本地转发模式下Portal集中认证典型配置举例(V7)

wlan接入 Portal AAA **殷俊** 2016-01-28 发表

本文档介绍本地转发模式下Portal集中认证配置举例

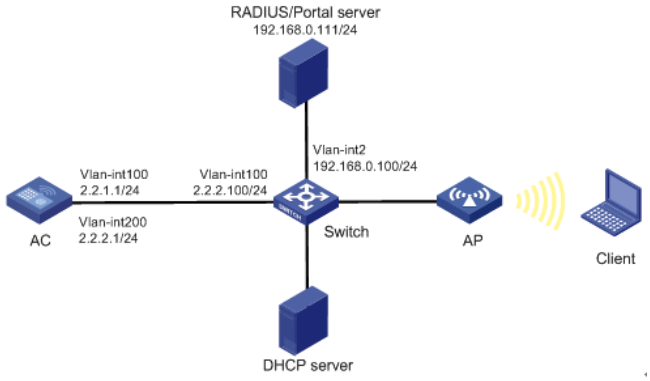
如下图所示，AP和Client通过DHCP服务器获取IP地址，iMC同时作为Portal服务器和RADIUS 服务器，要求：

1)Client在通过Portal认证前，只能访问Portal服务器；Client通过Portal认证后，可以访问外部网络。

2)AC采用直接方式的Portal认证。

3)客户端的数据流量直接由AP进行转发。

4)iMC服务器需要对用户授权信息进行动态修改或强制用户下线。



1. 配置IMC

下面以iMC为例（使用iMC版本为：iMC PLAT 7.1(E0303p13)、iMC EIA 7.1(F0302p08)、iMC EIP 7.1(F0302p08)）说明RADIUS server、Portal server和MAC绑定服务器的基本配置。

（1）配置RADIUS server

＃增加接入设备

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/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面。

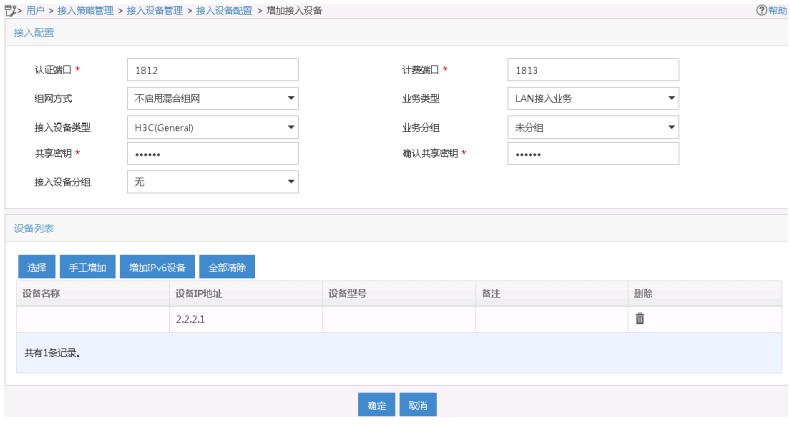
1)配置共享密钥为radius，该共享密钥与AC上配置RADIUS服务器时的密钥一致；

