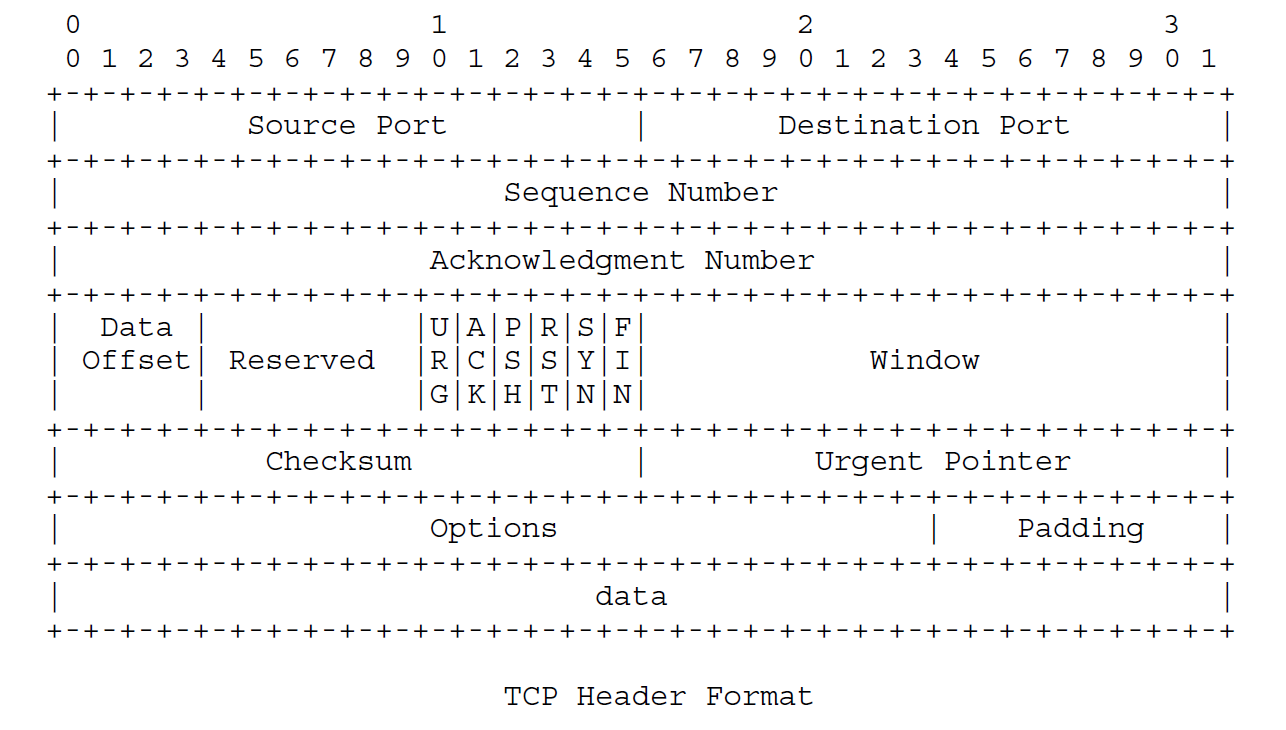
# RFC793

## 3 功能规范

### 3.1 头部格式

TCP段作为因特网数据报发送。IP报头包含多个信息字段，包括源和目标主机地址[2]。TCP头部跟在IP头部之后，提供特定于TCP协议的信息。这种划分允许存在除TCP之外的主机级协议。



