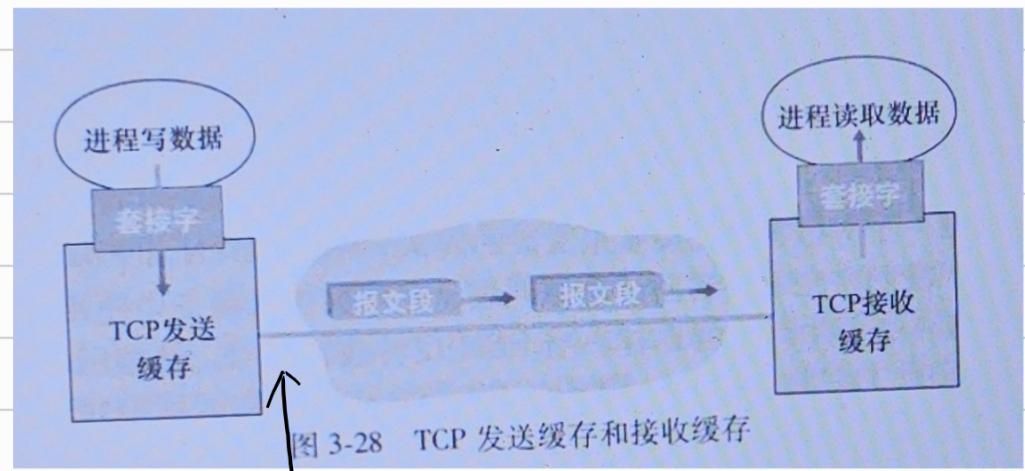


传输层

面向连接的运输 TCP

→ 先握手
全双工服务

将数据块配上 TCP 封装



TCP 报文段

TCP 报文结构

多端口，多连接

可靠的数据传输服务

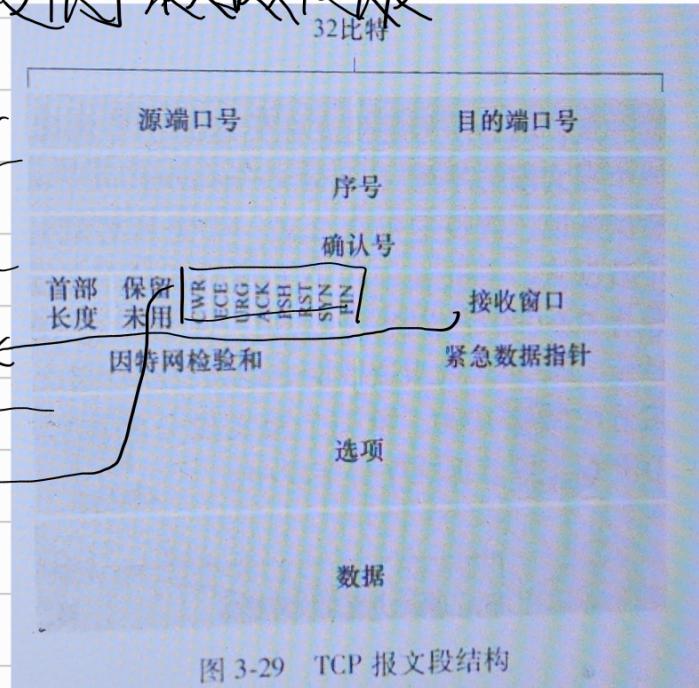
用于流量控制、按序接收方接受的字节数量

发送和接收方协商最大报文段长度 MSS

本段字节：

受限于最大报文段长度

32 比特



序号和确认号

序号：

→ TCP 把数据看成字节流

→ 序号就是该报文段中第一个字节的编号

例

500000 字节的文件

MSS 为 1000 字节

第一个报文段包含 0-999 字节，序号 = 0

第二个报文段包含 1000-1999 字节，序号 = 1000

第三个报文段包含 2000-2999 字节，序号 = 2000

确认号：

接收：已收到 ... 期望 ...

发送确认号，→ 提供累积确认

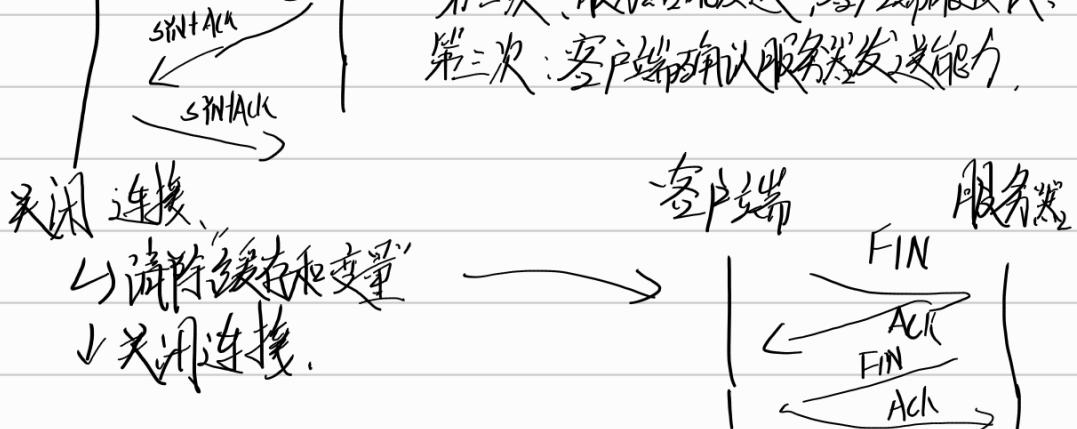
TCP 连接管理

客户端 服务器

SYN 报文

第一次：客户端能发送，服务器能接收

第二次：服务器能发送，客户端能接收



SYN洪泛攻击

攻击原理：

在TCP三次握手中，服务器收到SYN报后，会为连接分配资源进入半连接状态，等待客户端的ACK。

DOS/DDoS攻击

如客户端不回应ACK，服务器就会长时间保持连接，占用资源。

攻击者可以发送大量伪造的SYN报文，却不完成后续握手，导致服务器资源耗尽。

防御措施：SYN Cookie

思路：服务器在收到SYN时不立即分配资源，不记录状态。

工作方式：

1. 收到SYN生成一个Cookie（通过源IP、端口、时间戳，服务器私钥计算）
2. 服务器把这个Cookie编译进SYN+ACK的序号字段发给客户端
3. 如果客户端是真实的，会返回ACK，其中确认号包含Cookie
4. 服务器验证Cookie合法性后，再分配资源