基于MAC快速认证的本地转发配置案例

wlan接入 MAC地址认证 AAA 杨攀 2015-11-12 发表

一、本地转发MAC快速认证简介

为了加快提升手机用户使用WLAN的便利性，降低使用WLAN的门槛，在浙江移动省公司的牵头下，召集各个厂家包括华三、摩托、大唐、中兴、亚信一起开发了WLAN手机上网MAC快速认证功能。

使用该功能后，手机用户初次登陆WLAN，弹出Portal登陆页面，手工输入用户名和密码进行正常的PORTAL认证，与此同时，AC会将用户MAC等信息传递给后端MAC绑定服务器，以后该手机用户再次上网时就无需输入任何信息，AC会自动将用户信息传递给后台进行认证，从而免去了用户每次手工输入用户名和密码的麻烦，简化了上网流程。同时为了减轻AC对用户数据转发的压力，实现在无线控制器AC上对无线用户进行MAC快速认证，但认证成功后业务数据走AP本地转发。

MAC快速认证本地转发流程如下：

1、用户打开应用程序如浏览器，QQ等，进行上网操作。

2、AC检测到流量超过门限，通知MAC绑定服务器进行MAC检查。

3、MAC绑定服务器对MAC进行检查，如果已经绑定，则提取该MAC地址对应的用户名和密码，这时客户端在通过AP进行HTTP重定向发起portal认证。

4、AC向集团的AAA服务器进行认证请求，认证通过后，通知绑定服务器。

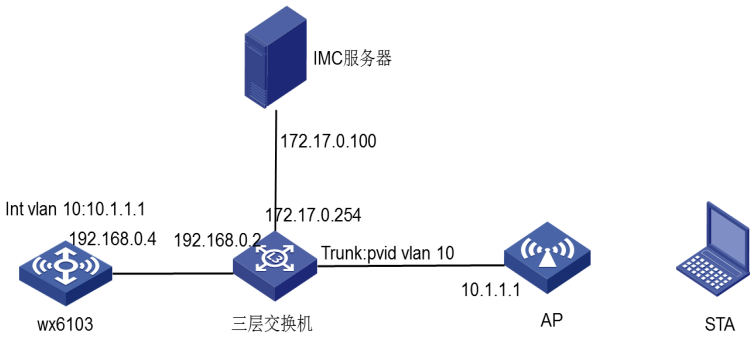
5、当认证完成之后，用户的数据流量通过AP走本地转发

二、组网需求：

如图1-1，总部的AC与分支机构的AP二层关联并作为DHCP server为无线客户端分配地址；wx6103作为无线客户端的网关并为AP分配地址，具体要求如下：

AC先向服务器发送MAC快速认证请求，如果用户第一次上线，则服务器向AC发起认证请求，用户认证成功后，AC将用户规则下发到AP设备上，用户报文在AP上直接做转发；如果用户不是第一次上线，用户不需要进行认证，用户报文在AP上直接转发。