源端口：16比特，源端口号；

目的端口：16比特，目的端口号；

序列号：32比特，此段中第一个数据字节的序列号（存在SYN时除外）。如果存在SYN，则序列号是初始序列号（ISN），第一个数据字节是ISN + 1。

确认号：32比特，如果设置了ACK控制位，则该字段包含该段的发送者期望接收的下一个序列号的值。建立连接后，始终会发送此连接。

数据偏移：4比特，TCP头中32位字的数目。这表示数据的起始位置。TCP头（甚至包括选项）是32位长的整数。

保留：6比特，保留供将来使用。必须为零。

控制位：6比特（从左到右）：

URG：紧急指针字段有效

ACK：确认字段有效

PSH：推送功能

RST：重置连接

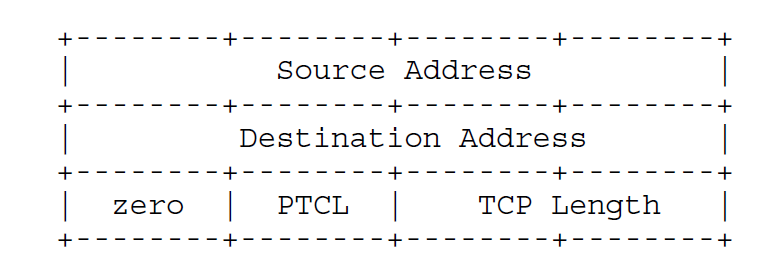
SYN：同步序列号

FIN：发送端没有更多数据

窗口：16比特，以确认字段中指示的数据字节数开始，该段的发送方愿意接收的数据字节数目。

校验和：16比特，校验和字段是标题和文本中所有16位字的一个补码和的16位补码。如果一个段包含要校验和的头和文本字节为奇数，则最后一个字节用零填充在右边，形成一个16位字用于校验和。填充值不作为段的一部分传输。在计算校验和时，校验和字段本身将替换为零。

校验和还包括一个96位伪头，在概念上作为TCP头的前缀。此伪标头包含源地址，目标地址，协议号和TCP长度。这为TCP提供了针对错误路由段的保护。此信息在Internet协议中承载，并通过TCP/IP网络接口在IP上的TCP调用的参数或结果中传输。



TCP长度是TCP报头长度加上数据的长度（这不是显式发送的数量，而是计算的），并且它不计算伪报头的12个字节。

紧急指针：16比特，该字段将紧急指针的当前值传递为该段中序列号的正偏移量。紧急指针指向紧急数据之后的字节的序列号（在RFC1122中被更正为指向紧急数据字节的序列号）。该字段仅在设置了URG控制位的段中进行解释。

选项：可变

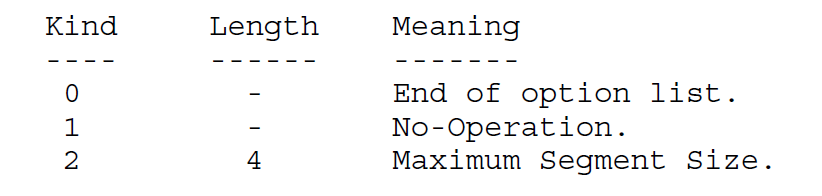
选项可能占用TCP标头末尾的空间，并且长度为8位的倍数。所有选项都包含在校验和中。选项可以从任何字节边界开始。选项格式有两种情况：

情况1：选项类型的单个字节。

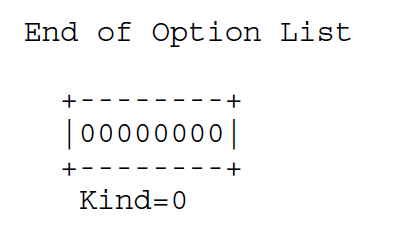
情况2：选项类型的字节，选项长度的字节和实际的选项-数据字节。

选项长度计算选项类型和选项长度的两个字节以及选项-数据字节数目。请注意，选项列表可能比数据偏移字段可能暗示的要短。超出选项结束选项的标题的内容必须是标题填充（即，零）。TCP必须实现所有选项。

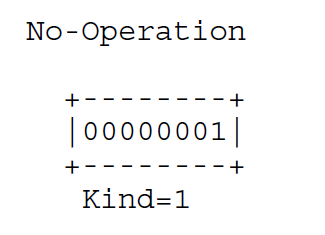
目前定义的选项包括（以字节表示的种类）：



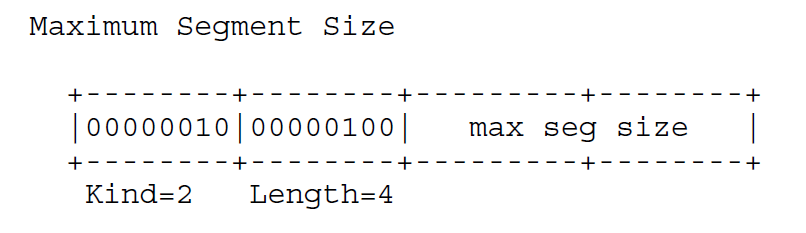
具体选项定义



此选项代码表示选项列表的结尾。根据数据偏移字段，这可能与TCP标头的末尾不一致。这在所有选项的末尾使用，而不是在每个选项的结尾处使用，并且只有在选项的末尾不与TCP头的末尾重合时才需要使用。



可以在选项之间使用该选项代码，例如，以对齐单词边界上的后续选项的开头。无法保证发件人将使用此选项，因此接收者必须准备好处理选项，即使他们不是从单词边界开始。



最大段大小选项数据：16位，如果存在此选项，则它会在发送此段的TCP上传达最大接收段大小。该字段只能在初始连接请求中发送（即，在设置了SYN控制位的段中）。如果未使用此选项，则允许任何段大小。