2)单击<手工增加>按钮，进入“手工增加接入设备”页面，填写起始IP地址为2.2.2.1，单击<确定>按钮完成操作；

3)其他配置采用页面默认配置即可；

4)单击<确定>按钮完成操作。

图1 增加接入设备



＃增加接入策略

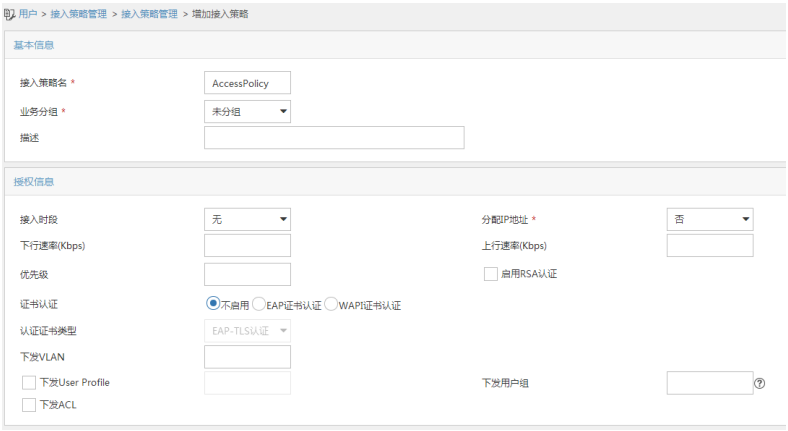
单击导航树中的[接入策略管理/接入策略管理]菜单项，单击<增加>按钮，进入“增加接入策略”页面。

1)填写接入策略名；

2)选择业务分组；

3)其它参数可采用缺省配置。

图2 增加接入策略配置



增加接入服务

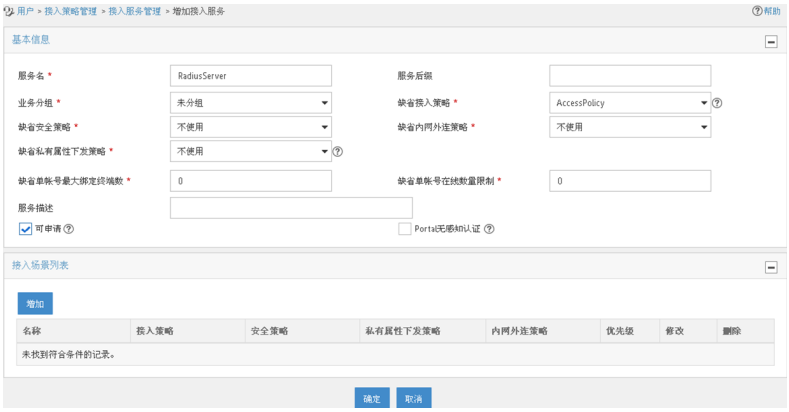
单击导航树中的[接入策略管理/接入服务管理]菜单项，单击<增加>按钮，进入“增加接入服务”页面。

1)填写服务名；

2)缺省接入策略选择已配置好的接入策略；

3)其它参数可采用缺省配置。

图3 增加接入服务配置



增加接入用户

单击导航树中的[接入用户管理/接入用户]菜单项，单击<增加>按钮，进入增加接入用户页面。

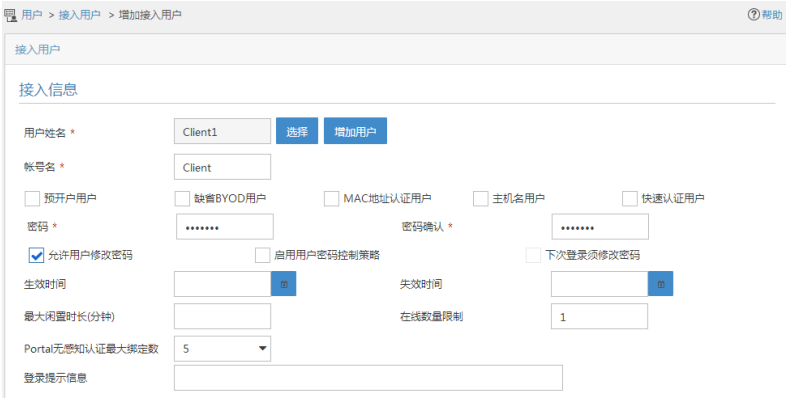
1)用户姓名选择可接入的用户；

2)填写账号名；

3)设置密码；

4)其它参数可采用缺省配置。

图4 增加接入用户



（2）配置Portal server

配置Portal认证服务。

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。

根据实际组网情况调整以下参数，本例中使用缺省配置。

图5 Portal认证服务器配置页面

配置IP地址组。

单击导航树中的[接入策略管理/Portal服务管理/IP地址组配置]菜单项，进入Portal 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。

