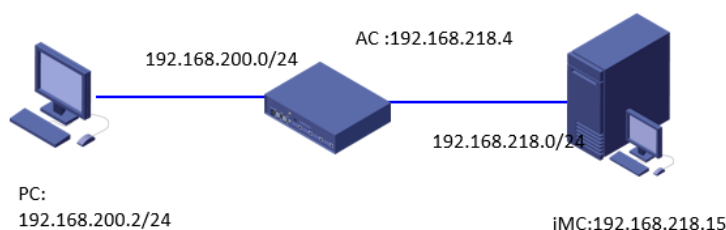


## 知 iMC EIA 7.2 E0408版本和V7设备配合实现有线MAC认证的典型配置案例

Portal 李树兵 2016-08-09 发表

MAC是目前常见的几种认证之一，很多的公司采用此种认证。本文档简单介绍目前iMC EIA最新版本7.2 E0408配合V7设备实现有线MAC认证。本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。本文档假设您已了解AAA、MAC认证。



此案例中认证PC的地址为192.168.200.2（当然，MAC认证之前客户端可以不配置地址，通过DHCP自动获取），网关为192.168.200.50，位于AC的interface vlan 100上，另一个接口地址为192.168.218.4，与iMC互联，iMC的地址为192.168.218.15，作为认证的RADIUS服务器。

iMC EIA版本信息：7.2 E0408

VAC版本信息：7.1.064, ESS 1111

```
mac-authentication //开启MAC认证
mac-authentication domain mac //设置MAC认证的domain域为mac
mac-authentication user-name-format mac-address with-hyphen //设置MAC认证的用户名的格式采用XX-XX-XX-XX-XX-XX
#
vlan 100 //配置连接的vlan，vlan 100
interface Vlan-interface100 //配置PC的网关
ip address 192.168.200.50 255.255.255.0
#
interface GigabitEthernet2/0 //配置连接iMC的接口
port link-mode route
ip address 192.168.218.4 255.255.255.0
#
interface GigabitEthernet3/0 //配置连接认证PC的接口
port link-mode bridge
port access vlan 100
mac-authentication //开启接口的MAC认证功能
snmp-agent //配置SNMP参数，用于iMC网管
snmp-agent local-engineid 800063A280000C2994455600000001
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 192.168.218.15 params securityname public v2c
radius scheme mac //配置 radius scheme mac
primary authentication 192.168.218.15 //指定认证的服务器地址为192.168.218.15
primary accounting 192.168.218.15 //指定计费的服务器地址为192.168.218.15
accounting-on enable //打开计费功能。在accounting-on功能处于使能的情况下，若集中式设备或分布式设备上的单板重启，则设备或单板会在重启之后发送accounting-on报文通知该方案所使用的RADIUS计费服务器，要求RADIUS服务器停止计费且强制该设备的用户下线。
key authentication cipher $c$3$aB4c1D9n+ogtXeoF4on0qPydGvYxrg== //配置认证的key，这里配置为h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。
```

key accounting cipher \$c\$3\$j4MZ6dSvKV0Meyxj1nAHdBy+Hcg0XA== //配置计费的key，这里配置为h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。这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。

user-name-format without-domain //配置认证用户不带domain域，对应iMC侧接入服务不能添加服务后缀

nas-ip 192.168.218.4 /指定设备发送RADIUS报文的源地址为192.168.218.4，iMC对应接入设备里面配置的地址也应该为192.168.218.4，否则会导致认证不成功。

domain mac //配置domain域mac

authorization-attribute idle-cut 10 10240000 //类似于V5设备上的idle-cut，用于在设备上检测用户是否在线。指定ISP域imc下的用户闲置切断时间为10分钟，闲置切断时间内产生的流量为10240000字节。

authentication lan-access radius-scheme mac //设置用户认证的radius方案为mac

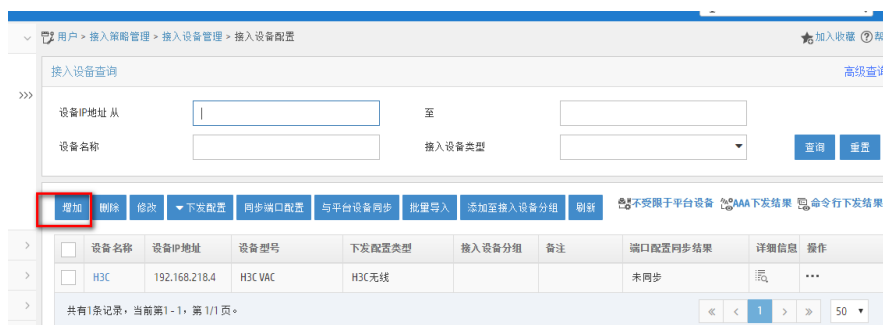
authorization lan-access radius-scheme mac //设置用户授权的radius方案为mac

