

知

WX3520X配合WBCD0插卡进行微信公众号认证报60013错误

wlan接入

谭奇伟

2023-04-08 发表

组网及说明

WX3520X，本地转发，旁挂核心交换机，WBCD0插卡连接在AC上，在WBCD0的本地绿洲界面配置了微信公众号认证

13:49

ceshi

自动连接

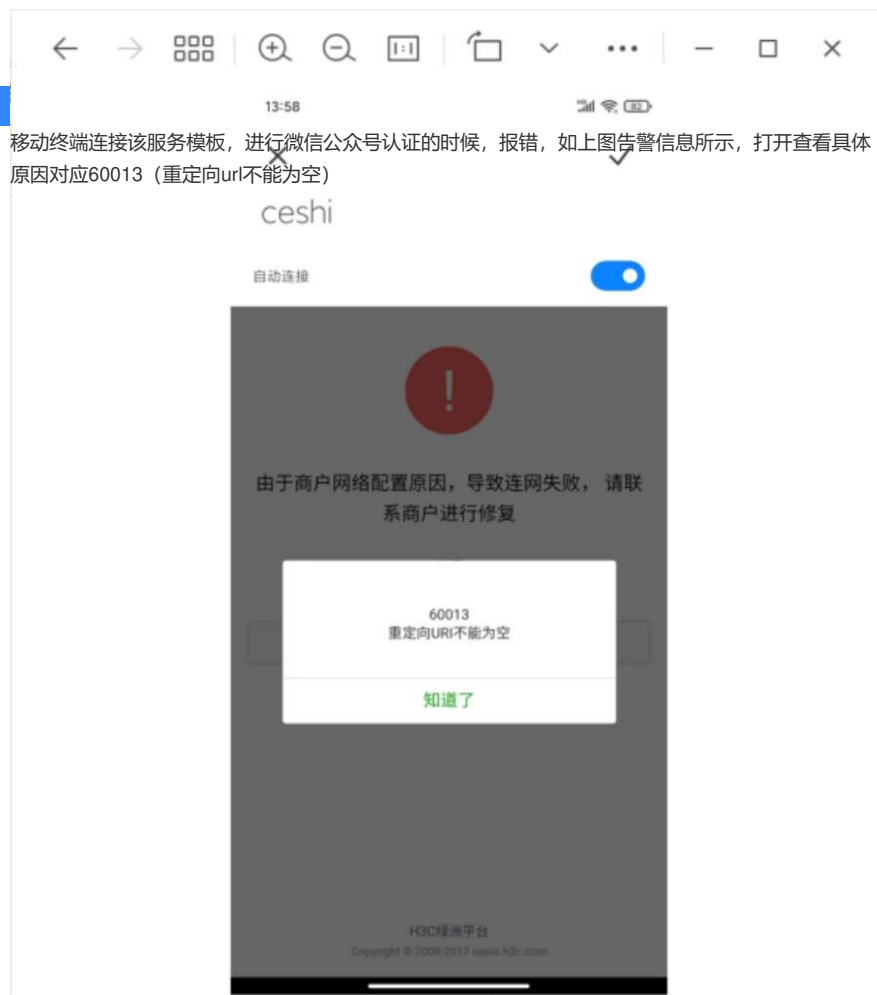
由于商户网络配置原因，导致连网失败，请联系商户进行修复

详情

意见反馈

H3C绿洲平台

Copyright © 2008-2017 oasis.h3c.com



移动终端连接该服务模板，进行微信公众号认证的时候，报错，如上图告警信息所示，打开查看具体原因对应60013（重定向url不能为空）

过程分析

1. 搜索知了案例对应60013的报错，本地转发需要在AC的无线业务vlanif口上配置IP地址，且添加 **port al client-gateway interface vlan x** // 此vlan可以是无线业务vlan的。查看AC的当前配置发现确实没有以上配置，遂增加以上配置，但增加配置后发现故障现象依旧。

检查无线服务模板认证相关配置和portal free-rule放通的域名和各IP地址也没有问题；

2. 对于错误原因码60013，是由于无线终端无法访问到WBCD0上本地绿洲的认证域名（oasisauth.h3c.com）导致的，对此可能有两个原因：①终端访问的这个域名不通；②终端访问这个域名被解析为公网地址。

