WX系列AC基于用户名的用户接入控制功能的配置

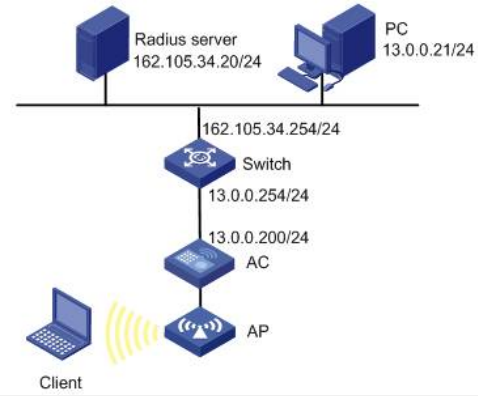
802.1X User Profile ACL 宋斌 2012-02-23 发表

WX系列AC基于用户名的用户接入控制功能的配置

一、 组网需求：

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

二、 组网图：



本配置举例中AC使用的是WX5002，IP地址是13.0.0.200/24；AP使用的是WA2200系列无线局域网接入点设备，IP地址从DHCP上动态获得，AC作为DHCP服务器，AP与AC是二层组网。

AP的配置请根据具体的AP和序列号进行配置。

Radius server的IP地址为162.105.34.20/24，网关是162.105.34.254/24，与无线网络是三层组网。Client上线后通过DHCP服务器获取IP地址，与AC、AP在相同的网段。PC的地址是13.0.0.21/24。交换机上有两个VLAN，与AC连接的VLAN接口地址13.0.0.254/24，与服务器相连的VLAN接口地址是162.105.34.254/24。整个网络路由可达。

三、 特性介绍：

User Profile（用户配置文件）提供一个配置模板，能够保存预设配置（一系列配置的集合）。用户可以根据不同的应用场景为User Profile配置不同的内容，比如CAR（Committed Access Rate，承诺访问速率）策略和QoS（Quality of Service，服务质量）策略等。

用户访问设备时，需要先进行身份认证。在认证过程中，认证服务器会将User Profile名称下发给设备，设备会立即启用User Profile里配置的具体内容。当用户通过认证访问设备时，设备将通过这些具体内容限制用户的访问行为。当用户下线时，系统会自动禁用User Profile下的配置项，从而取消User Profile对用户的限定。因此，User Profile适用于限制上线用户的访问行为，没有用户上线（可能是没有用户接入、或者用户没有通过认证、或者用户下线）时，User Profile是预设配置，并不生效。

采用User Profile特性之后，可以：

- 更精确地利用系统资源。比如，使用User Profile之前，只能基于接口/VLAN/全局等应用QoS策略，这个QoS策略限制的是一群用户；使用User Profile之后，可以基于用户应用QoS策略，这个QoS策略针对的是单个用户。
- 更灵活地限制用户访问系统资源。比如，使用User Profile之前，只能基于CAR列表/ACL或者对当前接口的所有流进行流量监管，当用户的物理位置移动时（比如从另一个接口接入），则需要在另外的接口配置流量监管功能；使用User Profile之后，可以基于用户进行流量监管，只要用户上线，认证服务器会自动下发相应的User Profile（配置了CAR策略），当用户下线，系统会自动取消相应的配置，不需要再进行手工调整。

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EAP。

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

关闭二层快转（仅WX5002系列需要配置此步骤）。

[AC] undo l2fw fast-forwarding

配置DHCP服务器。

[AC] dhcp enable
[AC] dhcp server ip-pool imc
[AC-dhcp-pool-imc] network 13.0.0.0 24

配置认证策略。

[AC] radius scheme for-imc
[AC-radius-for-imc] server-type extended
[AC-radius-for-imc] primary authentication 162.105.34.20
[AC-radius-for-imc] primary accounting 162.105.34.20
[AC-radius-for-imc] key authentication admin
[AC-radius-for-imc] key accounting admin
[AC-radius-for-imc] timer realtime-accounting 3
[AC-radius-for-imc] undo stop-accounting-buffer enable
[AC-radius-for-imc] accounting-on enable
[AC-radius-for-imc] quit

配置认证域。

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

把配置的认证域imc设置为系统缺省域。

[AC] domain default enable imc

配置ACL。

[AC] acl number 3001
[AC-acl-adv-3001] rule 0 permit ip destination 13.0.0.0 0.0.0.255
[AC-acl-adv-3001] quit

