EAD和MAC地址本地认证结合的配置（一）

陈玉龙 2006-10-14 发表

EAD和MAC地址本地认证结合的配置（一）

一、组网：

1． PC的IP地址为1.1.1.1/8，交换机VLAN1的IP地址为1.1.1.2/8；

2． PC接在交换机的G1/0/1口；

3． 使能端口安全机制，先进行mac-authentication认证，如果成功则表明认证通过，如果失败则再进行dot1x认证。

二、组网图：

无

三、配置步骤：

1. 使能端口安全机制

[Switch] port-security enable

2. 进入以太网Ethernet1/0/1端口视图

[Switch] interface Ethernet1/0/1

3. 配置端口的安全模式为mac-else-userlogin-secure-ext

[Switch-Ethernet1/0/1] port-security port-mode mac-else-userlogin-secure-ext

4. 配置使用系统默认域为用户的MAC认证域

[Switch] MAC-authentication domain system

5. 配置认证方式为使用MAC地址为用户名

[Switch] MAC-authentication authmode usernameasmacaddress usernameformat with-hyphen

6. 添加MAC认证的用户（用户名和密码都为需要进行验证的PC机MAC地址）

[Switch] local-user local-user 00-15-c5-0d-1a-34

7. 设置MAC认证的密码

[Switch-luser-00-15-c5-0d-1a-34] password simple 00-15-c5-0d-1a-34

8. 服务类型为局域网接入类型

[Switch-luser-00-15-c5-0d-1a-34] service-type lan-access

9. 设置交换机为RADIUS服务器

[Switch]local-server nas-ip 127.0.0.1 key huawei

10. 添加本地接入用户

[Switch] local-user huawei

11. 设置本地用户的服务类型及用户级别

[Switch-luser-huawei] service-type lan-access

12. 设置密码

[Switch-luser-huawei] password simple huawei

四、配置关键点：

1. MAC认证和802.1X认证必须同时为本地认证或者同时为远程认证时才能成功，否则只有MAC认证能够成功，802.1X认证任何时候都无法通过；

2. MAC地址本地认证时，用户名和密码要配置成小写格式；远程认证时，用户名和密码需要配置为与认证服务器一致；

3. 正在进行MAC地址认证的时候，无法更改或删除用户配置；

4. MAC认证和802.1x认证都必须使用system做为其认证域，而且认证时间比较长；

5. 此处以H3C S3600-EI的本地认证为例，其他交换机如H3C S5600、Quidway S3900和Quidway S5600等配置相同。