WX系列AC与Windows IAS配合实现下发用户ACL权限功能的配置

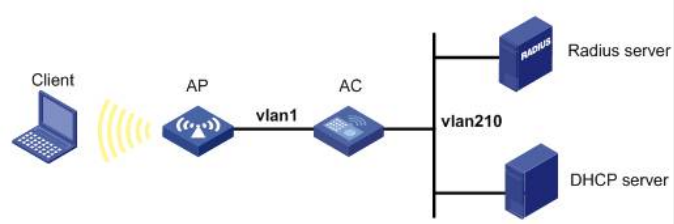
802.1X AAA ACL 宋斌 2012-03-14 发表

WX系列AC与Windows IAS配合实现下发用户ACL权限功能的配置

一、 组网需求：

WX系列AC、FIT AP、交换机、便携机（安装有无线网卡）、Windows IAS服务器、PC

二、 组网图：



本配置举例中的AP使用的是WA2200系列无线局域网接入点设备，AC使用的是WX6103系列无线控制器。Radius server的IP地址为8.1.45.67/24。Client和AP通过DHCP服务器获取IP地址。

Client通过认证后允许访问网络8.1.0.0/16即VLAN210，其他网络资源不允许访问。

三、 特性介绍：

下发ACL是接入设备与Radius服务器配合来对用户访问网络的权限进行控制。用户认证通过后根据Radius服务器报文中的ACL内容，对用户可以访问哪些网络资源，不可以访问哪些网络资源进行控制。

网络管理员可以通过下发ACL对用户访问网络的权限进行控制，具有很强的灵活性和适应性。

四、 主要配置步骤：

在Dot1x接入端配置802.1x和认证。

启用端口安全port-security，配置Dot1x认证方式为CHAP。

```
[AC] port-security enable
[AC] dot1x authentication-method chap
```

配置认证策略。

```
[AC] radius scheme radius
[AC-radius-radius] primary authentication 8.1.45.67
[AC-radius-radius] primary accounting 8.1.45.67
[AC-radius-radius] key authentication radius
[AC-radius-radius] key accounting radius
[AC-radius-radius] nas-ip 8.1.61.3
[AC-radius-radius] accounting-on enable
[AC-radius-radius] quit
```

配置认证域。

```
[AC] domain radius
[AC-isp-radius] authentication lan-access radius-scheme radius
[AC-isp-radius] authorization lan-access radius-scheme radius
[AC-isp-radius] accounting lan-access radius-scheme radius
[AC-isp-radius] quit
```

把配置的认证域cams设置为系统缺省域。

```
[AC] domain default enable radius
```

配置ACL。

```
[AC] acl number 3000
[AC-acl-adv-3000] rule 0 permit ip destination 8.1.0.0 0.0.255.255
[AC-acl-adv-3000] rule 1 deny ip
```

配置无线口，并在无线口启用端口安全（802.1x认证）。

[AC] vlan 10
[AC-vlan10] quit
[AC] interface WLAN-ESS10
[AC-WLAN-ESS10] port access vlan 210
[AC-WLAN-ESS10] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS10] quit

配置无线服务模板。

[AC] wlan service-template 10 clear
[AC-wlan-st-10] ssid radius
[AC-wlan-st-10] bind WLAN-ESS 10
[AC-wlan-st-10] service-template enable
[AC-wlan-st-10] quit

配置AP模板并绑定无线服务模板。

[AC] wlan ap wa2220x model WA2220X-AGP
[AC-wlan-ap-wa2220x] serial-id 210235A29E007C000009
[AC-wlan-ap-wa2220x] radio 2
[AC-wlan-ap-wa2220x-radio-2] channel 3
[AC-wlan-ap-wa2220x-radio-2] max-power 6
[AC-wlan-ap-wa2220x-radio-2] service-template 10
[AC-wlan-ap-wa2220x-radio-2] radio enable

配置VLAN虚接口

[AC] vlan 210
[AC] quit
[AC] interface vlan 210
[AC-Vlan-interface210] ip address 8.1.61.3 24
[AC] interface Vlan-interface 1
[AC-Vlan-interface210] ip address 7.0.0.61 24
[AC-Vlan-interface1] dhcp select relay
[AC-Vlan-interface1] dhcp relay server-select 1

