4.2 WireShark 分析 IP 数据包格式_物联网 / 嵌入式工程师 - 慕课网

> 慕课网慕课教程 4.2 WireShark 分析 IP 数据包格式涵盖海量编程基础技术教程，以图文图表的形式，把晦涩难懂的编程专业用语，以通俗易懂的方式呈现给用户。

TCP/IP 协议中，TCP 协议和 IP 协议分别完成不同的任务。

TCP 是用来检测网络传输中的差错。

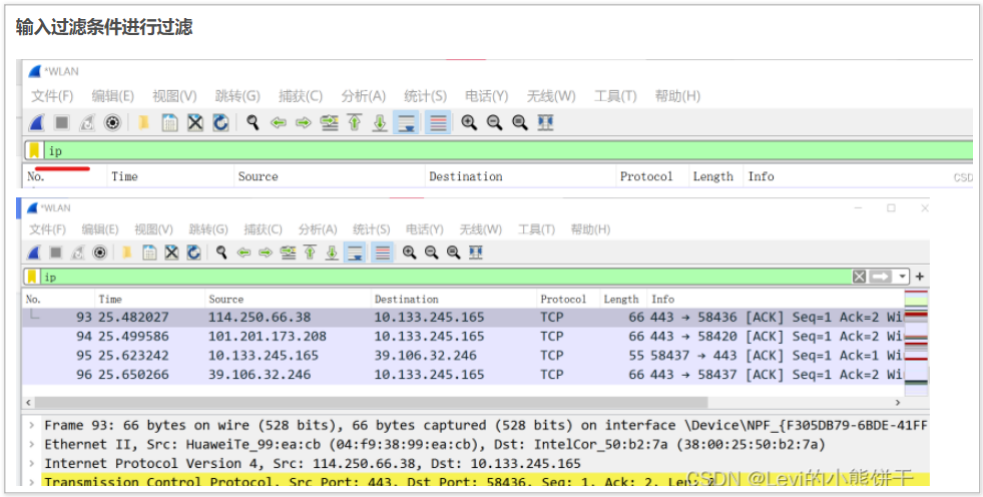
IP 协议可以将多个交换网络连接起来，在源地址和目的地址之间传送数据包。同时，它还提供数据重新组装功能，以适应不同网络对数据包大小的要求。

在 TCP/IP 协议中，使用 IP 协议传输的数据包就是 IP 数据包。

IP 报文是在网络层传输的数据单元，也叫 IP 数据报。

- 版本：IP 协议的版本，目前的 IP 协议版本号为 4，下一代 IP 协议版本号为 6。
- 首部长度：IP 报头的长度。固定部分的长度（20 字节）和可变部分的长度之和。共占 4 位。最大为 1111，即 10 进制 的 15，代表 IP 报头的最大长度可以为 15 个 32bits（4 字节），也就是最长可为 15*4=60 字节，除去固定部分的长度 20 字节，可变部分的长度最大为 40 字节。
- 服务类型：Type Of Service。
- 总长度：IP 报文的总长度。报头的长度和数据部分的长度之和。
- 标识：唯一的标识主机发送的每一份数据报。通常每发送一个报文，它的值加一。当 IP 报文长度超过传输网络的 MTU（最大传输单元）时必须分片，这个标识字段的值被复制到所有数据分片的标识字段中，使得这些分片在达到最终目的地时可以依照标识字段的内容重新组成原先的数据。

- 标志：共 3 位。R、DF、MF 三位。目前只有后两位有效，DF 位：为 1 表示不分片，为 0 表示分片。MF：为 1 表示“更多的片”，为 0 表示这是最后一片。
- 片位移：本分片在原先数据报文中相对首位的偏移位。（需要再乘以 8）
- 生存时间：IP 报文所允许通过的路由器的最大数量。每经过一个路由器，TTL 减 1，当为 0 时，路由器将该数据报丢弃。TTL 字段是由发送端初始设置一个 8 bit 字段. 推荐的初始值由分配数字 RFC 指定，当前值为 64。发送 ICMP 回显应答时经常把 TTL 设为最大值 255。
- 协议：指出 IP 报文携带的数据使用的是那种协议，以便目的主机的 IP 层能知道要将数据报上交到哪个进程（不同的协议有专门不同的进程处理）。和端口号类似，此处采用协议号，TCP 的协议号为 6，UDP 的协议号为 17。ICMP 的协议号为 1，IGMP 的协议号为 2.
- 首部校验和：计算 IP 头部的校验和，检查 IP 报头的完整性。
- 源 IP 地址：标识 IP 数据报的源端设备。
- 目的 IP 地址：标识 IP 数据报的目的地址。



- IP 层相关信息

```
Internet Protocol Version 4, Src: 114.250.66.38, Dst: 10.133.245.165
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xa255 (41557)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 118
    Protocol: TCP (6)
    Header Checksum: 0xed23 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.250.66.38
    Destination Address: 10.133.245.165
```

练习：

大家自己用 WireShark 抓一个包，查看 IP 的结构。并截图上传。

全文完