H3C 无线控制器 Portal MAC-Trigger 快速认证典型配置举例(V7)

目 录

1 简介

本文档介绍 Portal MAC-Trigger 快速认证配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的无线控制器和接入点产品，不严格与具体硬件版本对应，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 AAA、Portal、WLAN 特性。

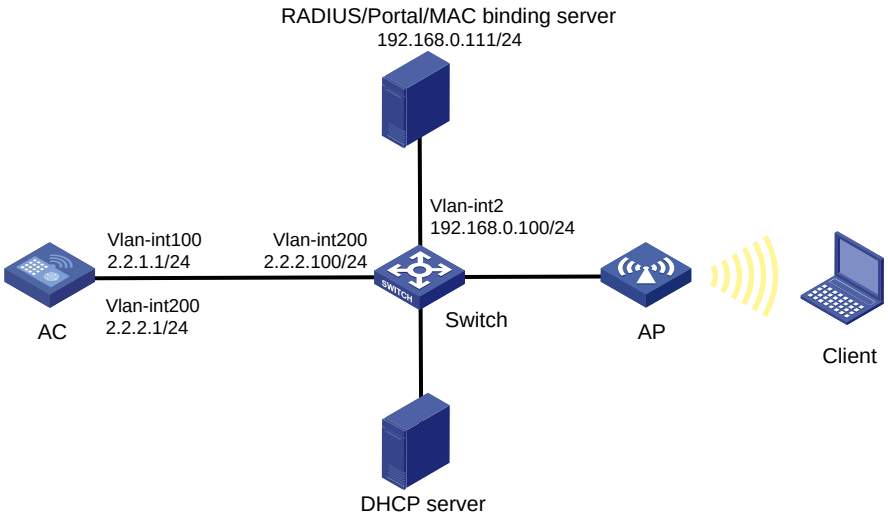
3 配置举例

3.1 组网需求

如图 1 所示，AP 和 Client 通过 DHCP 服务器获取 IP 地址，iMC 同时作为 Portal 认证服务器和 Portal Web 服务器、RADIUS 服务器和 MAC 绑定服务器，要求：

- AC 采用直接方式的 Portal 认证。
- Client 在通过 Portal 认证前，只能访问 Portal Web 服务器；Client 通过 Portal 认证后，可以访问外部网络。
- 在 Client 的流量达到 1024000 字节之前，允许 Client 访问外部网络资源，一旦流量达到 1024000 字节，则触发 MAC 快速认证。
- 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。
- 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。

图1 Portal 基于 MAC 地址的快速认证组网图



3.2 配置思路

- 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。
- 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。
- 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。
- 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。
- 为了防止用户上线过程中，动态授权信息下发失败，需要配置 RADIUS DAE 服务器功能。

3.3 配置注意事项

- 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、Portal Web 服务器和 MAC 绑定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（本例以服务模板视图下开启 Portal 认证为例）。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。

3.4 配置步骤

3.4.1 配置 iMC

说明

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。

- 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2 增加接入设备

(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3 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。

- 填写 IP 地址组名；
- 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；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

