WX系列AC与iMC配合实现下发用户ACL权限功能的配置

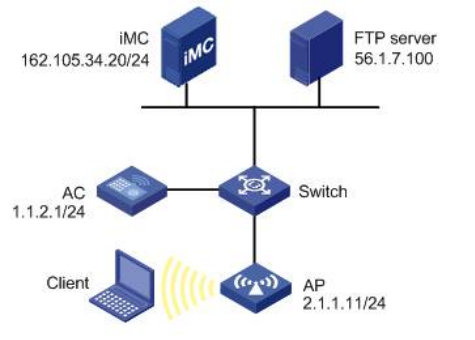
802.1X AAA ACL 宋斌 2012-03-14 发表

WX系列AC与iMC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）、iMC服务器、PC

二、 组网图：



本配置举例中的AC使用的是WX5002无线控制器，AP使用的是WA2100无线局域网接入点设备。

本配置举例中，AC通过VLAN2接入Switch，VLAN2的IP地址为1.1.2.1/24，AP通过VLAN1接入Switch，AP的IP地址为2.1.1.11/24，iMC的IP地址为162.105.34.20/24。网络中有一个FTP服务器，IP地址为56.1.7.100。各个设备间路由可达。交换机Switch启动DHCP服务向Client分配IP地址，客户端Client的网关在AC（VLAN2）。Client认证通过后，iMC向Client下发ACL3221，禁止Client访问FTP服务器。

三、 特性介绍：

ACL（Access Control List，访问控制列表）提供了控制用户访问网络资源和限制用户访问权限的功能。当用户上线时，如果RADIUS服务器上配置了授权ACL，则设备会根据服务器下发的授权ACL对用户所在端口的数据流进行控制；在服务器上配置授权ACL之前，需要在设备上配置相应的ACL规则。管理员可以通过改变服务器的授权ACL设置或设备上对应的ACL规则来改变用户的访问权限。

授权ACL下发一般可应用在如下场合：接入同一AC的同一SSID的多个用户，分别使用不同的资源，或限制用户使用部分网络资源。

四、 主要配置步骤：

在Dot1x接入端配置802.1x和认证。

配置VLAN虚接口。

```
[AC] interface Vlan-interface2
[AC-Vlan-interface2] ip address 1.1.2.1 255.255.255.0
```

启用端口安全Port-security，配置Dot1x认证方式为EAP。

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

配置radius scheme。

```
[AC] radius scheme testscheme2
[AC-radius-testscheme2] server-type extended
[AC-radius-testscheme2] primary authentication 162.105.34.20
[AC-radius-testscheme2] primary accounting 162.105.34.20
[AC-radius-testscheme2] key authentication testkey2
[AC-radius-testscheme2] key accounting testkey2
[AC-radius-testscheme2] user-name-format without-domain
[AC-radius-testscheme2] quit
```

配置domain。

```
[AC] domain testdomain2
[AC-isp-testdomain2] authentication lan-access radius-scheme testscheme2
```

[AC-isp-testdomain2] authorization lan-access radius-scheme testscheme2
[AC-isp-testdomain2] accounting lan-access radius-scheme testscheme2
[AC-isp-testdomain2] quit

配置下发的ACL。

[AC] acl number 3221
[AC-acl-adv-3221] rule deny ip destination 56.1.7.100 0
[AC-acl-adv-3221] quit

配置无线接口WLAN-ESS。

[AC]interface WLAN-ESS 1
[AC-WLAN-ESS1] port access vlan 2
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS1] port-security tx-key-type 11key
[AC-WLAN-ESS1] undo dot1x handshake
[AC-WLAN-ESS1] quit

配置无线服务模板service-template 1。

[AC] wlan service-template 1 crypto
[AC-wlan-st-1] ssid testssid2
[AC-wlan-st-1] authentication-method open-system
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] cipher-suite tkip
[AC-wlan-st-1] security-ie wpa
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

建立AP，并在AP下绑定服务模板，AP的配置要根据具体的AP和序列号进行配置。

[AC] wlan ap ap2100 model WA2100
[AC-wlan-ap-ap2100] serial-id 210235A22W0079000256
[AC-wlan-ap-ap2100] radio 1
[AC-wlan-ap-ap2100-radio-1] service-template 1
[AC-wlan-ap-ap2100-radio-1] radio enable
[AC-wlan-ap-ap2100-radio-1] quit
[AC-wlan-ap-ap2100] quit

iMC配置

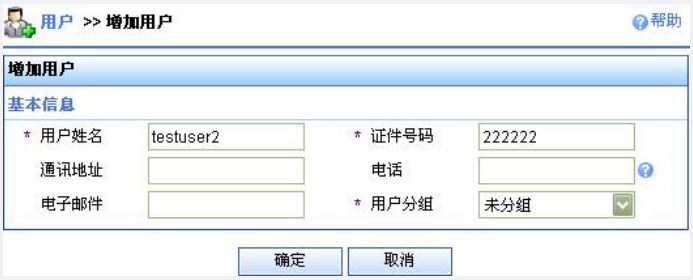
在iMC上配置Dot1x认证项（iMC版本：3.20-E2403）如下：

（1）正确安装iMC并导入证书，然后从iMC上添加设备AC（配置略）。

（2）增加接入设备，其中共享密钥要与步骤2中配置一致。

（3）增加服务：配置基本信息中的服务名和服务后缀（与步骤2中的domain name配置一致），授权信息中的证书认证、认证证书类型、认证证书子类型和下发ACL，其他信息可保持缺省值。

（4）增加用户，配置用户testuser2不加入特定组。



（5）增加接入用户：使用“选择”按钮选择前一步的用户，并配置帐号名，密码，在线用户数，以及在第（3）步中建立的服务。相关绑定信息保留缺省值。

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 vlan 2

Index=139 ,Username=testac2@testdomain2
MAC=001b-1109-a32b ,IP=N/A
 Total 1 connection(s) matched.

display connection ucibindex 139
Index=139 , Username=testac2@testdomain2
MAC=001b-1109-a32b
IP=N/A
Access=8021X ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS1:285
Initial VLAN=2, Authorization VLAN=N/A
```

ACL Group=3221
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2008-09-02 13:58:58 ,Current=2008-09-02 14:06:15 ,Online=00h07m17s
Total 1 connection matched.

（3）Client不能访问FTP服务器56.1.7.100，能正常访问其他网络资源。