处理数据包发现多余两个字节

时间：2015/12/9

背景：

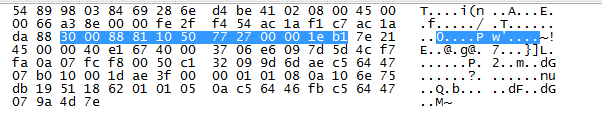


图 1 原数据包内容

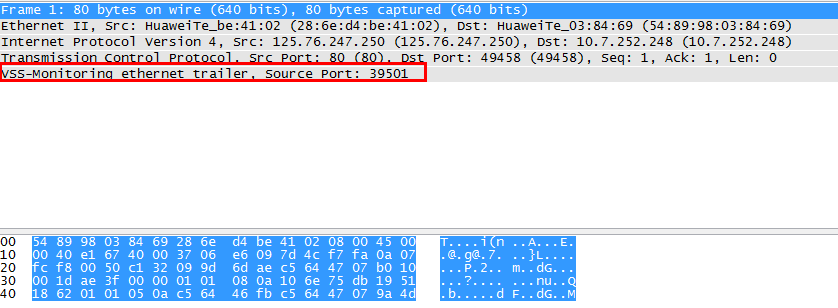


图 2 处理之后数据包内容

分析：发现处理之后数据包内容中多了9a 4d两个字节，之后被wireshark解析成了数据包被截断了；发现内层IP包中表示长度为64Byte，IP字段长度20Byte,TCP字段长度44字节，那么正好，为什么多了这两个字节，通过对比处理之前数据包发现，这两个字节是包含在PPP帧内部，查资料发现这两个字节为PPP内层封装的FCS校验；那么如何判断PPP数据包内是否函数字节校验呢？因为GRE头中没有表示内层PPP协议的描述，而PPP头也是只是用7e 21压缩头来表示当前数据的传送协议，没有其他信息表示PPP帧内含有2字节FCS；那么只能从IP中拿到该数据包长度，并矫正写入pcap\_dump中数据长度；

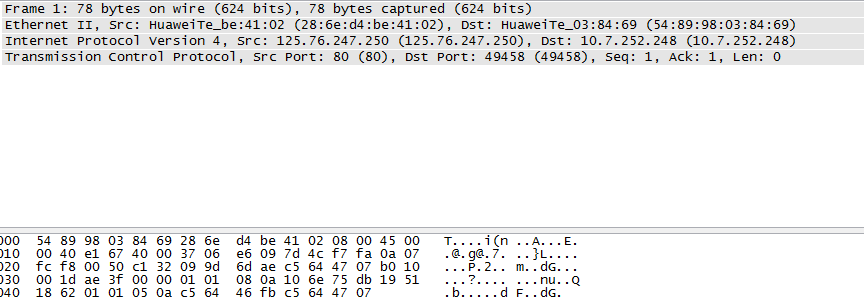


图 3 修改之后处理结果