# S5120V2-SI与第三方服务器802.1X认证失败

二层链路聚合 lumm 2019-10-22 发表

## 组网及说明

**交换机通过运营商专线连接服务器**

## 问题描述

客户配置802.1x后通过第三方客户端认证失败，另外一台我司交换机S5560及另一台华为交换机同样配置情况下能正常使用。客户的第三方客户端无法进行什么设置，通过debug及客户描述认证用户名是通过识别PC的mac地址生成，在客户端部分只需要输入密码。客户使用第三方客户端pc在接入s5120v2上认证失败。（无法抓包）

## 过程分析

1、在认证失败debug信息中, 是因为找不到服务器无法发出报文才失败的, 但这个是设备给服务器发的第2个报文, 第一次交互是正常收发的,所以这里很奇怪。

*Jan 1 01:21:25:178 2013 h3c_14#_09 RADIUS/7/EVENT:
Processing AAA request data.
*Jan 1 01:21:25:178 2013 h3c_14#_09 RADIUS/7/EVENT:
Got request data successfully, primitive: authentication.
*Jan 1 01:21:25:178 2013 h3c_14#_09 RADIUS/7/EVENT:
Getting RADIUS server info.
*Jan 1 01:21:25:178 2013 h3c_14#_09 RADIUS/7/ERROR:
Failed to get server info.
*Jan 1 01:21:25:178 2013 h3c_14#_09 RADIUS/7/EVENT:
Sent reply message successfully.
*Jan 1 01:21:25:179 2013 h3c_14#_09 RADIUS/7/EVENT:
Processing AAA request data.
*Jan 1 01:21:25:179 2013 h3c_14#_09 RADIUS/7/EVENT:
PAM_RADIUS: Sent authentication request successfully.
*Jan 1 01:21:25:179 2013 h3c_14#_09 DOT1X/7/EVENT: AAA processed authentication request: Result=Processing, UserMAC=0023-9e04-1764, VLANID=123, Interface=GigabitEthernet1/0/1.
*Jan 1 01:21:25:180 2013 h3c_14#_09 RADIUS/7/EVENT:
PAM_RADIUS: Processing RADIUS authentication.
*Jan 1 01:21:25:180 2013 h3c_14#_09 RADIUS/7/EVENT:
PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 3
*Jan 1 01:21:25:180 2013 h3c_14#_09 DOT1X/7/EVENT: Received authentication response with code 8: UserMAC=0023-9e04-1764, VLANID=123, Interface=GigabitEthernet1/0/1.
*Jan 1 01:21:25:181 2013 h3c_14#_09 DOT1X/7/EVENT: BE is in Fail state: UserMAC=0023-9e04-1764, VLANID=123, Interface=GigabitEthernet1/0/1.
*Jan 1 01:21:25:181 2013 h3c_14#_09 DOT1X/7/PACKET:
Transmitted a packet on interface GigabitEthernet1/0/1

2、怀疑是在认证第二阶段服务器不可达导致的（服务器端问题），通过以下操作在实验室复现，打开debug信息，现场反馈的debug信息一致，在进行第二次认证的时候获取服务器失败，导致认证失败。

（1）1x EAP认证方式，并可以radius认证成功。

（2）通过down端口或者down服务器，认证一次将服务器状态置为block。

（3）再打开端口、服务器，再认证一次并收集debug信息观察是否跟现场debug一致

3、以上实验确认服务器block引起的认证失败，但是服务器为什么会block呢，前期已排查链路问题。因此对客户设备进行远程，通过state primary authentication active将服务器状态保证为active后进行认证，依旧认证失败。

[h3c_14#_09]display radius scheme
Total 1 RADIUS schemes
---
RADIUS scheme name: rds
Index: 0
Primary authentication server:
Host name: Not Configured
IP : 10.152.255.47 Port: 1812
VPN : Not configured
State: Active
Test profile: Not configured
Weight: 0
Primary accounting server:

Host name: Not Configured
IP : 10.152.255.47 Port: 1813
VPN : Not configured
State: Active
Weight: 0

