**IP 数据包结构：**


如图，一个刻度表示1个二进制位（比特）。

1-1.版本4位，表示版本号，目前最广泛的是4=B1000，即常说的 IPv4；相信 IPv6以后会广泛应用，它能给世界上每个纽扣都分配一个 IP 地址。

1-2.头长4位，数据包头部长度。它表示数据包头部包括多少个32位长整型，也就是多少个4字节的数据。无选项则为5（红色部分）。

1-3.服务类型，包括8个二进制位，每个位的意义如下：

过程字段：3位，设置了数据包的重要性，取值越大数据越重要，取值范围为：0（正常）~7（网络控制）

延迟字段：1位，取值：0（正常）、1（期特低的延迟）

流量字段：1位，取值：0（正常）、1（期特高的流量）

可靠性字段：1位，取值：0（正常）、1（期特高的可靠性）

成本字段：1位，取值：0（正常）、1（期特最小成本）

保留字段：1位 ，未使用

1-4.包裹总长16位，当前数据包的总长度，单位是字节。当然最大只能是65535，及64KB。

2-1.重组标识16位，发送主机赋予的标识，以便接收方进行分片重组。

2-2.标志3位，他们各自的意义如下：

保留段位(2)：1位，未使用

不分段位(1)：1位，取值：0（允许数据报分段）、1（数据报不能分段）

更多段位(0)：1位，取值：0（数据包后面没有包，该包为最后的包）、1（数据包后面有更多的包）

2-3.段偏移量13位，与更多段位组合，帮助接收方组合分段的报文，以字节为单位。

3-1.生存时间8位，经常 ping 命令看到的 TTL（Time To Live）就是这个，每经过一个路由器，该值就减一，到零丢弃。

3-2.协议代码8位，表明使用该包裹的上层协议，如 TCP=6，ICMP=1，UDP=17等。

3-3.头检验和16位，是 IPv4数据包头部的校验和。

4-1.源始地址，32位4字节，我们常看到的 IP 是将每个字节用点（.）分开，如此而已。

5-1.目的地址，32位，同上。

6-1.可选选项，主要是给一些特殊的情况使用，往往安全路由会当作攻击而过滤掉，普联（TP_LINK）的TL-ER5110路由就能这么做。

7-1.用户数据。

**TCP 数据包结构：**


1-1.源始端口16位，范围：0-65535。
1-2.目的端口，同上。
2-1.数据序号32位，TCP 为发送的每个字节都编一个号码，这里存储当前数据包数据第一个字节的序号。
3-1.确认序号32位，为了安全，TCP 告诉接受者希望他下次接到数据包的第一个字节的序号。
4-1.偏移4位，类似 IP，表明数据距包头有多少个32位。
4-2.保留6位，未使用，应置零。
4-3.紧急比特 URG—当 URG＝1时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据，应尽快传送(相当于高优先级的数据)。
4-3.确认比特 ACK—只有当 ACK＝1时确认号字段才有效。当 ACK＝0时，确认号无效。**参考 TCP 三次握手**
4-4.复位比特 RST(Reset) —当 RST＝1时，表明 TCP 连接中出现严重差错（如由于主机崩溃或其他原因），必须释放连接，然后再重新建立运输连接。**参考 TCP 三次握手**
4-5.同步比特 SYN—同步比特 SYN 置为1，就表示这是一个连接请求或连接接受报文。**参考 TCP 三次握手**
4-6.终止比特 FIN(FINal)—用来释放一个连接。当 FIN＝1时，表明此报文段的发送端的数据已发送完毕，并要求释放运输连接。
4-7.窗口字段16位，窗口字段用来控制对方发送的数据量，单位为字节。TCP 连接的一端根据设置的缓存空间大小确定自己的接收窗口大小，然后通知对方以确定对方的发送窗口的上限。
5-1.包校验和16位，包括**首部**和**数据**这两部分。在计算检验和时，要在 TCP 报文段的前面加上12字节的伪首部。
5-2.紧急指针16位，紧急指针指出在本报文段中的紧急数据的最后一个字节的序号。
6-1.可选选项24位，类似 IP，是可选选项。
6-2.填充8位，使选项凑足32位。
7-1.用户数据……

**UDP 数据包结构：**