某据点插拔一根网线导致其他流量中断一分钟问题

STP ARP攻击防御 **付尧** 2021-03-11 发表

组网及说明

交换机a（网关）分别连接接入交换机b，c，d

问题描述

插拔a连接b网线，重新插上时，c ping d下连终端，或者ping网关有一分钟丢包。

过程分析

a为根桥，设备stp快速收敛，不通时各设备表项没有异常，流统发现流量丢在了汇聚设备上，抓包查看封装报文也没有问题
进一步检查汇聚设备配置，发现如下配置：
arp ip-conflict log prompt
arp user-ip-conflict record enable
arp source-mac filter
arp source-mac aging-time 64
arp source-mac threshold 15
arp active-ack enable
arp source-suppression enable
arp source-suppression limit 32
现场配置了源MAC地址固定的ARP攻击检测功能，配置了filter模式。 而且门限配置成了15，即设备在5秒内收到同一个源mac发送的arp广播请求报文个数超过15个，就会认为是攻击，将这个mac下黑洞处理。
下黑洞后，根据配置的aging-time 64，黑洞表项64S后老化

拔出汇聚交换机下连一根光钎，网络无影响，插上后，会产生TC，并在整个二层网内透传TC报文。
下行接入设备收到TC后，会发起针对已经学习到的arp的广播探测报文（arp广播请求报文）
只要发起的arp广播请求报文超过15个，设备就会认为是arp攻击，针对接入设备的源mac下发黑洞，导致流量异常。

解决方法

现场去掉arp source-mac filter配置后，测试流量正常

建议：

1） 源MAC地址固定的ARP攻击检测功能，阈值建议按照默认配置来，或者往大了调，15个实在太小了。另外不建议配置成filter模式，建议配置成arp source-mac monitor模式

2） arp source-suppression，limit也配置的有点小了，建议安装默认配置来，或者往大了调

另外，现场没有arp攻击的情况存在，可建议不开启arp防攻击功能。