图1-1 AC为无线客户端分配地址配置组网图



三、配置步骤：

3.1配置AC

#创建vlan 1的三层虚机接口，并为该接口配置IP地址，其中VLAN 1用于和IMC服务器之间进行通信。

system-view

[AC] interface vlan-interface 1

[AC-Vlan-interface10] ip address 192.168.0.4 24

[AC-Vlan-interface10] quit

#创建VLAN 10及其对应的VLAN接口，并为该接口配置IP地址，其中VLAN10用于和AP之间进行通信。

system-view

[AC] vlan 10

[AC-vlan10] quit

[AC] interface vlan-interface 10

[AC-Vlan-interface10] ip address 10.1.1.1 24

[AC-Vlan-interface10] quit

创建VLAN 30及其对应的VLAN接口，并为该接口配置IP地址，其中VLAN 30用于起Portal服务。

[AC] vlan 30

[AC-vlan30] quit

[AC] interface vlan-interface 30

[AC-Vlan-interface30] ip address 30.1.1.1 24

[AC-Vlan-interface30] quit

配置AC的以太网1/0/1口的类型为Trunk口并允许所有VLAN通过，用于与AP、无线客户端、IMC之间通信。

[AC] interface g1/0/1

[AC-Bridge-Aggregation1] port link-type trunk

[AC-Bridge-Aggregation1] port trunk permit vlan all

[AC-Bridge-Aggregation1] quit

（1）配置DHCP服务

使能DHCP功能。

[AC] dhcp enable

配置DHCP地址池10，用于为AP动态分配地址。

[AC] dhcp server ip-pool vlan10

[AC-dhcp-pool-10] network 10.1.1.0 24

[AC-dhcp-pool-10] gateway-list 10.1.1.1

[AC-dhcp-pool-10] dns-list 10.1.1.1

[AC-dhcp-pool-10] quit

配置DHCP地址池30，用于为Client动态分配地址。

[AC] dhcp server ip-pool vlan30

[AC-dhcp-pool-30] network 30.1.1.0 24

[AC-dhcp-pool-30] gateway-list 30.1.1.1

[AC-dhcp-pool-30] dns-list 30.1.1.1

[AC-dhcp-pool-30] quit

（2）配置WLAN-ESS接口

创建接口WLAN-ESS 30。

[AC] interface wlan-ess 30

配置端口的链路类型为Access，允许VLAN 30通过。

[AC-WLAN-ESS30] port access vlan 30

[AC-WLAN-ESS30] quit

(3)配置无线服务模板

创建clear类型的服务模板30。

[AC] wlan service-template 30 clear

设置当前服务模板的SSID为portal-local。

[AC-wlan-st-30] ssid portal-local

将WLAN-ESS30接口绑定到服务模板30。

[AC-wlan-st-30] bind wlan-ess 30

开启用户本地转发功能。

[AC-wlan-st-30] client forwarding-mode local

开启无线客户端透传DHCP报文到AC的功能。

[AC-wlan-st-30] client dhcp-server centralized

使能服务模板。

[AC-wlan-st-30] service-template enable

[AC-wlan-st-30] quit

在AC下绑定无线服务模板

创建AP模板，名称为officeap，型号名称选择WA3628i-AGN，并配置序列号。

[AC] wlan ap ap1 model WA3628i-AGN

[AC-wlan-ap-ap1] serial-id 210235A42MB108000002

[AC-wlan-ap-ap1] map-configuration apcfg.txt

进入radio 1射频视图。

[AC-wlan-ap-ap1] radio 1

配置射频的工作信道为161。

[AC-wlan-ap-ap1-radio-1] channel 161

将服务模板30绑定到AP的radio 1口。

[AC-wlan-ap-ap1-radio-1] service-template 30

[AC-wlan-ap-ap1-radio-1] radio enable

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1]quit

(4)配置Portal认证

配置Portal服务器地址为172.17.0.100，并指定服务器对应的url。

[AC] portal server imc ip 172.17.0.100 key simple h3c url http://172.17.0.100:8080/portal

