无线高级优化特性之——上行arp抑制

VLAN 朱恺 2022-11-24 发表

问题描述

对于一些大型网络，树形的网络结构，往往核心网关都是集中在某几台交换机路由器设备上。
伴随终端可能是海量的无线终端，手机APP也有可能存在遍历arp的扫描行为（例如XX视频app），一打开应用在后台就开始arp扫描网络中的设备。
会遇到一些场景下，交换机arp的pps并发性能受限，没办法全部处理，造成偶发的卡顿，终端网络不通等故障。这些场景往往都是饭点，或者学校上下课，大量终端密集漫游的时候。
现在还有很多终端每次无线漫游就会请求一下网关arp，当核心交换机出现arp并发pps丢包时就会导致漫游查询arp失败，漫游后网络不通，终端就表现出反复的wifi离开。

这些问题的背后往往就是一个原因：arp并发太多，导致网络设备处理不了。

解决方法

那么如何优化这个问题呢。能否做到针对性的拦截。
除了常规的二层隔离、端口隔离的命令之外，还可以考虑下无线的一个高级优化特性：RROP 上行arp抑制。
具体命令：
rrop ul-arp attack-suppression enable [threshold threshold-value] [block-time time]
开启AP上行ARP攻击抑制功能。 缺省情况下，AP上行ARP攻击抑制功能处于关闭状态。
开启本功能后，在1秒内，当AP收到某一无线客户端的ARP请求/应答报文个数超过门限值时，则认为受到了该无线客户端的ARP报文攻击，AP会在配置的阻断时间间隔内丢弃该无线客户端的所有ARP请求/应答报文。当环境中无线客户端发送的ARP报文过多时，建议开启本功能。

这在对终端数量多，网关核心设备性能有线的场景下非常有用。建议各位工程师参考配置一下，百益无一害。