第五章 传输层 TCP协议的特点和TCP报文段

流：流入到进程或从进程流出的字节序列。

TCP的特点：
（1）TCP是面向连接（虚连接）的传输层协议。
（2）每一条TCP连接只能有两个端点，每一条TCP连接只能是点对点的。
（3）TCP提供可靠交付的服务，无差错、不丢失、不重复，按序到达。即可靠有序，不丢不重。
（4）TCP提供全双工通信。因此TCP连接两端都有**发送缓存**和**接受缓存**；
　　发送缓存中**为准备发送的数据**和**已发送但 尚未收到确认的数据**。
　　接受缓存中为**按序到达但尚未接受应用程序读取的数据**和**不按序到达的数据**。
（5）TCP面向字节流； TCP把应用程序交下来的数据看成仅仅是一连串的无结构的字节流。

（重点）TCP报文段

TCP传送的数据单元称为**报文段**。一个TCP报文段分为**TCP首部**和**TCP数据**两部分，整个TCP段作为IP数据报的数据部分封装在IP数据报中。

TCP的首部的前20B是固定的。TCP报文段的首部最短为20B，后面的4N字节都是需要而增加的选项，通常长度为4B的整数倍。

下图为TCP报文段

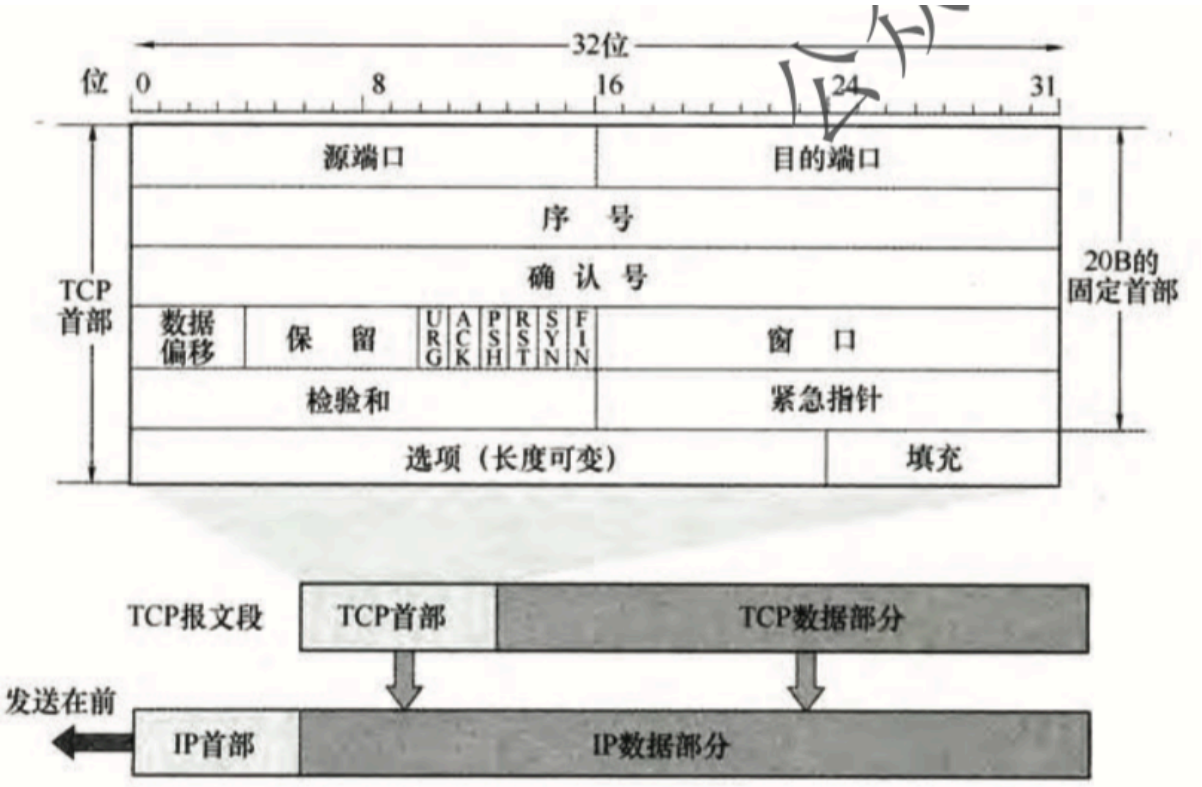

图 5.6 TCP 报文段

各字段意义如下：

（1）源端口和目的端口字段：**各占2B**。

（2）序号字段：**占4B**。TCP是面向字节流的（即TCP传送时是住个字节传送的），所以TCP连接传送的数据流中的每个字节都编上一个序号。序号字段的值指的是本报文段所发送的数据的第一个字节的序号。

例如：一报文段的序号字段值为301，而携带的数据共有100B，标明本报文段的数据的最后一个字节的序号是400，估下一个报文段的数据序号应从401开始

（3）确认号字段：占**4B**，是期望收到对方的下一个报文度的数据的第一个字节的序号。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收到。

（4）**数据偏移（即首部长度）**：占**4位**。这里不是IP数据报分片的

那个数据偏移，而是表示**首部长度**。它**指**出TCP报文段的数据起始处距离TCP报文段的起始处有多远。

数据偏移的单位是32位，（以4B为计算单位。）因此当此字段值为15时，达到TCP首部的最大长度为60B。

（5）保留字段：占6位，保留为以后使用过，但目前应置为0.

（6）紧急位URG：URG=1时，表明紧急指针字段有效。它告诉系统报文段中有紧急数据，应尽快传送。但URG需要和紧急指针配套使用，即数据从第一个字节到紧急指针所指字节就是紧急数据。

（7）确认位ACK：只有当ACK=1时，确认号字段才有效。当ACK=0时，确认号无效。

TCP规定，在连接建立后所有传送的报文段都必须把ACK置1.

（8）推送位PSH：接收TCP收到PSH=1的报文段，就尽快地交付给接收应用进程，而不再等到整个缓存都填满后再向上交付。

（9）复位位RST：RST=1时，表明TCP连接中出现严重差错，必须释放连接，然后再重新建立运输连接。

（10）同步位SYN：同步SYN=1表示这是一个连接请求或连接接受报文。

当SYN=1，ACK=0，表明这是一个连接请求报文，对方若同意建立连接，则在相应报文中使用SYN=1，ACK=1。即SYN=1表示这是一个连接请求或连接接受报文。

（11）终止位FIN：用来释放一个连接。**FIN=1表明此报文段的发送方的数据已发送完毕**，并**要求释放传输连接**。

（12）窗口字段：占2B。它指出现在允许对方发送的数据量，接收方数据缓存空间是有限的，故用窗口值作为接收方让发送方设置其发送窗口的依据，单位为字节。

（13）校验和：**占2B**，校验和字段检验的**范围包括首部和数据两部**

分。

在计算校验和时，和UDP一样，要在TCP报文段的前面加上12B的伪首部，只需将UDP伪首部的第4个字段，即协议字段的17改成6，其他的和UDP一样。

（14）紧急指针字段：**占16位**，URG=1才有意义，指出在本报文段中**紧急数据共有多少字节**（**紧急数据放在本报文段数据的最前面。**）

（15）选项字段：长度可变，TCP规定了一种选项，即最大报文段长度（MSS），**MSS是TCP报文段中的数据字段的最大长度**。

（16）填充字段：这是为了**使整个首部长度为4B的整数倍**。