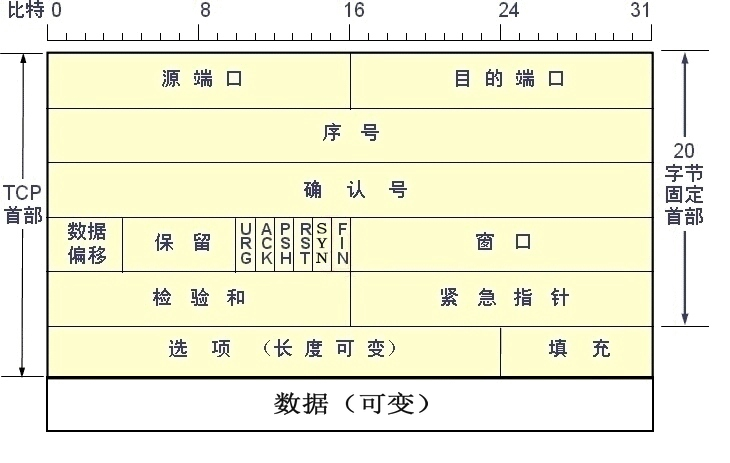
**TCP 报文格式**





TCP（Transmission Control Protocol 传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议。

TCP 报文段的报头有 10 个必需的字段和 1 个可选字段。报头至少为 20 字节。报头后面的数据是可选项。

1）源端口（16位）

标识发送报文的计算机端口或进程。一个 TCP 报文段必须包括源端口号，使目的主机知道应该向何处发送确认报文。

2）目的端口（16位）

标识接收报文的目的主机的端口或进程。

3） 序号（也叫序列号）（32位）

用于标识每个报文段，使目的主机可确认已收到指定报文段中的数据。当源主机用于多个报文段发送一个报文时，即使这些报文到达目的主机的顺序不一样，序列号也可以使目的主机按顺序排列它们。

在 SYN 标志未置位时，该字段指示了用户数据区中第一个字节的序号；在 SYN 标志置位时，该字段指示的是初始发送的序列号。

在建立连接时发送的第一个报文段中，双方都提供一个初始序列号。TCP 标准推荐使用以 4ms 间隔递增 1 的计数器值作为这个初始序列号的值。使用计数器可以防止连接关闭再重新连接时出现相同的序列号。

对于那些包含数据的报文段，报文段中第一个数据字节的数量就是初始序列号，其后数据字节按顺序编号。如果源主机使用同样的连接发送另一个报文段，那么这个报文段的序列号等于前一个报文段的序列号与前一个报文段中数据字节的数量之和。例如，假设源主机发送 3 个报文段，每个报文段有 100 字节的数据，且第一个报文段的序列号是 1000，那么第二个报文段的序列号就是 1100（1000 + 100），第三个报文段的序列号就是 1200（1100 + 100）。

如果序列号增大至最大值将复位为 0。

4）确认号（32位）

目的主机返回确认号，使源主机知道某个或几个报文段已被接收。如果 ACK 控制位被设置为 1，则该字段有效。确认号等于顺序接收到的最后一个报文段的序号加 1，这也是目的主机希望下次接收的报文段的序号值。返回确认号后，计算机认为已接收到小于该确认号的所有数据。

例如，假设源主机发送 3 个报文段，每个报文段有 100 字节的数据，且第一个报文段的序列号是 1000，那么接收到第一个报文段后，目的主机返回含确认号1100 的报头。接收到第二个报文段（其序号为 1100 ）后，目的主机返回确认号 1200。接收到第三个报文段后，目的主机返回确认号 1300 。

目的主机不一定在每次接收到报文段后都返回确认号。在上面的例子中，目的主机可能等到所有 3 个报文段都收到后，再返回一个含确认号 1300 的报文段。但是如果目的主机再发回确认号之前等待时间过长，源主机会认为数据没有到达目的主机，并自动重发。

上面的例子中，如果目的主机接收到了报文段号为 1000 的第一个报文段以及报文段号为 1200 的最后一个报文段，则可返回确认号 1100，但是再返回确认号 1300 之前，应该等待报文段号为 1100 的中间报文段。

5） 数据偏移（首部长度）（4位）

TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远，即首部长度。由于 TCP 报头的长度随 TCP 选项字段内容的不同而变化，因此报头中包含一个指定报头字段的字段。该字段以 32 比特为单位，所以报头长度一定是 32 比特的整数倍，有时需要在报头末尾补 0 。如果报头没有 TCP 选项字段，则报头长度值为 5 ，表示报头一个有 160 比特，即 20 字节。

6）保留位（6位）

由跟在数据偏移字段后的 6 位构成， 全部为 0 。

7）控制位（6位）

紧急 URG：此位置 1，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。

确认 ACK：仅当 ACK = 1 时确认号字段才有效，TCP 规定，在连接建立后所有传达的报文段都必须把 ACK 置 1。

推送 PSH：当两个应用进程进行交互式的通信时，有时在一端的应用进程希望在键入一个命令后立即就能够收到对方的响应。在这种情况下，TCP 就可以使用推送（push）操作，这时，发送方 TCP 把 PSH 置 1 ，并立即创建一个报文段发送出去，接收方收到 PSH = 1 的报文段，就尽快地（即“推送”向前）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。

