

知 S5130S-52P-EI-做认证服务器周期性收到异常认证报文

802.1X MAC地址认证 李敏 2022-09-05 发表

组网及说明

客户端-接入交换机-**认证交换机**-其他交换机-**核心交换机**-radius服务器

问题描述

客户那边在认证交换机上配置1x认证结合mac认证，目前认证情况都是正常的，但是客户的radius服务器每隔两分钟会收一个未知mac (000f-e207-f2e0) 的认证请求，查询mac是我们华三设备的mac

过程分析

1、抓包查看也能看到认证交换机携带此mac的报文来认证000f-e207-f2e0

cid:image007.jpg@01D88594.50E30960

```
01:44.015282 10.120.48.26 10.120.49.43 RADIUS 360 Access-Request id=6
01:44.015282 10.120.48.26 10.120.49.43 RADIUS 360 Access-Request id=6, Duplicate Request
01:44.016679 10.120.49.101 10.120.49.43 TCP 66 49675 -> 51663 [SYN, ACK, ECN] Seq=0 Ack
01:44.016679 10.120.49.101 10.120.49.43 TCP 66 [TCP Out-Of-Order] 49675 -> 51663 [SYN,
01:44.016752 10.120.49.43 10.120.49.101 TCP 66 51663 -> 49675 [SYN, ECN, CWR] Seq=0 Win
01:44.016752 10.120.49.43 10.120.49.101 TCP 66 [TCP Out-Of-Order] 51663 -> 49675 [SYN,
01:44.016752 10.120.49.43 10.120.49.101 TCP 60 51663 -> 49675 [ACK] Seq=1 Ack=1 Win=105
01:44.016752 10.120.49.43 10.120.49.101 TCP 60 [TCP Dup ACK 360#1] 51663 -> 49675 [ACK]
01:44.016752 10.120.49.43 10.120.49.101 DCERPC 270 Bind: call_id: 218, Fragment: Single, 3
01:44.016752 10.120.49.43 10.120.49.101 TCP 270 [TCP Retransmission] 51663 -> 49675 [PSH
01:44.017201 10.120.49.101 10.120.49.43 DCERPC 182 Bind_ack: call_id: 218, Fragment: Singl
01:44.017201 10.120.49.101 10.120.49.43 TCP 182 [TCP Retransmission] 49675 -> 51663 [PSH
01:44.017649 10.120.49.43 10.120.49.101 RPC_NETLOG... 654 NetrLogonSamLogonEx request
01:44.017649 10.120.49.43 10.120.49.101 TCP 654 [TCP Retransmission] 51663 -> 49675 [PSH
01:44.018290 10.120.49.101 10.120.49.43 RPC_NETLOG... 174 NetrLogonSamLogonEx response

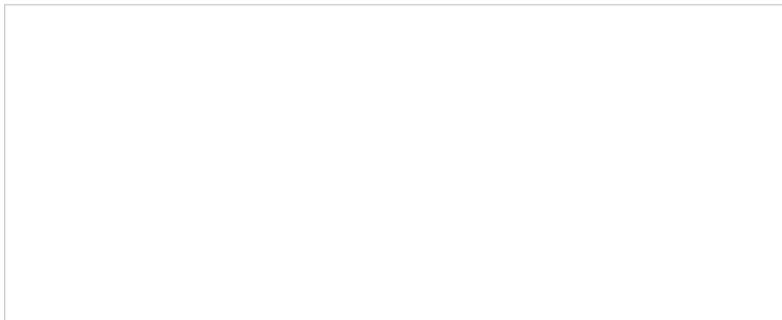
es on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{106BC84B-EF16-4F11-B97E-2A0874A854E9}, id 0
NewH3CTe_79:88:97 (10:19:65:79:88:97), Dst: NewH3CTe_86:7e:01 (34:6b:5b:86:7e:01)
Version 4, Src: 10.120.48.26, Dst: 10.120.49.43
ocol, Src Port: 12352, Dst Port: 1812

quest (1)
er: 0x6 (6)

2661509b0df2ac6d2d13843e9568e815
o this request is in frame 370]
Pairs
ame(1) 1=14 val=000fe207f2e0
entifier(32) 1=5 val=H3C
l-Protocol(7) 1=6 val=PPP(1)
l-Station-Id(30) 1=19 val=10-19-65-79-88-9A
-Specific(26) 1=33 vnd=H3C(25506)
ig-Station-Id(31) 1=19 val=00-0F-E2-07-F2-E0
rt-Type(61) 1=6 val=Ethernet(15)
-Specific(26) 1=28 vnd=H3C(25506)
```

2、debug看，000f-e207-f2e0这个mac就是从1/0/1口上来的，对认证来说不是问题，正常处理流程正常来讲协议报文应该不能触发认证，但是协议报文不触发认证是依靠我们在rxtx对一些典型协议进行判断的。88A7是HGMP报文的协议类型，比较冷门，如果没有下协议acl那就是当做普通数据报文处理了，当前版本HGMP协议报文是没有下发acl规则的。综上，当前的行为对我们来说是正常的。

3、1/0/1口下联的是华三的交换机s3600-52P-Ei，3600这款设备支持HGMP



AaBbCcC AaBbCcC 图1 AaB AaBcCcDd 步骤1 A AaBbCcC AaBbCcC • AaBbC • AaBbCc (1) AaB

1、建议现场从组网和配置上考虑下，3600E这个设备上使能HGMP是否有必要，能否去掉

	设备进行堆叠时，如果各台设备的软件版本和主设备不同，主设备的软件会被传送到其他设备，然后这台设备使用主设备的软件重新启动。
HGMP	集群管理协议可以简化网络管理，同时实现了集群拓扑的管理和trace MAC功能。 开启集群管理功能的情况下，不但可以减少重复配置交换机的工作，还可以实现对分散的交换机进行远程管理，大大减少了组网配置的工作量。 集群拓扑管理能够以图形化方式显示集群所属网络的拓扑结构，并提供黑名单功能。 Trace MAC就是在集群管理的网络中通过MAC或IP地址，跟踪相应设备所处的位置。

