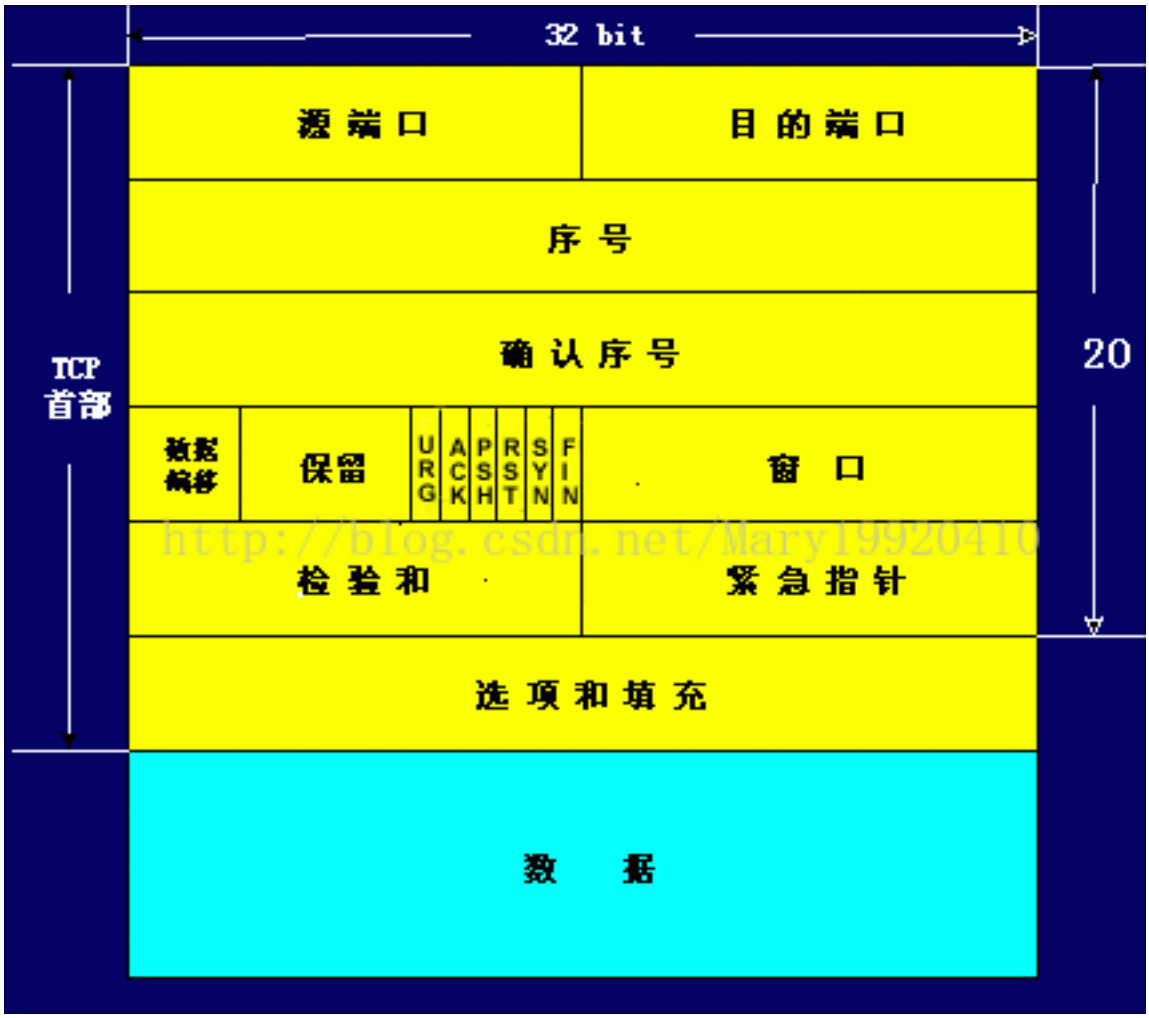
二、TCP报文, UDP报文, IP报文详解

- 参考：
  IP报文格式详解_海阔天空sky的博客-CSDN博客_ip报文格式详解

