某局点 S5570S-54S-EI 802.1X认证慢问题

802.1X 苏亚东 2024-04-01 发表

问题描述

客户现场测试拨测1X认证，认证软件和认证系统都是深信服，我司设备做接入认证设备。在终端点击认证上线时，需要点击多次才能认证上线

过程分析

1、 查看交换机上debug，发现存在认证失败的记录，认证失败的原因是radius服务器恢复了03号认证拒绝报文：

*Mar 27 11:42:31:477 2024 BGL-1F-D02-OAES-S5570S-02 RADIUS/7/PACKET:
Message-Authenticator=0x4c7664c7e60e7dbeb3f83a6714b5e252
*Mar 27 11:42:31:477 2024 BGL-1F-D02-OAES-S5570S-02 RADIUS/7/PACKET:
03 fe 00 26 75 4f 12 68 73 29 5f 88 a6 3d 67 0d
02 af 28 be 50 12 4c 76 64 c7 e6 0e 7d be b3 f8
3a 67 14 b5 e2 52
*Mar 27 11:42:31:478 2024 BGL-1F-D02-OAES-S5570S-02 RADIUS/7/EVENT: Sent reply message successfully.
*Mar 27 11:42:31:478 2024 BGL-1F-D02-OAES-S5570S-02 RADIUS/7/EVENT: PAM_RADIUS: Processing RADIUS authentication.
%Mar 27 11:42:31:479 2024 BGL-1F-D02-OAES-S5570S-02 DOT1X/6/DOT1X_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/5-MACAddr=e4a8-dfc8-f998-VLANID=42-Username=wujinlong_daz-ErrCode=8; User failed 802.1X authentication.

(1) Code域

长度为1个字节，用于说明RADIUS报文的类型，如表1-1所示。

表1-1 Code域的主要取值说明

Code	报文类型	报文说明
1	Access-Request认证请求包	方向Client->Server，Client将用户信息传输到Server，请求Server对用户身份进行验证。该报文中必须包含User-Name属性，可选包含NAS-IP-Address、User-Password、NAS-Port等属性
2	Access-Accept认证接受包	方向Server->Client，如果Access-Request报文中的所有Attribute值都可以接受（即认证通过），则传输该类型报文
3	Access-Reject认证拒绝包	方向Server->Client，如果Access-Request报文中存在任何无法被接受的Attribute值（即认证失败），则传输该类型报文
4	Accounting-Request计费请求包	方向Client->Server，Client将用户信息传输到Server，请求Server开始/停止计费。该报文中的Acct-Status-Type属性用于区分计费开始请求和计费结束请求
5	Accounting-Response计费响应包	方向Server->Client，Server通知Client已经收到Accounting-Request报文，并且已经正确记录计费信息

2、同时在PC上抓包确认，发现pc发送eapol-start后，设备并未进行响应:

3、了解到第三方认证软件的认证方式是由认证终端主动发起，查看交换机上配置，并配配置单播触发，而是定时周期发送的组播触发：

#
interface GigabitEthernet1/0/5
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 42 untagged
port hybrid pvid vlan 42
mac-vlan enable
broadcast-suppression 5
multicast-suppression 1
unicast-suppression 1
stp edged-port
mac-address max-mac-count 1
undo mac-address max-mac-count enable-forwarding
dot1x
dot1x mandatory-domain sangfor_ad

```
 dot1x critical vlan 42
 dot1x critical eapol
 undo dot1x unauthenticated-user aging enable
 mac-authentication
 mac-authentication domain sangfor_ad
 mac-authentication parallel-with-dot1x
#
```

4、因此建议现场修改配置，将接口上1x的认证触发方式修改为单播触发后测试正常：

1. 2. 设备端主动触发方式

设备端主动触发方式用于支持不能主动发送EAPOL-Start报文的客户端，例如Windows XP自带的802.1X客户端。设备主动触发认证的方式分为以下两种：

- 组播触发：设备每隔一定时间（缺省为30秒）主动向客户端组播发送Identity类型的EAP-Request帧来触发认证。
- 单播触发：当设备收到源MAC地址未知的报文时，主动向该MAC地址单播发送Identity类型的EAP-Request帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

解决方法

1、接口上1x的认证触发方式修改为单播触发。