accounting lan-access radius-scheme mac //设置用户计费的radius方案为mac

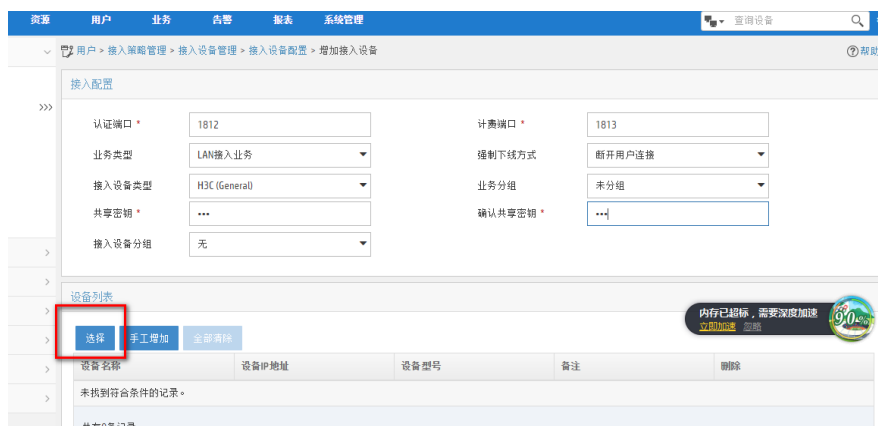
## 二.iMC配置：

iMC网管加入设备的过程略过，从iMC增加接入设备开始。

### 第一步：增加接入设备



点击到增加设备的页面，选择“增加”选项

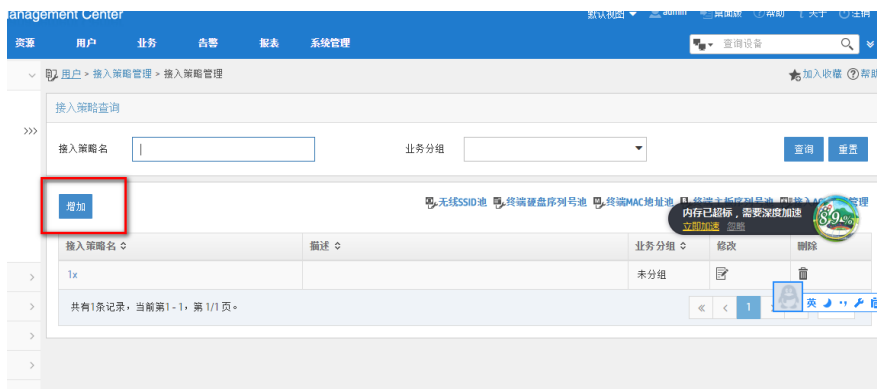


802.1x认证、portal认证以及MAC认证业务类型需要选择“LAN接入业务”，否则认证的时候会提示“no this user”，输入共享密钥，此处密钥需要和设备上配置radius scheme里面认证和计费的密钥一致。点击“选择”增加设备，此处需要先将设备通过iMC网管之后才可以看到。

