iMC-EIA终端MAC地址池控制策略典型配置

Radius 罗孝晨 2016-11-24 发表

iMC-EIA的终端MAC地址池功能是通过管理一个允许接入的MAC地址池列表或者一个禁止接入的MAC地址池列表来限制用户对网络的使用。终端MAC地址池和接入策略中“启用终端MAC地址控制”一起配合使用。只有在接入策略中选中该选项，MAC地址管理才会生效。 MAC地址列表的类型（允许接入或禁止接入）由接入控制类型决定，具体说明如下：

（1）修改接入控制类型页面，配置接入控制类型为允许接入：操作员可以配置允许接入MAC地址列表。接入用户上线时，如果该用户的MAC地址在允许接入MAC地址列表中，则用户成功上线；如果该用户的MAC地址不在列表中，则用户不能上线。当接入MAC地址列表为空时，用户接入网络不受该功能限制，所有用户可正常接入网络。

（2）修改接入控制类型页面，配置接入控制类型为禁止接入：操作员可以配置禁止接入MAC地址列表。接入用户上线时，如果该用户的MAC地址在禁止接入MAC地址列表中，则用户不能上线。如果该用户的MAC地址不在列表中，则用户正常上线。

该功能重点在于iMC-EIA要获得终端MAC地址。根据Radius报文得知，Radius报文CODE=1（即认证请求报文）中Calling-Station-Id(31)号属性为终端MAC地址，如下图所示：

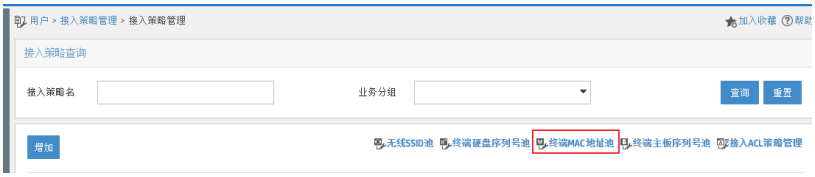
```
CODE = 1.
ID = 229.
ATTRIBUTES:
  User-Name(1) = "luoluo@ead".
  Password(2) = "$$$".
  NAS-IP-Address(4) = 3232264100.
  NAS-Identifier(32) = "AC".
  NAS-Port(5) = 16809992.
  NAS-Port-Id(87) = "0100008000000008".
  NAS-Port-Type(61) = 19.
  Service-Type(6) = 2.
  Framed-Protocol(7) = 255
  Calling-Station-Id(31) = "64-9A-BE-5E-D2-66".
  Called-Station-Id(30) = "68-66-BA-5E-C6-B0:......".
  Acct-Session-Id(44) = "11611212230270059b0061".
  Framed-IP-Address(8) = 3232237607.
  hw_Connect_ID(26) = 678.
  hw_Product_ID(255) = "H3C WX5540E".
  hw_IP_Host_Addr(60) = "192.168.8.39 64:9a:be:5e:d2:66".
  hw_Nas_Startup_Timetamp(59) = 1477841044.
```

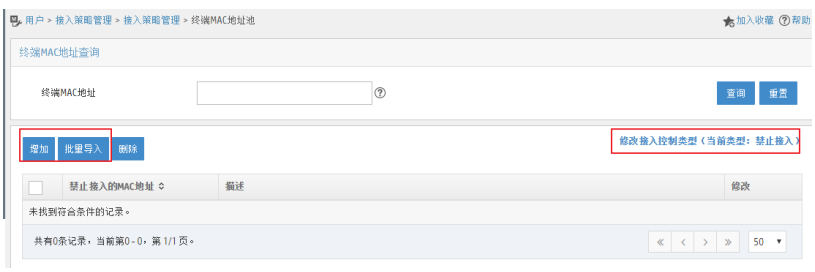
此案例采用Portal认证方式，对于Portal认证的配置此处不再进行详细讲解，参考KMS中Portal认证典型配置案例即可。