配置Portal免认证规则1，用于放行AC上起portal的接口能够与portal服务器通信。

[AC] portal free-rule 1 source interface bridge-aggregation1 destination any

配置AC通过WLAN获取Portal用户信息。

[AC] portal host-check wlan

配置RADIUS方案portal。

[AC] radius scheme portal

#配置认证、计费和授权服务器的IP地址为172.17.0.100。

[AC-radius-portal] primary authentication 172.17.0.100

[AC-radius-portal] primary accounting 172.17.0.100

配置与认证、计费和授权服务器交互报文时的共享密钥均为h3c。

[AC-radius-portal] key authentication simple h3c

[AC-radius-portal] key accounting simple h3c

指定发送给RADIUS方案portal中RADIUS服务器的用户名不得携带域名。

[AC-radius-portal] user-name-format without-domain

配置设备发送RADIUS报文使用的源IP地址为192.168.0.4。

[AC-radius-portal] nas-ip 192.168.0.4

[AC-radius-portal] quit

配置AAA认证域portal。

[AC] domain portal

设置ISP域的认证、授权和计费方法均为RADIUS方式。

[AC-isp-portal] authentication portal radius-scheme portal

[AC-isp-portal] accounting portal radius-scheme portal

[AC-isp-portal] authorization portal radius-scheme portal

[AC-isp-portal] quit

[AC] interface vlan-interface 30

配置接口VLAN 30为Portal直接认证的接口。

[AC-Vlan-interface30] portal server imc method direct

指定从接口接入的IPv4 Portal用户使用认证域为portal。

[AC-Vlan-interface30] portal domain portal

配置接口发送Portal报文使用的IPv4源地址为192.168.0.4。

[AC-Vlan-interface30] portal nas-ip 192.168.0.4

开启Portal本地转发功能。

[AC-Vlan-interface30] portal forwarding-mode local

#配置MAC绑定服务器的IP和UDP端口，缺省值为5010

[AC-Vlan-interface30] portal mac-trigger server ip 172.17.0.100

#配置MAC快速认证功能在接口下使能

[AC-Vlan-interface30] portal mac-trigger enable

[AC-Vlan-interface30] quit

配置arp-snooping功能。

[AC] arp-snooping enable

#配置learn-ipaddr功能

[AC] wlan client learn-ipaddr enable

3.2配置SW

#为vlan 1配置对应接口IP地址，用于和AC之间通信。

system-view

[SW] interface vlan-interface 1

[SW-Vlan-interface1] ip address 192.168.0.2 24

[SW-Vlan-interface1] quit

配置SW与Router连接的物理接口的类型为Trunk，允许所有VLAN通过。

[SW] interface gigabitethernet 1/0/1

[SW-GigabitEthernet1/0/1] port link-type trunk

[SW-GigabitEthernet1/0/1] port trunk permit vlan all

[SW-GigabitEthernet1/0/1] quit