1)填写IP地址组名；

2)输入起始地址和终止地址，输入的地址范围中应包含用户主机的IP地址；

3)选择业务分组，本例中使用缺省的“未分组”；

4)选择IP地址组的类型为“普通”。

图6 增加IP地址组配置页面

增加Portal设备。

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Portal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。

1)填写设备名；

2)版本选择“CMCC 1.0”；

3)指定IP地址为与接入用户相连的设备接口IP；

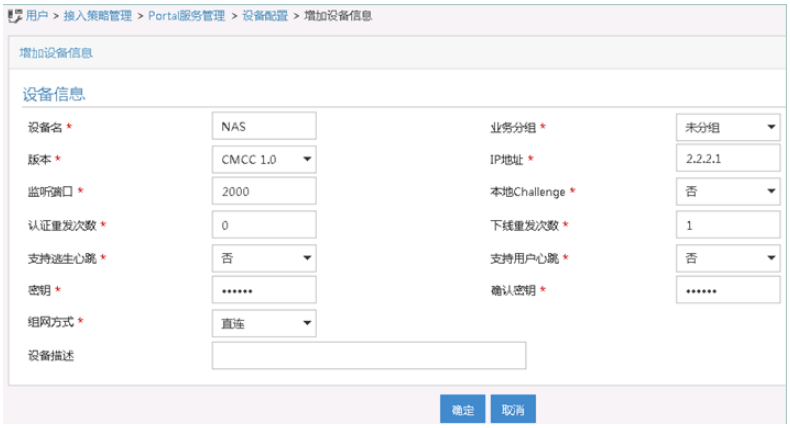
4)选择是否支持逃生心跳功能和用户心跳功能，本例中选择否。

5)输入密钥，与AC上的配置保持一致；

6)选择组网方式为直连；

7)其它参数可采用缺省配置。

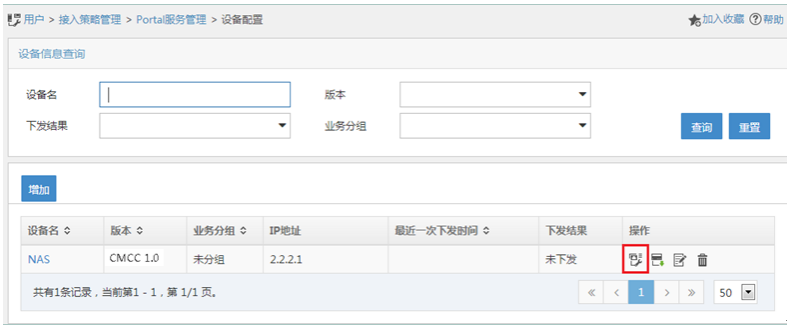
图7 增加设备信息配置页面



Portal设备关联IP地址组。

在Portal设备配置页面中的设备信息列表中，点击NAS设备的<端口组信息管理>链接，进入端口组信息配置页面。

图8 设备信息列表



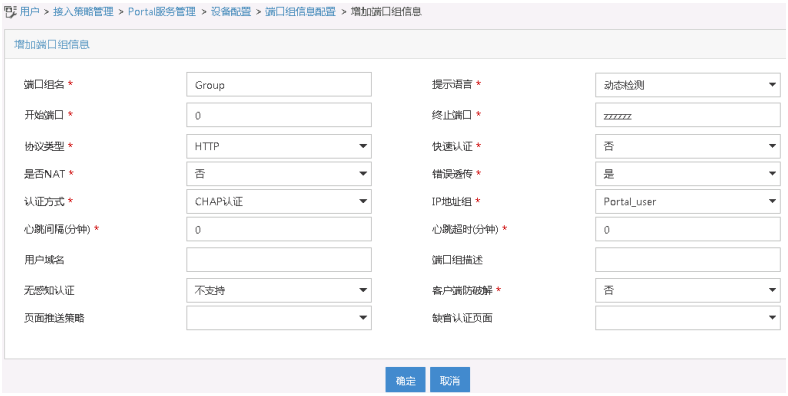
在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

