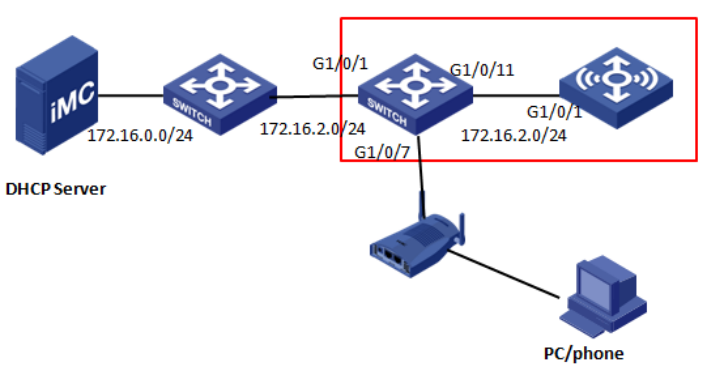
BYOD 寻尚岩 2013-07-26 发表

iMC UAM BYOD功能与AC结合实现8021x快速接入认证的典型配置

一、组网需求

基于H3C iMC UAM的BYOD可与无线Portal、8021x、无线MAC配合使用。BYOD结合无线MAC认证无法进行安全检查，8021x认证或者portal认证可以解决这一问题。本文以BYOD结合8021x认证为例，BYOD结合8021x认证主要是将终端与已有账号绑定，直接使用已有账号认证并根据终端类型应用不同的安全控制策略，需要注意的是终端第一次接入网络时，由于认证通过前还未获取IP地址，所以默认接入规则必须为证书认证，等终端MAC地址信息已经写入UAM中时，默认接入规则将不再起作用。

二、组网图



注：

1：UAM从E0401版本开始支持BYOD；

2：图中红色区域为WX3010，为便于理解，将其中的交换网板模拟为一交换机；

3：AP属于VLAN 4，由AC动态分配IP；

4：终端属于VLAN 8，由iMC服务器分配IP；

三、配置步骤

1.交换机配置

划分业务VLAN 2，15口为与交换板相连接口。

[1234]vlan 2

[1234-vlan2]port g2/0/15

[1234]inter vlan 2

[1234-Vlan-interface2]ip address 172.16.2.3 255.255.255.0

配置静态路由

[1234]ip route-static 172.16.8.0 24 172.16.2.2

2.交换板配置

划分业务VLAN

[H3C]vlan 2，

[H3C-vlan2]port g1/0/1

为vlan2分配IP地址

[H3C-vlan2]inter vlan 2

[H3C-Vlan-interface2]ip address 172.16.2.2 24

G1/0/7口与AP相连，所以需放通VLAN 4，且为AP供电

[H3C-GigabitEthernet1/0/7]poe enable

[H3C-GigabitEthernet1/0/7]port access vlan 4

G1/0/11口为内置与AC互联端口，该端口需配置成trunk类型，且必须允许业务vlan2和AP所属vlan4通过（用户vlan经过ap时会被打上vlan 4的标签）

[H3C-GigabitEthernet1/0/7]inter g1/0/11

[H3C-GigabitEthernet1/0/11]port link-type trunk

[H3C-GigabitEthernet1/0/11]port trunk permit vlan 2 4

[H3C-GigabitEthernet1/0/11]port trunk pvid vlan 2

3.AC配置

G1/0/1口为内置与交换板互联端口，该端口需配置成trunk类型，且必须运行业务vlan2和AP所属vlan4通过

[AC]inter g1/0/1

[AC-GigabitEthernet1/0/1]port link-type trunk

[AC-GigabitEthernet1/0/1]port trunk permit vlan 2 4

[AC-GigabitEthernet1/0/1]port trunk pvid vlan 2

[AC-GigabitEthernet1/0/1]vlan 2

为业务vlan分配IP

[AC-vlan2]inter vlan 2

[AC-Vlan-interface2]ip address 172.16.2.1 24

开启DHCP功能为AP分配IP地址

[AC]dhcp enable

[AC]dhcp server ip-pool ap

[AC-dhcp-pool-ap] network 172.16.4.0 mask 255.255.255.0

指定AP网关

[AC-dhcp-pool-ap] gateway-list 172.16.4.1

划分用户vlan

[AC]vlan 8

[AC-vlan8]inter vlan 8

[AC-Vlan-interface8]ip add 172.16.8.1 24

BYOD功能要求用户IP地址由DHCP agent分配，这样UAM才能根据DHCP特征识别终端信息，所以AC需配置dhcp中继，DHCP服务器IP为iMC服务器地址

