H3C无线控制器本地Portal认证典型配置举例(V7)

wlan接入 Portal AAA 李晨光 2016-07-01 发表

本文档介绍本地Portal认证的典型配置举例。

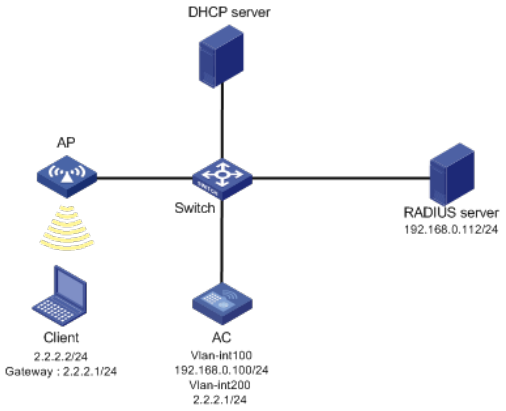
本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解Portal认证的特性。

如图1所示，DHCP服务器为AP和Client分配IP地址。现要求：

- AC同时承担Portal Web服务器和Portal认证服务器的职责。
- 采用RADIUS服务器作为认证/计费服务器。
- 采用直接方式的Portal认证。



1.1 配置思路

- 为了使用户可以在VLAN内的任何二层端口上访问网络资源，且移动接入端口时无须重复认证，必须开启Portal用户漫游功能。
- 在采用本地转发模式的无线组网环境中，AC上没有Portal客户端的ARP表项，为了保证合法用户可以进行Portal认证，需要开启无线Portal客户端合法性检查功能。
- 短时间内Portal客户端的频繁上下线可能会造成Portal认证失败，需要关闭Portal客户端ARP表项固化功能。
- 为了使RADIUS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。
- 编辑认证页面，保存为abc.zip，并上传到AC存储介质的根目录。

1.1 配置步骤

1.1.1 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 192.168.0.100 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

