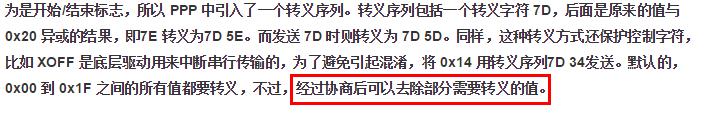
PPP协议报文转义字符分析

时间：2015/11/6

背景：网航数据包中存在大量的GRE封装的PPP数据包文，且PPP中包含着大量的分片包；在使用ipdecap\_extend程序进行处理过程中发现，PPP数据包中存在着转义字符例如0x11（UDP协议号），转义成0x7d 0x31；但是在其他数据包中同样协议字段0X06（TCP协议）没有做转义；参考网上文档中所描述的情况来说



转义部分:

* IP字段 目的IP



* TCP sequence number字段；P100,



* UDP 协议（0x7e 0x31）
* payload字段P7

结论：在抓到的数据包中发现任何一个部分都有可能有PPP转义之后的字符；但是相同区间中都包含着小于0x20的字节，而没有被转义；按照引用材料所述，转义部分是需要协商的，而不是固定按照小于0x20的字节就需要转义，从而表明通过查找0x7d进行反转义是没有问题的；