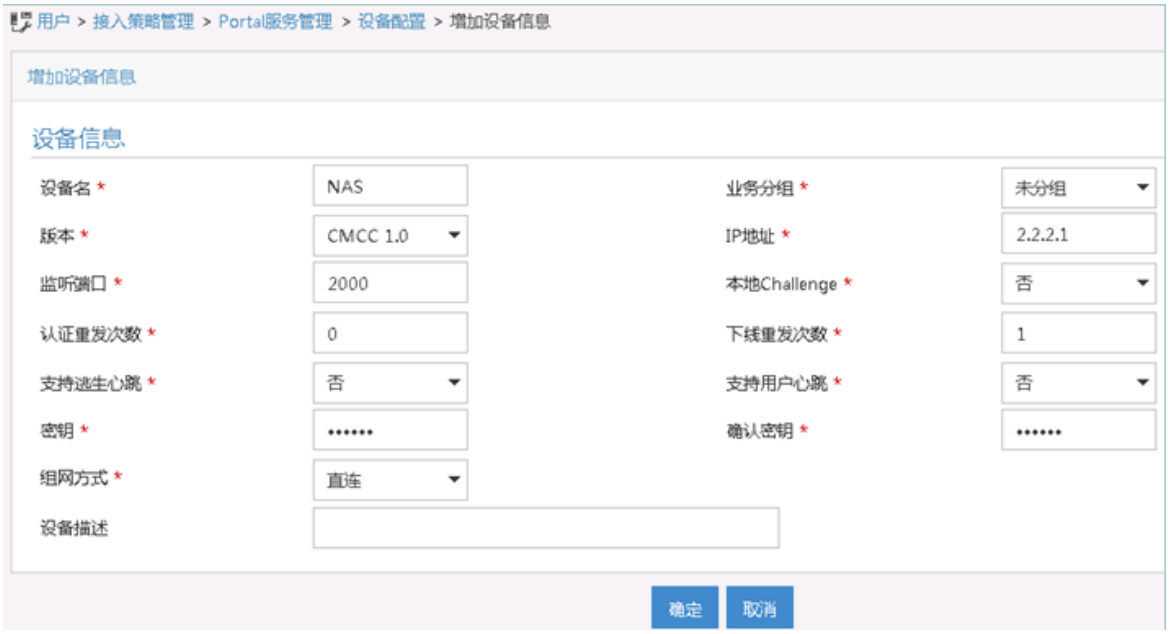
图4 增加 IP 地址组配置页面

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。

- 填写设备名；
- 版本选择“CMCC 1.0”；
- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 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。
- 输入密钥，与 AC 上的配置保持一致；
- 选择组网方式为直连；
- 其它参数可采用缺省配置。

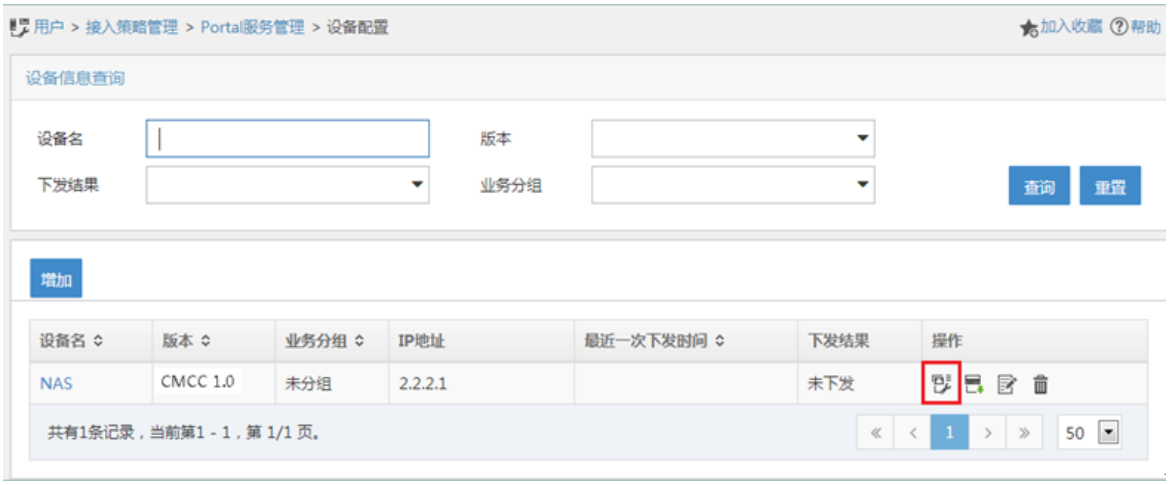
图5 增加设备信息配置页面



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，单击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

