

知 某局点portal认证页面访问失败经验案例

Portal 殷俊 2019-02-28 发表

组网及说明

分层AC组网，认证点在Central AC，转发点在AP；
Central AC双机热备份；
portal认证服务器为IMC

问题描述

现场局点有一分层AC组网配置portal+无感知认证，认证点在central AC，转发点在AP上。在central AC上有一本地SSID无线portal认证均正常，但是下联分支上的SSID portal页面始终无法弹出，两个SSID使用同一domain和radius策略，分属不同地址段，一个VLAN 301，一个VLAN 401
在分支处使用有线无线测试弹出结果一致：

向 Portal Server 发送请求超时。
抱歉，您暂时不能使用 Portal Web 认证进行宽带上网，请与管理员联系。

AC设备侧主要配置：

```
#
wlan service-template 2
ssid A-WiFi
vlan 301
client forwarding-location ap
client-security authentication-location central-ac
portal enable method direct
portal domain imc
portal bas-ip 10.212.30.150
portal apply web-server imc
portal apply mac-trigger-server imc
service-template enable

#
wlan service-template 3
ssid A-WiFi
vlan 301
portal enable method direct
portal domain imc
portal bas-ip 10.212.30.150
portal apply web-server imc
portal apply mac-trigger-server imc
service-template enable

#
portal web-server imc
url http://10.212.0.80:80/portal
url-parameter apmac ap-mac
url-parameter ssid ssid
url-parameter userip source-address
url-parameter usermac value source-mac

#
portal server imc
ip 10.212.0.80 key cipher $c$3$VkJT8tta72jPA8+1dSEWGvvtKvKuBUBDA3/L0Ww4m
```

过程分析

由于总部无线业务与分支无线业务共用一个portal认证服务，只是业务vlan不同，可以判断认证服务器侧portal服务正常；
对于故障业务终端，尝试直接ping认证服务器IP地址可达，无丢包，可以判断链路没问题；
尝试无线终端在浏览器直接输入portal url是否能打开，发现直接输入url也无法访问，怀疑是否与分层AC组网相关，但理论上AP是本地转发，应当不涉及分层AC模块；
尝试PC有线侧接入AP上行接入交换机，相同业务情况下浏览器中直接输入portal url仍然无法访问，排除分层AC组网问题以及无线转发问题，怀疑是中间有线侧链路中其他设备对portal服务有策略限制；
尝试问题复现时，PC有线直连接入交换机情况下，PC侧直接抓包定位，通过抓包分析，发现终端与服务

务器侧80端口http报文有正常交互，并未限制，说明中间链路不存在问题；
最终通过服务器侧抓包以及日志分析，发现终端的请求报文发送到认证服务器，但服务器响应报文回复给了另一个AC地址，经确认，现场在IMC上添加了主备Central AC，但AC的配置中并未添加portal重定向携带设备bas-ip配置，导致IMC侧无法判断请求报文是从哪台设备发送的，因此无法区分响应哪台设备，从而导致页面无法显示。

解决方法

在portal web-server下配置重定向url中携带设备bas-ip配置,但配置时参数需要写nasip服务器才能识别，具体的IP地址实际为设备上服务模板下配置的bas-ip地址，具体配置如下：

```
portal web-server imc
```

```
url-parameter nasip value x.x.x.x
```