[AC]dhcp relay server-group 1 ip 172.16.0.9

配置用户vlan工作在中继模式

[AC-Vlan-interface8]dhcp select relay

指定分配IP的DHCP server，这样终端用户获取IP时，UAM就会从DHCP request请求中提取dhcp 特征识别终端信息

[AC-Vlan-interface8]dhcp relay server-select 1

认证相关信息配置：

使能端口安全，类似于交换机全局dot1x作用：

[H3C]port-security enable

证书认证只能采用eap认证方式

[H3C]dot1x authentication-method eap

配置radius 认证信息

[AC-Vlan-interface8]rad sch h3c

标准模式不支持EAD，尽量选择扩展模式

[AC-radius-h3c]server-type extended

[AC-radius-h3c]primary authentication 172.16.0.9

[AC-radius-h3c]primary accounting 172.16.0.9

[AC-radius-h3c]key authentication h3c

[AC-radius-h3c] key accounting h3c

配置domain 8021x,并引用h3c

[AC]domain 8021x

[AC-isp-8021x] authentication lan-access radius-scheme h3c

[AC-isp-8021x] authorization lan-access radius-scheme h3c

[AC-isp-8021x] accounting lan-access radius-scheme h3c

创建服务模板3，与AP关联后使用密文发送数据

[AC] wlan service-template 3 crypto

创建8021x认证时使用的ssid

[AC-wlan-st-3] ssid x_dot1x

绑定无线虚拟接口3

[AC-wlan-st-3] bind WLAN-ESS 3

配置在帧加密时使用的加密套件为tkip或者ccmp

[AC-wlan-st-3] cipher-suite tkip

[AC-wlan-st-3] cipher-suite ccmp

设置在AP发送信标和探查响应帧时携带WPA IE，即认证方式为WPA

[H3C-wlan-st-3]security-ie wpa

激活服务模板3（激活前需创建无线接口3）

[AC-wlan-st-3] service-template enable

创建无线虚拟接口3

[AC]inter WLAN-ESS 3

允许用户vlan通过

[AC-WLAN-ESS1]port access vlan 8

对接入用户采用基于MAC的802.1X认证，且允许端口下有多个802.1X用户

[H3C-WLAN-ESS3]port-security port-mode userlogin-secure-ext

开启11key类型的密钥协商功能：

[H3C-WLAN-ESS3]port-security tx-key-type 11key

指定用户的认证域为8021x：

[H3C-WLAN-ESS3]dot1x mandatory-domain 8021x

注册AP并进行设置

[AC]wlan ap x_byod_ap

[AC-wlan-ap-x_byod_ap] serial-id 210235A29E0087000090

[AC-wlan-ap-x_byod_ap] radio 1

[AC-wlan-ap-x_byod_ap-radio-1]service-template 3

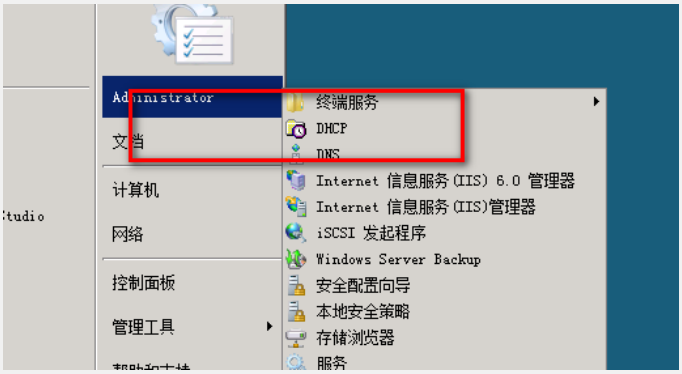
[AC-wlan-ap-x_byod_ap-radio-1]radio enable

