

某局点WX5580H配置portal认证对接第三方AAA服务器，portal认证异常问题经验案例

Portal 徐猛 2020-04-30 发表

组网及说明

常规无线组网。无线控制器使用WX5580H，portal和AAA服务器使用的是第三方的服务器。

问题描述

现场终端关联无线后，能正常弹出portal页面，但是输入用户名密码后，会提示认证失败。

过程分析

1.检查设备配置，无线portal认证失败问题中常见的几个注意点：

- (1) portal host-check enable配置了
- (2) 现场为集中转发，设备上也配置了无线终端业务网段的IP地址。
- (3) 结合绿洲做portal认证的时候：AC上需要配置portal client-gateway 【interface **】接口配置为和绿洲能通的三层接口

其中前两点均作了配置，第三点因为未结合绿洲，所以也不涉及。其他的配置检查了下，也并未发现异常。

2.于是在AC和核心互通的接口上，作了镜像抓包，我们对报文进行分析。

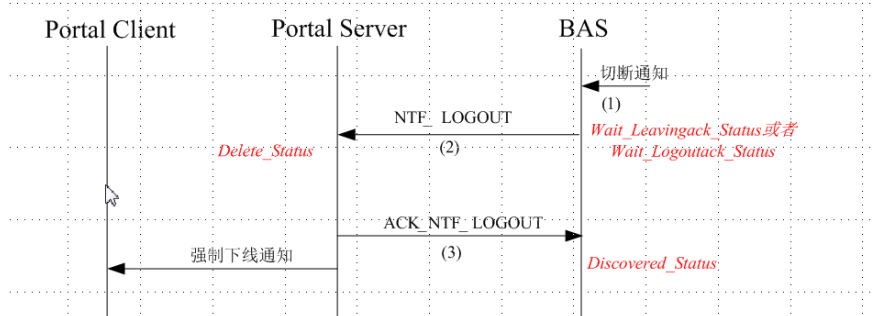
```
7 2020-04-23 17:35:08.802514 192.168.112.130 192.168.112.212 RADIUS 356 Access-Request(1) (id=234, l=314)
8 2020-04-23 17:35:08.802701 192.168.112.212 192.168.112.130 RADIUS 188 Access-Accept(2) (id=234, l=146)
9 2020-04-23 17:35:08.803841 192.168.112.130 192.168.112.212 portal 90 PORTAL_NTF_LOGOUT (SerNo=19041)
10 2020-04-23 17:35:08.803859 192.168.112.212 192.168.112.130 ICMP 118 Destination unreachable (Port unreachable)
11 2020-04-23 17:35:08.807838 192.168.112.212 192.168.112.130 portal 85 PORTAL_REQ_AUTH (SerNo=19080)
12 2020-04-23 17:35:09.044376 192.168.112.130 192.168.112.212 RADIUS 356 Access-Request(1) (id=235, l=314)
13 2020-04-23 17:35:09.044552 192.168.112.212 192.168.112.130 RADIUS 188 Access-Accept(2) (id=235, l=146)
14 2020-04-23 17:35:09.045615 192.168.112.130 192.168.112.212 portal 90 PORTAL_NTF_LOGOUT (SerNo=19089)
15 2020-04-23 17:35:09.045632 192.168.112.212 192.168.112.130 ICMP 118 Destination unreachable (Port unreachable)
16 2020-04-23 17:35:10.799144 192.168.112.212 192.168.112.130 portal 85 PORTAL_REQ_AUTH (SerNo=19041)
17 2020-04-23 17:35:10.802374 192.168.112.130 192.168.112.212 RADIUS 356 Access-Request(1) (id=236, l=314)
18 2020-04-23 17:35:10.802566 192.168.112.212 192.168.112.130 RADIUS 188 Access-Accept(2) (id=236, l=146)
19 2020-04-23 17:35:10.803423 192.168.112.130 192.168.112.212 portal 90 PORTAL_NTF_LOGOUT (SerNo=19041)

Pap/Chap: PAP
Rsv: 0
SerialNo: 19041
ReqId: 0
UserIP: 10.83.9.20
UserPort: 0
ErrCode: 0
AttrNum: 1
Attribute Value Pairs:
000 00 0d 48 18 0d 77 20 0b c7 1e 9c fa 08 00 45 00 ..H..w.....E.
010 00 4c 91 50 00 fe 11 c8 a8 c0 a8 70 82 c0 a8 ..LP.....p...
020 70 64 07 00 c3 14 00 38 ea 09 01 08 01 00 2a 61 ..S.....AAA
030 00 00 0a 53 09 14 00 00 01 05 20 41 41 41 70 ...S.....AAA
040 77 05 0a 05 03 74 05 04 20 01 75 24 60 01 72 60 REJECTED_authen
050 7a 05 20 72 05 71 72 05 73 72
```

根据抓包看，设备给AAA服务器发了认证请求，AAA服务器给设备回了认证通过。但是紧接着，设备给portal服务器发送了NTF_logout报文。查看报文详细内容，发现有提示AAA拒绝授权的字段。怀疑是认证阶段，AAA服务器向设备通告的报文中，携带了拒绝授权之类的字段。导致设备认为该服务器无法做授权，从而直接通告portal服务器用户以下线。

Portal认证的基本原理 H3C

(2) 强制下线流程



- BAS设备一般提供命令切断用户连接，或者由于外部事件所引起的BAS设备发现用户已经异常也要及时通知Portal Server。
- BAS设备通过发送NTF_LOGOUT报文给Portal Server来通知用户已经下线。
- Portal Server收到NTF_LOGOUT报文后，需要向BAS发送ACK_NTF_LOGOUT报文确认收到的NTF_LOGOUT报文，这个报文由于外部事件BAS也可能收不到。同时，Portal Server应该通知用户网络中断，这个通知过程可能会失败，此时无法通知用户网络连接已经中断。

解决方法

后续让现场将认证域下，直接将portal的授权功能做了关闭，后续测试正常。同样，如果AAA不支持做计费，同样可以将计费做关闭。

```
#
domain drcrom2
```

authorization-attribute idle-cut 120 1024000
authentication portal radius-scheme drcomtest
authorization portal none
accounting portal radius-scheme drcomtest
#