配置路由，保证启动Portal之前各Client、服务器和AC之间的路由可达。（略）

(2) 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200。

[AC-wlan-st-st1] vlan 200

配置接入的Portal用户使用认证域为dm1。

[AC-wlan-st-st1] portal domain dm1

使能无线服务模板。

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

[AC-wlan-st-service] 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

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

(3) 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 192.168.0.112

[AC-radius-rs1] primary accounting 192.168.0.112

[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

(4) 配置认证域

创建名为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

指定ISP域dm1下的用户闲置切断时间为15分钟，闲置切断时间内产生的流量为1024字节。

[AC-isp-dm1] authorization-attribute idle-cut 15 1024

[AC-isp-dm1] quit

(5) 配置Portal认证

配置Portal Web服务器的URL为http://2.2.2.1/portal。

[AC] portal web-server newpt

[AC-portal-websvr-newpt] url http://2.2.2.1/portal

配置设备重定向给用户的Portal Web服务器的URL中携带参数wlanuserip。

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

配置Portal Web服务器类型为CMCC。

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

[AC-portal-websvr-newpt] quit

在接口Vlan-interface200上使能直接方式的Portal认证。

[AC] interface vlan-interface 200

[AC–Vlan-interface100] portal enable method direct

在接口Vlan-interface200上引用Portal Web服务器newpt。

[AC–Vlan-interface200] portal apply web-server newpt

[AC–Vlan-interface200] quit

创建本地Portal Web 服务器，进入本地Portal Web服务器视图，并指定使用HTTP协议和客户端交互认证信息。

[AC] portal local-web-server http

配置本地Portal Web服务器提供的缺省认证页面文件为abc.zip（设备的存储介质的根目录下必须已存在该认证页面文件，否则功能不生效）。

[AC–portal-local-websvr-http] default-logon-page abc.zip

[AC–portal-local-websvr-http] quit

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

1.1.2 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

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 100通过。

[Switch] interface gigabitethernet 1/0/2

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

[Switch-GigabitEthernet1/0/2] port access vlan 100

使能PoE功能。

[Switch-GigabitEthernet1/0/2] poe enable

[Switch-GigabitEthernet1/0/2] quit

1.1.3 配置RADIUS服务器

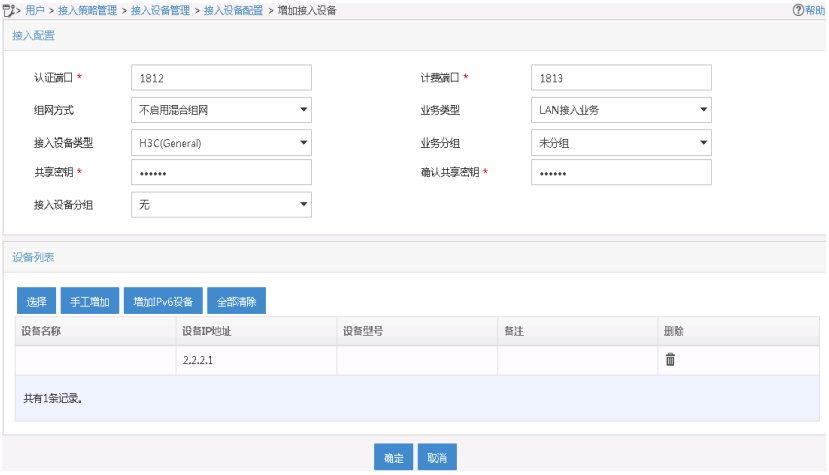
下面以iMC为例（使用iMC版本为：iMC PLAT 7.1(E0303p13)、iMC EIA 7.1(F0302p08)、iMC EIP 7.1(F0302p08)）说明RADIUS server的基本配置。

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。

- 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。
- 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。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

