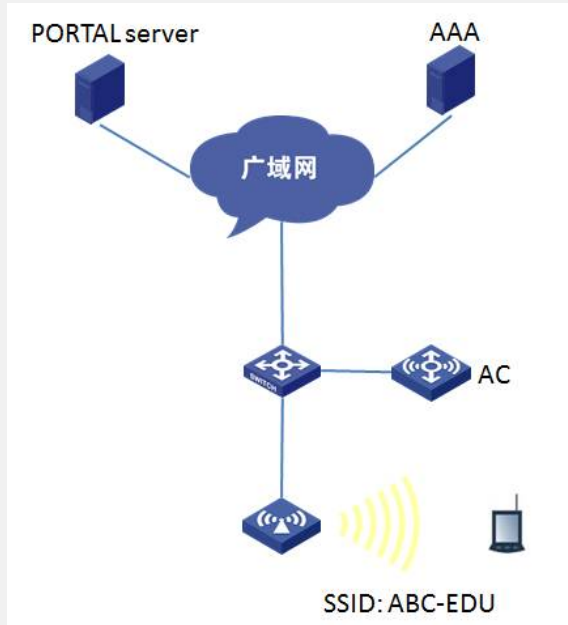


### 某局点Portal认证nas-ip接口配置NAT导致认证故障的经验案例

#### 一、组网拓扑：

某校园网局点采用了我司WX6000系列高性能无线控制器，管理800多个AP，为校区学生宿舍、图书馆、教室提供无线接入服务，并使用我司IMC做无线Portal认证，AC作为接入BAS认证设备，并且承担无线用户的NAT出口。



#### 二、问题描述：

收到客户投诉，大量用户突然无法通过Portal认证登陆，Portal页面提交用户名、密码点击登陆后返回错误信息“接入设备无响应”。出现故障时，已经上线的用户不受影响，但是新用户无法登陆。过几十分钟时间故障突然消失，然后再次复线，故障出现比较随机。

#### 三、问题定位过程：

首先，我们怀疑AC和Portal服务器之间的网络偶发故障，导致新用户无法通过Portal认证。但通过AC携带nas-ip源地址ping Portal服务器，大包无丢包，延迟抖动正常，而且终端的portal页面都能正常打开，所以基本可以排除AC和Portal服务器IP层不通的故障。

于是，我们进一步排查AC和Portal Server之间的Portal协议，以及和Radius服务器之间的Radius协议交互是否正常。先在AC上通过debug portal packet/debug radius packet进行调试分析，发现当出现故障时portal调试信息中未见任何portal和radius的debug信息输出。从这个现象看，常规的理解是AC未收到Portal服务器发送过来的Portal认证报文（UDP：2000）。可能的原因包括AC配置了错误的nas-ip、服务器配置接入设备参数错误等。检查了设备和服务器的相关配置，并未发现明显问题，于是最终通过抓包来裁决，通过抓取AC和Portal服务器之间交互的报文来定位。抓包信息如下：

