S5800交换机频繁出现CPU利用率高问题案例分析

CPU 翁青山 2017-06-22 发表

某局点反馈，S5800设备使用过程中，CPU利用率突然上升到100%，之后客户业务马上受到影响，登录设备查看进程发现arp占79%，但过了几分钟后CPU又回到原来水平了。该故障情况不定时出现，每次出现持续一段时间。

1、根据诊断信息，可以确定占用CPU最多的进程是ARP任务。现场通过抓包确认，CPU高时，设备收到较多ARP报文。
2、查看设备配置，发现配置了arp detection功能。在配置了ARP Detection功能后，设备会将收到的ARP报文重定向到CPU进行检查，这样可能会导致当网络中存在攻击者恶意构造大量ARP报文发往设备，会导致设备的CPU负担过重，从而造成其他功能无法正常运行甚至设备瘫痪。这种情况下，可以启用ARP报文限速功能来控制上送CPU的ARP报文的速率。但现场配置arp报文限速功能后，cpu依然很高，后来关闭了arp detection功能后，故障仍然存在。
3、继续排查，通过现场在CPU高时打印上送cpu的报文，以及收集如下信息查看arp进程的具体调用栈情况。
[S5800]_h
[S5800-hidecmd]dis task 110 slot 1 cpu 0
[S5800-hidecmd]dis task 110 slot 2 cpu 0
通过查看任务调用信息，发现下面的配置导致ARP进程偏高：
arp anti-attack source-mac filter
arp广播报文默认上cpu处理，而arp 单播回应报文只有目的mac是设备本身才会上送cpu，默认情况下目的mac不是自己的不上，配置该命令后，导致过路的arp也会上送cpu。
该命令的作用是：使能源MAC地址固定的ARP攻击检测之后，该特性会对上送CPU的ARP报文按照源MAC地址和VLAN进行统计。当在一定时间（5秒）内收到某固定源MAC地址的ARP报文超过设定的阈值，不同模式的处理方式存在差异：在filter模式下会打印Log信息并对该源MAC地址对应的ARP报文进行过滤；在monitor模式下只打印Log信息，不过滤ARP报文。
如果超过阈值，因为模式为filter，因此会下发ACL规则到硬件，丢弃ARP的攻击报文。另外，丢弃一段时间后，软件还会删除之前下发的ACL，并重新检测。由于ACL的添加、删除涉及到操作硬件寄存器，而且因为ACL条目优先级排序，添、删ACL会引起块搬移（比如插入或移除整个ACL表中间的某一条，那么其后面的所有条目都要进行搬移），如果频繁添、删ACL，而且设备中已经存在较多ACL条目的时候，就会导致CPU占用率偏高。

现场通过取消arp anti-attack source-mac filter命令（或把filter改成monitor），设备的CPU已恢复正常。

1、该问题的本质是现网环境中存在arp攻击，现场应该及时排查arp攻击源，否则大量的arp报文上送到网关，到时候可能也承受不住；
2、若环境中可能存在arp攻击时，可以配置arp anti-attack source-mac monitor来监测arp攻击情况，当发生arp攻击时，设备会产生arp攻击LOG告警信息，并且不会影响到设备CPU利用率；