[AC-wlan-ap-x_byod_ap-radio-1]radio 2

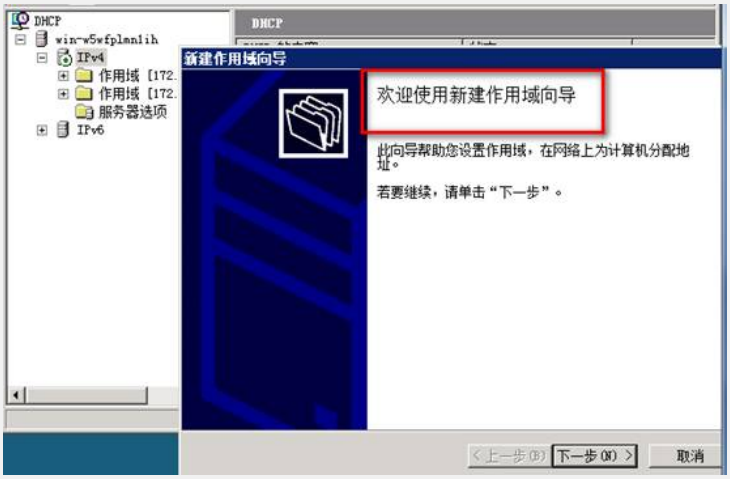
[AC-wlan-ap-x_byod_ap-radio-2]service-template 3

[AC-wlan-ap-x_byod_ap-radio-2]radio enable

4.DHCP server配置，需安装DHCP server和DNS server，具体安装过程略

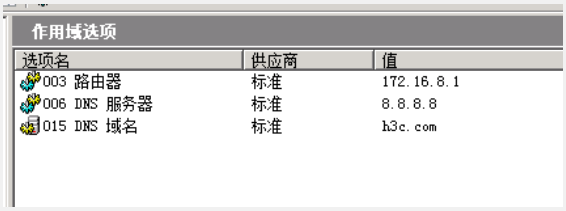


新建IPV4作用域(DHCP server保证已授权)



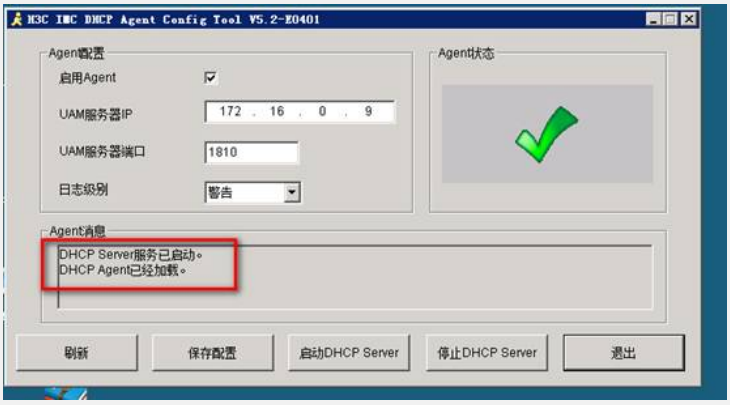
点击下一步输入作用域名称，配置地址池

指定网关为172.16.8.1，dns为8.8.8.8,



服务器选项再次指定DNS

安装dhcp agent（UAM安装包内有安装文件）插件，过程略，安装配置完成后启动agent插件：

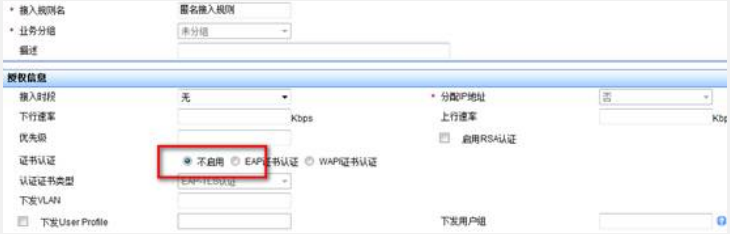


5.iMC侧配置，byod结合8021x认证适用于已经存在接入账号，该账号用不同的终端认证时，接受的安全控制策略也不相同。本例要求PC认证时必须使用iNode客户端且进行安全检查，手机认证上线时只需下发ACL，ACL要求手机不能访问172.16.0.11，具体的配置包括