4、经过上述修改服务器状态，但是也无法认证成功的现象，认为有以下两种可能：

（1）802.1X在5130通过RADIUS认证，RADIUS报文在发送时会根据MTU（Framed-MTU=1450）做IP分片，如果设备和服务器之间有互备防火墙且防火墙是逐包策略，2个分片报文可能会送到2个不同的防火墙上，防火墙无法收齐重组失败而丢弃报文，设备上会因收不到应答而认证失败。

分析：

*Jan 1 07:17:43:710 2013 h3c_14#_09 RADIUS/7/PACKET:
H3c-Nas-Startup-Timestamp=1356998378
*Jan 1 07:17:43:711 2013 h3c_14#_09 RADIUS/7/EVENT:
Sent request packet successfully.
*Jan 1 07:17:43:712 2013 h3c_14#_09 RADIUS/7/PACKET:
01 fb 05 9f 33 0a 0b 7f fa cd e7 23 8d 26 51 60

debug信息中可以看到失败的radius报文长度为0x59f（1439）加上报文头长度一定大于1450会IP分片。

解决方法：

这种情况可以通过调大MTU处理，interface Vlan-interface123视图下配置mtu，如果mtu无法配置更大，可以通过radius方案下的attribute translate和attribute reject命令减少发送的属性减短报文长度，与S5560能认证的debug对比裁剪报文。

（2）如果仅调大5130的MTU，防止发送时IP分片，仍然失败，曾经遇到过Cisco ISE服务器只能处理1200以下的报文，长度超过这个的RADIUS报文 ISE处理不了，所以还是会认证失败，现场的服务器处理S5560的报文长度1266成功的。

## 解决方法

通过dot1x eap-tls-fragment to-server命令设置分片多次发送，命令是18年7月份支持的，命令不支持，可以通过裁剪属性减短报文长度，参考长度1266裁剪。

*Apr 1 18:19:10:758 2013 sw3 RADIUS/7/EVENT:
Sent request packet successfully.
*Apr 1 18:19:10:761 2013 sw3 RADIUS/7/PACKET:
01 f8 04 f2 e2 e4 85 43 70 d6 ec 7e 71 2a 52 64

配置radius属性禁用规则，减短报文长度

```
radius scheme rds
 primary authentication 10.152.255.47
 primary accounting 10.152.255.47
 key authentication cipher $c$3$pkxbyG1MlmlwiHQsXPbBW0IFxuBCZ8iO1Q==
 key accounting cipher $c$3$3kdoIs2BwYdmlP611Edh6TyUFrcuXncGzQ==
 attribute translate
 attribute reject H3C-NAS-Port-Name access-request
 attribute reject H3c-AVPair access-request
 attribute reject H3c-Ip-Host-Addr access-request
 attribute reject H3c-Nas-Startup-Timestamp access-request
 attribute reject H3c-Product-Id access-request
```

attribute reject (RADIUS scheme view)

**attribute reject**命令用来配置RADIUS属性禁用规则。

**undo attribute reject**命令用来删除RADIUS属性禁用规则。

【命令】

**attribute reject** *attr-name* { { **access-accept** | **access-request** | **accounting** } * | { **received** | **sent** } * }

【使用指导】

当设备发送的RADIUS报文中携带了RADIUS服务器无法识别的属性时，可以定义基于发送方向的属性禁用规则，使得设备发送RADIUS报文时，将该属性从报文中删除。

当RADIUS服务器发送给设备的某些属性是不希望收到的属性时，可以定义基于接收方向的属性禁用规则，使得设备接收RADIUS报文时，不处理报文中的该属性。

当某些类型的属性是设备不希望处理的属性时，可以定义基于类型的属性禁用规则。

只有在RADIUS属性解释功能开启之后，RADIUS属性禁用规则才能生效。

一个属性只能按照一种方式（按报文类型或报文处理方向）进行禁用。

执行**undo attribute reject**命令时，如果不指定属性名称，则表示删除所有RADIUS属性禁用规则。