配置SW与AP连接的物理接口属性，使能POE为AP供电，类型为Trunk，允许所有VLAN通过，且PV
ID设置为10。

[SW] interface gigabitethernet 1/0/2

[SW-GigabitEthernet1/0/2] poe enable

[SW-GigabitEthernet1/0/2] port link-type trunk

[SW-GigabitEthernet1/0/2] port trunk permit vlan all

[SW-GigabitEthernet1/0/2] port trunk pvid vlan 10

[SW-GigabitEthernet1/0/2] quit

创建VLAN20，并配置对应接口的IP地址，用于和IMC服务器之间通信。

[SW] vlan 20

[SW-vlan30] quit

[SW] interface vlan-interface 20

[SW-Vlan-interface30] ip address 172.17.0.254 24

[SW-Vlan-interface30] quit

3.2 map.txt配置文件

编辑AP的配置文件map.txt。

system-view

#http://172.17.0.100:8080/portal//配置portal服务器地址为

172.17.0.100，并指定服务器对应的url

portal server imc ip 172.17.0.100 key simple h3c url

#destination any//配置portal免认证规则1，用于放行AP上起portal

的接口能够与portal服务器通信

portal free-rule 1 source interface GigabitEthernet 1/0/1

#配置ap通过WLAN获取Portal用户信息。

portal host-check wlan

#创建vlan 30

vlan 30

#创建VLAN30对应接口，并接入接口VLAN30视图

interface vlan 30

#接口下指定portal服务器并配置为直接认证方式

portal server imc method direct

#配置接口发送portal报文使用的源地址为AC的地址

portal nas-ip 192.168.0.4

#配置MAC快速认证功能在接口下使能

portal mac-trigger enable

#进入到AP的物理接口

interface GigabitEthernet 1/0/1

#配置接口GigabitEthernet1/0/1类型为Trunk

port link-type trunk port

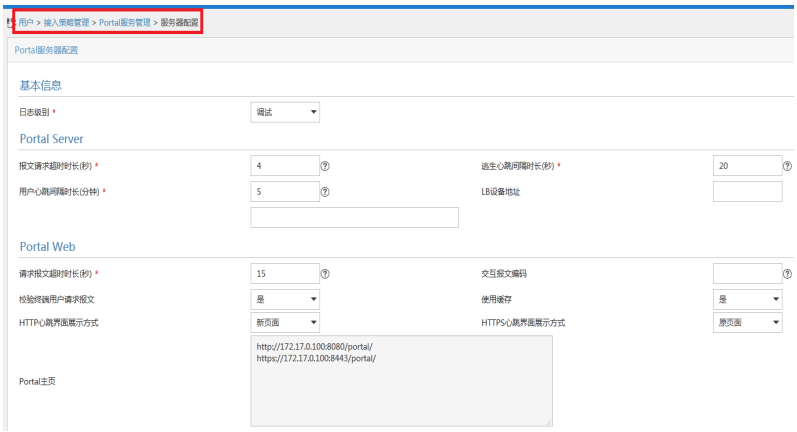
配置接口GigabitEthernet1/0/1允许所有VLAN通过

trunk permit vlan all

四、 IMC的配置

4.1配置Portal服务器。

登录进入iMC管理平台，选择“用户”页签，单击导航树中的[接入策略管理/Portal服务管理/服务器配置]菜单项，进入服务器配置页面，使用缺省配置。

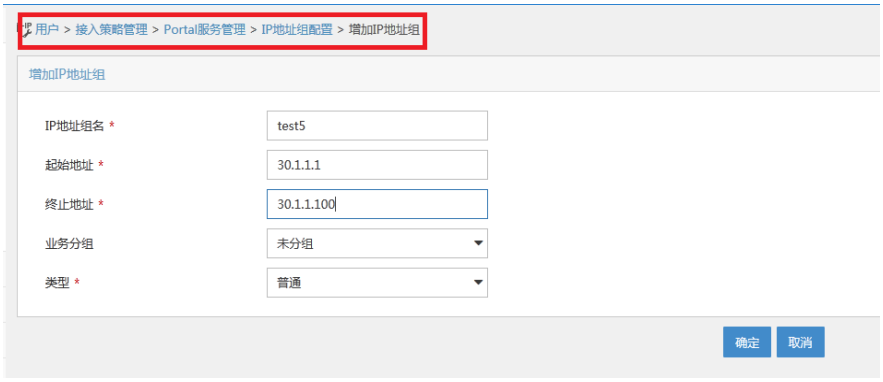


配置IP地址组。

选择“用户”页签，单击导航树[接入策略管理/Portal服务管理/ IP地址组配置]菜单项，进入IP地址组配置页面，在该页面中单击<增加>按钮，进入增加IP地址组配置页面。

- 输入IP地址组名：test5；
- 输入起始地址：30.1.1.1；
- 输入终止地址：30.1.1.100；

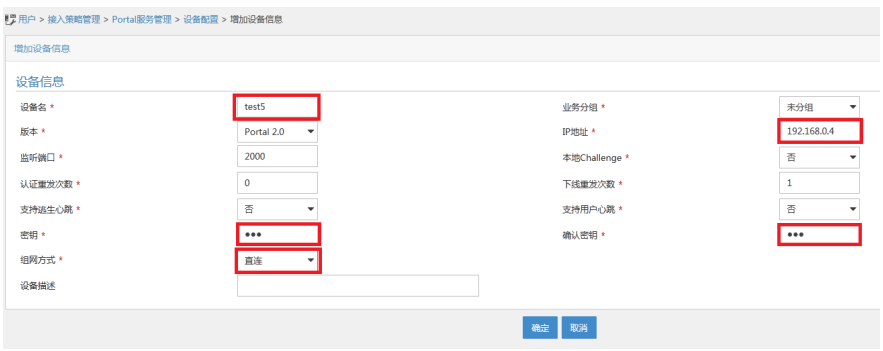
其他采用缺省配置，单击<确定>按钮完成操作



增加Portal设备。

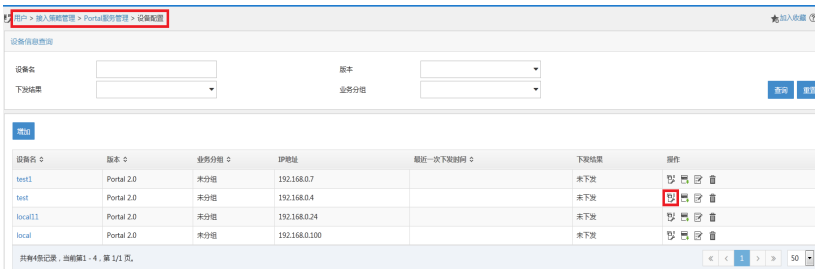
选择“用户”页签，单击导航树中的[接入策略管理/Portal服务管理/设备配置]菜单项，进入设备配置页面。在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 输入设备名：test5；
- 输入IP地址：即AC上配置的portal bas-ip地址，192.168.0.4；
- 输入密钥：h3c，与AC上配置的portal server密钥一致；
- 组网方式改为“直连”类型；
- 其他采用默认配置，单击<确定>按钮完成操作。