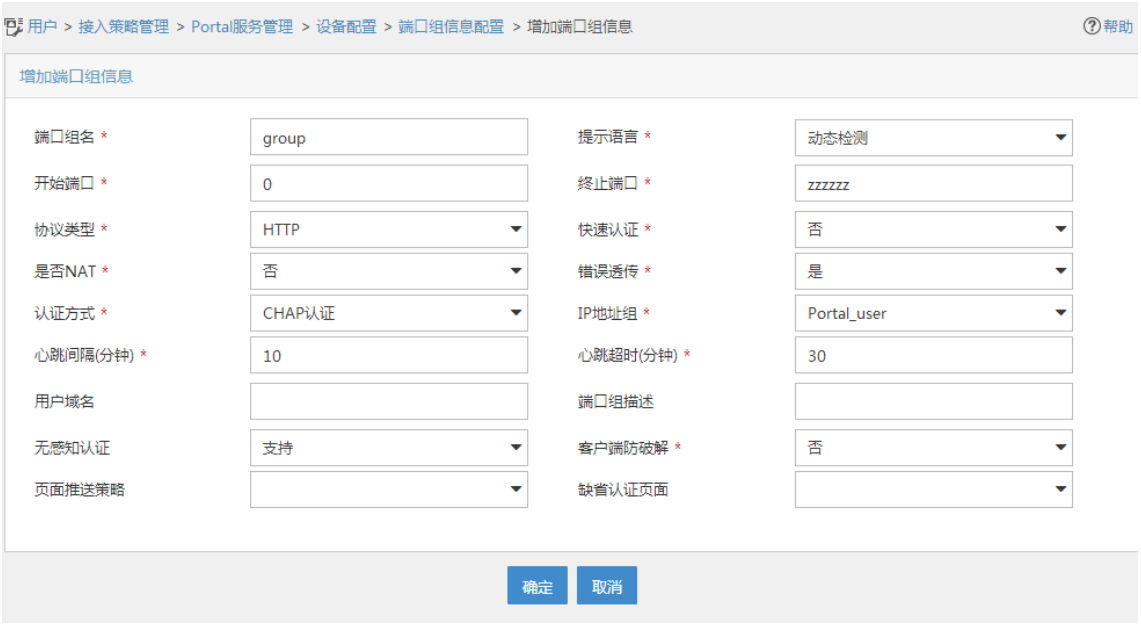
图6 设备信息列表



在端口组信息配置页面中单击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 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；
- 无感知认证选择“支持”；
- 其它参数可采用缺省配置。

