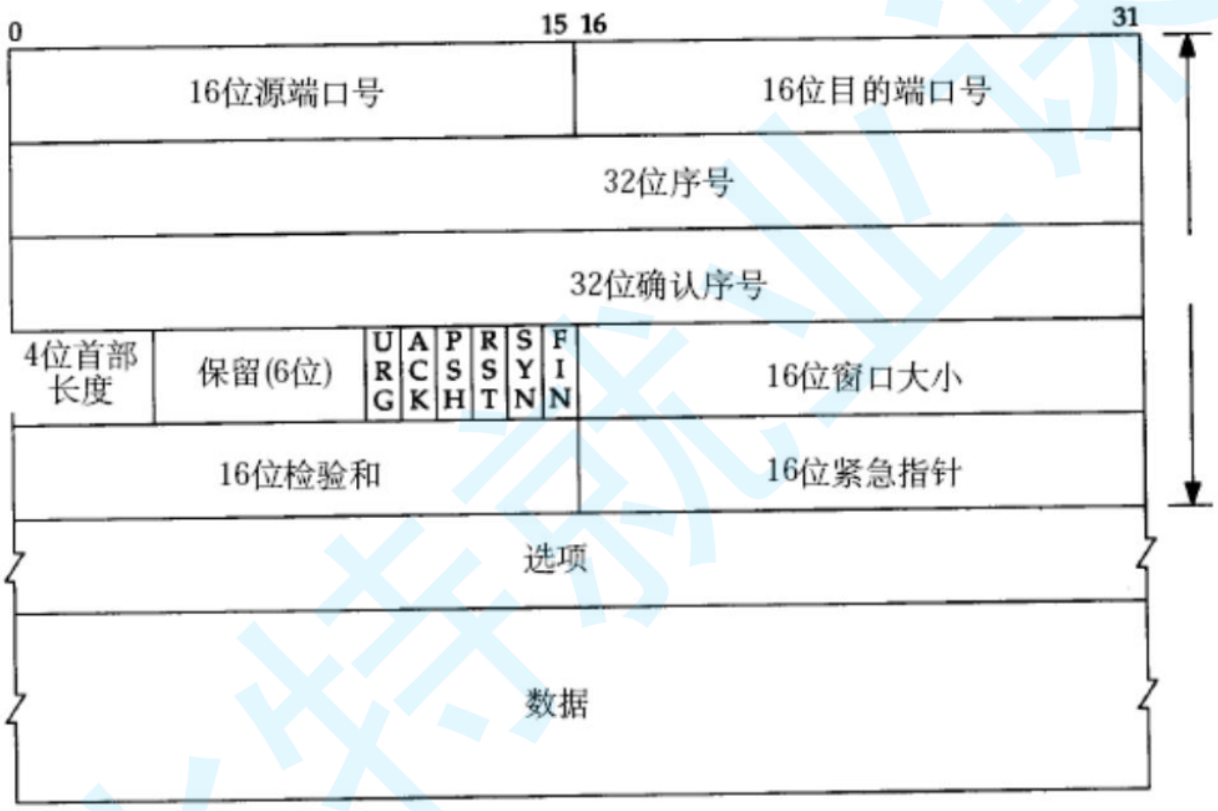
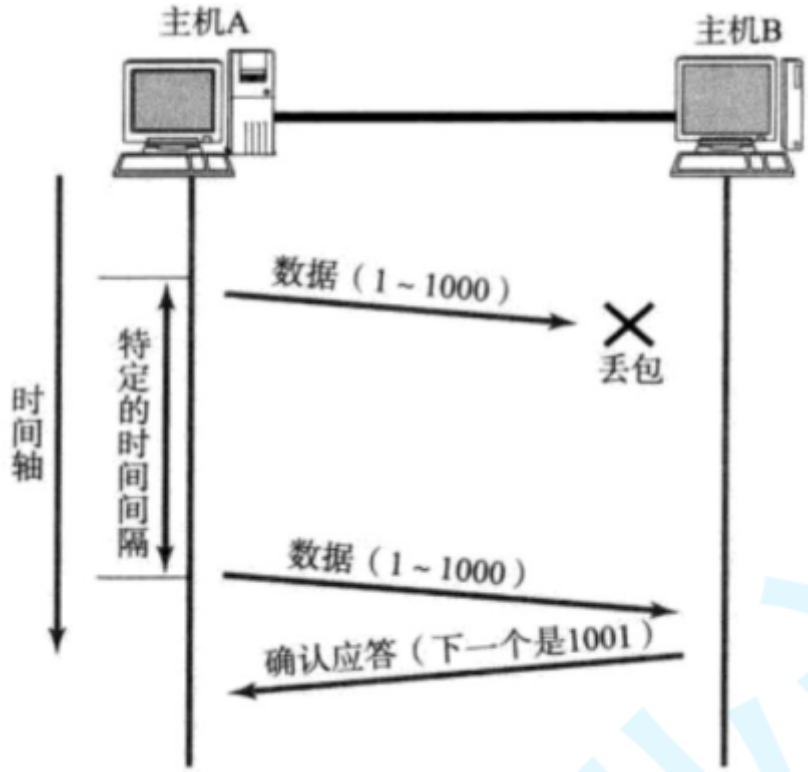
1. Tcp协议格式



