

# 某局点S6520X-54QC-EI radius给portal用户下发授权acl与实际不符以及radius报文携带属性如何区分无线和有线

Radius Portal 刘倩 2024-06-01 发表

## 组网及说明

组网不涉及

## 告警信息

告警信息不涉及

## 问题描述

- 1.终端进行portal认证, 认证通过时候下发授权acl为3200, 后续安全检查通过后再次下发授权acl 3201,但是终端认证通过后获取到的授权acl为3201
- 2.无线和有线终端都在交换机上进行portal认证, 其中无线终端在IMC显示的类型也是有线

## 过程分析

1. debugging看报文交互过程, 看最终服务器下发的授权acl就是3020

\*Feb 21 03:02:00:185 2021 DC-OA-GSW-01&04 RADIUS/7/PACKET:

User-Name="006\007ODVbTUhRyYn6GUwxdgMsKmKHdnk= test02"

Service-Type=Framed-User

State=0x46456e764f513846

Class=0x46456e764f513846

Termination-Action=Default

**Filter:**

Session-Timeout=86400

Acct-Interim-Interval=3600

H3c-Server-String=[]

2.抓包看radius报文发出的授权acl为3020,

```
1 2024-05-20 16:27:50.107432 10.60.254.1 10.60.2.41 RADIUS Access-Request id=69
2 2024-05-20 16:27:50.142380 10.60.2.41 10.60.254.1 RADIUS Access-Accept id=69
3 2024-05-20 16:27:50.161257 10.60.254.1 10.60.2.41 RADIUS Accounting-Request id=69
4 2024-05-20 16:27:50.162241 10.60.2.41 10.60.254.1 RADIUS Accounting-Response id=69
5 2024-05-20 16:28:04.307048 10.60.2.41 10.60.254.1 UDP 40984 → 1812 Len=103
```

Frame 2: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on Ethernet II, Src: Hangzhou, Id: 48:d5 (0c:da:41:1d:48:d5), Dst: 04:a9:59:da:9a:84 (04:a9:59:da:9a:84) Internet Protocol Version 4, Src: 10.60.2.41, Dst: 10.60.254.1 User Datagram Protocol, Src Port: 1812, Dst Port: 41728 RADIUS Protocol Code: Access-Accept (2) Packet identifier: 0x45 (69) Length: 181 Authenticator: e5e8904c2ed3fa429404144bb0fdefd3 [This is a response to a request in frame 1] [Time from request: 0.034948000 seconds] Attribute Value Pairs AVP: t=User-Name(1) l=40 val=006\abwqPQRQFnVvRbhtK1dx2yE6fc= test02 AVP: t=Service-Type(6) l=6 val=Framed(2) AVP: t=State(24) l=10 val=654e434d4654436e AVP: t=Class(25) l=10 val=654e434d4654436e AVP: t=Termination-Action(29) l=6 val=Default(0) AVP: t=Filter-Id(11) l=6 val=3020 AVP: t=Session-Timeout(27) l=6 val=86400 AVP: t=Acct-Interim-Interval(85) l=6 val=3600

计费开始后radius服务器再次发出一个udp报文, 里面携带了授权acl3021, 但是这个报文和前面的radius报文不同, 比较特殊

```
4 2024-05-20 16:27:50.162241 10.60.2.41 10.60.254.1 RADIUS Accounting-Response id=69
5 2024-05-20 16:28:04.307048 10.60.2.41 10.60.254.1 UDP 40984 → 1812 Len=103
```

Frame 5: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on Ethernet II, Src: Hangzhou, Id: 48:d5 (0c:da:41:1d:48:d5), Dst: 04:a9:59:da:9a:84 (04:a9:59:da:9a:84) Internet Protocol Version 4, Src: 10.60.2.41, Dst: 10.60.254.1 User Datagram Protocol, Src Port: 40984, Dst Port: 1812 Data: 140a0067ed83012f994dccc3ff4fada10155bbe332c29303030303030 [Length: 103]

3.最后一个报文是私有报文,目的端口是1812. H3C的IMC RADIUS服务器使用session control报文向设备发送授权信息的动态修改请求以及断开连接请求. 使能RADIUS session control功能后, 设备会打开知名UDP端口1812来监听并接收RADIUS服务器发送的session control报文. 所以需要开启radius session-control enable功能进行修改授权acl.

4.针对无线用户认证通过后在IMC上也显示有线用户. imc根据收到的radius的30号属性中是否携带SSID或者radius的61号属性值为18或19判断是无线的认证. 当前这个测试用户设备发来的认证请求报文中没有30号属性, 61号属性携带的是15, 导致EIA判断为有线场景.

无线的vlan接口下配置portal nas-port-type wireless-other

### 1.1.70 portal nas-port-type

portal nas-port-type命令用来配置接入设备发送的RADIUS请求报文的NAS-Port-Type属性类型

undo portal nas-port-type命令用来恢复缺省情况.

**【命令】**

```
portal nas-port-type { 802.11 | adsl-cap | adsl-dmt | async | cable | ethernet | g.3-fax | hdlc  
| idsl | isdn-async-v110 | isdn-async-v120 | isdn-sync | piafs | sdsl | sync | virtual | wireles  
s-other | x.25 | x.75 | xdsl }  
undo portal nas-port-type
```

**【缺省情况】**

接入设备发送的RADIUS请求报文中的NAS-Port-Type属性类型为Ethernet，属性值为15。

**【视图】**

接口视图

**解决方法**

如上