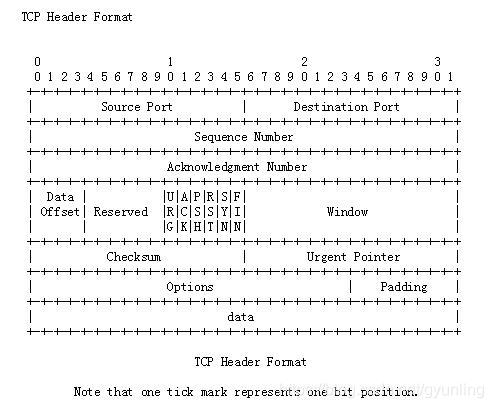
（一）前言  
       TCP 是一个基于连接的四层协议，提供全双工地，可靠地传输系统。它能够保证数据被远程主机接收。并且能够为高层协议提供flow-controlled 服务。

（二）TCP 报文格式(rfc793)

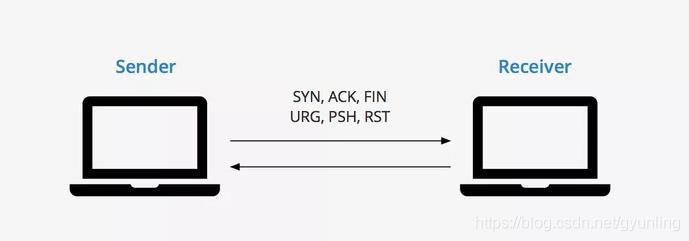


各个Field说明：

    源端口（Source Port）：长度为16 bits（2个字节）。源端口。  
    目的端口（Destination Port）：长度为16 bits（2个字节）。目的端口。  
    序列号（Sequence Number）：长度为32 bits（4个字节）。指定了当前数据分片中分配给第一字节数据的序列号。在TCP传输流中每一个字节为一个序号。如果TCP报文中flags标志位为SYN，该序列号表示初始化序列号(ISN)，此时第一个数据应该是从序列号ISN+1开始。  
    确认序列号（Acknowledgment Number）：长度为32bits（4个字节）。表示TCP发送者期望接受下一个数据分片的序列号。该序号在TCP分片中Flags标志位为ACK时生效。序列号分片的方向和流的方向同方向，而确认序列号分片方向和流方向反方向。

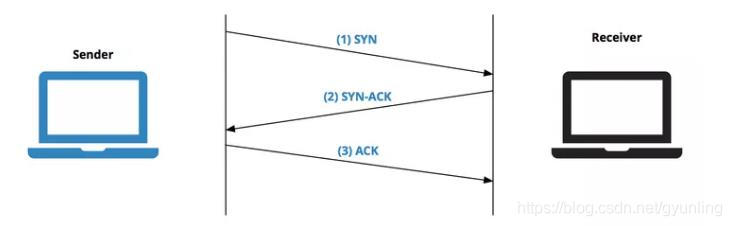
    数据偏移或首部长度（Data Offset/Header Length）: 长度为4bits。数据偏移也叫首部长度。因为首部长度实际也说明了数据区在分片中的起始偏移值。它表示TCP头包含了多少个32-bit的words。因为4bits在十进制中能表示的最大值为15，32bits表示4个字节，那么Data Offset的最大可表示15\*4=60个字节。所以TCP报头长度最大为60字节。如果options fields为0的话，报文头长度为20个字节。  
    预留字段（Reserved field）：长度为6bits。值全为零。预留给以后使用。  
    标志位(Flags): 长度为6bits。表示TCP包特定的连接状态。一个标签位占一个bit，从低位到高位值依次为FIN,SYN,RST,PSH,ACK,URG。新定义的TCP头还扩展了ECE,CWR,NS.  
    窗口（Window）：长度16bits（2个字节）。表示滑动窗口的大小，用来告诉发送端接收端的buffer space的大小。接收端buffer大小用来控制发送端的发送数据数率，从而达到流量控制。最大值为65535.  
    校验和（Checksum）：长度16bits（2个字节）。用来检查TCP头在传输中是否被修改。  
    紧急指针（Urgent pointer）：长度为16bits（2个字节）。表示TCP片中第一个紧急数据字节的指针。只有当URG标志置1时紧急指针才有效。  
    选项和填充（Option和pading）：可变长度。表示TCP可选选项以及填充位。当选项不足32bits时，填充字段加入额外的0填充。  
    数据（Data）：长度可变。用来存储上层协议的数据信息。可以为空。比如在连接建立和连接中止时。

