

本文档介绍了本地Portal认证限制最大接入用户数的典型配置，每一账户仅供当前一人使用，该账户若有用户在线，则其他人不能再用此账户登录上线。

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。

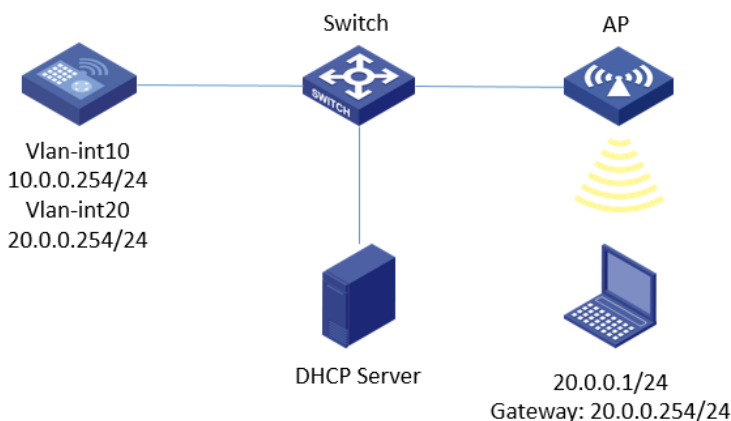
本文档假设您已了解Portal认证的特性。

如图所示，DHCP服务器为AP和Client分配IP地址。

AC同时承担Portal Web服务器和Portal认证服务器的职责。

计费方式采用本地计费。

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。

编辑认证页面，保存为abc.zip，并上传到AC存储介质的根目录。

1.2 配置步骤

(1) 配置AC接口

#创建VLAN 10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 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 10.0.0.254 24
[AC-Vlan-interface10] quit
```

#创建VLAN 20 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 20
[AC-vlan20] quit
[AC] interface vlan-interface 20
[AC-Vlan-interface] ip address 20.0.0.254 24
[AC-Vlan-interface] 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local-portal。
```

```
[AC-wlan-st-st1] ssid local-portal
```

#使能无线服务模板。

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

```
[AC-wlan-st-st1] 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219801A0CNC1380114
54。
[AC] wlan ap office model WA4320i-ACN
[AC-wlan-ap-office] serial-id 219801A0CNC138011454
#进入Radio视图。
[AC-wlan-ap-office] radio 2
#将无线服务模板st1绑定到radio 2, 绑定业务vlan, 并开启射频。
[AC-wlan-ap-office-radio-2] service-template st1 vlan 20
[AC-wlan-ap-office-radio-2] radio enable
(3) 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, 认证方式为本地, 授权方式为本地, 计费方式为本地。
[AC-isp-dm1] authentication portal local
[AC-isp-dm1] authorization portal local
[AC-isp-dm1] accounting portal local
#配置用户计费开始失败策略, 当用户计费开始失败时, 强制用户下线。
[AC-isp-dm1] accounting start-fail offline
#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
(4) 配置Portal认证。
#配置Portal Web服务器的URL为http://20.0.0.254/portal
[AC] portal web-server newpt
[AC-portal-websvr-newpt] url http://20.0.0.254/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
#配置接入的Portal用户使用认证域为dm1。
[AC-wlan-st-st1] portal domain dm1
[AC-wlan-st-st1] 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
(5) 配置本地Portal认证的用户名和密码
#创建本地用户名和密码。
[AC] local-user 123 class network
[AC-luser-network-123] password simple 123
[AC-luser-network-123] service-type portal
#限制最大接入用户数为1。
[AC-luser-network-123] access-limit 1
[AC-luser-network-123] quit
(6) 配置Switch
#创建VLAN 10, 用于转发AC和AP间CAPWAP隧道内的流量。
<Switch> system-view
[Switch] vlan 10
```

```
[Switch-vlan10] quit
#创建VLAN 20, 用于转发Client无线报文。
[Switch] vlan 20
[Switch-vlan20] quit
#配置Switch与AC相连的接口的属性为Trunk, 允许VLAN 10和VLAN 20通过。
[Switch] interface gigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[Switch-GigabitEthernet1/0/1] quit
#配置Switch与AP相连的接口的属性为Access, 并允许VLAN 10通过。
[Switch] interface gigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 10
#使能PoE功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

关键配置为:

```
[AC-isp-dm1] accounting portal local
[AC-isp-dm1] accounting start-fail offline
[AC-luser-network-123] access-limit 1
```

测试结果如下:

(1) 不做用户数限制时, Portal认证成功后, 查看Portal用户表项, 可看到多个用户

```
[AC] display portal user all
Total portal users: 2
Username: 123
  AP name: ap3
  Radio ID: 3
  SSID: 4600
  Portal server: N/A
  State: Online
  VPN instance: N/A
  MAC      IP          VLAN  Interface
  c894-bb8d-3c83 10.1.1.2    10   WLAN-BSS1/0/3
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
```

```
Username: 123
  AP name: ap3
  Radio ID: 2
  SSID: 4600
  Portal server: N/A
  State: Online
  VPN instance: N/A
  MAC      IP          VLAN  Interface
  34f6-4bc9-48b1 10.1.1.5    10   WLAN-BSS1/0/2
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
```

(2) 做用户数限制后, 第一个终端登录, 可认证成功, 访问网络。第二个终端登录, 终端页面上会显示已认证成功, 但此终端不可上网, 设备上无此终端的Portal用户表项。

```
[AC] display portal user all
Total portal users: 1
Username: 123
  AP name: ap3
```

Radio ID: 3

SSID: 4600

Portal server: N/A

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
c894-bb8d-3c83	10.1.1.2	10	WLAN-BSS1/0/3

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