复位 RST：用于复位相应的 TCP 连接

同步 SYN：仅在三次握手建立 TCP 连接时有效。当 SYN = 1 而 ACK = 0 时，表明这是一个连接请求报文段，对方若同意建立连接，则应在相应的报文段中使用 SYN = 1 和 ACK = 1。因此，SYN 置 1 就表示这是一个连接请求或连接接受报文。

终止 FIN：用来释放一个连接。当 FIN = 1 时，表明此报文段的发送方的数据已经发送完毕，并要求释放运输连接。

8）窗口（16位）

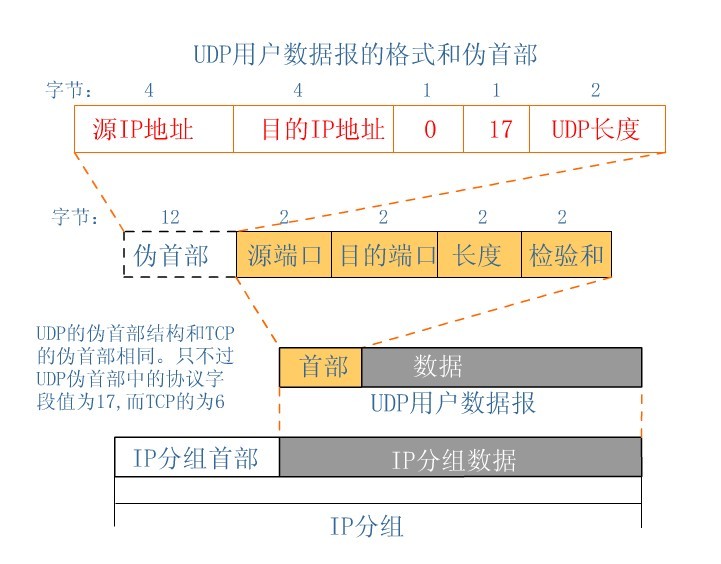
此字段用来进行流量控制，这个值是本机期望一次接收的字节数，即发送数据的窗口大小。告诉对方在不等待确认的情况下，可以发来多大的数据。这里表示的最大长度是2^16 - 1 = 65535，如需要使用更大的窗口大小，需要使用选项中的窗口扩大因子选项。

指发送本报文段的一方的接收窗口（而不是自己的发送窗口）。

9）校验和（16位）

源主机和目的主机根据 TCP 报文段以及伪报头的内容计算校验和。在伪报头中存放着来自 IP 报头以及 TCP 报文段长度信息。与 UDP 一样，伪报头并不在网络中传输，并且在校验和中包含伪报头的目的是为了防止目的主机错误地接收存在路由的错误数据报。

伪首部，又称为伪包头（Pseudo Header）：是指在 TCP 的分段或 UDP 的数据报格式中，在数据报首部前面增加源 IP 地址、目的 IP 地址、IP 分组的协议字段、TCP 或 UDP 数据报的总长度等共12字节，所构成的扩展首部结构。此伪首部是一个临时的结构，它既不向上也不向下传递，仅仅只是为了保证可以校验套接字的正确性。



10）紧急指针（16位）

仅在 URG = 1 时才有意义，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），即指出了紧急数据的末尾在报文中的位置，注意：即使窗口为零时也可发送紧急数据。

如果 URG 为 1 ，则紧急指针标志着紧急数据的结束。其值是紧急数据最后 1 字节的序号，表示报文段序号的偏移量。例如，如果报文段的序号是 1000，前 8 个字节都是紧急数据，那么紧急指针就是 8 。紧急指针一般用途是使用户可中止进程。

11）选项、填充字段

可能包括“窗口扩大因子”、“时间戳”等选项。长度可变，最长可达 40 字节，当没有使用选项时，TCP 首部长度是 20 字节。

填充用于保证任选项为 32bit 的整数倍。

12）数据（长度可变）

TCP 首部结束之后的部分

UDP 报文格式



UDP 是 User Datagram Protocol 的简称， 中文名是用户数据报协议，是一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。

1）源端口（2 字节）：发送方端口号

2）目的端口（2 字节 ）：接收方端口号

3）报文长度（2 字节）：UDP 用户数据报的总长度，以字节为单位。

4）校验和（2 字节）：检测 UDP 用户数据报在传输中是否有错，有错就丢弃。

用于校验 UDP 数据报的数字段和包含 UDP 数据报首部的“伪首部”。

伪首部，又称为伪包头（Pseudo Header）：是指在 TCP 的分段或 UDP 的数据报格式中，在数据报首部前面增加源 IP 地址、目的 IP 地址、IP 分组的协议字段、TCP 或 UDP 数据报的总长度等共12字节，所构成的扩展首部结构。此伪首部是一个临时的结构，它既不向上也不向下传递，仅仅只是为了保证可以校验套接字的正确性。



5）数据：UDP 的数据部分如果不为偶数需要用 0 填补，就是说，如果数据长度为奇数，数据长度加“1”。