问题②是比较常见的原因，需要在AC上配置dns代理实现无线终端访问这个域名时被解析为内网WBCD0的地址，AC上的具体配置为：

```
[AC] dns-proxy enable
```

```
[AC] dns server 8.8.8.8 // 公网dns server
```

```
[AC] dns server 114.114.114.114 // 公网dns server
```

```
[AC] ip host oasisauth.h3c.com 172.25.252.18 // WBCD0插卡的固定IP地址，需要将终端访问oasisauth.h3c.com域名时被解析的内网地址。
```

在AC上添加了以上配置后，终端进行认证时发现故障现象仍然依旧；

3. 此时无线终端 ping oasisauth.h3c.com仍然能通，另外找了一台PC连接该wifi后通过nslookup oasisauth.h3c.com命令，发现解析出来的地址仍然是公网的IP地址，这说明终端仍然通过公网dns而非通过AC作为dns代理服务器进行的地址解析；

4. 询问现场后发现终端的DHCP地址池在核心上而非AC上，遂在核心设备上查看地址池发现如下配置：

```
[HS-dhcp-pool-vlanyewu] dns-list 8.8.8.8
```

```
[HS-dhcp-pool-vlanyewu] dns-list 114.114.114.114
```

基于以上配置，终端获取IP后不会通过AC作为dns服务器解析地址，而是直接去公网dns服务器进行地址解析。

于是在地址池上增加如下配置，并将其放置在两个公网dns地址之前，以使终端优先使用AC作为dns服务器进行域名解析：

```
[HS-dhcp-pool-vlanyewu] dns-list 172.25.252.17 // AC上的IP地址，端口是up状态的
```

注意：如果是集中转发，则dhcp地址池上必须指定网关是AC（无线业务vlanif的地址）

完成以上配置后终端认证故障依旧，使用PC执行nslookup oasisauth.h3c.com命令，发现依旧解析的是公网地址，而非本地WBCD0的地址。

5. 怀疑是否还是去公网dns server进行域名解析，于是将核心DHCP地址池中的dns-list 8.8.8.8和dns-list 114.114.114.114去掉，只保留dns-list指向AC。但调整配置后故障依旧，此时出现的新问题是终端 ping oasisauth.h3c.com 不通，且通过nslookup oasisauth.h3c.com命令发现回显是：“DNS request time out”即DNS请求超时。这说明终端首先没有去公网DNS服务器进行域名解析，而在尝试使用AC作为DNS服务器时出现了问题。

6. 用终端ping AC的地址：172.25.252.17发现不通，检查发现free-rule中并未放通这个地址，于是添加了free-rule放通，但发现情况完全没有改变。

此时陷入僵局。。。

思考一段时间后发现该局点使用的是本地转发，思考是否AP将终端访问172.25.252.17的流量进行了拦截（是否配置了ACL或者其它拦截措施）。

于是telnet到AP上，发现AP上有基于vlan的二层隔离配置，而放通的mac只有网关设备（核心）的MAC地址，这就是造成终端访问不到AC的IP地址的原因，因此终端访问AC（DNS代理服务器）的DNS请求也被二层隔离拦截，因此在前述核心DHCP server上同时配置AC和公网DNS地址的情况下，终端先尝试将DNS请求发给AC发现不通，然后将DNS请求送往公网DNS服务器造成解析出来的仍然是公网的oasisauth.h3c.com的域名，而去掉两个公网DNS地址后，终端的DNS请求到AC不通。

于是通过map文件给AP下发的二层隔离放通mac中添加了AC的mac，在此操作之后，终端的认证一切正常。

另外需要说明的是：PC不支持微信公众号认证，只有移动终端支持。

在完成认证后，现场又发现了另外一个问题，就是终端访问公网域名使DNS解析很慢，打微信语音电话几乎不通。

而连接另外一个wifi时（不通的业务vlan），则没有这个问题。可以明确这和DNS有关。

于是去核心交换机上查看另一个正常业务vlan地址池下，配置的第一个dns-list是该局点所使用的运营商节点的一个公网DNS地址，终端到达这个地址的延时显著低于到达8.8.8.8和114.114.114.114这两个公网DNS。

于是在AC上新增了一条配置：dns server xxxx // 运营商节点的一个公网DNS地址，且放置在8.8.8.8和114.114.114.114之前。

基于以上配置调整，问题彻底解决。

解决方法

1. map文件给AP放通基于vlan二层隔离的AC的mac地址；
2. 该局点使用运营商节点的一个公网DNS地址，让DNS域名解析的回复更快。