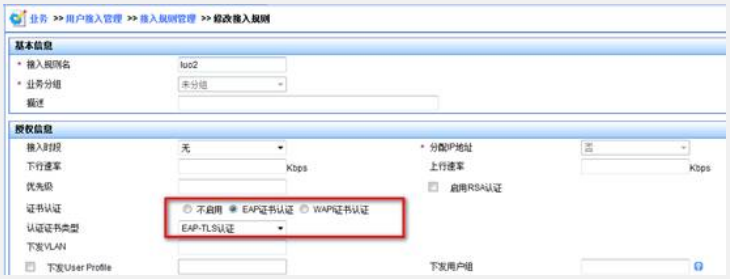
增加接入设备，和常规配置一致

创建三个接入规则，一个匿名接入规则，另外两个 接入规则分别用于不同的接入场景：

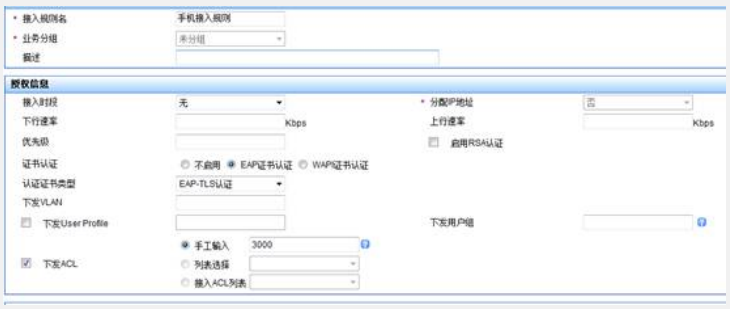
匿名接入规则



PC用接入规则



手机接入规则：

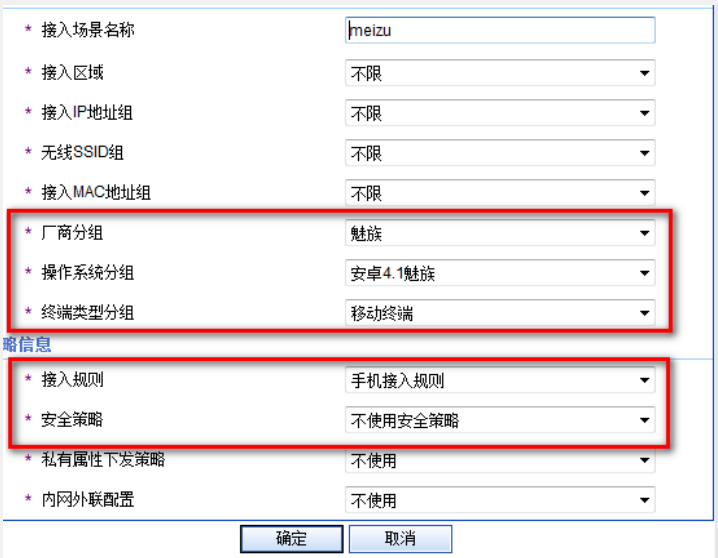


配置已有账号luo2并引用认证服务，在线数量设置为3，这样可以多个终端同时在线

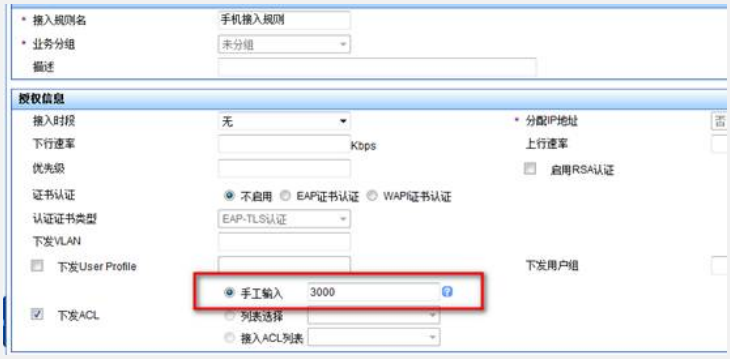
配置已有账号luo2引用的服务，该服务有两个接入场景（注意：缺省接入规则为匿名接入规则，终端第一次上线时，需保证该规则为证书认证方式，终端认证通过后，则对该规则没有要求）

PC场景对应PC接入，接入规则为luo2

Meizu场景对应手机接入：



手机接入规则：



设备acl配置：

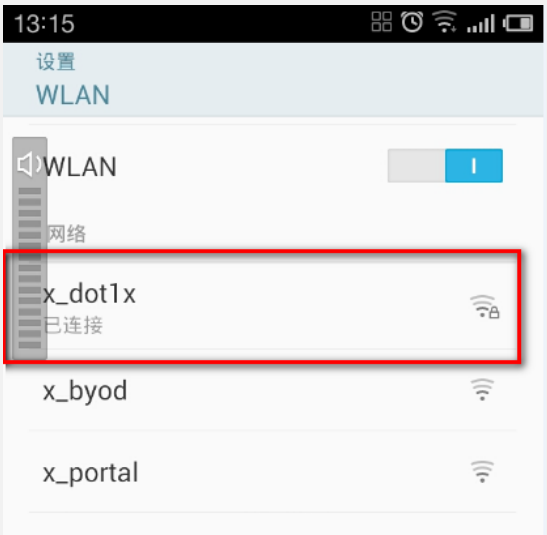
```
[AC]dis ac
[AC]dis acl 3000
Advanced ACL  3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 deny ip destination 172.16.0.11 0
 rule 1 permit ip

[AC]
```