一、配置iMC的Portal认证基本配置项，如Portal设备、端口组、IP地址组等，此处不再进行详细描述。下面重点讲解终端MAC地址控制的配置要点。

（1）用户-接入策略管理-接入策略管理中修改Portal认证所用的接入策略，勾选认证绑定信息中“启用终端MAC地址控制”选项，如下图所示：

（2）添加终端MAC地址池的接入列表，具体位置如下图所示：



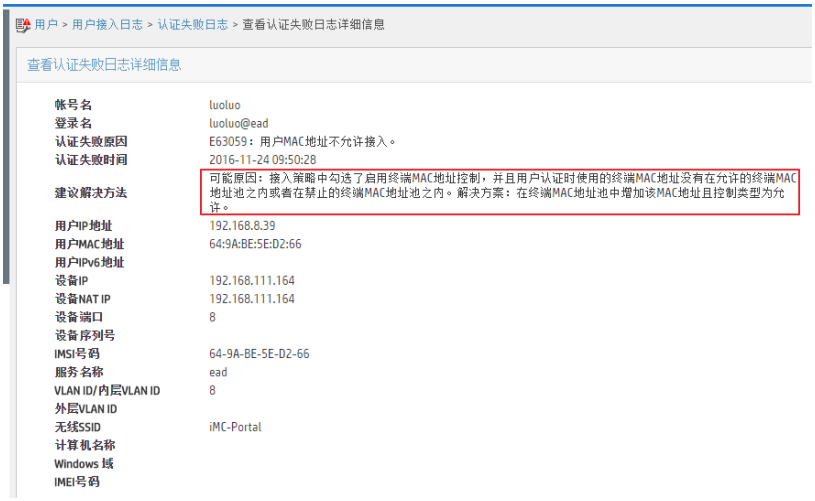


此处可以修改接入控制类型，如上图所示接入控制类型为“禁止接入”，即操作员可以配置禁止接入MAC地址列表。接入用户上线时，如果该用户的MAC地址在禁止接入的MAC地址列表中，则用户不能上线。如果该用户的MAC地址不在列表中，则用户正常上线。

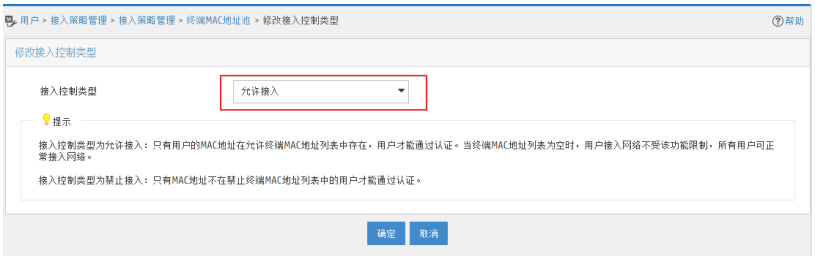
此案例中手工添加某一终端的终端MAC地址，当终端MAC数量过多时，可以采用批量导入接入MAC地址的方法将一定量的接入MAC地址导入MAC地址列表中。如下图所示：

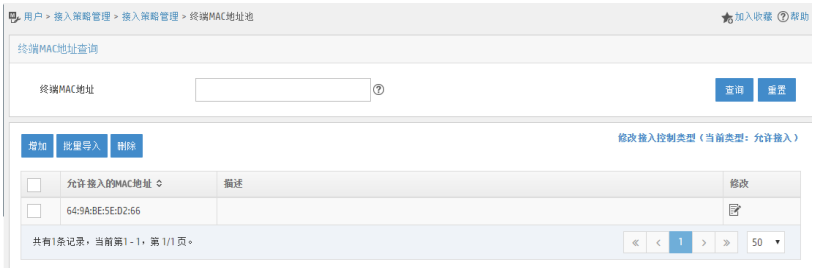
二、使用终端进行验证，连接Portal认证所用的SSID，在Portal认证页面输入用户名和密码后，点击上线按钮，效果如下图所示：

