

# 知 AC对接U-Center 2.0 定制开发认证页面-终端portal认证失败，报“向设备发送请求超时”

Portal 谭奇伟 2024-01-01 发表

## 组网及说明

AC旁挂核心，对接U-Center 2.0 定制开发扫码认证页面（portal认证），AC和U-Center均处于内网环境。

## 告警信息

无

## 问题描述

终端认证失败，报“向设备发送请求超时”，U-Center的portal日志亦记录相关的原因。

## 过程分析

一般认证终端或者认证服务器报“向设备发送请求超时”，是指按照portal协议，认证服务器向AC发送的req\_info（如果选择chap模式，则是req\_challenge）报文没有收到来自AC侧回应的Ack\_info（chap模式是Ack\_challenge）报文。

可能与如下原因有关：

- ① 认证服务器没有将req\_info（req\_challenge）报文发给正确的AC；
- ② 认证服务器发送的req\_info（req\_challenge）报文被中间设备拦截或者丢弃，导致没有送达AC；
- ③ AC收到的req\_info（req\_challenge）报文被认为是无效报文被丢弃；
- ④ AC的portal相关进程异常而没有正确处理该报文；
- ⑤ AC正确处理后发送给认证服务器的Ack\_info（Ack\_challenge）报文被中间设备拦截或者丢弃，导致没有送到认证服务器。

对此，在AC和交换机连接端口的交换机侧端口做镜像抓包，同时AC上开启如下debug：

```
<AC> debug portal error
<AC> debug portal event
<AC> debug portal packet
<AC> debug radius all
<AC> debug radius error
```

然后让终端去连接以复现故障，抓包发现U-Center 2.0给AC发送了4条req\_info报文，但是AC均没有回复ack\_info的报文，

而且报文发送的源IP是对的，也就是说U-Center将报文发给了正确的AC：

No.	Time	Source	Destination	Protocol	Vlan	Length	Info
191915	2023-12-25 11:25:59.887113	10.185.206.216	172.51.0.253	Portal		76	REQ_INFO
203189	2023-12-25 11:27:31.974747	10.185.206.216	172.51.0.253	Portal		76	REQ_INFO
221534	2023-12-25 11:29:51.237060	10.185.206.216	172.51.0.253	Portal		76	REQ_INFO
369059	2023-12-25 11:46:28.585273	10.185.206.216	172.51.0.253	Portal		76	REQ_INFO

然后查看AC上的portal debug日志，发现竟然没有任何与portal相关的debug信息，

为了进一步确认AC是否收到了portal报文，在AC上使用了底层抓包命令（相关命令不便对外公布），发现AC确实也收到了报文，但奇怪的是AC却没有portal debug日志的打印，

此时在AC上查看portal报文收发包的记录，发现portal报文的计数相比复现故障前并无增加，均是0，

但值得注意的是：portal报文统计中：Invalid packets计数从0增加到4，由此可以判断，AC将U-Center发送过来的4个req\_info报文识别为无效报文。

```
<AC>display portal packet statistics server
Portal server :
Invalid packets: 4
Pkt-Type          Total    Drops    Errors
REQ_CHALLENGE     0        0        0
ACK_CHALLENGE     0        0        0
REQ_AUTH          0        0        0
ACK_AUTH          0        0        0
REQ_LOGOUT        0        0        0
ACK_LOGOUT        0        0        0
AFF_ACK_AUTH      0        0        0
NTF_LOGOUT        0        0        0
REQ_INFO          0        0        0
ACK_INFO          0        0        0
NTF_USERDISCOVER  0        0        0
NTF_USERIPCHANGE  0        0        0
AFF_NTF_USERIPCHAN 0        0        0
ACK_NTF_LOGOUT    0        0        0
NTF_HEARTBEAT     0        0        0
NTF_USER_HEARTBEAT 0        0        0
ACK_NTF_USER_HEARTBEAT 0        0        0
NTF_CHALLENGE     0        0        0
NTF_USER_NOTIFY   0        0        0
AFF_NTF_USER_NOTIFY 0        0        0
```

那么为什么AC会将这四条报文识别为无效报文呢？我们打开这四条报文携带的属性与正常req\_info报文进行对比，发现这四条req\_info报文携带的userip（终端IP地址均是0），这就是AC认为报文无效的根本原因：