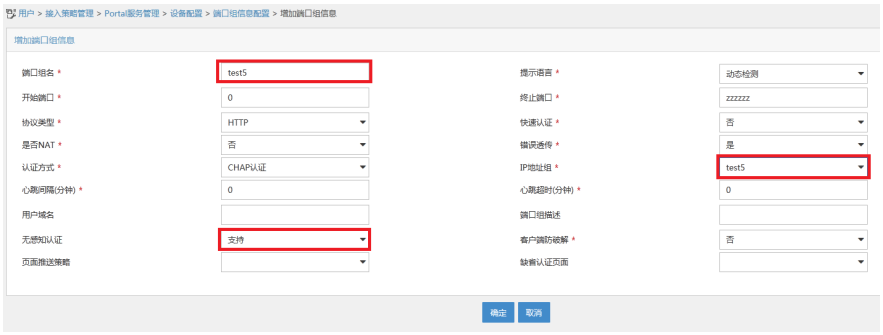
增加端口组信息。

在Portal设备配置页面中的设备信息列表中，单击“ ”图标，进入端口组信息配置页面。



在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 输入端口组名：test5；
- 选择IP地址组：test5；
- 选择支持无感知认证；
- 其他采用默认配置，单击<确定>按钮完成操作。



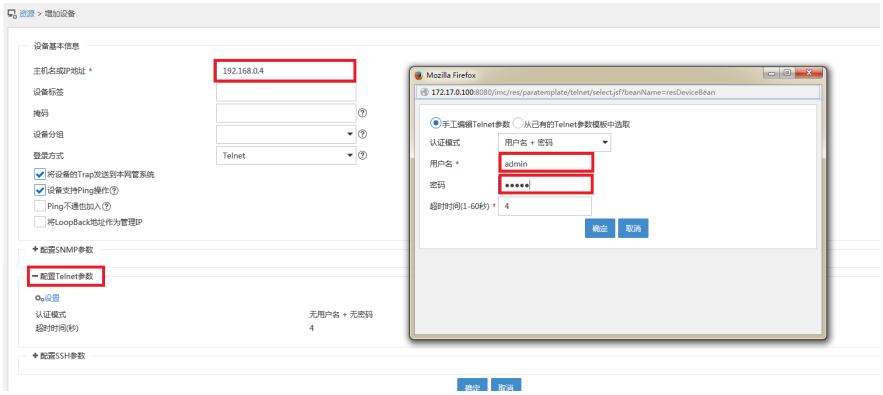
4.2 配置接入服务

增加接入设备

选择“资源”标签，单击导航树中的[增加设备]菜单项，进入增加设备视图下。

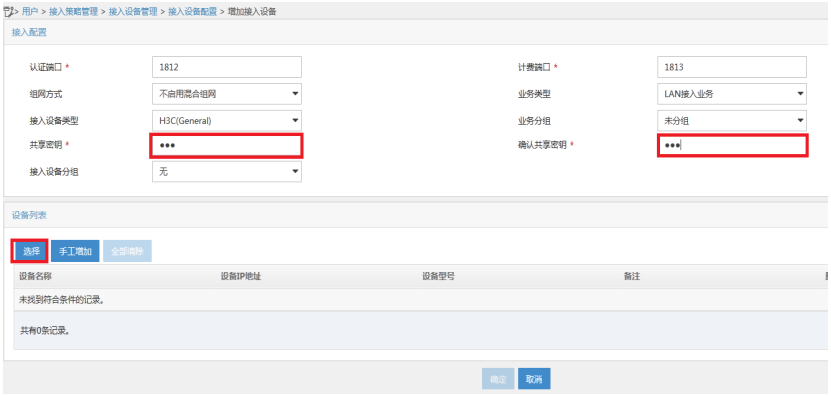
设置设备的IP地址为192.168.0.4，也就是和设备交互报文的地址。

点击配置Telnet选项

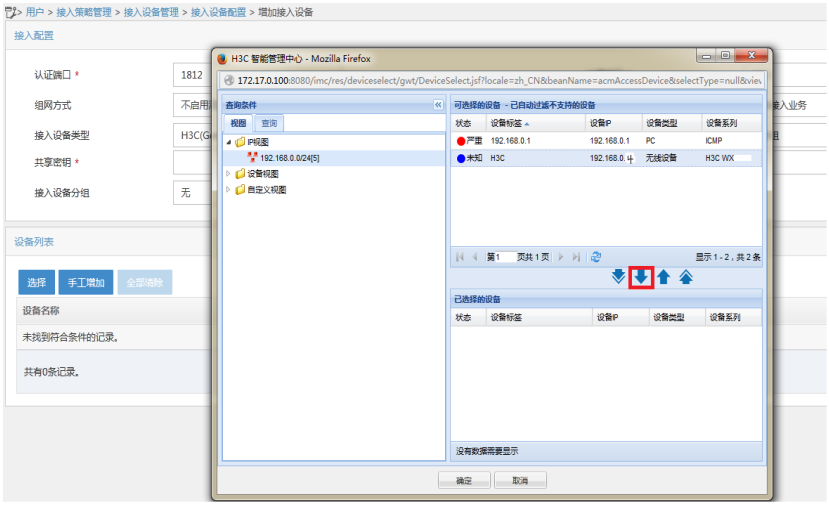


选择“用户”标签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面。在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置与AC交互报文时使用的认证、计费共享密钥为“h3c”，该密码与AC配置RADIUS方案时的地址一致；