填充：可变，TCP头填充用于确保TCP头结束并且数据在32位边界上开始。填充由零组成。

### 3.2 术语

在我们讨论TCP的操作之前，我们需要介绍一些详细的术语。维护TCP连接需要记住几个变量。我们设想这些变量存储在称为传输控制块或TCB的连接记录中。

存储在TCB中的变量包括本地和远程套接字号，连接的安全性和优先级，指向用户的发送和接收缓冲区的指针，指向重新传输队列和当前段的指针。

另外，与发送和接收序列号有关的几个变量也存储在TCB中。

发送序列变量

SND.UNA：发送未确认的

SND.NXT：发送下一个

SND.WND：发送窗口

SND.UP：发送紧急指针

SND.WL1：用于最后一次窗口更新的段序列号

SND.WL2：用于最后一次窗口更新的段确认号

ISS：初始发送序列号

接收序列变量

RCV.NXT：接收下一个

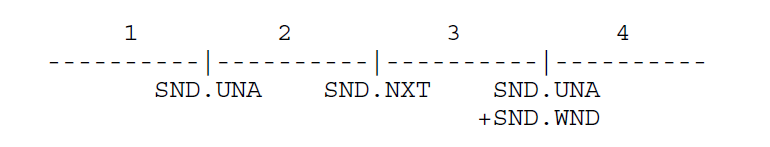
RCV.WND：接收窗口

RCV.UP：接收紧急指针

IRS：初始接收序列号

下面的图表可能有助于将这些变量中的一些关联到序列空间。

发送序列空间



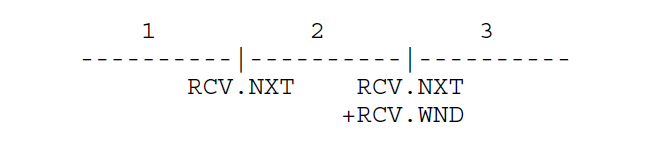
1、已确认的序列号

2、未确认数据的序列号

3、允许新数据传输的序列号

4、未来允许的序列号

接收序列空间



1、已确认的序列号

2、允许新接收的序列号

3、未来允许的序列号

在讨论中还经常使用一些变量，这些变量从当前段的字段中获取它们的值。

当前段变量

SEG.SEQ：段序列号

SEG.ACK：段确认号

SEG.LEN：段长度

SEG.WND：段窗口

SEG.UP：段紧急指针

SEG.PRC：段优先值

连接在其生命周期中通过一系列状态进行。状态是：LISTEN，SYN-SENT，SYN-RECEIVED，ESTABLISHED，FIN-WAIT-1，FIN-WAIT-2，CLOSE-WAIT，CLOSING，LAST ACK，TIME-WAIT和虚构状态CLOSED。CLOSED是虚构的，因为它表示没有TCB时的状态，因此没有连接。简言之状态的含义：

LISTEN：表示等待来自任何远程TCP和端口的连接请求。

SYN-SENT：表示在发送连接请求后等待匹配的连接请求。

SYN-RECEIVED：表示在收到并发送连接请求后等待确认连接请求确认。

ESTABLISHED：表示开放连接，接收的数据可以传递给用户。 连接的数据传输阶段的正常状态。

FIN-WAIT-1：表示等待来自远程TCP的连接终止请求，或者对先前发送的连接终止请求的确认。

FIN-WAIT-2：表示等待来自远程TCP的连接终止请求。

CLOSE-WAIT：表示等待本地用户的连接终止请求。

CLOSING：表示等待来自远程TCP的连接终止请求确认。

LAST-ACK：表示等待先前发送到远程TCP的连接终止请求的确认（其包括对其连接终止请求的确认）。

TIME-WAIT：表示等待足够的时间传递以确保远程TCP收到其连接终止请求的确认。

CLOSED：表示根本没有连接状态。

TCP连接从一个状态进展到另一个状态以响应事件。事件是用户呼叫，OPEN，SEND，RECEIVE，CLOSE，ABORT和STATUS；传入的段，特别是那些包含SYN，ACK，RST和FIN标志的段；和超时。

图6中的状态图仅说明状态变化以及导致事件和结果动作，但既不解决错误条件也不解决与状态变化无关的动作。

在后面的部分中，提供了有关TCP对事件的反应的更多细节。注意：此图仅是摘要，不得视为总规格。