**现场抓包**

No.	Time	Source	Destination	Protocol	Vlan	Length	Info
13	2023-08-14 19:56:14.739900	192.168.1.3	3.3.3.1	Portals		60	REQ_CHALLENGE
14	2023-08-14 19:56:14.758002	3.3.3.1	192.168.1.3	Portals		76	ACK_CHALLENGE
15	2023-08-14 19:56:14.766600	192.168.1.3	3.3.3.1	Portals		102	REQ_AUTH
18	2023-08-14 19:56:14.798000	3.3.3.1	192.168.1.3	Portals		50	ACK_AUTH
30	2023-08-14 19:56:14.796700	192.168.1.1	3.3.3.1	Portals		60	REQ_AUTH

**正常以证报文, req-info/req-challenge都是填写了userIP的,也就是无线终端IP地址**

**UserIP: 3.3.3.3**

**这个没有填userip,也就是无线STA的IP地址**

**Frame 23753: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface Wi-Fi\_42E43F48-1034-4705-9803-1475601046F5**

**Version: Version 2 (2)**

**Type: REQ\_DINFO (9)**

**UserIP: 0.0.0.0**

在U-Center上进一步查看,发现其发送的报文的userip属性确实没有填写。

```
}, msg='success', rowCount=null, status=0)
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:13,895 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: =====请求日志开始=====
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:13,895 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: 请求方式 : GET
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:13,895 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: 请求url : https://10.189.189.189/portal/entrance/http_index.jsp?userinfo=ibHLf1t14Mm5w6EzIK1v7MNB9SL&2FhZ6nPv9bfArqKqK1M2fmHP7Y1J0l&2F8zFz35HAZ2Z82Bus8vNTp0YdEzWcny&2Fm9280BE9M1&2Bq0MHTZxANtuzf12L52f0rqadNCs7&2FFC%2F&28oq&3D&3D&language=chinese&userPublicIp=10.50.85.94&userip=::ffff:10.50.85.94
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:13,895 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: =====请求日志结束=====
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:44,018 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: *****响应日志开始*****
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:44,019 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: 响应url : https://10.189.189.189/portal/entrance/http_index.jsp?userinfo=ibHLf1t14Mm5w6EzIK1v7MNB9SL&2FhZ6nPv9bfArqKqK1M2fmHP7Y1J0l&2F8zFz35HAZ2Z82Bus8vNTp0YdEzWcny&2Fm9280BE9M1&2Bq0MHTZxANtuzf12L52f0rqadNCs7&2FFC%2F&28oq&3D&3D&language=chinese&userPublicIp=10.50.85.94&userip=::ffff:10.50.85.94
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:44,019 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: 响应code: 200
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:44,019 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: 响应resBody:7
向设备发送请求超时
{"portServerErrorCode": "124", "portServerErrorCodeDesc": "向设备发送请求超时", "e_c": "portServerErrorCode", "e_d": "portServerErrorCodeDesc", "errorNumber": "7"}
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:44,019 com.h3c.dz kf.uc2linker.common.conf.network.interceptor.HttpLogInterceptor[INFO]: *****响应日志结束*****
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:44,019 com.h3c.dz kf.uc2linker.common.conf.network.converter.fastjson.FastJsonResponseBodyConverter[ERROR]: 返回解析失败, 尝试使用其他方式解析
[ForkJoinPool.commonPool-worker-18] 2023-12-24 11:22:44,019 com.h3c.dz kf.service.impl.AuthServiceImp[ERROR]: error >>> SSO认证出错;
```

那么是否是AC在页面重定向的时候没有发送userip的属性给U-Center呢？

检查AC上的portal web-server xxx下，也有配置url-parameter userip source-address，而且现场发现如果通过在电脑上输入一个没有free-rule放通的IP地址来重定向得到二维码，那么此时手机扫码可以认证成功，而对应二维码的页面上就有userip地址属性，这说明AC给终端重定向的时候是携带了该属性的。

经过现场进一步了解，现场工程师测试的时候是在电脑上粘贴一个固定的认证页面的url来弹出二维码，这个url里面当然没有携带终端的信息，改用输入一个没有free-rule放通的IP地址来重定向得到的认证web的url里面携带了这个属性，因此可以认证成功。

而使用固定的url导致认证失败经进一步排查是U-Center定制页面中有需要完善的地方，经相关开发人员完善后认证成功。

**解决方法**

U-Center定制页面中有需要完善的地方，经相关开发人员完善后认证成功。