合肥工业大学

计算机网络

课程报告

报告题目	浅谈 TCP 协议中的异常连接释放请求
学　　号	2019216864
学生姓名	吴忠恒
专业班级	物联网工程 19-1 班
指导教师	周健

2022 年 11 月 20 日

目录

1 **引言** 1
1.1 TCP 简介 1
1.2 TCP 报文格式 1

2 TCP/IP **协议连接管理** 3
2.1 建立连接 3
2.2 释放连接 4

3 TCP **协议异常连接释放** 5
3.1 双方同时发出释放请求，又同时发出同步确认 6
3.2 A/B 连接已连接，B 又收到 A 迟到的释放请求 7
3.3 A/B 连接已连接，B 又收到 A 迟到的释放确认 8
3.4 A/B 连接已连接，B 又收到 A 迟到的释放请求和释放确认 8

4 **总结** 9

A **附录一** 10

1 引言

1.1 TCP 简介

TCP 协议，即传输控制协议的主要作用是在不可靠的网络上为应用层提供面向连接的，端到端的可靠字节流服务。从需要网络通信的应用进程上来看，TCP 协议为其屏蔽了底层的通信网络，提供了一个端到端的可靠信道。

不同于 TCP/IP 协议的任何一层，TCP 的运行机制具有诸多繁杂的细节。这是由其下层 IP 协议的不可靠导致的。由于一个 IP 分组从发送端到接收端需要经过多个网络，这些网络提供的服务和性能各不相同，在传输的过程的过程中很容易出现丢包，出错，延迟，失序，丢失，重复等异常情况。同时，IP 协议只提供尽力而为的无连接服务，也就是说，IP 协议并不会对上述的异常加以纠正。于是 TCP 就要在 IP 协议提供的不可靠服务上实现可靠服务。

1.2 TCP 报文格式

在 TCP 中传递数据的形式是 TCP 报文段。一个 TCP 报文段由 20 个字节的头部，一个可选部分和一个用户数据部分组成。需要注意的是 TCP 的报文长度不是无限的，一方面 TCP 报文长度受到 IP 报文长度 $2^{16}-1=65535$ 个字节的限制；另一方面，网络的数据报传输存在上线，也被称为最大传输单元。在协议实现中，通常报文段的大小尤其上层的应用层决定，其最大程度被成为 MSS。MSS 在 TCP 通信时双方的通信实体协商决定，常用的默认值为 1500 字节，536 字节和 512 字节。

图 1.1 TCP 报文段格式

TCP 报文具体格式如图 1.1所示。各字段的含义如下。

- 源端口和目的端口字段

  端口是传输层与应用层的服务接口。传输层的复用和分用功能都要通过端口才能实现。

- 序号字段

  序号字段的值则指的是本报文段所发送的数据的第一个字节的序号。TCP 协议中的流量控制，拥塞控制等机制均依赖则报文首部的序号。

- 确认号字段

  是期望收到对方的下一个报文段的数据的第一个字节的序号。如果没有确认好，在流量控制环节，发送方就有可能重复发送报文段，导致数据重复。

- 控制标志

  1. URG 是紧急标记位，当 URG=1 时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据，应尽快传送
  2. ACK 是确认报文标志，只有当 ACK=1 时确认号字段才有效。当 ACK 0 时，确认号无效
  3. PSH 标志表明 TCP 通信中的目标段必须尽快发送数据
  4. RST 是复位标志。当 TCP 连接发生故障时，将此标志置为 1，通知通信双方实现重新同步。
  5. SYN=1 时表明该报文为发起连接请求的控制报文。
  6. FIN=1 时表明该报文为发起连接释放请求的控制报文。

- 窗口字段

  该字段用来让对方设置发送窗口的依据，是滑动窗口等基于窗口的流量控制机制的基础。

- 检验和

  检验和字段检验的范围包括首部和数据这两部分。在计算检验和时，要在 TCP 报文段的前面加上 12 字节的伪首部。通过计算该校验和，TCP 实现了对报文数据的差错控制

- 可选字段

  可选字段提供了相应的扩展机制，用于实现除 TCP 首部以外的拓展功能

2 TCP/IP 协议连接管理

TCP 是一种面向连接的运输协议，在数据传输之前必须创建连接，在数据传输结束后必须释放连接，因此，TCP 连接管理主要在于连接建立和连接释放两个方面。TCP 在连接过程中采用的是客户端/服务器端模式，该模式是一个不对成的过程，，TCP 连接的一方处于被动状态，一方处于主动状态。主动要求建立连接的主机和被动的主机经过一系列消息交换，建立一条点对点，完全双工的信道。