图1 增加接入设备

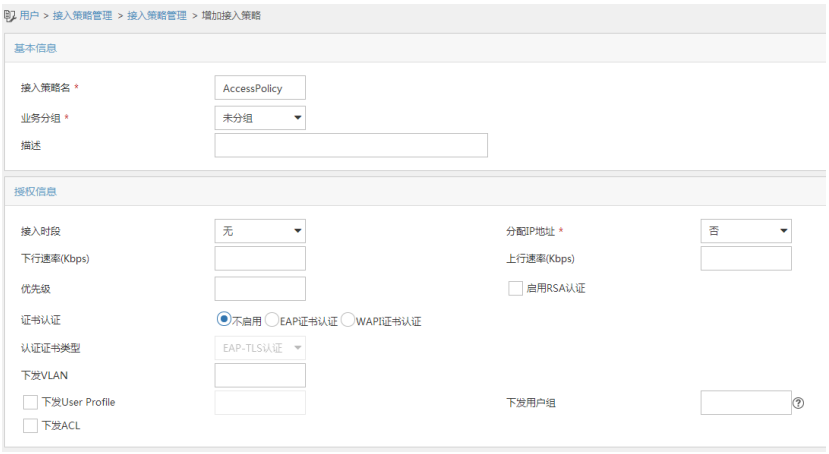


增加接入策略

选择“用户”页签，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。

- 填写接入策略名；
- 选择业务分组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入策略配置

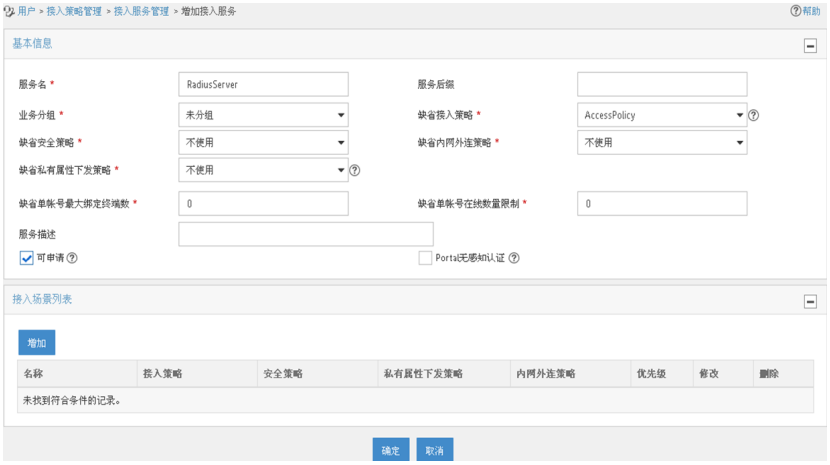


增加接入服务

选择“用户”页签，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。

- 填写服务名；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加接入服务配置

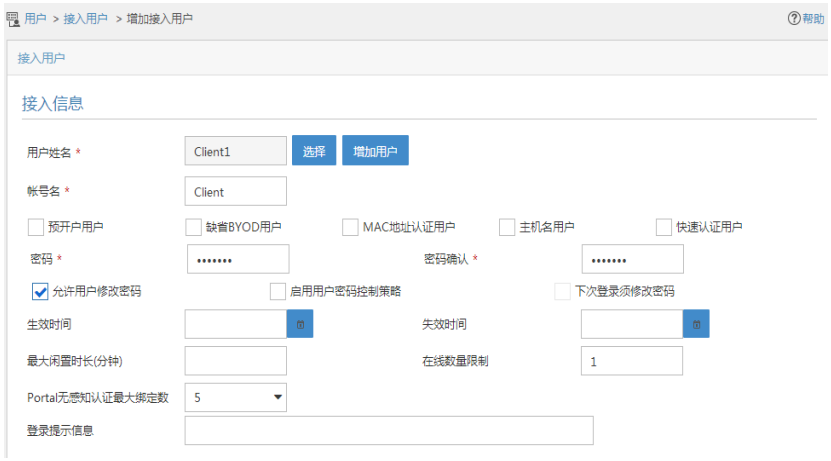


增加接入用户

选择“用户”页签，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。

- 如果用户已存在，用户姓名选择可接入的用户，如果用户不存在，则需要单击<增加用户>按钮添加新用户；
- 填写账号名；
- 设置密码；
- 其它参数可采用缺省配置。

图4 增加接入用户



1.2 验证配置

用户通过网页方式进行Portal认证。用户在通过认证前，发起的所有Web访问均被重定向到Portal认证页面（http://2.2.2.1/portal），在通过认证后，可访问非受限的互联网资源。

通过执行以下显示命令查看AC上生成的Portal在线用户信息。

```
[AC] display portal user all
Total portal users: 1
Username: Client
  Portal server:newpt
  State: Online
  VPN instance: N/A
  MAC            IP              VLAN    Interface
  0024-d705-c686 2.2.2.2         200     Vlan-interface200
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

1.3 配置文件

- AC：

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 vlan 200
 portal domain dm1
 service-template enable
#
interface Vlan-interface100
 ip address 192.168.0.100 255.255.255.0
```

```
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
 portal enable method direct
 portal apply web-server newpt
#
 radius session-control enable
#
radius scheme rs1
 primary authentication 192.168.0.112
 primary accounting 192.168.0.112
 key authentication cipher $c$3$Sqgqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
 key accounting cipher $c$3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
 user-name-format without-domain
#
domain dm1
 authorization-attribute idle-cut 15 1024
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal none
#
 portal host-check enable
#
 portal roaming enable
 undo portal refresh arp enable
#
portal web-server newpt
 url http://2.2.2.1/portal
 server-type cmcc
 url-parameter wlanuserip source-address
#
portal local-web-server http
 default-logon-page abc.zip
#
wlan ap office model WA4320i-ACN
 serial-id 219801A0CNC138011454
 radio 1
 radio 2
  radio enable
  service-template st1
#
```

· Switch：

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
poe enable
```

· 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。

· AC上配置的Portal认证服务器和Portal Web服务器的服务器类型必须与实际服务器一

致（本例以中国移动为例）。

· 设备重定向给用户的Portal Web服务器的URL默认是不携带参数，需要根据实际应用手动添加需要携带的参数信息

· 若在VLAN接口视图下开启Portal认证，只能采用集中转发；若在服务模板视图下开启Portal认证，则本地转发和集中式转发都支持（本例以VLAN接口视图下开启Portal认证为例）。

· 如果本地Portal Web服务器提供的缺省认证页面文件需要更新，需要undo default-logon-page后重新配置，否则新页面不会生效。