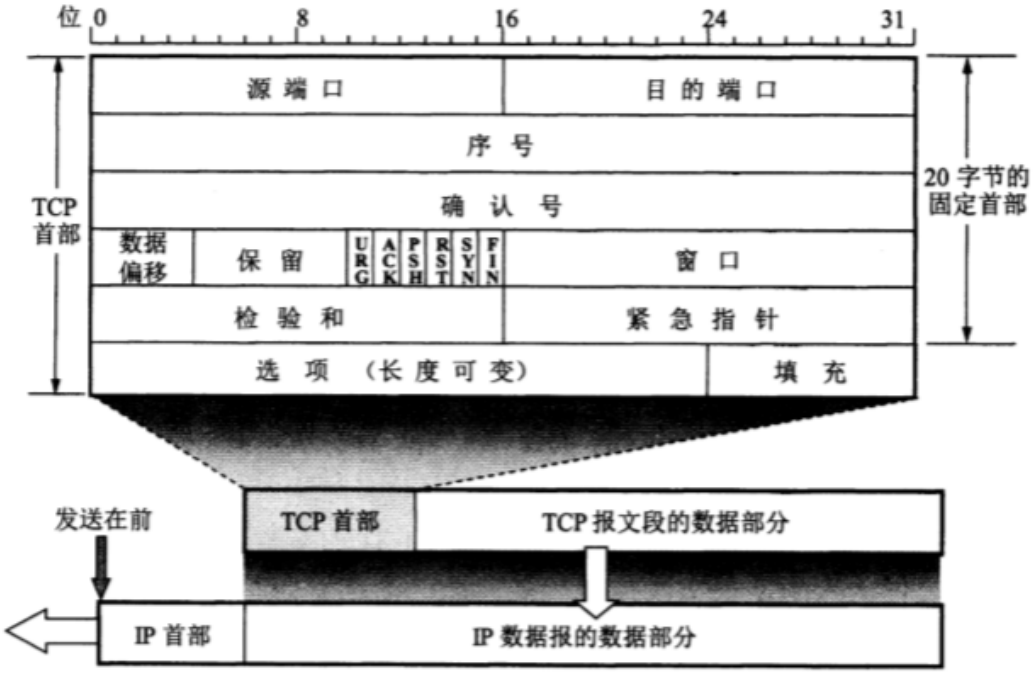

图 5-14 TCP 报文段的首部格式

一个TCP报文段由**首部**和**数据载荷**两部分组成。

由20字节固定首部和最大20字节的扩展首部构成

TCP数据部分最多有$65535-20-20=65495$个字节，65535也就是64k，减去IP头20，减去TCP头20

TCP数据部分通常有1460字节，因为可能经过以太网，MTU最大字节是1500，数据部分就是1460字节

源端口字段

- 占16比特，写入源端口号，用来标识发送该TCP报文段的应用进程

目的端口

- 占16比特，写入目的端口号，用来标识接收该TCP报文段的应用进程

序号字段

- 占32个比特，取值范围是[0, $2^{32}-1$]，序号增加到最后一个后，下一个序号又回到0
- 指出本TCP报文段数据载荷的第一个字节的序号

确认号字段

- 占32比特，取值范围[0, $2^{32}-1$]，确认号增加到最后一个后，下一个确认号又回到0
- 指出期望收到对方下一个TCP报文段的数据载荷的第一个字节的序号，同时也是对之前收到的所有数据的确认

若确认号为n，则表明到序号n-1为止的所有数据都已正确接收，期望接收序号为n的数据

ACK

- 确认标志位：取值为1时确认字段才有效；取值为0时确认号字段无效

TCP规定，在连接建立后，所有传送的TCP报文段都必须把ACK置1

数据偏移字段

- 占4比特，并以4字节为单位
- 用来指出TCP报文段的数据载荷部分得的起始处距离TCP报文段的起始处有多远（实际上指出了TCP报文段的首部长度）由于首部固定长度为20字节，因此，数据偏移字段的最小值为二进制的0101。首部最大长度为60字节，二进制为1111

保留字段

- 占6比特，保留位今后使用，目前置为0

窗口字段

- 占16比特，以字节为单位
- 指出发送本报文的一方的接收窗口
- 窗口值作为接收方让发送方设置其发送窗口的依据
- 以接收方的接收能力来控制发送方的的发送能力，称为流量控制
- 发送窗口大小从拥塞窗口和接收窗口中取小者

校验和字段

- 占16比特，用来检查包括TCP报文段的首部和数据载荷两部分。
- 在计算校验和时，要在TCP报文段的前面加上12字节的伪首部
- 把伪首部第4个字段中的17改为6。UDP是17，TCP是6

同步标志为SYN

- 在TCP连接建立时用来同步序号。

终止标志位FIN

- 用来释放TCP连接，FIN=1表明是TCP连接释放报文段

复位标志RST

- 用来复位TCP连接
- 当RST=1时，表明TCP连接出现了异常，必须释放连接，然后再重新建立连接
- RST置1还可以用来拒绝一个非法的报文段或拒绝打开一个TCP连接

推送标志位PSH

- 接收方的TCP收到该标志位为1的报文段会尽快上交应用进程，而不必等到接收缓存都填后再向上交付

紧急标志位URG

- 取值为1时紧急指针字段有效；取值为0时紧急指针字段无效

紧急指针

- 占16比特，以字节为单位，用来指明紧急数据的长度
- 当发送方有紧急数据时，可将紧急数据插队到发送缓存的最前面，并立刻封装到一个TCP报文段中进行发送。紧急指针会指出本报文段数据载荷部分包含多长的紧急数据，紧急数据之后是普通数据

选项部分

- 最大报文段长度MSS选项：TCP报文段数据载荷部分的最大长度
- 窗口扩大选项：为了扩大窗口，提高吞吐率
- 时间戳选项：用来计算往返时间RRT；用来处理序号超范围情况，又称为防止序号绕回PAWS
- 选择确认选项：用来实现选择确认功能

填充

- 由于选项的长度可变，因此使用填充来确保报文段首部能被4整除（因为数据偏移字段，也就是首部长度字段，是以4字节为单位）