1)填写端口组名；

2)选择IP地址组，用户接入网络时使用的IP地址必须属于所选的IP地址组；

3)其它参数可采用缺省配置。

图9 增加端口组信息配置页面



最后单击导航树中的[接入策略管理/业务参数配置/系统配置手工生效]菜单项，使以上Portal认证服务器配置生效。

2. 编辑AP配置文件

使用文本文档编辑AP的配置文件，将配置文件命名为map.txt，并将配置文件上传到AC存储介质上。配置文件内容和格式如下：

System-view

vlan 200

interface gigabitethernet1/0/1

port link-type trunk

port trunk permit vlan 200

3. 配置AC

(1)配置AC的接口

创建VLAN 100及其对应的VLAN接口，并为该接口配置IP地址。AP将获取该IP地址与AC建立CAPWAP隧道。

system-view

[AC] vlan 100

[AC-vlan100] quit

[AC] interface vlan-interface 100

[AC-Vlan-interface100] ip address 2.2.1.1 24

[AC-Vlan-interface100] quit

创建VLAN 200及其对应的VLAN接口，并为该接口配置IP地址。Client将使用该VLAN接入无线网络。

[AC] vlan 200

[AC-vlan200] quit

[AC] interface vlan-interface 200

[AC-Vlan-interface200] ip address 2.2.2.1 24

[AC-Vlan-interface200] quit

(2)配置静态路由

配置到iMC的静态路由。

[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100

(3)配置无线服务

创建无线服务模板st1，并进入无线服务模板视图。

[AC] wlan service-template st1

配置SSID为service。

[AC-wlan-st-st1] ssid service

配置无线服务模板VLAN为VLAN200。

[AC-wlan-st-st1] vlan 200

配置客户端数据报文转发位置为AP。

[AC–wlan-st-newst] client forwarding-location ap

[AC-wlan-st-service1] quit

创建AP，配置AP名称为office，型号名称选择WA4320i-ACN，并配置序列号219801A0CNC138011454。

[AC] wlan ap office model WA4320i-ACN

[AC-wlan-ap-office] serial-id 219801A0CNC138011454

指定AP的配置文件为map.txt。

[AC-wlan-ap-office] map-configuration map.txt

进入Radio 2视图。

[AC-wlan-ap-office] radio 2

将无线服务模板st1绑定到radio 2，并开启射频。

[AC-wlan-ap-office-radio-2] service-template st1

[AC-wlan-ap-office-radio-2] radio enable

[AC-wlan-ap-office-radio-2] quit

[AC-wlan-ap-office] quit

(4)配置RADIUS方案

创建名称为rs1的RADIUS方案，并进入该方案视图。

[AC] radius scheme rs1

配置RADIUS方案的主认证和主计费服务器及其通信密钥。

[AC-radius-rs1] primary authentication 192.168.0.111

[AC-radius-rs1] primary accounting 192.168.0.111

[AC-radius-rs1] key authentication simple radius

[AC-radius-rs1] key accounting simple radius

配置发送给RADIUS服务器的用户名不携带ISP域名。

[AC-radius-rs1] user-name-format without-domain

[AC-radius-rs1] quit

使能RADUIS session control功能。

[AC]radius session-control enable

(5)配置认证域

创建名称为dm1的ISP域并进入其视图。

[AC] domain dm1

为Portal用户配置AAA认证方法为RADIUS。

[AC-isp-dm1] authentication portal radius-scheme rs1

为Portal用户配置AAA授权方法为RADIUS。

[AC-isp-dm1] authorization portal radius-scheme rs1

为Portal用户配置AAA计费方法为none，不计费。

[AC-isp-dm1] accounting portal none

[AC-isp-dm1] quit

配置系统缺省的ISP域为dm1，所有接入用户共用此缺省域的认证和计费方法。若用户登录时输入的用户名未携带ISP域名，则使用缺省域下的认证方法。

[AC] domain default enable dm1

(6)配置Portal认证

配置Portal认证服务器，名称为newpt，IP地址为192.168.0.111，密钥为明文portal，监听Portal报文的端口为50100。

[AC] portal server newpt