No.	Time	Source	Destination	Protocol	Packet length	Info
134	4.188942	10.10.8.1	211.71.36.130	UDP	60	Source port: cisco-sccp Destination port: 59540
137	4.188959	10.10.8.1	211.71.36.130	UDP	243	Source port: cisco-sccp Destination port: 50200
140	4.735173	10.10.8.1	211.71.36.130	UDP	90	Source port: cisco-sccp Destination port: 50200
170	4.733540	10.10.8.1	211.71.36.130	UDP	60	Source port: cisco-sccp Destination port: 59542
172	4.738070	10.10.8.1	211.71.36.130	UDP	122	Source port: cisco-sccp Destination port: 50200
176	4.775143	10.10.8.1	211.71.36.130	UDP	70	Source port: cisco-sccp Destination port: 59543
273	8.188290	10.10.8.1	211.71.36.130	UDP	70	Source port: cisco-sccp Destination port: 59544
440	15.064822	10.10.8.1	211.71.36.130	UDP	60	Source port: cisco-sccp Destination port: 59545
441	15.069770	10.10.8.1	211.71.36.130	UDP	148	Source port: cisco-sccp Destination port: 50200
513	18.053755	10.10.8.1	211.71.36.130	UDP	90	Source port: cisco-sccp Destination port: 50200
544	19.489976	10.10.8.1	211.71.36.130	UDP	90	Source port: cisco-sccp Destination port: 50200
568	20.488845	10.10.8.1	211.71.36.130	UDP	90	Source port: cisco-sccp Destination port: 50200
1117	37.872618	10.10.8.1	211.71.36.130	UDP	90	Source port: cisco-sccp Destination port: 50200
1159	39.489255	10.10.8.1	211.71.36.130	UDP	90	Source port: cisco-sccp Destination port: 50200

```

# Frame 440: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
# Ethernet II, Src: Cisco_2F1D1C0 (0018742F1D1C0), Dst: 3ba_2f_333c (681f132f333c)
# Internet Protocol Version 4, Src: 10.10.8.1 (10.10.8.1), Dst: 211.71.36.130 (211.71.36.130)
# User Datagram Protocol, Src Port: cisco-sccp (2000), Dst Port: 59545 (59545)
Source Port: cisco-sccp (2000)
Destination Port: 59545 (59545)
Length: 24
# Checksum: 0d98a [validation disabled]
[Stream index: 12]
# Data (16 Bytes)
Data: 0100100e76400000a0a0e110000000
[Length: 16]

```

(AC nas-ip为211.71.36.130, Server IP为10.10.8.1)

抓包中可以看到Portal服务器向设备发送了大量的UDP 2000认证报文，但AC未予以处

理和回应服务器。所以故障的直接原因已经明确，即AC丢弃了或者未处理Portal服务器发送的认证协议报文，导致用户无法通过Portal认证上线。

但AC为什么会丢弃Portal服务器认证报文？

进一步排查了Portal相关配置并核对了抓包，AC上定义的portal server IP也与抓包中的Server IP 10.10.8.1也完全一致。Portal相关配置没有问题，那为什么AC不处理服务器发送的报文呢？

难道服务器发送的报文格式有问题？可能性不大。如果报文有错误，AC也应该有debug报错提示信息输出，可是AC上debug portal packet未见任何信息。所以问题应当仍然在AC本身。

再次检查了AC的所有配置，最终疑点落在NAS-IP接口的NAT配置上。

```
#
interface Vlan-interface15
ip address 211.71.36.130 255.255.255.128
nat outbound 3998
#
interface Vlan-interface3998
ip address 192.168.255.254 255.255.255.0
portal server weixin method direct
portal domain weixin
portal nas-port-type wireless
portal nas-ip 211.71.36.130
#
```

原来，AC上配置了NAT，AC作为用户的私网IP地址网关，并通过NAT提供外网访问。NAT的出接口即nas-ip (211.71.36.130) 同时也作为NAT转换的源IP。问题即在此，当portal的端口2000被无线终端访问外网的NAT会话占用后，会导致服务器发送向UDP 2000端口的Portal协议报文被AC直接转发到内网用户，从而不能正确处理portal协议报文导致认证失败。而当2000端口释放后，Portal又能重新处理。故出现了故障时而出、时而消失的现象。

#### 四、定位结论及过程总结：

问题根因已明确，nas-ip接口配置NAT，当UDP2000端口号被NAT会话占用后，导致Portal协议报文无法正常处理。

从排障的整个过程看，通过常规的PING包检查链路，以及检查AC服务器配置都不能直接找到故障原因。后续通过抓取debug找到第一个线索，即AC未正常处理Portal协议报文；NAS-IP接口配置NAT是第二个线索（不同于常规的应用）。通过逐步的分析和顺藤摸瓜，最终定位到由于NAT会话占用Portal协议端口UDP2000导致Portal认证失败。

#### 五、问题解决：

H3C的无线产品NAPT暂不支持预留特定的端口号，比如2000。只能在NAT出接口配置NAT地址池，且NAT池中要剔除nas-ip地址，即可解决该问题。示例配置如下：

```
nat address-group 1 211.71.36.131 211.71.36.133
#
interface Vlan-interface15
ip address 211.71.36.130 255.255.255.128
nat outbound 3998 address-group 1
#
```