证书配置：

手机、UAM侧分别分别安装证书，具体配置略。

PC认证，由于是802.1x认证，终端第一次认证通过后还未获取到IP，所以UAM无法判断终端类型，即不能应用安全控制策略，所以UAM会强制用户下线并应用新的策略。

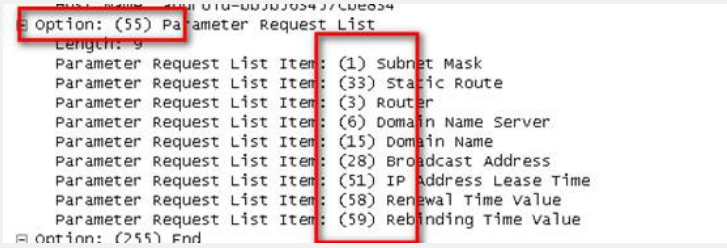
手机认证：



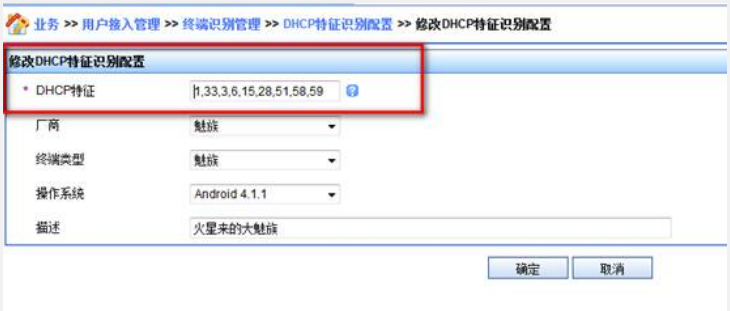
在线用户信息：

可以看出UAM已经通过DHCP特征方式识别出终端类型并应用了不同的安全策略，具体的识别过程如下：

终端在向DHCP server获取IP时会发生dhcp request请求，报文如下：从中可以看出该终端的dhcp 特征码为1,33,3,6,15,28,51,58,59，



而这些特征码是和在UAM中之前预定义的魅族特征码相一致，也就是说只要某个终端的DHCP特征码是这个值，均会被识别为魅族。DHCP特征码中的厂商、终端类型和操作系统信息均需要提前添加。



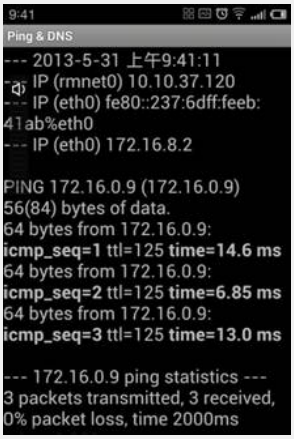
首先增加厂商信息：

然后增加终端类型

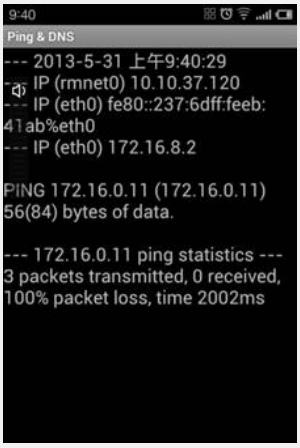
增加操作系统信息，该信息可通过抓包或者从portal日志里面获取

手机认证时：

手机ping172.16.0.9时:



Ping 172.16.0.11时:



可见，已经达到了预期的效果

四、注意事项

1：该认证方式前提要求已经在UAM侧创建了账号，认证时输入账号信息即可；

2：终端第一次认证上线时，由于未获取IP，所以UAM不会识别终端信息， 也不会应用终端的场景信息，等终端认证通过并获取IP后；终端第二次认证时才会匹配场景信息。

3：第一次认证上线时，默认接入规则需为证书认证；

4：客户端证书名称必须与认证账号一至；

5：如果用系统自带客户端认证，则终端第一次认证通过后，终端并不会立即下线，只有等终端打开域名并跳转至BYOD页面后才会下线并应用新的控制策略。