图7 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。

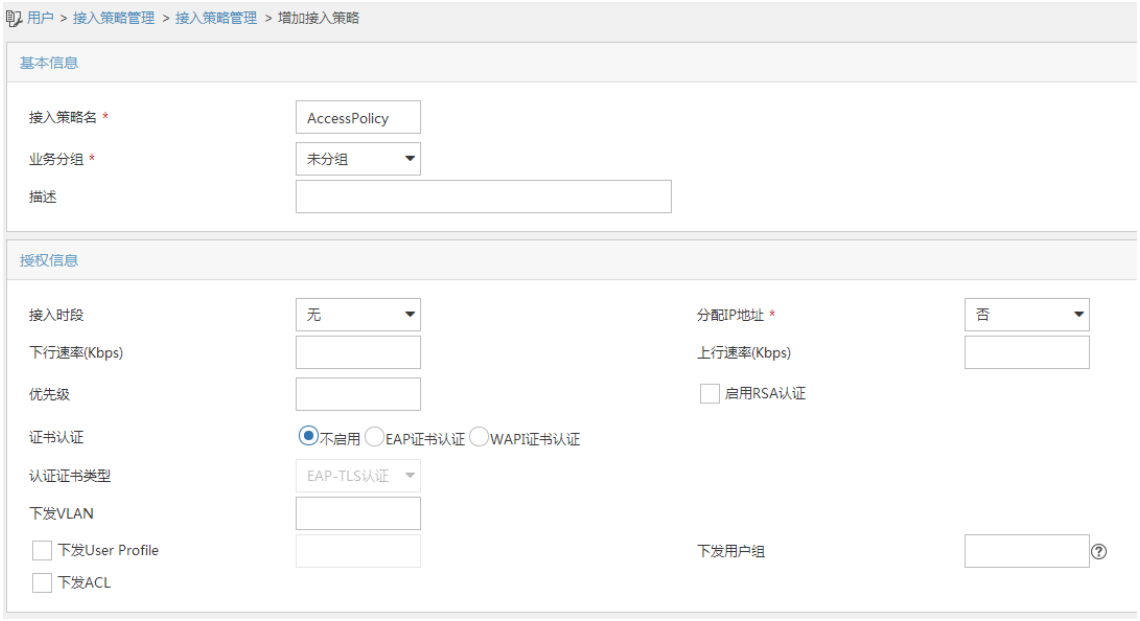
(3) 配置 MAC 绑定服务器

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，并单击<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；
- 其它参数可采用缺省配置。

