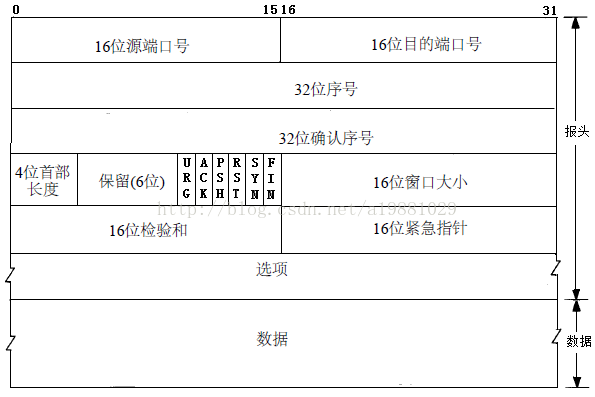
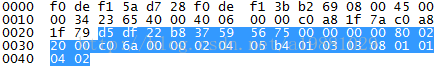
TCP（Transmission Control Protocol）传输控制协议是一种面向连接的、可靠的、基于字节流的传输层协议

TCP报文格式：



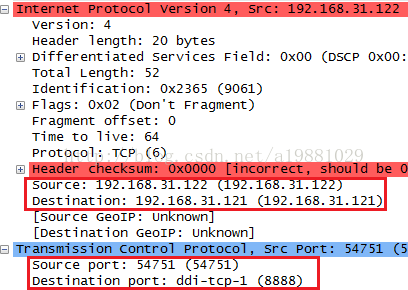


****源端口号****（2字节）：

    d5 df（54751）

****目的端口号****（2字节）：

    22 b8（8888）



TCP报头中的源端口号和目的端口号同IP数据报中的源IP与目的IP唯一确定一条TCP连接

****序号****（4字节）：

    37 59 56 75

    用来标识TCP发端向TCP收端发送的数据字节流

****确认序号****（4字节）：

    由于该报文为SYN报文，ACK标志为0，故没有确认序号（ACK标志为1时确认序号才有效）

    一旦连接建立，该值将始终发送（同ACK标志）

****首部长度****（4位）：报文头长度（单位：位）/32

    1000（转化为10进制为8，8\*32/8 = 32，该报文报头长度为32个字节）

    存在该字段是因为TCP报头中任选字段长度可变

    报头不包含任何任选字段则长度为20字节；4位所能表示的最大值为1111，转化为10进制为15，15\*32/8 = 60，故报头最大长度为60字节

****标志位****（12位）：

    0000 00010010

****Reserved****：

    000~ ~~~~~~~~

****ECN（Explicit Congetsion Notification）****：

    ~~~0 ~~~~~~~~ = N / NS / Nonce Sum：有效排除潜在的ECN滥用，RFC 3540

    ~~~~ 0~~~~~~~ = C / CWR（Congestion Window Reduced）：拥塞窗口减少标志

    ~~~~ ~0~~~~~~ = E / ECE / ECN-Echo：ECE / ECN标志

****Control Bits****：

    ~~~~ ~~0~~~~~ = U / Urgent：紧急指针有效性标志

    ~~~~ ~~~1~~~~ = A / Acknowledgment：确认序号有效性标志，一旦一个连接建立起来，该标志总被置为1，即除了请求建立连接报文（仅设置Syn标志位为1），其它所有报文的该标志总为1

    ~~~~ ~~~~0~~~ = P / Push：Push标志（接收方应尽快将报文段提交至应用层）

    ~~~~ ~~~~~0~~ = R / Reset：重置连接标志

    ~~~~ ~~~~~~1~ = S / Syn：同步序号标志

    ~~~~ ~~~~~~~0 = F / Fin：传输数据结束标志

****窗口大小****（2字节）：TCP流量控制通过连接的每一端声明窗口大小进行控制（接收缓冲区大小）

    20 00（00100000 00000000）= 8192

    由于2字节能够表示的最大正整数为65535，故窗口最大值为65535

****检验和****（2字节）：检验和覆盖整个TCP报文段；强制字段，由发送端计算存储，由接收端进行验证

    2e 2f

****紧急指针****（2字节）：当Urgent标志置1时，紧急指针才有效

    00 00

****任选字段****（0 - 40字节）：

    每个选项格式如下：

|  |  |  |
| --- | --- | --- |
| 选项类型 | 选项总长度 | 选项内容 |

    说明如下：

|  |  |  |
| --- | --- | --- |
| ****说明**** | ****占用字节数**** | ****值**** |
| 选项类型 | 1 | 0-255 |
| 选项总长度 | 1 | length |
| 选项内容 | length - 2 |  |

    可选选项如下：

|  |  |  |  |
| --- | --- | --- | --- |
| ****Kind**** | ****Length**** | ****Description**** | ****References**** |
| 0 | 1 | End of option list. | RFC 793 |
| 1 | 1 | No operation. | RFC 793 |
| 2 | 4 | MSS, Maximum Segment Size. | RFC 793 |
| 3 | 3 | WSOPT, Window scale factor. | RFC 1323 |
| 4 | 2 | SACK permitted. | RFC 2018 |
| 5 | Variable. | SACK. | RFC 2018, RFC 2883 |
| 6 | 6 | Echo. (obsolete). | RFC 1072 |
| 7 | 6 | Echo reply. (obsolete). | RFC 1072 |
| 8 | 10 | TSOPT, Timestamp. | RFC 1323 |
| 9 | 2 | Partial Order Connection permitted. | RFC 1693 |
| 10 | 3 | Partial Order service profile. | RFC 1693 |
| 11 | 6 | CC, Connection Count. | RFC 1644 |
| 12 | 6 | CC.NEW | RFC 1644 |
| 13 | 6 | CC.ECHO | RFC 1644 |
| 14 | 3 | Alternate checksum request. | RFC 1146 |
| 15 | Variable. | Alternate checksum data. | RFC 1146 |
| 16 |  | Skeeter. |  |
| 17 |  | Bubba. |  |
| 18 | 3 | Trailer Checksum Option. |  |
| 19 | 18 | MD5 signature. | RFC 2385 |
| 20 |  | SCPS Capabilities. |  |
| 21 |  | Selective Negative Acknowledgements. |  |
| 22 |  | Record Boundaries. |  |
| 23 |  | Corruption experienced. |  |
| 24 |  | SNAP. |  |
| 25 |  |  |  |
| 26 |  | TCP Compression Filter. |  |
| 27 | 8 | Quick-Start Response. | RFC 4782 |
| 28 | 4 | User Timeout. | RFC 5482 |
| 29 |  | TCP-AO, TCP Authentication Option. | RFC 5925 |
| 30 |  | MPTCP |  |
| 31 - 252 |  |  |  |
| 253 |  | RFC3692-style Experiment 1. | RFC 4727 |
| 254 |  | RFC3692-style Experiment 2. | RFC 4727 |
| 255 |  |  |  |

    {02 04 05 b4} {01} {03 03 08} {01} {01} {04 02}

    MSS + No operation + WSOPT + No operation + No operation + SACK permitted

参考资料：

[www.networksorcery.com/enp/protocol/tcp.htm](http://www.networksorcery.com/enp/protocol/tcp.htm)