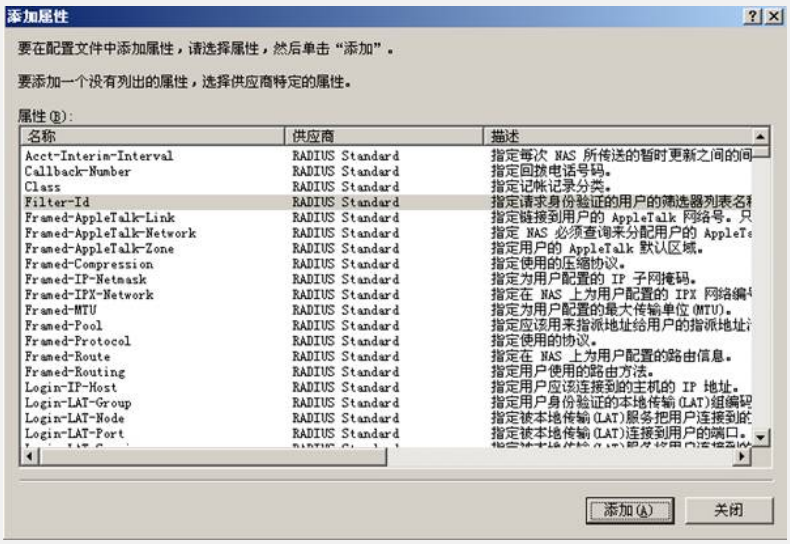
Windows IAS配置

在Windows IAS上配置ACL下发，需要在用户使用的“远程访问策略”中添加Filter-ID属性，配置方法如下：

（1）进入Internet 验证服务的远程访问策略，双击选取用户所使用的访问策略，点击<编辑配置文件>按钮，弹出“编辑拨入配置文件”窗口。

（2）在“编辑拨入配置文件”窗口中选取“高级”页签，点击<添加>按钮，弹出“添加属性”窗口。

（3）在“添加属性”中选取Filter-ID选项，双击Filter-ID，弹出“多值属性信息”对话框。

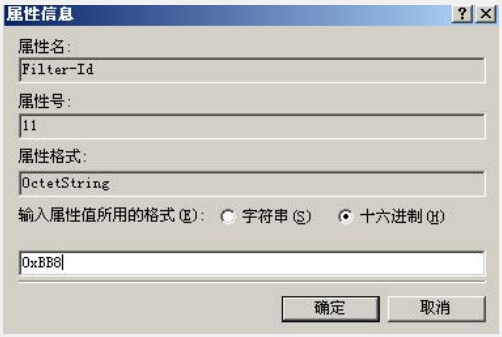


（4）在“多值属性信息”对话框中点击<添加>按钮，弹出“属性信息”窗口。

（5）在“属性信息”窗口中配置Fileter-ID属性值，我司字符串和十六进制格式均支持。FilterID属性数字表示ACL NUMBER。

l 设置输入属性值所用的格式为以字符串形式下发，下发的格式类型需要接入设备端支持。

l 设置输入属性值所用的格式为以十六进制数的形式下发，下发的格式类型需要接入设备端支持。



完后点击<确定>按钮，完成属性添加。

（6）完成属性添加后如下，点击<应用>按钮，然后确定完成。

五、 结果验证：

（1） Client连接 SSID，输入用户名和密码，上线成功。

（2）在AC上执行display connection可以看到有对应的Client的MAC地址，且ACL正确下发。

```
display connection ucibindex 1174
Index=1174, Username=test@radius
MAC=0810-742d-a88d
IP=N/A
Access=8021X ,AuthMethod=CHAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS10:78
Initial VLAN=10, Authorization VLAN=N/A
ACL Group=3000
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2008-09-14 17:05:38 ,Current=2008-09-14 17:05:51 ,Online=00h00m13s
Total 1 connection matched.
```

（3）Client可以访问网络8.1.0.0/16即VLAN210，其他网络资源不能访问。