iMC UAM终端接入MAC地址管理功能的配置

802.1X Portal **何颖** 2013-05-31 发表

iMC UAM终端接入MAC地址管理功能的配置

一、 组网需求：

5.1及以后的iMC UAM版本提供终端的接入MAC地址管理功能。接入MAC地址管理通过管理一个允许接入的MAC地址列表或者一个禁止接入的MAC地址列表来限制用户对网络的使用。具体组网需求依赖身份认证组网，该功能只是身份认证基础上的扩展功能，跟具体组网无关。

本案例所用UAM版本为UAM 5.2 E0402版本。

二、 组网图：

无

三、 配置步骤：

MAC地址列表的类型有允许接入和禁止接入。如图1所示，点击【业务】|【用户接入管理】|【接入场景管理】|【接入MAC地址管理】，进入接入MAC地址管理设置界面，其中“修改接入控制类型”即为设置开关。点击该链接可进行控制类型设置。

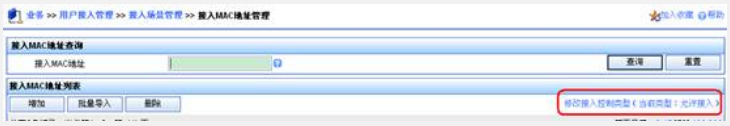

图1 接入MAC地址管理

控制类型由管理员根据业务需求设置，具体说明如下：

- 修改接入控制类型页面，配置接入控制类型为允许接入：管理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。
- 修改接入控制类型页面，配置接入控制类型为禁止接入：管理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。

本案例以控制类型为允许接入为例对此功能进行详细描述。

1、 按照上文所述，修改控制类型为允许接入。在此表中增加允许接入的MAC地址。增加的方式有两种：手工增加和批量导入。手工增加较简单，不做描述。本案例以批量导入方式增加MAC地址列表。首先，收集允许接入的MAC地址列表，编辑对应的文档为txt格式文件。如图2所示，用户的MAC地址和描述信息分两列，中间以空格分隔。点击“批量导入”，将该文本文件选择后导入，如图3所示，选择分隔符为空格（实际操作以实际分隔符为准），根据案例中提供的txt文件为例，选择接入MAC地址为第一列，描述为文件中的第二列。

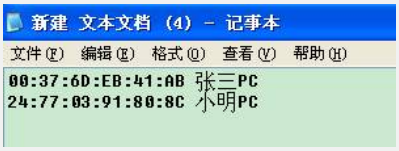

图2 MAC地址信息

图3 批量导入接入MAC地址

点击“确定”后，接入MAC地址信息就全部批量导入到iMC系统中，如图4所示。

图4 批量导入结果

2、 接入MAC地址管理和服务配置管理中“启用接入MAC地址控制”一起配合使用，只有在服务中选中该选项，MAC地址管理才会生效。因此，设置完接入MAC地址列表后，点击【业务】|【用户接入管理】|【接入规则管理】，增加一个接入规则，例如取名为“普通业务规则”。如图5所示，在规则中的“认证绑定信息”里选择“启用接入MAC地址控制”。确定后即可生效。

图5 认证绑定信息

3、 创建帐号所用的服务，例如服务名为mac，根据实际需求选择制定其他策略。比如本案例选择缺省接入规则为“普通接入规则”，同时也对该帐号做EAD，因此启用安全检查策略为xun_disk_pass。

图6创建服务

4、 创建帐号mactest，绑定服务mac。

图7 帐号信息

根据上述配置，测试效果如下：

l 当帐号所在终端MAC地址为24:77:03:91:80:8C时认证成功。

图8 认证成功效果图

l 当同样的账号在终端MAC地址为00:24:D6:9A:5E:D6的PC上认证时失败。

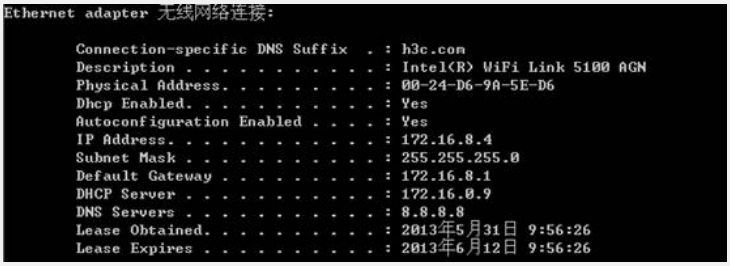

图9 禁止接入的终端认证失败效果图

l 当将MAC地址00:24:D6:9A:5E:D6添加到UAM允许接入的MAC地址列表中后，10:30:34时刻再起发起的身份认证成功（本案例的测试中该账号结合EAD认证，效果图同时演示EAD认证不通过的情况）。

图10 允许接入后的认证成功效果图

四、 配置关键点：

1） 接入MAC地址管理和服务配置管理中“启用接入MAC地址控制”一起配合使用，只有在服务中选中该选项，MAC地址管理才会生效。

2） 此功能目前仅支持MAC认证、802.1X认证和二层portal等多种认证方式，但三层Portal认证不支持此功能。