WX系列AC实现Portal+LDAP功能的典型配置（账号的姓名使用中文）

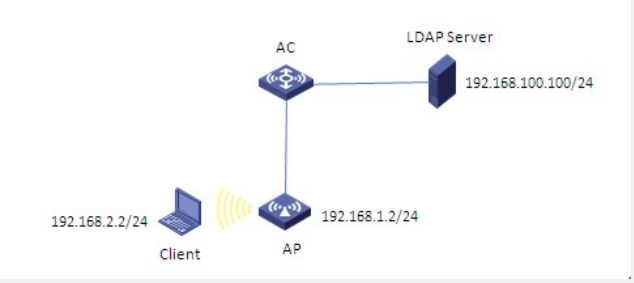
Portal LDAP AAA **王森森** 2012-05-30 发表

WX系列AC实现Portal+LDAP功能的典型配置（账号的姓名使用中文）

一、组网需求：

WX系列AC、FIT AP、便携机（安装有无线网卡）、LDAP服务器

二、组网图：



本典型配置举例中AC使用WX5004无线控制器，AP和Client通过DHCP方式获取IP地址。WX5004上LDAP Server属于VLAN 100（网关192.168.100.1/24），AP属于VLAN 10（网关192.168.1.1/24），Client属于VLAN 20（网关192.168.2.1/24）。

三、特性介绍：

LDAP是一种基于TCP/IP的目录访问协议，用于提供跨平台的、基于标准的目录服务。LDAP协议的典型应用是用来保存系统的用户信息，如Microsoft的Windows操作系统就是使用了Active Directory Server来保存操作系统的用户、用户组等信息，用于用户登录Windows时的认证和授权。LDAP的目录服务功能建立在Client/Server的基础之上。所有的目录信息存储在LDAP服务器上。LDAP服务器就是一系列实现目录协议并管理存储目录数据的数据库程序。目前，Microsoft的Active Directory Server、IBM的Tivoli Directory Server和Sun的Sun ONE Directory Server都是常用的LDAP服务器软件。

使用LDAP协议进行认证时，其基本的工作流程如下：

（1）LDAP客户端使用LDAP服务器管理员DN与LDAP服务器进行绑定，与LDAP服务器建立连接并获得查询权限。

（2）LDAP客户端使用认证信息中的用户名构造查询条件，在LDAP服务器指定根目录下查询此用户，得到用户的DN。

（3）LDAP客户端使用用户DN和用户密码与LDAP服务器进行绑定，检查用户密码是否正确。

使用LDAP协议进行授权时，操作与认证过程相似，只是在查询用户时，除获得用户DN外，还可以获得用户信息中的授权信息。如果只需要查询用户时获得的授权信息，则可不再进行后面的操作，如果还需要其他授权信息可以在获得相应查询权限后，继续再对其他授权信息进行查询。

四、主要配置步骤：

AC配置：

#创建VLAN，端口加入VLAN，并配置VLAN接口IP地址。
system-view
[AC] vlan 10
[AC –vlan10] port GigabitEthernet 1/0/1
[AC –vlan10] quit
[AC] vlan 20
[AC –vlan20] quit
[AC] vlan 100

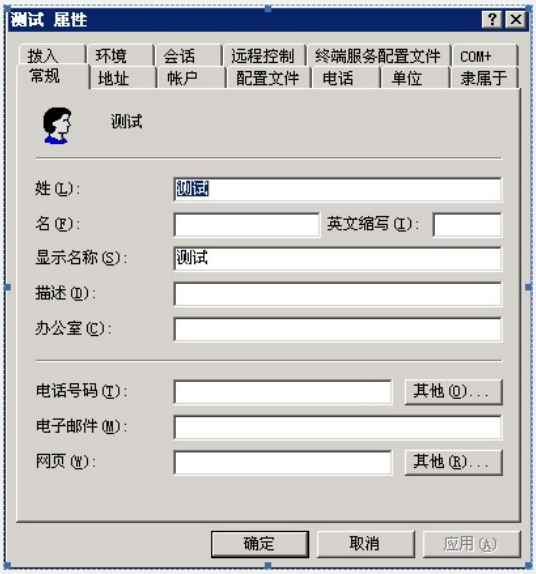
[AC –vlan100] port GigabitEthernet 1/0/2
[AC –vlan100] quit
[AC] interface Vlan-interface10
[AC-Vlan-interface10] ip address 192.168.1.1 255.255.255.0
[AC-Vlan-interface10] quit
[AC] interface Vlan-interface20
[AC-Vlan-interface20] ip address 192.168.2.1 255.255.255.0
[AC-Vlan-interface20] quit
[AC] interface Vlan-interface100
[AC-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
[AC-Vlan-interface100] quit
#配置DHCP server。
[AC] dhcp enable
[AC] dhcp server ip-pool pool01
[dhcp server ip-pool pool01] network 192.168.1.0 mask 255.255.255.0
[dhcp server ip-pool pool01] gateway-list 192.168.1.1
[dhcp server ip-pool pool01] quit
[AC] dhcp server ip-pool pool02
[dhcp server ip-pool pool02] network 192.168.2.0 mask 255.255.255.0
[dhcp server ip-pool pool02] gateway-list 192.168.2.1
[dhcp server ip-pool pool02] quit
[AC] dhcp server forbidden-ip 192.168.1.1
[AC] dhcp server forbidden-ip 192.168.2.1
#配置LDAP方案。
[AC] ldap scheme ldap1
[AC-ldap- ldap1] authentication-server 192.168.100.100
[AC-ldap- ldap1] login-dn cn=administrator,cn=users,dc=wlan,dc=com
[AC-ldap- ldap1] login-password simple 1
[AC-ldap- ldap1] user-parameters search-base-dn cn=users,dc=wlan,dc=com
[AC-ldap- ldap1] user-parameters user-name-attribute samaccountname
[AC-ldap- ldap1] quit
#配置ISP域。
[AC] domain ldap
[AC-isp-ldap] authentication default ldap-scheme ldap1
[AC-isp-ldap] authorization default none
[AC-isp-ldap] accounting default none
[AC-isp-ldap] quit
#配置系统缺省的ISP域为ldap。
[AC] domain default enable ldap
#配置本地Portal服务。
[AC] portal server ldap ip 192.168.1.1 url http://192.168.1.1/portal/logon.htm
[AC] portal local-server http
[AC] interface Vlan-interface20
[AC-Vlan-interface20] portal server ldap method direct
[AC-Vlan-interface20] quit
#配置WLAN ESS接口。
[AC] interface WLAN-ESS 1
[AC-WLAN-ESS1] port access vlan 20
[AC-WLAN-ESS1] quit
#配置service-template服务模板。
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid H3C
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
#配置ap01。
[AC] wlan ap ap01 model WA2210-AG
[AC-wlan-ap-ap01] serial-id 210235A29DB094004423
[AC-wlan-ap-ap01] radio 1
[AC-wlan-ap-ap01-radio-1] service-template 1
[AC-wlan-ap-ap01-radio-1] radio enable
[AC-wlan-ap-ap01-radio-1] quit
[AC-wlan-ap-ap01] quit
注：user-parameters user-name-attribute samaccountname命令用来配置用户查询的用户属性，允许账户的姓名使用中文。