TCP报文



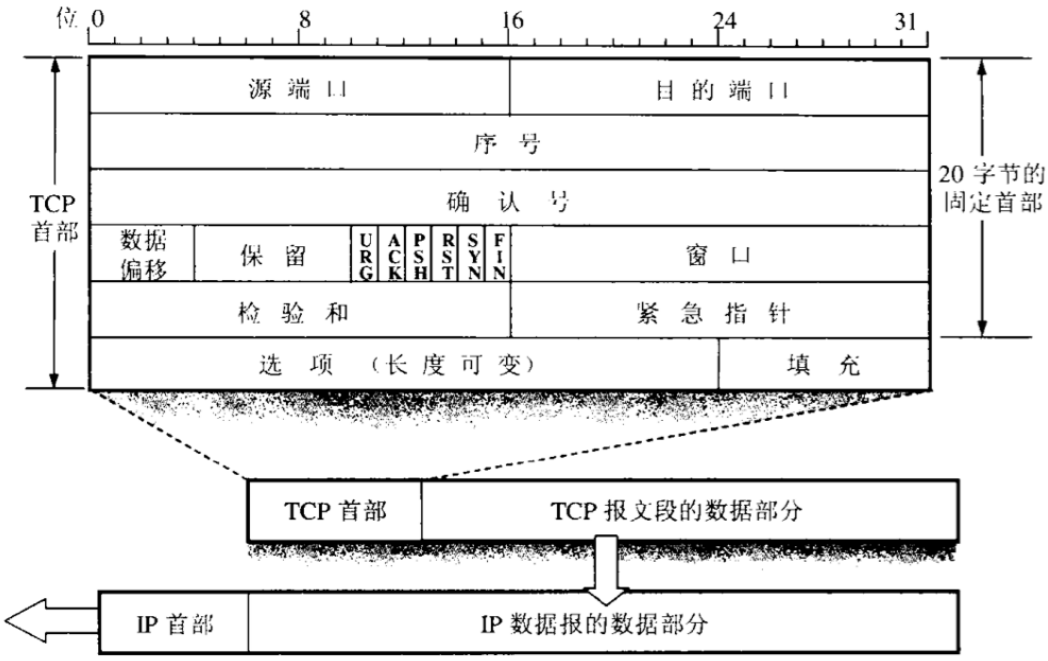
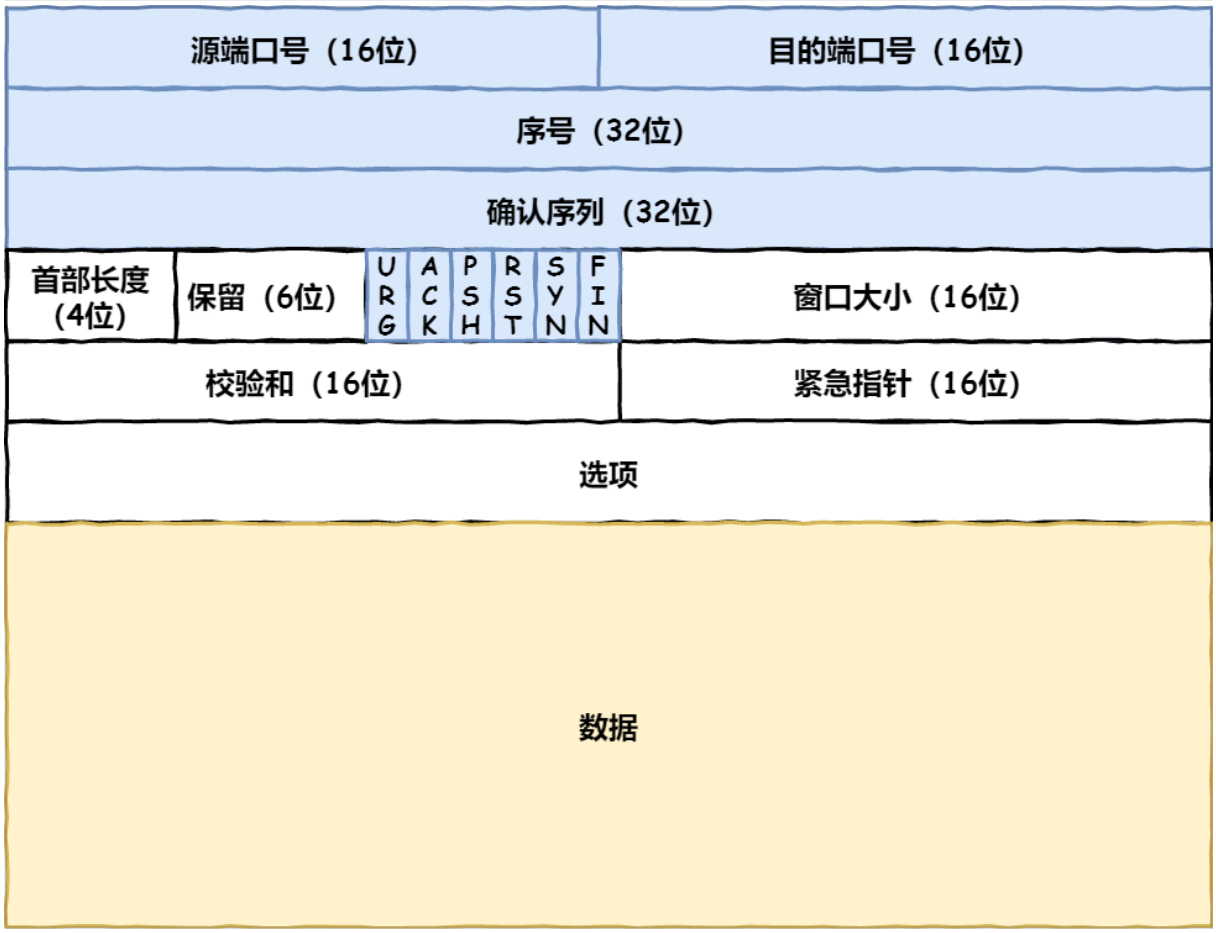


