链滴

tcp 报文分析

作者：flyue

原文链接：https://ld246.com/article/1530363267288

来源网站：链滴

使用wireshark抓取到的包：

主要分为五层：

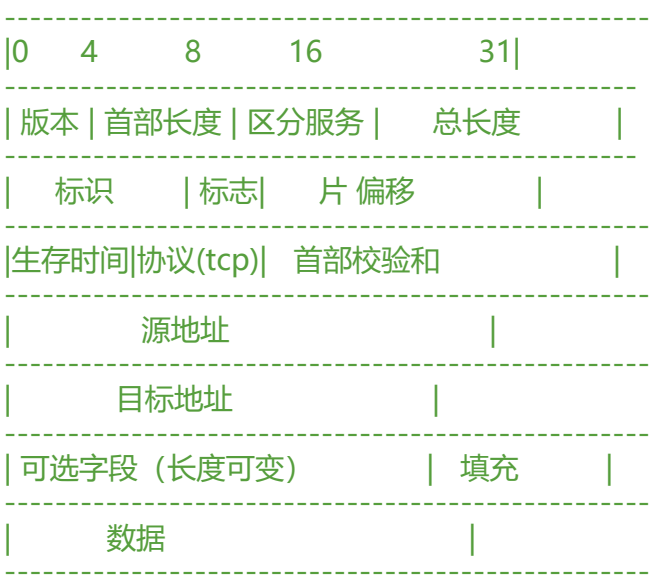
1. Frame:物理层的数据帧概况

- wireshark抓取的报文没有该层的数据，猜测和网卡有关,其中定义了数据链路层使用的协议
- 回环地址使用的是:NULL/Loopback ,其他常见还有 Ethernet

2. Ethernet II: 数据链路层以太网帧头部信息

- wireshark抓取到的包从该层开始: 用来显示源mac地址、目标mac地址
- 回环协议该层占用:4位16进制数据(02 00 00 00)
- Ethernet占用: 12位16进制数据(c0 61 18 f5 3e 62 58 fb 84 09 65 a5)
- 前6位目标mac地址，后6位源mac地址 最后2位表示互联网层用的协议ipv4 ： 0x0800表示用IP协议

3. 互联网层IP包头信息:



1. 版本:4bit表示(4位二进制,example: 0100) --> ipv4 or ipv6
2. 首部长度: 用4bit表示:

- 这个字段表示的数的单位是32bit(4个字节)
- 表示含义为ip包的包头长度，是指从"版本" 到"目的IP地址"结束(可能还会有填充,32bit为单位的系)

3. 区分服务：占 8bit ，不关心具体内容，跳过
4. 总长度: ip包的总长度

- 从"版本"开始,一直到数据包的末尾.
- 单位是 8bit (一个字节)

5. 源IP地址：
6. 目标IP地址:
7. 传输层tcp数据信息: 也就是"互联网层"中的"数据"
    - tcp首部(tcp头部):固定20个字节
    - 开头是原端口和目标端口
    - 原端口： 16bit
    - 目标端口: 16 bit
    - 20个字节后就是tcp真正的数据了

案例分析：

tcpdump详解:

https://www.cnblogs.com/f-ck-need-u/p/7064286.html

https://www.cnblogs.com/bass6/p/5819928.html