- 源/目的端口号: 表示数据是从哪个进程来, 到哪个进程去;
- 4 位 TCP 报头长度: 表示该 TCP 头部有多少个 32 位 bit(有多少个 4 字节); 所以TCP 头部最大长度是 15 * 4 = 60
- 6位标记位:
    - URG: 紧急指针是否有效
    - ACK: 确认号是否有效
    - PSH: 提示接收端应用程序立刻从 TCP 缓冲区把数据读走
    - RST: 对方要求重新建立连接; 我们把携带 RST 标识的称为复位报文段
    - SYN: 请求建立连接; 我们把携带 SYN 标识的称为同步报文段
    - FIN: 通知对方, 本端要关闭了, 我们称携带 FIN 标识的为结束报文段

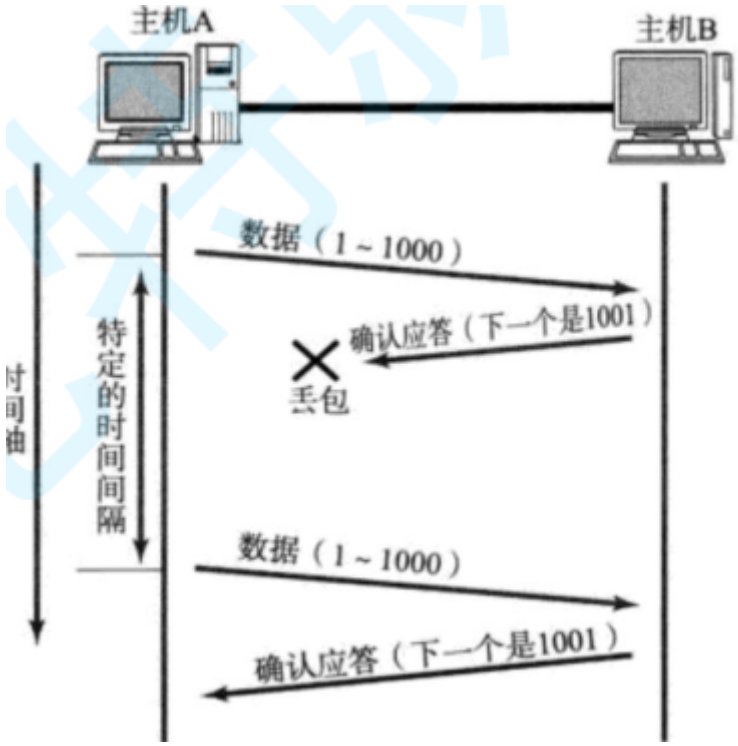
2. 超时重传机制

数据丢失的情况:



- 主机 A 发送数据给 B 之后, 可能因为网络拥堵等原因, 数据无法到达主机 B;
- 如果主机 A 在一个特定时间间隔内没有收到 B 发来的确认应答, 就会进行重发;

确认应答丢失的情况:



因此主机 B 会收到很多重复数据. 那么 TCP 协议需要能够识别出那些包是重复的包, 并且把重复的丢弃掉.

这时候我们可以利用前面提到的序列号, 就可以很容易做到去重的效果.那么, 如果超时的时间如何确定?

TCP 为了保证无论在任何环境下都能比较高性能的通信, 因此会动态计算这个最大超时时间.

- Linux 中(BSD Unix 和 Windows 也是如此), 超时以 500ms 为一个单位进行控制, 每次判定超时重发的超时时间都是 500ms 的整数倍.
- 如果重发一次之后, 仍然得不到应答, 等待 2*500ms 后再进行重传.
- 如果仍然得不到应答, 等待 4*500ms 进行重传. 依次类推, 以指数形式递增.
- 累计到一定的重传次数, TCP 认为网络或者对端主机出现异常, 强制关闭连接

3. 链接管理机制