

知 某局点S5130S-28P-EI 802.1X认证失败的经典案例

802.1X Radius AAA 王燕 2019-09-22 发表

组网及说明

不涉及

问题描述

现有环境中我方H3C交换机S5130S-28P-EI与第三方认证平台进行认证对接，在对接后发现客户端总是认证失败，客户端使用的是该第三方认证平台的客户端。

过程分析

客户端有一瞬间显示认证成功，但是立马就显示为认证失败，进入了guest vlan，guest vlan功能成功。在交换机上显示有上线成功而后认证失败的报文提示，如下：

```
%Jan 25 19:43:27:653 2013 H3C DOT1X/6/DOT1X_LOGIN_SUCC: -IfName=GigabitEthernet1/0/1-MACAddr=4439-c433-b3e8-VLANID=107-Username=20186087; User passed 802.1X authentication and came online.
```

```
%Jan 25 19:43:27:672 2013 H3C DOT1X/6/DOT1X_LOGOFF: -IfName=GigabitEthernet1/0/1-MACAddr=4439-c433-b3e8-VLANID=107-Username=20186087-ErrCode=0; 802.1X user was logged off.
```

交换机开debug，抓取认证时的认证报文，发现在认证过程中有如下一个报文：

```
*Jan 25 20:46:27:507 2013 H3C DOT1X/7/EVENT: PAE is in Authenticated state: UserMAC=4439-c433-b3e8, VLANID=107, Interface=GigabitEthernet1/0/1.
```

```
*Jan 25 20:46:27:507 2013 H3C DOT1X/7/EVENT: Sent authorization request: UserMAC=4439-c433-b3e8, VLANID=107, Interface=GigabitEthernet1/0/1.
```

```
*Jan 25 20:46:27:507 2013 H3C RADIUS/7/EVENT:
```

```
PAM_RADIUS: Processing RADIUS authorization.
```

```
*Jan 25 20:46:27:507 2013 H3C RADIUS/7/ERROR:
```

```
PAM_RADIUS: Authorization scheme is different from authentication scheme.
```

```
*Jan 25 20:46:27:511 2013 H3C DOT1X/7/EVENT: AAA processed authorization request: Result= Failure, UserMAC=4439-c433-b3e8, VLANID=107, Interface=GigabitEthernet1/0/1.
```

```
*Jan 25 20:46:27:512 2013 H3C DOT1X/7/PACKET:
```

```
Transmitted a packet on interface GigabitEthernet1/0/1.
```

报文提示AAA授权失败

后面将domain中的授权和计费这两个参数改为none进行测试，

domain leagsoft

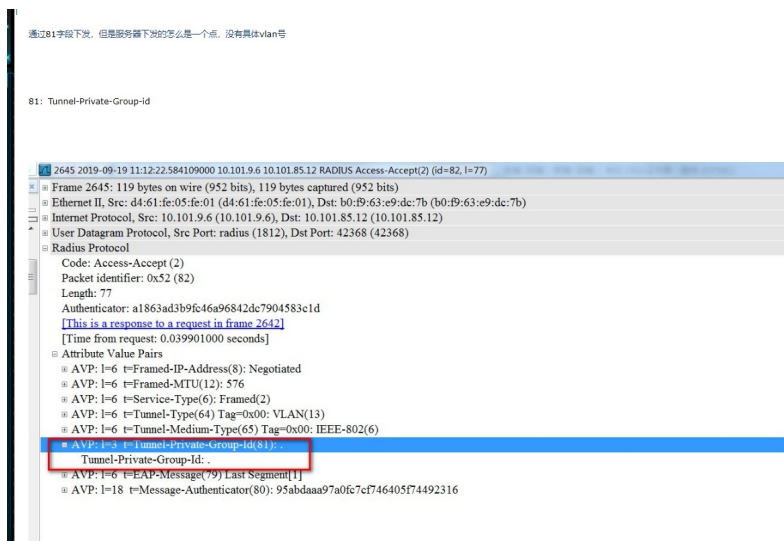
```
authentication lan-access radius-scheme uniaccess
```

```
authorization lan-access none
```

```
accounting lan-access none
```

发现客户端能认证成功，但是所在端口没有获取下发的vlan号，从而进入了vlan 1默认vlan号。

抓包发现，授权下发字段为“ ”：



解决方法

第三方认证平台更改了认证平台后台的字符串格式vlan格式，然后重启了认证模块后，授权vlan号成功下发。