图 5-14　TCP 报文段的首部格式



一行是4个字节（32位），TCP首部有6行，就是24个字节。但是TCP报头的长度是不确定的（有一行是可选项），所以不包含任何可选字段的TCP报头长度就是20字节（也就是说TCP的固定首部为20字节）

---

1. **端口号**：用来标识一台计算机的不同的应用进程

- 源端口：源端口和IP地址的作用是标识报文的返回地址
- 目的端口：指明接收方计算机上的应用程序接口

> **TCP报头中的源端口号和目的端口号同IP数据报中的源IP与目的IP唯一确定一条TCP连接**

2. **序列号**（initial sequence number）和**确认号**（acknowledge number）：

   - 是TCP可靠传输的关键部分，序列号（也叫报文段序号）是指本报文段发送的数据组的第一个字节的序号。在TCP传送的流中，每一个字节一个序号。（e.g. 一个报文段的序号为300，此报文段数据部分共有100字节，那么下一个报文段的序号为400）所以序号确保了TCP传输的有序性。

   - 确认号ack，指明下一个期待收到的字节序号，表明该序号之前的所有数据已经正确无误的收到。确认号只有当ACK位为1时才有效。比如建立连接时，SYN报文的ACK标志位为0（注意ack和ACK不一样）

   > **序列号**：在建立连接时由计算机生成的随机数作为其初始值，通过 SYN 包传给接收端主机，每发送一次数据，就「累加」一次该「数据字节数」的大小。**用来解决网络包乱序问题。**
   >
   > **确认应答号**：指下一次「期望」收到的数据的序列号，发送端收到这个确认应答以后可以认为在这个序号以前的数据都已经被正常接收。**用来解决不丢包的问题。**

3. 数据偏移/**首部长度**：4位(bits)

   由于首部可能含有可选项内容(选项)，因此TCP报头的长度是不确定的（报头不包含任何任选字段则长度为20字节）。

   数据偏移占4位，它指出数据部分的开始位置距离TCP报文段的开始位置有多远。

   数据偏移的单位是4字节（32位），由于4位二进制的数最多能表示15（10进制），所以数据偏移的最大值就是：4*15 = 60字节（15个单位）

   这也是TCP首部的最大长度（固定是20字节，也就是说选项部分的长度不能超过40字节）

4. **保留**：

   占6位，保留为今后使用，但目前应该设置为0

5. **控制位**：

   每一个标志位表示一个控制功能，共六个

   1. *URG*：

      紧急指针标志，为1时表示紧急指针有效，为0则忽略紧急指针

   2. *ACK*：

      确认序号标志，为1表示确认号ack有效，为0表示报文中不含确认信息，忽略acknowledge number

`TCP 规定除了最初建立连接时的 SYN 包之外该位必须设置为 1`

3. *PSH*：

   push标志，为1表示是带有push标志的数据，指示接收方在接收到该报文段以后，应该尽快将这个报文段交给应用程序，而不是在缓冲区排队

4. *RST*：

   重置连接标志，用于重置由于主机崩溃或其他原因而出现错误的连接。或者用于拒绝非法的报文段和拒绝连接请求

5. *SYN*：

   同步序号，用于建立连接过程，在连接请求中，SYN=1和ACK=0表示该数据段没有使用捎带的ack；而连接应答应该捎带一个ack，即SYN=1和ACK=1

6. *FIN*：

   finish标志，用于终止连接，为1时表示发送方已经没有数据发送了，即关闭本方数据流（等对方也回fin=1的时候，才是真正关闭，如果对方还没回fin=1，说明数据还没有传完，本方就继续接收数据，直到对方发来fin=1）

