S5130S-HI系列交换机有线802.1X使用windows自带客户端认证异常经验案例

802.1X 葛松炜 2020-08-30 发表

组网及说明

不涉及

问题描述

现场使用S5130S-HI系列交换机，结合第三方RADIUS服务器，进行终端电脑的有线802.1X认证，电脑直连交换机进行认证，但是发现认证通过后电脑无法正常上网，电脑使用的是windows自带的客户端进行的认证

过程分析

首先我们查看设备侧802.1X相关配置，可以看到现场使用的是EAP中继方式，但是配置上没有什么明显问题，且交换机与RADIUS服务器互ping可以通信。因为现场处于开局状态，只使用一个口进行测试，于是让现场直接收集debugging dot1x all和debugging radius all的信息，查看一下debug信息，观察是否是服务器的问题导致认证失败。

```
#
 dot1x
 dot1x authentication-method eap
#
radius scheme sensetimeradius
 primary authentication 10.151.1.248
 primary accounting 10.151.1.248
 key authentication cipher $c$3$VlUaBXvVhtV5Nna57g9popb7m+8SQ4MhU4Kxp8hnsQ==
 key accounting cipher $c$3$DhTobwxPpFz1WP1ZPkMr5nrNt0XxWRUD64W0P+edAQ==
 user-name-format without-domain
#
domain sensetimeradius
 authentication lan-access radius-scheme sensetimeradius
 authorization lan-access radius-scheme sensetimeradius
 accounting lan-access radius-scheme sensetimeradius
#
interface GigabitEthernet1/0/6
 stp edged-port
 dot1x
 dot1x mandatory-domain sensetimeradius
 dot1x port-method portbased
#
```

查看debug信息，截取其中片段可以发现，交换机有发送EAP报文，并且有收到终端的响应：

```
*Aug 19 16:58:09:617 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF DOT1X/7/EVENT: Sending EAP packet: Identifier=2, type=1.
*Aug 19 16:58:09:618 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF DOT1X/7/PACKET:
Transmitted a packet on interface GigabitEthernet1/0/6.
Destination Mac Address=c8f7-503f-f1be
Source Mac Address=743a-208a-f02f
VLAN ID=1
Mac Frame Type=888e
Protocol Version ID=1
Packet Type=0
Packet Length=5.
-----Packet Body-----
Code=1
Identifier=2
Length=5.
*Aug 19 16:58:17:134 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF DOT1X/7/PACKET:
Received a packet on interface GigabitEthernet1/0/6.
Destination Mac Address=0180-c200-0003
Source Mac Address=c8f7-503f-f1be
Mac Frame Type=888e
Protocol Version ID=1
Packet Type=0
```

Packet Length=15.
-----Packet Body-----
Code=2
Identifier=2
Length=15.

查看RADIUS交互，发现交换机是有将认证请求报文成功发送至RADIUS服务器的：
*Aug 19 16:58:17:173 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/PACKET:
User-Name="zhangyibin"
NAS-Identifier="ASCNHZTR-AS-S5130S-29FA-02-IRF"
EAP-Message=0x0202000f017a68616e67796962696e
Message-Authenticator=0x00000000000000000000000000000000
Framed-MTU=1450
Framed-Protocol=PPP
Called-Station-
NAS-Port-Type=Ethernet
H3c-Ip-Host-Addr="0.0.0.0 c8:f7:50:3f:f1:be"
Calling-Station-
H3C-NAS-Port-Name="GigabitEthernet1/0/6"
NAS-Port=16801793
NAS-Port-
H3c-AVPair="nas:ifindex=6"
Acct-Session-
Service-Type=Framed-User
NAS-IP-Address=10.156.1.5
H3c-Product-
H3c-Nas-Startup-Timestamp=1597820936
*Aug 19 16:58:17:175 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF DOT1X/7/EVENT: **AAA processed authentication request: Result=Processing, UserMAC=c8f7-503f-f1be, VLANID=1, Interface=GigabitEthernet1/0/6**.
*Aug 19 16:58:17:175 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: **Sent request packet successfully**.

后续设备有成功接收到RADIUS服务器的回应报文：
*Aug 19 16:58:17:177 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Sent request packet and create request context successfully.
*Aug 19 16:58:17:177 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Added request context to global table successfully.
*Aug 19 16:58:17:177 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Processing AAA request data.
*Aug 19 16:58:17:211 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Reply Socket Fd recieved EPOLLIN event.
*Aug 19 16:58:17:212 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: **Received reply packet succuessfully**.
*Aug 19 16:58:17:212 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Found request context, dstIP: 10.151.1.248, dstPort: 1812, VPN instance: --(public), socketFd: 77, pktID: 127.
*Aug 19 16:58:17:212 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: The reply packet is valid.
*Aug 19 16:58:17:213 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Decoded reply packet successfully.
至此，发现debug信息中没有明显的报错信息，结合现场反馈的是认证显示的是通过，但是很快电脑就显示“身份验证失败”无法上网，怀疑跟认证客户端有关，于是让现场使用inode客户端进行802.1X认证来测试。现场测试后反馈，使用inode客户端可以正常进行认证，且终端能一直保持正常上网，因此可以断定非设备配置问题，而是windows自带客户端导致。

解决方法

设备在配置802.1X认证时，会缺省开启在线用户握手功能， 开启设备的在线用户握手功能后，设备会定期（时间间隔通过命令dot1x timer handshake-period设置）向通过802.1X认证的在线用户发送握手请求报文（EAP-Request/Identity），以定期检测用户的在线情况。如果设备连续多次（通过命令dot1x retry设置）没有收到客户端的应答报文（EAP-Response/Identity），则会将用户置为下线状态。
让现场undo dot1x handshake后，现场反馈使用windows客户端可以正常通过认证且用户不会很快出现下线情况。这是因为部分802.1X客户端不支持与设备进行握手报文的交互，因此建议在这种情况下，关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线