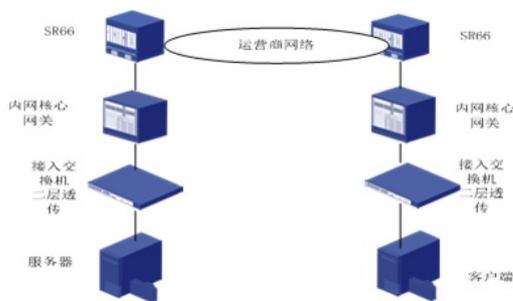


某运营商客户SR6608路由器DVPN网络TFTP下载失败的问题

ADVPN FTP/TFTP 傅昆 2014-07-25 发表

一 组网:

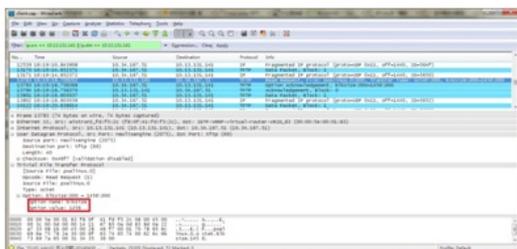


二 问题描述:

某运营商在国内五个分支节点部署了DVPN网络, 近期项目实施完成, 割接业务上线。在上线过程中发现, 分支节点内网客户端通过DVPN网络到另一个分支节点的内网TFTP服务器进行下载时, 无法下载成功, 且提示“time-out”的错误信息

三 过程分析:

RFC1350规定: TFTP协议传输文件的报文大小为固定512字节。通过现场抓包发现, 客户将这个值改成了协商方式获取且协商大小为1456字节, 见下图的“tftp-blocksize”字段数值:



客户使用的DVPN网络, 加上IP头开销, 导致Tunnel上实际能传输的报文小于MTU值, 造成在传输1456字节大小的TFTP报文时, 会产生分片。而客户的TFTP客户端又没有报文的重组能力, 造成Server端一直在重传第一个TFTP数据报文。

对于TFTP报文来说, TFTP头部4字节+UDP头部8字节+IP头部20字节=32, 也就是说TFTP在IP链路开销为32字节。由于协商出tftp-blocksize大小之后, 数据报文总长度为: $1456+32=1488$ 字节 > 1460字节 (Tunnel上实际生效的MTU), 所以客户业务报文才会被分片。

从这要的推导似乎只要配置Tunnel的MTU为1488字节就可以了。其实并不是这样的, 因为再加上DVPN的开销 $1488+36=1524 > 1500$ (网络上大部分设备接口默认MTU), 这样必然会在物理出接口上进行分片, DVPN的对端设备就会存在重组的压力。

所以需要将物理接口的MTU, 也做相应的配置(至少可以保证本设备不产生分片)。再考虑网络上还可能有其他设备的接口MTU值为1500字节, 那一旦有这种设备, 必然产生分片, 这种情况下为了避免分片过多, Tunnel口还是配置本接口能力最大值为好, 咱们Tunnel接口的 MTU能力最大值就是2000字节。

四 解决方法:

从上面的分析得出以下两种解决方案:

1. 建议客户按照TFTP RFC 1305规定: 修改tftp-blocksize 为固定大小512字节;
2. 调整设备侧的MTU, MTU的调整值: Tunnel = 2000字节; 物理接口 ≥ 2040 字节

(考虑到分片处理效率, IP分片有个“报文大小需要能够被8整除”的原则。

上面两种方法应该都可以解决问题, 建议使用第一种。