6. **窗口**：

   占2个字节(16位)，窗口值是[0, 2^16 -1]之间的整数。窗口指的是发送本报文段的一方的接收窗口（而不是自己的发送窗口）

   窗口值可以告诉对方：从本报文段首部的确定号算起，接收方目前允许对方发送的数据量

   之所以要有这个限制，是因为接收方的数据缓存空间是有限的

7. **校验和**：

   - 占2个字节(16位），奇偶校验。校验和字段检验的范围包括首部和数据这两个部分（整个TCP报文段）
   - 由发送端进行计算和存储，由接收端进行验证

   TCP协议之校验和 - 简书

   > 原码、反码、补码：原码, 反码, 补码 详解 - ziqiu.zhang - 博客园

8. **紧急指针**：

   占2个字节。只有当URG标志设置为1时紧急指针才有效。它指出本报文段中的紧急数据的字节数（紧急数据结束后就是普通数据）。因此紧急指针指出来紧急指针的末尾在报文段中的位置。当所有紧急数据都处理完时，TCP就告诉应用程序恢复到正常操作。（注意即使窗口为0也可以发送紧急数据）

9. **选项（选项和填充）**：

   - 长度可变，最长可达40字节，当没有选项的时候，TCP的首部长20字节。
   - 常见的可选字段是**最大报文长度**，又称为**MSS**（Maximun Segment Size）
   - 每个连接方通常都在通信的第一个报文段（为建立连接而设置SYN标志为1的那个段）中

指明这个选项，它表示本端所能接受的最大报文段的长度。

- 选项长度不一定是32位的整数倍，所以要加填充位，即在这个字段中加入额外的零，从而保证TCP头是32的整数倍

10. **数据**部分：

TCP报文段中的数据部分是可选的。在一个连接建立和一个连接终止时，双方交换的报文段仅有TCP首部。如果一方没有数据要发送，也使用没有任何数据的首部来确认收到的数据。在处理超时的许多情况中，也会发送不带任何数据的报文段

UDP报文

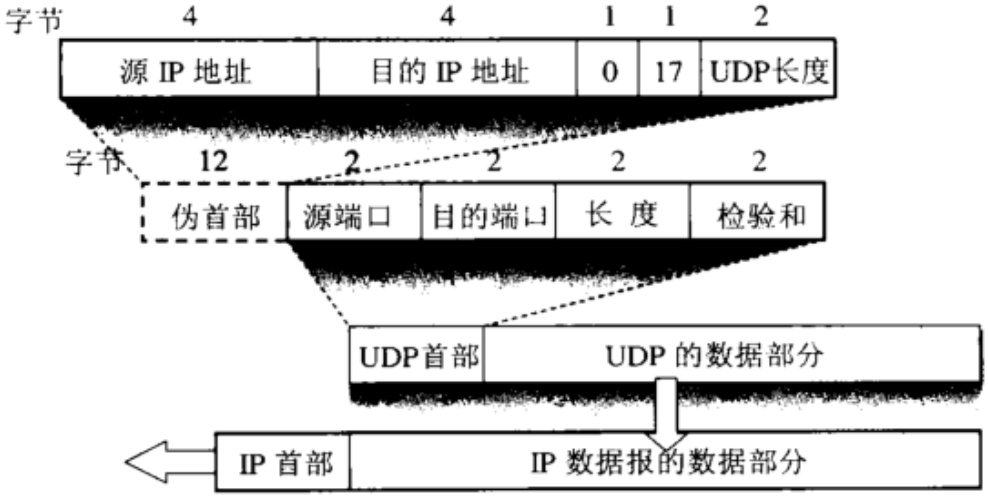


图 5-5　UDP 用户数据报的首部和伪首部

- 用户数据报UDP有两个字段：数据字段和首部字段
- 首部字段很简单，只有8个字节，由四个字段组成，每个字段的长度都是两个字节(16位)

1. **源端口号**：在需要对方回信时选用。不需要时可全用0。

2. **目的端口号**：这在终点交付报文时必须要使用到。

3. **长度**：UDP用户数据报的长度，其最小值是8（仅有首部没有数据）

4. **校验和**：校验UDP用户数据报在传输中是否有错，有错就丢弃

IP报文

IP报文是在网络层传输的数据单元，也叫IP数据报。IP报文格式如下图（图片来源：百度百科）

1. **版本**（4位）：表示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

2. **首部长度**（4位）：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

3. **服务类型**（1字节）：Type Of Service

4. **总长度**（2字节）：IP报文的总长度。报头的长度和数据部分的长度之和

5. **标识**（2字节）：唯一的标识主机发送的每一分数据报。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

6. **标志**（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

7. **片位移**（13位）：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）

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。

9. **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.

10. **首部校验和**：计算IP头部的校验和，检查IP报头的完整性。

11. **源IP地址**：标识IP数据报的源端设备。

12. **目的IP地址**：标识IP数据报的目的地址。