图8 增加接入策略配置

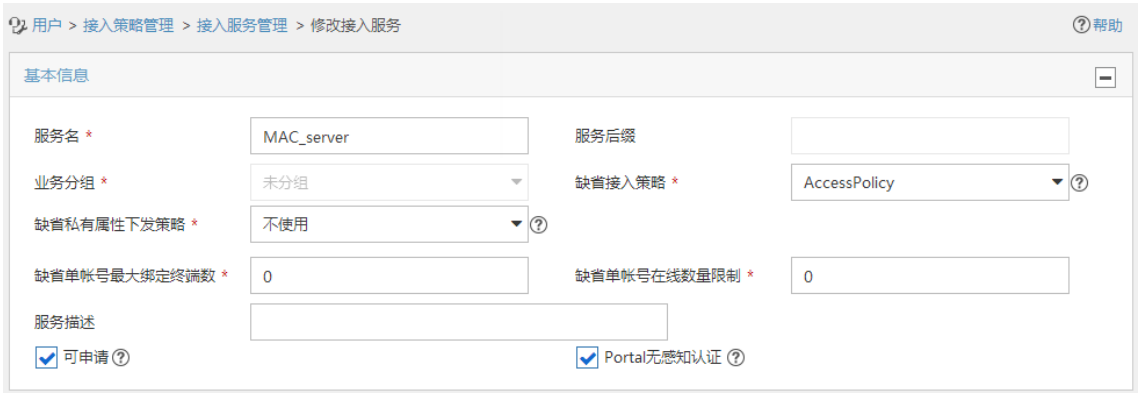


增加接入服务

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

- 填写服务名；
- 缺省接入策略选择已配置好的接入策略；
- 勾选“Portal 无感知认证”；
- 其它参数可采用缺省配置。

图9 增加接入服务配置



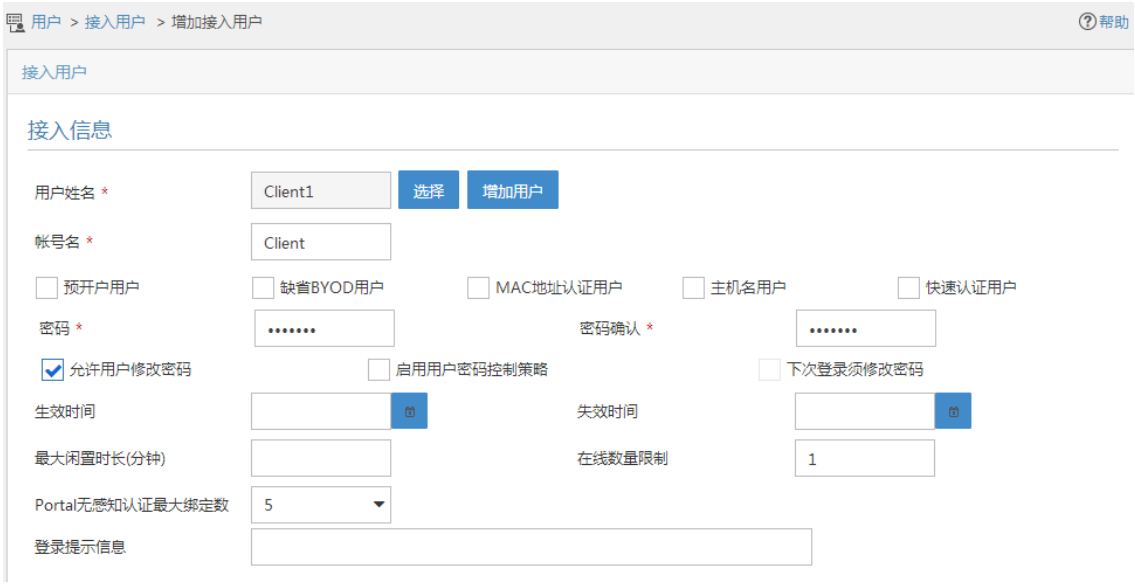
增加接入用户

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

- 用户姓名选择已经存在的可接入的用户或单击<增加用户按钮>，增加一个新用户；

- 填写账号名；
- 设置密码；
- 设置“Portal 无感知认证最大绑定数”；
- 其它参数可采用缺省配置。

图10 增加接入用户



配置系统参数

单击导航树中的[接入策略管理/业务参数配置/系统配置]菜单项，并单击[终端管理参数配置]对应的<配置>按钮，进入终端管理参数配置页面。

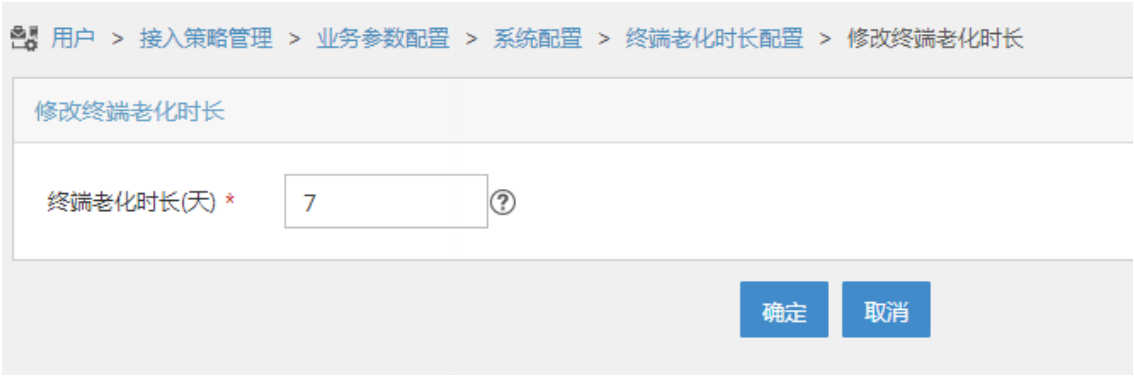
“非智能终端 Portal 无感知认证”可根据实际需要启用或禁用，本例中为启用。

图11 配置终端管理参数

单击导航树中的[接入策略管理/业务参数配置/系统配置]菜单项，单击[终端老化时长]对应的<配置>按钮，然后单击<修改>，进入终端老化时长配置页面。

根据实际需要配置终端老化时间，本例中采用默认值。

图12 配置终端老化时长



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，使以上配置生效。

3.4.2 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
```

3.4.3 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。

```
<AC> 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 服务器的静态路由。

```
[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 200。

```
[AC-wlan-st-st1] vlan 200
```

配置客户端数据报文转发位置为 AP。

```
[AC-wlan-st-service1] 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
```

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
```

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
[AC] radius dynamic-author server
```

设置 RADIUS DAE 客户端的 IP 地址为 192.168.0.111，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius。

```
[AC-radius-da-server] client ip 192.168.0.111 key simple radius
[AC-radius-da-server] quit
```

(5) 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 RADIUS。

```
[AC-isp-dm1] accounting portal radius-scheme rs1
```

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
```

(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，监听 Portal 报文的端口为 50100。

```
[AC] portal server newpt
[AC-portal-server-newpt] ip 192.168.0.111
[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（这三个参数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，以便放行访问 Portal Web 服务器的流量，让用户可以正常访问 Portal Web 服务器。