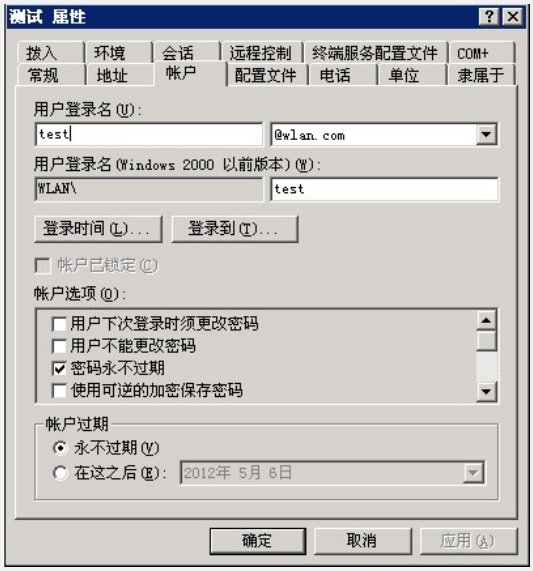
LDAP配置：

#在Users组新建用户“测试”。

（1）在LDAP服务器上，选择[开始/管理工具]中的[Active Directory用户和计算机]，打开Active Directory用户管理界面。

（2）选择Users组，右键新建姓名为“测试”、用户登录名为“test”的账户，并设置密码。配置如下图所示：

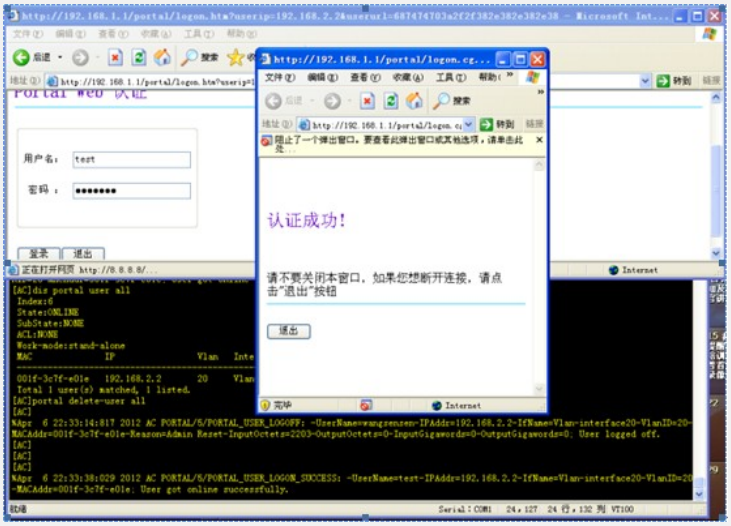




五、结果验证：

（1）Client关联到ssid：H3C，此时Client会自动获取192.168.2.0/24网段的地址，网关为192.168.2.1。

（2）打开Client上的IE浏览器，输入地址：http://1.1.1.1，按回车键，网页会自动跳转到Portal认证页面，输入用户名和密码，鼠标点击logon按钮，认证成功。如下图所示：


Portal Web 认证
用户名：
test
密码：
登录
退出
http://192.168.1.1/portal/logon.cg...
认证成功!
请不要关闭本窗口，如果您想断开连接，请点击"退出"按钮
退出
[AC]dis portal user all
Index:6
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC
IP
Vlan
001f-3c7f-e01e
192.168.2.2
20
Total 1 user(s) matched, 1 listed.
[AC]portal delete-user all
%Apr 6 22:33:14:817 2012 AC PORTAL/5/PORTAL_USER_LOGOFF: -UserName=wangzenzen-IPAddr=192.168.2.2-IfName=Vlan-interface20-VlanID=20-MACAddr=001f-3c7f-e01e-Reason=Admin Reset-InputOctets=2203-OutputOctets=0-InputGigawords=0-OutputGigawords=0; User logged off.
%Apr 6 22:33:38:029 2012 AC PORTAL/5/PORTAL_USER_LOGON_SUCCESS: -UserName=test-IPAddr=192.168.2.2-IfName=Vlan-interface20-VlanID=20-MACAddr=001f-3c7f-e01e; User got online successfully.