S7506E-X设备上的网关IP地址迁移到上联的核心S10506X后，偶发无法ping通S10506X上的网关地址

ARP 转发不通 **姚智祥** 2021-12-22 发表

组网及说明

整个网络分为园区网络（办公网）和数据中心网络，一对105X作为数据中心核心与网关，数据中心全网是VLAN 2，数据中心下面都是二层网络，两对S7506E作为下面的两台汇聚交换机。园区网络是一套ADCampus单leaf架构，园区网络和数据中心网络之间是一对三层防火墙连接的。

问题描述

将行政楼S7506E-X设备上的网关IP地址迁移到上联的核心S10506X后，偶发Campus园区终端无法访问行政楼服务器，行政楼服务器经过行政楼S7506E-X无法ping通S10506X上的网关地址。

过程分析

1. 通过故障时间收集的设备信息和诊断日志分析，故障时行政楼S7506E-X设备上将核心S10506X的网关Mac（58:c7:ac:e8:22:01）置为黑洞Mac。

#正常情况下
<FuWuQi_S7506EX>dis clock
12:17:45.573 UTC Fri 12/10/2021
mac=58:c7:ac:e8:22:01 vlan=2 GPORT=0x0 Trunk=14 SDHit Group=Learnt

#故障时候
<FuWuQi_S7506EX>dis clock
16:14:58.981 UTC Fri 12/10/2021
mac=58:c7:ac:e8:22:01 vlan=2 GPORT=0x0 modid=0 port=0 Static SDHit DiscardSrc DiscardDest Group=StaSrcDstDis

[FuWuQi_S7506EX-probe]dis clock
16:18:19.798 UTC Fri 12/10/2021
mac=58:c7:ac:e8:22:01 vlan=2 GPORT=0x0 modid=0 port=0 Static SDHit DiscardSrc DiscardDest Group=StaSrcDstDis

查看底层黑洞mac添加记录，发现是arp模块下发的
[FuWuQi_S7506EX-probe]debug l2 c 1 sl 0 chip 0 mac/add/show
4864. 2021/12/10 16:14 30.552891: [karp/1]DRV_MAC_AddAddr: ifIndex=0x0, usVlanID=2, uiStatus=0x00000040, uiCtlFlag=0, aucMacAddress=58c7-ace8-2201.
4865. 2021/12/10 16:14 30.552974: [karp/1]Begin, params: Modid=0, Port=0, Tgid=-1, Vid=2, VsiId=4294967295, Gport=0Mac=58c7-ace8-2201, Type=0x00000040.

2. 查看行政楼S7506E-X设备上的配置，发现设备上开启了源MAC地址固定的ARP攻击检测，即arp source-mac filter功能。

本特性根据ARP报文的源MAC地址对上送CPU的ARP报文进行统计，在5秒内，如果收到同一源MAC地址（源MAC地址固定）的ARP报文超过一定的阈值，则认为存在攻击，系统会将此MAC地址添加到攻击检测表项中。对于已添加到源MAC地址固定的ARP攻击检测表项中的MAC地址，在等待设置的老化时间后，会重新恢复成普通MAC地址。

结合以上信息，可以判断故障原因为行政楼S7506E-X设备开启了“源MAC地址固定的ARP攻击检测功”，当核心S10506X往行政楼S75EX发送的arp报文达到攻击阈值，触发被下发黑洞mac。导致源mac为105x核心mac的流量被丢弃。

解决方法

1、建议删除“arp source-mac filter”命令，或修改为“arp source-mac monitor”。