配置Qos Policy。

[AC] traffic classifier ipv4
[AC-classifier-ipv4] if-match acl 3001
[AC-classifier-ipv4] quit
[AC] traffic behavior ipv4
[AC-behavior-ipv4] filter deny
[AC-behavior-ipv4] quit
[AC] qos policy ipv4
[AC-qospolicy-ipv4] classifier ipv4 behavior ipv4
[AC-qospolicy-ipv4] quit

配置Qos Profile。

[AC] user-profile c DOT1X
[AC-user-profile-DOT1X-c] qos apply policy ipv4 inbound
[AC-user-profile-DOT1X-c] quit
[AC] user-profile c enable

配置无线服务模板。

[AC] wlan service-template 1 crypto
[AC-wlan-st-1] ssid admin-crypto
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
[AC-wlan-st-1] authentication-method open-system
[AC-wlan-st-1] quit

配置无线口，并在无线口启用端口安全（802.1x认证）。

[AC] interface WLAN-ESS 1
[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] undo dot1x multicast-trigger

[AC-WLAN-ESS1] quit

使能无线模板。

[AC] wlan service-template 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

配置AP并绑定无线服务模板。

[AC] wlan ap 2200 model WA2220E-AG
[AC-wlan-ap-2200] radio 2 type dot11g
[AC-wlan-ap-2200-radio-2] channel 10
[AC-wlan-ap-2200-radio-2] service-template 1
[AC-wlan-ap-2200-radio-2] radio enable
[AC-wlan-ap-2200-radio-2] quit
[AC-wlan-ap-2200]quit

配置VLAN虚接口。

[AC] interface Vlan-interface1
[AC-Vlan-interface1] ip address 13.0.0.200 255.255.255.0

配置缺省路由。

[AC-Vlan-interface1] ip route-static 0.0.0.0 0.0.0.0 13.0.0.254

iMC配置

在iMC上配置Dot1x认证项（iMC版本：用户接入管理组建3.20-E0401L04）如下：

组件信息　专业版（试用），将于2008年11月16日失效。

组件	版本	许可数量	已使用数量	失效日期
智能管理平台	3.20-E2403	允许管理最大设备数：50	11	2008-11-16
用户接入管理组件	3.20-E0401L04	允许管理最大接入用户数：500	5	2008-11-17

（1）接入设备配置：

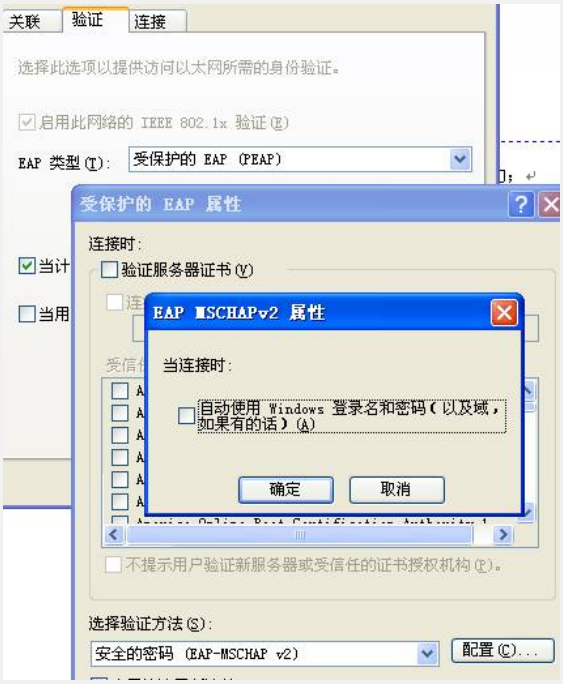
（2）配置服务配置：

（3）配置帐号用户：

（4）立即生效。

五、 结果验证：

（1）Client连接 SSID，输入用户名和密码，上线成功。



（2）使用display connection查看DOT1X用户，是否用户在线。查看连接的详细信息，确认qos-profile已经正确下发。

（3）在iMC上查看用户是否在线。

（4）从Client上Ping PC失败；使用display acl 3001查看报文匹配ACL。

（5）从Client上Ping认证服务器成功；使用display acl 3001查看报文没有匹配ACL。