- 选择接入设备类型为“H3C(General)”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作
- 点击“选择”按钮；



点击“IP视图”，选择自己要添加的设备，点击向下添加按钮

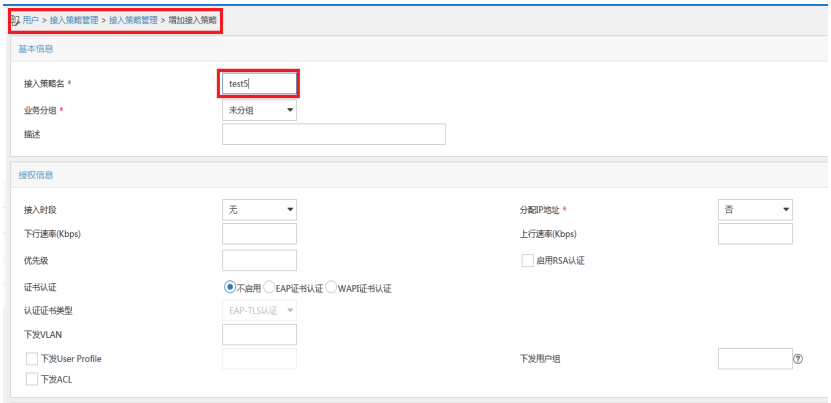


增加接入策略。

选择“用户”标签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略配置页面。在接入策略列表中点击<增加>按钮，进入增加接入策略页面。

- 接入策略名输入“test5”；
- 业务分组“未分组”；

其它参数采用缺省值，并单击<确定>按钮完成操作

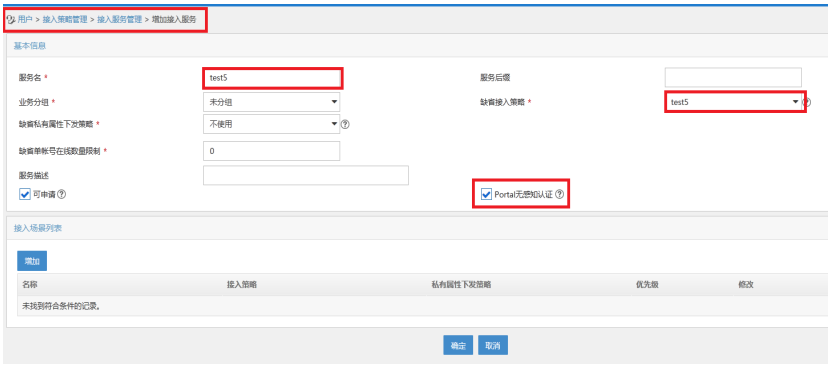


增加接入服务。

选择“用户”标签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务配置页面。在接入服务列表中点击<增加>按钮。