    TCP 采用全双工模式，在连接建立后和连接中止前进行数据传输，数据传输是单向的，从发送端传输给接受端。TCP通过序列号能够保证数据被接受端接受。TCP建立连接是通过三次握手的方式来建立连接的。



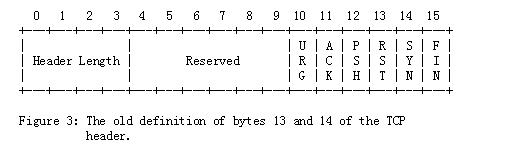
（三） TCP Flags

    TCP 在连接过程中，通过Flags标志位来表示传输过程中的连接状态。因此可以通过标志位来进行问题定位或者控制指定的连接是否提交。TCP 三次握手过程如下：

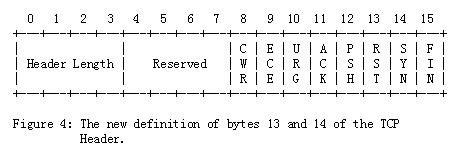


    对于旧版本的TCP头定义，Flags有6bits,新版TCP头对flags扩展了3bits。每个TCP flag对应于1bit位。所以旧版TCP头flags值有6个，新版扩展了3个值。从低位到高位分别是：FIN,SYN,RST,PSH,ACK,URG,ECE,CWR,NS。

    旧版TCP Flags字段：



    新版TCP Flags字段：



Flags值说明：

    FIN: "finished"简写。表示发送者以及发送完数据。通常用在发送者发送完数据的最后一个包中。  
    SYN: "Synchronisation"简写。表示三次握手建立连接的第一步，在建立连接时发送者发送的第一个包中设置flag值为SYN。  
    RST: "reset"简写。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。或者发送包发送到一个不是期望的                  目的主机时，接收端发送reset 重置连接标志的包。  
    PSH: "push"简写。通知接收端处理接收的报文，而不是将报文缓存到buffer中。  
    ACK: "Acknowledgment"简写。表示包已经被成功接收。  
    URG: "urgent"简写。通知接收端处理在处理其他包前优先处理接收到的紧急报文（urgent packets）。详见RFC6093。  
    ECE: "ECN-Echo"简写。ECN表示Explicit Congestion Notification。表示TCP peer有ECN能力。详见RFC3168。  
    CWR: "Congestion Window Reduced"简写。发送者在接收到一个带有ECE flag包时，将会使用CWR flag。 详见RFC3168。  
    NS: "nonce sum"简写。该标签用来保护不受发送者发送的突发的恶意隐藏报文的侵害。详见 RFC 3540。

（四） 使用tcpdump抓取响应flag值得报文

    因为TCP Flags 位于TCP头的第14个字节中。所有可以通过如下命令进行抓取：

    抓取FIN包: tcpdump -i eth0 "tcp[13] & 1"  -ennnv  
    抓取SYN包: tcpdump -i eth0 "tcp[13] & 2" -ennnv  
    抓取RST包: tcpdump -i eth0 "tcp[13] & 4" -ennnv  
    抓取PSH包: tcpdump -i eth0 "tcp[13] & 8" -ennnv  
    抓取ACK包: tcpdump -i eth0 "tcp[13] & 16" -ennnv  
    抓取URG包: tcpdump -i eth0 "tcp[13] & 32"  -ennnv

参考：  
    https://tools.ietf.org/html/rfc793  
    https://tools.ietf.org/html/rfc3168  
    https://tools.ietf.org/html/rfc3540