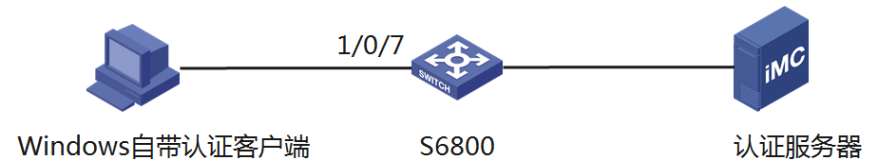
802.1x认证结合win客户端认证成功后周期性出现“正在尝试身份验证”的经典案例

802.1X　zhiliao_JTvNH　2018-09-05 发表

组网及说明



某局点有一台S6800做802.1x认证，客户端使用windows自带的客户端，设备mac与pc相连的接口的mac地址为9428-2e56-0644，pc的mac地址为3C-97-0E-03-44-7D

问题描述

在认证通过后，发现在PC网卡处大概十秒左右，会周期性的显示“正在尝试身份验证”，但是此提示不影响用户上网，也不会弹出认证界面。

检查交换机配置没有发现什么问题

```
# interface Ten-GigabitEthernet3/0/2
port link-mode bridge
stp edged-port
dot1x
undo dot1x handshake
```

在pc上，出现“正在尝试身份验证”时进行抓包发现，认证成功后，又继续开始了新一轮的认证过程

29	7.902054	94:28:2e:56:06:44	WistronI_03:44:7d	EAP	60 Success
87	19.819537	94:28:2e:56:06:44	Nearest	EAP	60 Request, Identity
88	19.829873	WistronI_03:44:7d	Nearest	EAP	26 Response, Identity
130	37.826933	WistronI_03:44:7d	Nearest	EAPOL	19 Start
131	37.828714	94:28:2e:56:06:44	WistronI_03:44:7d	EAP	60 Request, Identity
132	37.839730	WistronI_03:44:7d	Nearest	EAP	26 Response, Identity
133	37.855541	94:28:2e:56:06:44	WistronI_03:44:7d	EAP	60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
134	37.856043	WistronI_03:44:7d	Nearest	EAP	24 Response, Legacy Nak (Response Only)
135	37.861144	94:28:2e:56:06:44	WistronI_03:44:7d	EAP	60 Request, Protected EAP (EAP-PEAP)
136	37.862590	WistronI_03:44:7d	Nearest	TLSv1.2	360 Client Hello

过程分析

开始看到抓包时认为可能是win客户端有某种机制，会定时向交换机发送request报文，因为设备上的802.1x握手机制已经关闭了，但是仔细查看抓包信息后发现，request报文是由设备端发起的（source为9428-2e56-0644），而报文接收地址为0180-c200-0003的组播地址。

```
▷ Frame 87: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
◢ Ethernet II, Src: 94:28:2e:56:06:44 (94:28:2e:56:06:44), Dst: Nearest (01:80:c2:00:00:03)
   ▷ Destination: Nearest (01:80:c2:00:00:03)
   ▷ Source: 94:28:2e:56:06:44 (94:28:2e:56:06:44)
     Type: 802.1X Authentication (0x888e)
     Padding: 0000000000000000000000000000000000000000000000000000...
▷ 802.1X Authentication
```

由于win客户端属于不能主动触发认证的客户端类型，需要设备主动发起认证，而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。

缺省为组播触发方式。

但是查阅官网后发现组播触发方式有如下限制：若端口连接的802.1X客户端不能主动发起认证，且仅部分802.1X客户端需要进行认证，为避免不希望认证或已认证的802.1X客户端收到多余的认证触发报文，则需要开启单播触发功能。

在此案例中，由于开启了组播触发方式，已认证通过的win客户端认证成功后还会收到认证触发报文，因此pc网卡处会看到一直有“正在尝试身份验证”字样出现。

解决方法

将802.1x的触发方式由默认的组播方式改为单播方式后问题解决

接口视图下：

undo dot1x multicast-trigger
dot1x unicast-trigger