- 服务名输入“test5”；
- 缺省接入策略“test5”；
- 勾选portal无感知认证；

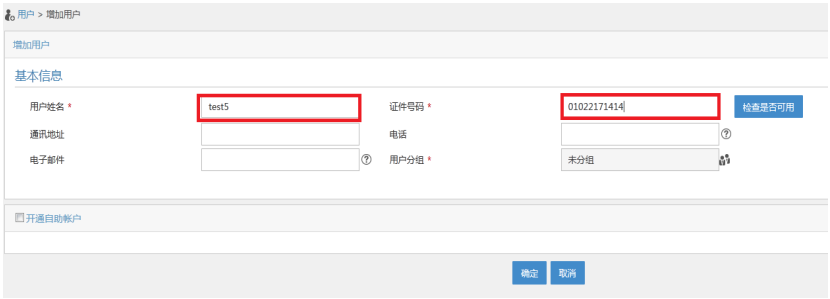
其它参数采用缺省值，并单击<确定>按钮完成操作。



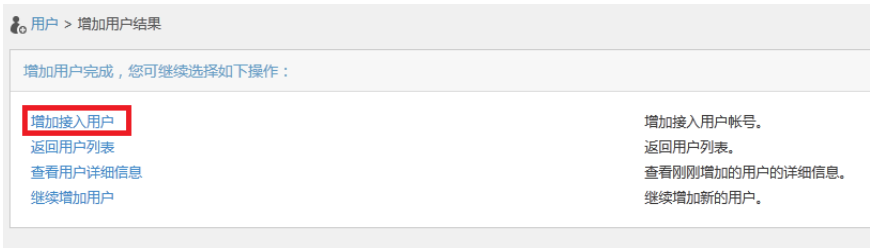
4.3增加接入用户。

选择“用户”标签，单击导航树中的[接入用户管理/接入用户]菜单项，进入到接入用户配置页面。在接入用户列表中点击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“test5”；
- 输入证件号码“01022171414”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。



点击“确定”按钮，选择“增加接入用户”。



- 账号名输入“test5”；
- 密码输入“test5”；
- 强portal无感知认证最大数设置为10；
- 勾选接入服务“test5”；

	服务名	服务后缀	状态	分配IP地址
☐	123		可申请	
☐	dot1x		可申请	
☐	lcoal		可申请	
☐	mac		可申请	
☐	macpsk	cams	可申请	
☐	portal		可申请	
☐	test		可申请	
☐	test2		可申请	
☐	test3		可申请	
☐	test4		可申请	
☑	test5		可申请	
☐	test6	portal	可申请	

单击<确定>按钮完成操作。

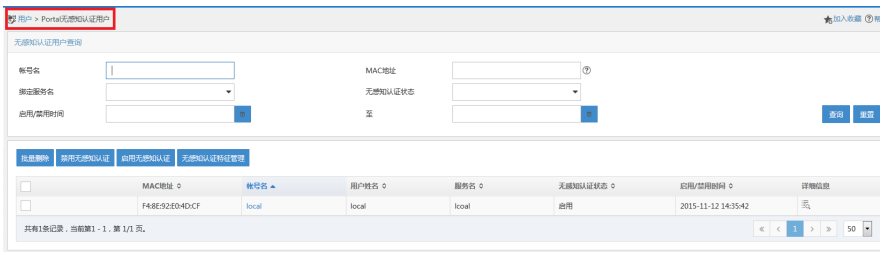
五、验证配置

(1)用户使用智能终端通过浏览器访问网络，重定向到Portal认证页面。用户输入用户名、密码、服务等认证信息，进行上线认证。

(2)认证成功后，用户下线。

(3)用户再次使用该智能终端访问网络，这时不需要输入用户名和密码，直接上线。

(4)此时可在iMC上观察到绑定该智能终端MAC地址信息



配置思路：

· 为实现AC与Portal服务器通信，在AC上配置到portal服务器的静态路由；

· 在AC上配置DHCP功能，使得AC统一分配、集中管理无线客户端的地址；

· 为实现MAC快速认证，在AC和AP上配置MAC快速认证；

· 为了使AP能够直接转发Client报文，需要在AC的服务模板下开启本地转发功能，同时通过下发map-configuration文件来对AP进行配置实现本地转发。

配置注意事项：

· AC和AP上都要配置从WLAN获取用户信息的功能；

· AC和AP上都需要配置触发无感知认证的功能。

· 配置AP的序列号时请确保该序列号与AP唯一对应，AP的序列号可以通过AP设备背面的标签获取。

· 配置MAC认证服务器必须在使能三层Portal认证的接口下使能。

· 为使MAC快速认证功能生效，必须保证配置了MAC绑定服务器的IP和UDP端口信息，且接口使能了Portal。