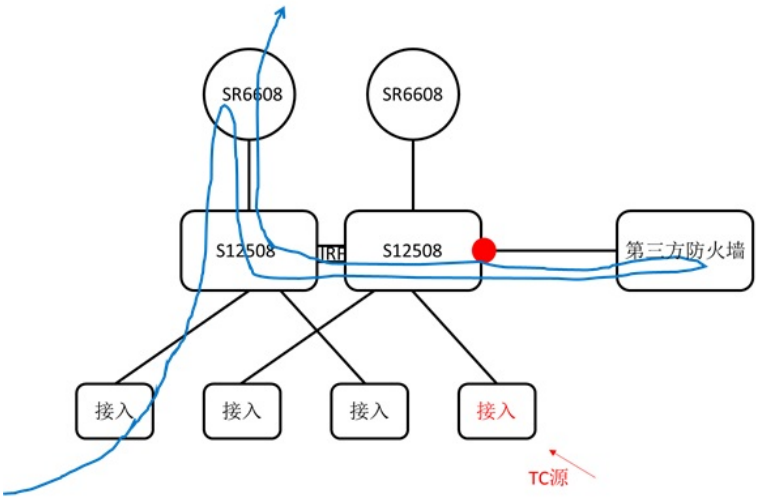
某局点S12500 收到TC概率出现业务中断问题

STP 张文宁 2020-02-28 发表

组网及说明

拓扑：如下图所示，两台SR66起了vrrp主备作为全网终端的网关，两台S12508堆叠作为核心汇聚，S12508旁挂了第三方的防火墙，所有跨网段流量转发均需要经过防火墙防护。



问题描述

问题：2020-2-10 11:00左右业务报障，部分终端业务访问缓慢 （此前还有故障时间点2-16的20:00、1-21的11:54、等7次），看到故障时间点设备有TC报文、防火墙新建会话和并发数量非常大。

观察到的异常点：

1. 故障时思科接入收到6个TC报文，整网泛红。
2. 故障时接入交换机有接近千级的mac漂移。
3. 故障时候迪普防火墙会话和并发非常大。

恢复过程：进行防火墙的主备倒换后业务恢复正常。

过程分析

1、现场二层网络域大，交换机收到TC报文后会刷新mac表，此过程中会存在短暂的未知单播泛洪流量。是否这些流量会泛洪到了迪普防火墙导致会话数突增，迪普防火墙挂死?

///经排查组网，确实会泛洪到迪普交换机，但是迪普侧确认收到目的mac非自己的报文会直接丢弃，这些泛洪流量理论上并不会导致迪普防火墙的异常。

2、H3C交换机记录到思科交换机6509下的vrrp mac有漂移，其中最新一次是2-10日，思科下接的是IPS设备。是否可能很多流量是经过ips的，在2-10 11时左右此处故障导致终端大量原有会话超时，因此发起了大量的新连接导致迪普防火墙异常?

///经梳理组网流量模型，出现故障的业务不经过下接的IPS设备，因此故障与此处mac漂移无关。另外此处mac漂移经核实是由于SR6604接入的专线不稳定联动的VRRP切换导致的VRRP虚mac漂移，属于正常现象。

3、是否交换机软硬件在故障时间点有异常未能正常转发流量导致终端大量会话超时，大量重连导致迪普防火墙异常?

///经排查确认，组网中S12508，S7600等并未发现相关软硬件故障。同时排查组网发现组网不合理，备框所有流量都是跨irf链路转发的，但根据峰值流量和时间点记录，故障时候并未见拥塞等情况，因此可以排除。

4、迪普防火墙会话突增，并发突增，迪普是否有相关异常日志记录？是否有异常报文的特征？是否可能是迪普应用层面应用本身发生异常导致异常?

///经和现场工程师确认，迪普侧没有会话异常时的特征记录，应用层是否发生异常在排查确认中。

综上，设备侧未见明显相关异常，建议客户主要排查第三方防火墙设备异常原因，排除TC源，优化组网。

2月20日，问题再次复现，防火墙会话再次被打爆，第三方防火墙确认之前确认机制有误，收到目的mac非自己的也会上送cpu处理。

定位结论：

第三方设备链路模块等问题产生大量TC报文，流量模型配置导致大量单播报文泛洪给防火墙，防火墙被打爆引起业务异常。

解决方法

解决方法：

1、第三方处理解决tc和防火墙实现机制，同时优化组网。