

为什么通过抓包发现从S6500交换机上发出大量连续的ARP请求报文

一、问题描述:

某客户反映通过抓包软件在我们65上抓包，结果显示从65上发出了大量的ARP请求报文且报文十分规律，如果交换机上有三个直连的网段：192.168.1.0/24，192.168.2.0/24和192.168.3.0/24位，那么ARP请求报文从192.168.1.1开始一直发送到192.168.1.255，中间存在少量的间断；然后在192.168.2.0和192.168.3.0网段中按照上述规律发送ARP请求报文，如此反复下去并导致CPU利用率比较高。用户怀疑我们的65是否存在故障。

二、分析和结论:

其实65只有在通过ARP表项查找某主机的IP地址和MAC地址的对应关系没有找到的时候，才会发送ARP请求报文。仔细分析不难发现，如果有一台主机，不停的去轮询Ping某个网段的所有主机，而当该网段的一些IP地址并没有被使用时，65上就肯定不会存在这些IP地址的ARP表项，那么我们的65会向这些并不存在的主机IP发送ARP请求报文，也就造成客户认为我们的65出现了故障。其实我们的65只是按照报文转发的流程进行处理，并没有任何问题。

真正的问题来自于扫描源。一旦发现此类情况，就需要通过各种手段来排查扫描源。