查看用户接入日志-认证失败日志，能够看到认证失败的原因及建议的解决方案，如下图所示：



当修改接入控制类型为“允许接入”，并添加同样的终端MAC地址之后，进行Portal认证测试，测试效果如下图所示，认证成功：

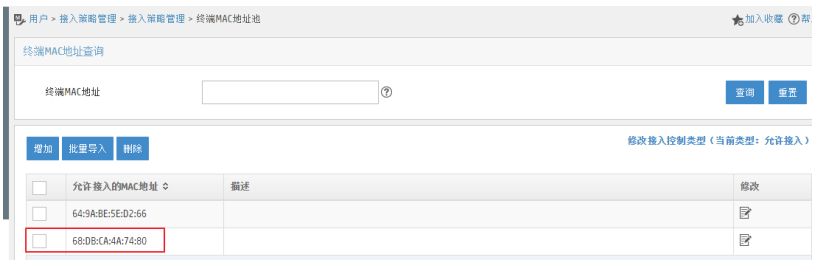




三、与接入策略中“绑定用户MAC”功能搭配使用效果（注：接入策略管理-业务参数配置-系统配置-用户绑定信息配置中MAC地址的自学习数量为1）

（1）当终端MAC控制列表为允许接入，且增加终端MAC地址时，测试认证效果如下：

（2）在终端MAC地址池中再添加一个终端MAC地址，根据MAC地址自学习数量为1的设置，使用刚刚添加的终端进行认证测试，使用与测试效果如下：

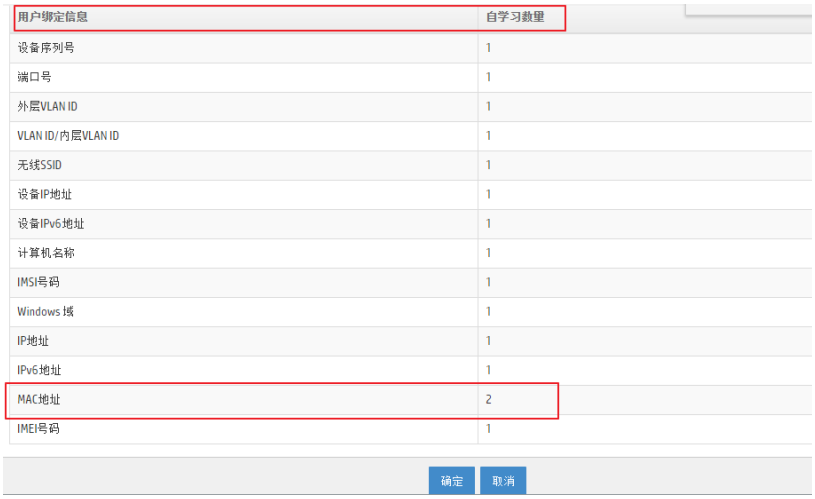


认证失败，提示MAC地址绑定检查失败。通过上述实验我们能够分析出，当接入策略里同时启用绑定用户MAC地址和启用终端MAC地址控制两项功能时，绑定用户MAC地址的优先级高于终端MAC地址控制。当接入用户的绑定信息中用户MAC地址没有被绑定时，即使在终端MAC地址为允许接入且配置了终端MAC地址列表时，终端仍然无法认证通过。

可以通过如下方法使第二个终端能认证通过：

（1）手工在接入用户的绑定信息列表中添加终端的MAC地址信息。

（2）修改用户绑定信息配置中，用户MAC地址的自学习数量，使终端第一次认证时能够自主绑定用户MAC，如下图所示：



（1）认证方式务必要保证设备能够在认证请求报文中上传终端MAC地址。

（2）接入策略中要勾选“启用终端MAC地址控制”

（3）MAC地址列表的控制类型有且只能设置一种，即“允许接入”和“禁止接入”只能设置一种方式，一旦控制类型确认且添加终端MAC地址后，不能直接改变控制类型。需要先将MAC地址列表删除后才能进行控制类型变更。

（4）MAC地址输入方式可以参考如下样例：XX:XX:XX:XX:XX:XX或者XX-XX-XX-XX-XX-XX或者XXXX-XXXX-XXXX以上三种方式。