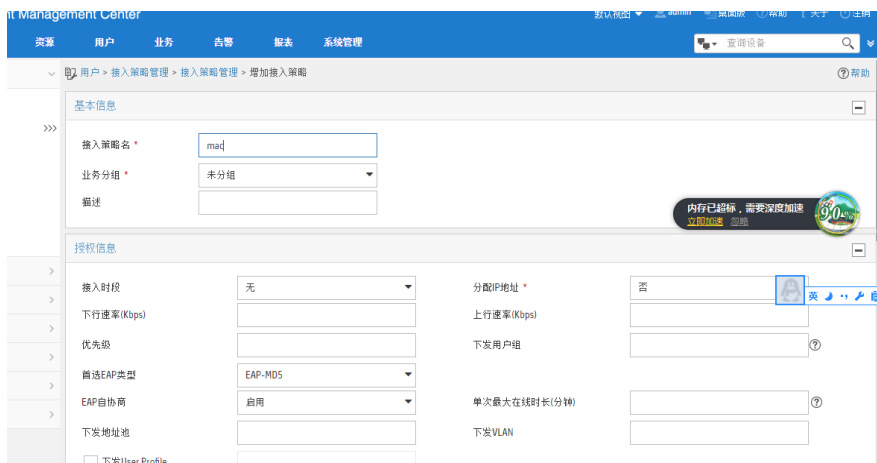


选择好之后如上图，点击确认即可添加成功。

### 第二步：增加接入策略

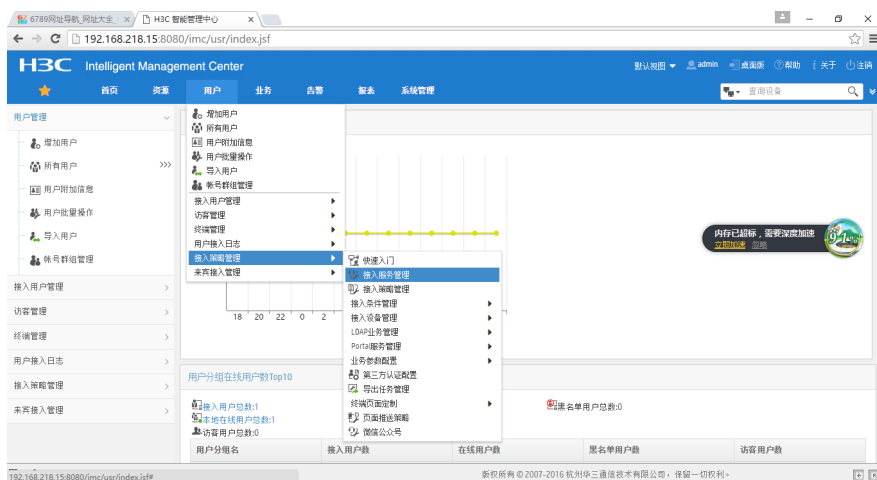


点击接入策略管理页面，点击“增加”选项进行接入策略的增加

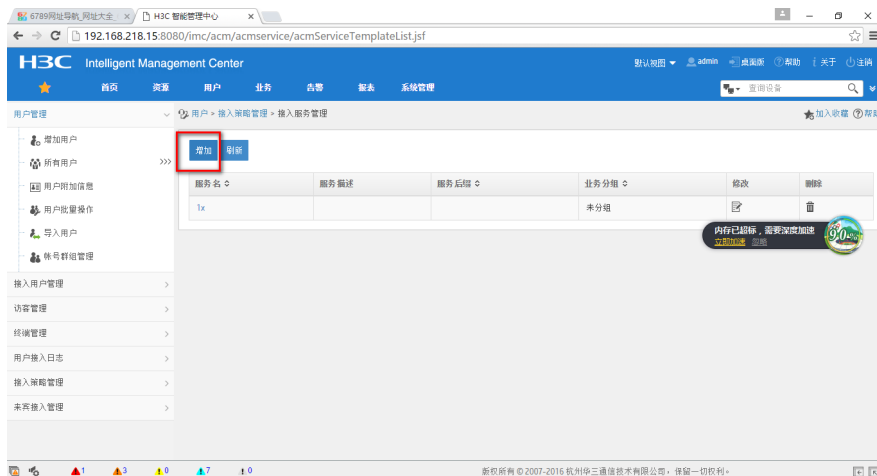


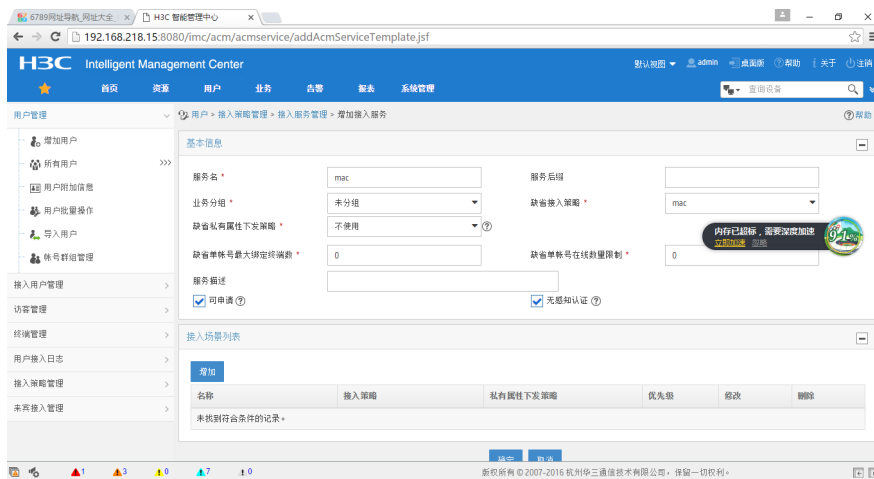
输入策略名，如果没有其他安全要求或者用户限速等要求的话直接点击下面的确定即可。

第三步：增加接入服务



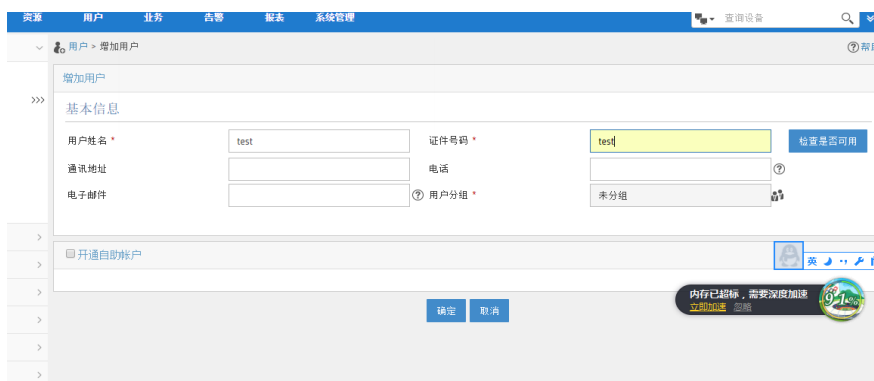
点击接入服务管理，点击“增加”选项进行接入服务的增加





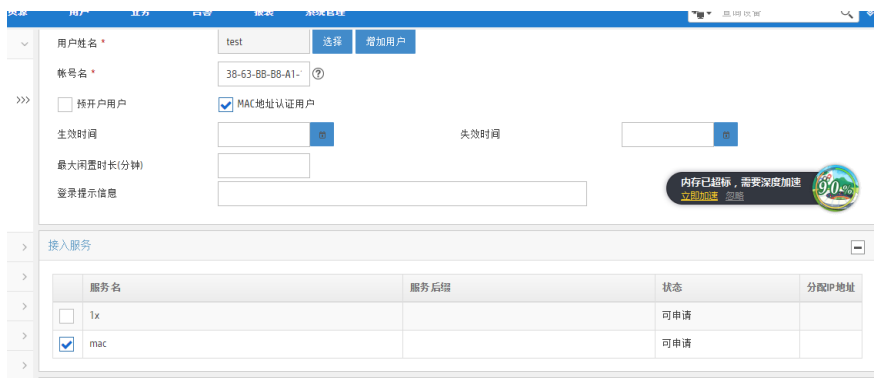
输入服务名，缺省接入策略选择为刚刚配置的“mac”，其他的按照默认即可。

第四步：增加接入用户,点击“用户”，选择“增加用户”来增加平台用户



点击确认即可。

增加平台用户成功，选择增加接入用户



输入接入用户的用户名用户名为MAC地址，格式为XX-XX-XX-XX-XX-XX，选择“MAC地址认证用户”，密码无需添加，自动将mac地址设置为密码。接入服务选择刚刚配置的“mac”，点击确定即可完成配置。

三.验证配置：

MAC认证终端无感知，接口连接之后就开始了MAC认证。可以在IMC和设备上查看在线用户

[H3C-GigabitEthernet3/0]dis mac-authentication connection

Total connections: 1

Slot ID: 0

User MAC address: 3863-bbb8-a21a

```

Access interface: GigabitEthernet3/0
Username: 38-63-bb-b8-a2-1a
Authentication domain: mac
Initial VLAN: 100
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL ID: N/A
Authorization user profile: N/A
Termination action: Default
Session timeout period: 86400 s
Online from: 2016/08/07 18:45:23
Online duration: 0h 7m 7s
[H3C-GigabitEthernet3/0]dis mac-authentication interface g3/0
Global MAC authentication parameters:
  MAC authentication      : Enabled
  User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
    Username             : mac
    Password             : Not configured
  Offline detect period  : 300 s
  Quiet period           : 60 s
  Server timeout         : 100 s
  Authentication domain  : mac
Online MAC-auth wired users : 1
Silent MAC users:
  MAC address  VLAN ID  From port  Port index
GigabitEthernet3/0 is link-up
  MAC authentication      : Enabled
  Carry User-IP          : Disabled
  Authentication domain   : Not configured
  Auth-delay timer        : Disabled
  Re-auth server-unreachable : Logoff
  Guest VLAN             : Not configured
  Guest VLAN auth-period  : 30 s
  Critical VLAN           : Not configured
  Host mode               : Single VLAN
  Max online users        : 4294967295
  Authentication attempts : successful 1, failed 3
  Current online users    : 1
    MAC address  Auth state
    3863-bbb8-a21a  Authenticated

```

略