```
[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
```

配置接入的 Portal 用户使用认证域为 dm1。

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

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
[AC-wlan-st-st1] quit
```

(7) 配置 Portal 基于 MAC 地址的快速认证

创建 MAC 绑定服务器 mts，并进入 MAC 绑定服务器视图。

```
[AC] portal mac-trigger-server mts
```

配置用户免认证流量的阀值为 1024 字节。

```
[AC-portal-mac-trigger-server-mts] free-traffic Threshold 1024000
```

配置 MAC 绑定服务器的地址为 192.168.0.111。

```
[AC-portal-mac-trigger-server-mts] ip 192.168.0.111
```

配置 MAC 绑定服务器类型为 CMCC。

```
[AC- mac-trigger-server-mts] server-type cmcc
[AC-portal-mac-trigger-server-mts] quit
```

在无线服务模板上应用 MAC 绑定服务器 mts。

```
[AC] wlan service-template st1
[AC-wlan-st-st1] portal apply mac-trigger-server mts
```

开启无线服务模板。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-st1] quit
```

3.4.4 配置 Switch

创建 VLAN 100，用于转发 AC 和 AP 间 CAPWAP 隧道内的流量。

```
<Switch> 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 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
```

配置 VLAN 200 接口的 IP 地址。

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] 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
```

3.5 验证配置

通过执行以下显示命令可查看 MAC 绑定服务器配置。

```
[AC] display portal mac-trigger-server name mts
Portal mac trigger server name: mts
  Version                     : 1.0
  Server type                 : CMCC
  IP                          : 192.168.0.111
  Port                        : 50100
  VPN instance                : Not configured
  Aging time                  : 300 seconds
  Free-traffic threshold      : 1024000 bytes
  NAS-Port-Type               : Not configured
  Binding retry times         : 3
  Binding retry interval      : 1 seconds
  Authentication timeout      : 3 minutes
```

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://192.168.0.111:8080/portal），在通过认证后，可访问非受限的互联网资源。

用户在首次进行 Portal 认证时，需要手工输入用户名和密码。当用户再次上线时，将可以直接访问互联网资源，不会感知到 Portal 认证过程。

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: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC             IP                  VLAN    Interface
  0021-6330-0933  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
```

3.6 配置文件

- AC：

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 vlan 200
client forwarding-location ap
 portal enable method direct
portal domain ldap
portal apply web-server newpt
 portal apply mac-trigger-server mts
 service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
 ip route-static 192.168.0.0 16 2.2.2.100
#
 radius session-control enable
#
radius scheme rs1
 primary authentication 192.168.0.111
 primary accounting 192.168.0.111
 key authentication cipher $c$3$Sqgqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
 key accounting cipher $c$3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
 user-name-format without-domain
#
radius dynamic-author server
 client ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dm1
 authorization-attribute idle-cut 15 1024
```

```
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal radius-scheme rs1
#
portal host-check enable
 portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
#
 portal roaming enable
 undo portal refresh arp enable
#
 portal web-server newpt
 url http://192.168.0.111:8080/portal
 server-type cmcc
 url-parameter ssid ssid
 url-parameter wlanacname value AC
 url-parameter wlanuserip source-address
#
portal server newpt
 ip 192.168.0.111
 server-type cmcc
#
portal mac-trigger-server mts
 ip 192.168.0.111
 server-type cmcc
 free-traffic threshold 1024000
#
wlan ap office model WA4320i-ACN
 serial-id 219801A0CNC138011454
 radio 1
 radio 2
  radio enable
  service-template st1
#
```

- Switch：

```
#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.100 255.255.255.0
#
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
```

4 相关资料

- 《H3C 无线控制器产品 配置指导(R5109)》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考(R5109)》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导(R5109)》中的“WLAN 配置指导”
- 《H3C 无线控制器产品 命令参考(R5109)》中的“WLAN 命令参考”