

知 某局点跨越公网集中转发无线终端严重丢包问题处理经验案例

王媛媛 2017-12-24 发表

某局点反馈该局点有400多个分支机构，其中有三个分支机构报无线终端上网卡顿。AC型号EWPX2W CMD0，版本是V5的R2308P28，AP型号WA2620I-ACN。该局点是典型的总部分支组网，AC、内网服务器部署在总部，AP部署在分支机构。无线终端都是某款型号的平板。无线终端的流量通过专线，跨越公网，到AC上进行集中转发。每个分支局点连接的平板使用内部开发的软件访问内网服务器的网页时，出现打开慢，卡顿或者直接打不开的现象。

无

首先需要明确问题现象。对于无线终端使用者来说无线使用卡顿，打开网页慢只是表象。无线上网卡顿问题，大多是延迟大或者丢包产生，所以需要进一步明确问题原因。针对于无线上网卡顿现象可以进行简单地终端Ping包测试来明确问题。

从AC侧Ping终端测试发现丢包率在50%左右。所以可以确定造成终端使用卡顿的原因是因为无线终端丢包严重。

客户反馈最近升级过内部使用的上网软件，极少数的分支局点出现上网卡顿的问题，终端型号只有某一款平板。丢包点可能在AC、有线链路、AP或者终端任意一点上，还需要做逐步的排查。

1. 排除终端的问题。现场协调了笔记本电脑来测试发现笔记本电脑也存在严重的丢包，所以基本可以排除终端的问题。
2. 寻找丢包规律。AC Ping终端1500字节的大包发现丢包率在60%左右。AC Ping终端300字节的小包时没有丢包，可以初步确定终端存在Ping大包丢小包不丢的情况。AC Ping终端1472字节的大包时丢包率为30%多。多次Ping大包测试发现大包字节越大，丢包率越高。遂进行反复测试寻找到丢包和不丢包的报文大小的临界值。最终测试发现AC Ping终端1404字节的报文不丢，但是Ping1405字节的报文丢包率20%多。而AC Ping AP即使是2000字节的大包丢包率也为0%。而1405字节恰好是LWAPP隧道报文开始分片的门限值，所以可以确定的是LWAPP隧道报文转发上有问题。可能是有线链路对隧道报文转发上有问题，也可能是AC或者AP处理隧道分片报文有问题。
3. 建议客户选取问题分支的AP修改为本地转发测试，使其终端流量不经过AC，也不经过隧道转发，这样可以排除AC的嫌疑。但是由于现场的一些客观原因无法实施。
4. 建议客户在AP上联交换机的接口进行镜像抓包确定丢包点，但由于现场不具备在AP上联口抓包的条件，暂时无法确定报文是丢在了AC和AP之间的有线侧还是丢在了AP和终端之间的无线侧。
5. 理论分析：通过以上的Ping包测试结合LWAPP集中转发的机制，初步怀疑还是专线链路上的网络设备对LWAPP隧道分片报文转发出现了问题导致丢包。虽然AP是通过LWAPP隧道注册到了AC上，但是AC Ping AP属于一个简单的ICMP报文，走的是最普通的路由转发。但是AC Ping终端时，由于无线终端的流量是集中转发，在AC和AP之间的有线报文其实走的是LWAPP隧道。LWAPP隧道报文是UDP报文。所以最大的可能性还是专线链路上中间网络设备对UDP的分片报文转发出现了问题，导致丢包。

协调客户进行更换专线出口测试。更换专线出口后，终端Ping大包不再丢包，无线上网使用正常。

1. 对于客户反馈的使用无线上网卡顿，慢等问题需要最终量化到延迟大小和丢包率多少上，同时还必须进行Ping大包小包测试。
2. 对于集中转发的组网，无线终端丢包需要在有线侧和无线侧分别进行Ping包测试。如果有条件可以选择一个AP改本地转发，AP上配置一个和终端同网段的三层接口地址Ping终端测试，明确报文是丢在了AC到AP的有线链路上还是AP到终端的无线链路上。
3. 也可以选择AP的上连的交换机接口进行镜像抓包，抓包时AC Ping终端测试，也可以明确丢包点。
4. 对于有专线链路的局点，如果以上测试由于客户局点的一些客观因素无法实施，还可以进行更换专线出口测试。由于更换了专线出口，中间经过的网络设备不一样。如果是中间设备对UDP分片报文转发出现了问题，通过更换专线出口基本也可以解决问题。
5. 对于总部分支机构，有专线组网的局点，专线链路对隧道分片报文的转发的影响不仅限于无线终端丢包，还常见于AP无法正常注册上线等情况。Debug AP的注册流程会发现AP注册流程都是终止在配置下发阶段，因为配置下发的响应报文也是一个需要分片的大包报文。如果遇到这种情况，也可以参考分析有线侧链路对UDP隧道分片报文转发影响可能性。