[AC-portal-server-newpt] ip 192.168.0.111 key simple portal

[AC-portal-server-newpt] port 50100

配置Portal认证服务器类型为CMCC。

[AC-portal-server-newpt] server-type cmcc

[AC-portal-server-newpt] quit

配置Portal Web服务器的URL为http://192.168.0.111:8080/portal。

[AC] portal web-server newpt

[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal

配置设备重定向给用户的Portal Web服务器的URL中携带参数ssid、wlanuserip和wlanacname，其值分别为AP的SSID、用户的IP地址和AC名称（与中国移动对接时必配）。

[AC-portal-websvr-newpt] url-parameter ssid ssid

[AC-portal-websvr-newpt] url-parameter wlanuserip source-address

[AC-portal-websvr-newpt] url-parameter wlanacname value AC

配置Portal Web服务器类型为CMCC。

[AC-portal-websvr-newpt] server-type cmcc

[AC-portal-websvr-newpt] quit

配置一条基于IPv4地址的Portal免认证规则，编号为0，目的地址为192.168.0.111，为了放通portal web server的地址。

[AC] portal free-rule 0 destination ip 192.168.0.111 24

开启无线Portal漫游功能。

[AC] portal roaming enable

关闭无线Portal客户端ARP表项固化功能。

[AC] undo portal refresh arp enable

开启无线Portal客户端合法性检查功能。

[AC] portal host-check enable

在无线服务模板st1上使能直接方式的Portal认证。

[AC] wlan service-template st1

[AC-wlan-st-st1] portal enable method direct

在无线服务模板st1上引用Portal Web服务器newpt。

[AC-wlan-st-st1] portal apply web-server newpt

使能无线服务模板st1。

[AC–wlan-st-st1] service-template enable

[AC-wlan-st-st1] quit

4. 配置Switch

创建VLAN 100，用于转发AC和AP间CAPWAP隧道内的流量。

system-view

[Switch] vlan 100

[Switch-vlan100] quit

创建VLAN 200，用于转发Client无线报文。

[Switch] vlan 200

[Switch-vlan200] quit

创建VLAN 2。

[Switch] vlan 2

[Switch-vlan2] quit

配置Switch与AC相连的GigabitEthernet1/0/1接口的属性为Trunk，允许VLAN 100和VLAN 200通过。

[Switch] interface gigabitethernet 1/0/1

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

[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200

[Switch-GigabitEthernet1/0/1] quit

配置Switch与AP相连的GigabitEthernet1/0/2接口属性为Access，并允许VLAN 200通过。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port link-type access

[Switch-GigabitEthernet1/0/2] port access vlan 200

使能PoE功能。

[Switch-GigabitEthernet1/0/2] poe enable

[Switch-GigabitEthernet1/0/2] quit

配置VLAN 100接口的IP地址。

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ip address 2.2.2.100 255.255.255.0

[Switch-Vlan-interface100] quit

配置VLAN 2接口的IP地址。

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0

[Switch-Vlan-interface2] quit

1)为了使用户正常访问Portal Web服务器，必须配置Portal免认证规则，放行访问Portal Web服务器的流量。

2)为了保证无线用户正常漫游，必须开启portal用户漫游功能以及关闭ARP表项固化功能。

3)无线服务模板下使能Portal时，必须配置portal host-check enable

4)为了使服务器对用户授权信息进行动态修改或强制用户下线，必须开启RADIUS session control功能。

5)为了将AP的GigabitEthernet1/0/1接口加入本地转发的VLAN 200，需要使用文本文档编辑AP的配置文件，并将配置文件上传到AC存储介质上。