2.1 建立连接

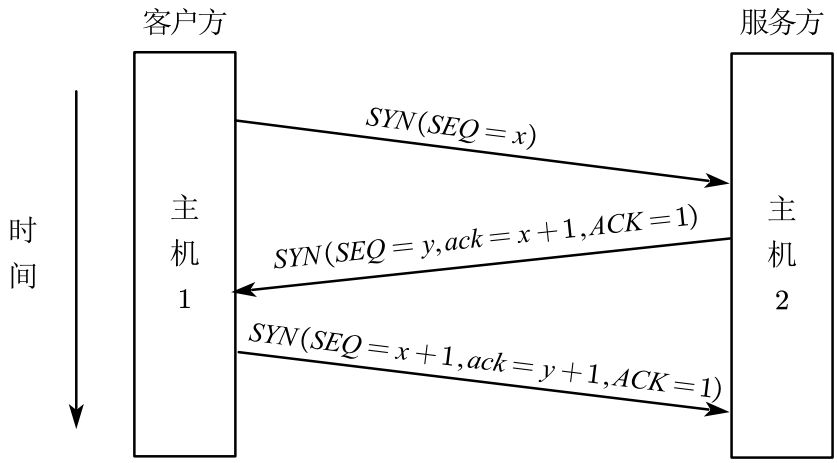

图 2.1 TCP 三次握手

TCP 采用名为三次握手的连接机制建立连接，过程如图 2.1。

- 第一次握手

  客户端到服务器。客户端向服务器提出连接建立请求，即发出同步请求报文。这个报文不包含任何用户数据，只是把 SYN 置为 1，ACK 置为 0，顺序号为 x，表明报文段为发起请求报文。

- 第二次握手

  服务器到客户端。服务器收到客户端的连接请求后，如果条件合适，就会向客户端发出同意建立连接的同步确认报文。该报文 SYN=1，顺序号为 y，表明这是个连接建立控制报文；ACK 标志位为 1，确认号字段 x+1，表明确认对方的请求。

- 第三次握手

客户端到服务器。客户端在收到服务器的同步确认报文后，向服务器发出确认报文。当服务器收到来自客户端的确认报文后，连接即被建立。此时的报文确认位为 1，表明这是确认报文；表明；SYN=0 表明这个确认可以直接开始传递数据。

2.2 释放连接

TCP 连接的释放过程基于四次挥手的释放机制，其流程如下：

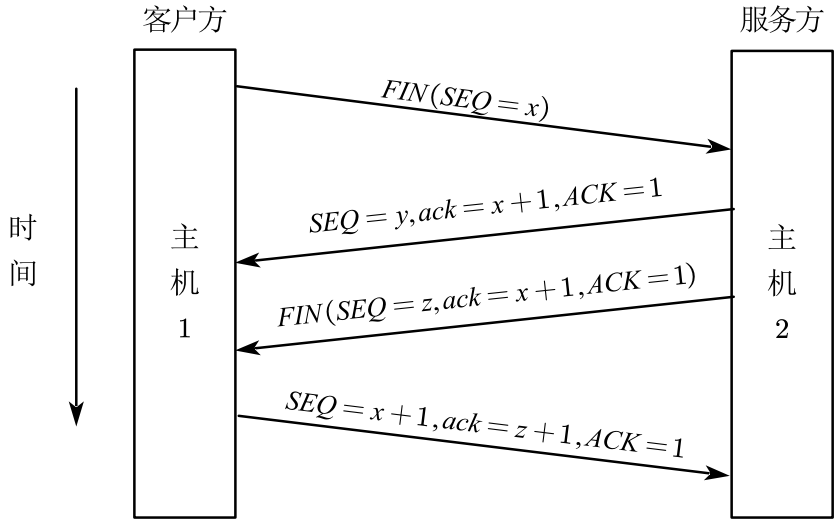

图 2.2 TCP 四次挥手

- 第一次:

  客户端到服务器。客户端向服务器发出一个连接释放报文。

- 第二次:

  服务器到客户端。服务器收到客户端的释放连接请求后，向客户端发出确认报文。

- 第三次:

  服务器到客户端。服务器在发送完最后的数据后，向客户端发出连接释放确认报文。

- 第四次:

  客户端到服务器。客户端在收到服务器连接释放报文后，向服务器发出确认报文。

3 TCP 协议异常连接释放

一个 TCP 连接在它的生命周期内会有不同的状态。

下图 3.1说明了 TCP 连接可能会有的状态，以及基于事件的状态转换。事件中有的是应用程序的操作，有的是接收到了网络发过来的请求。红线表明客户端的状态变迁路线；蓝色表明服务器端状态变迁路线；黑色的箭头则是异常状态变化。

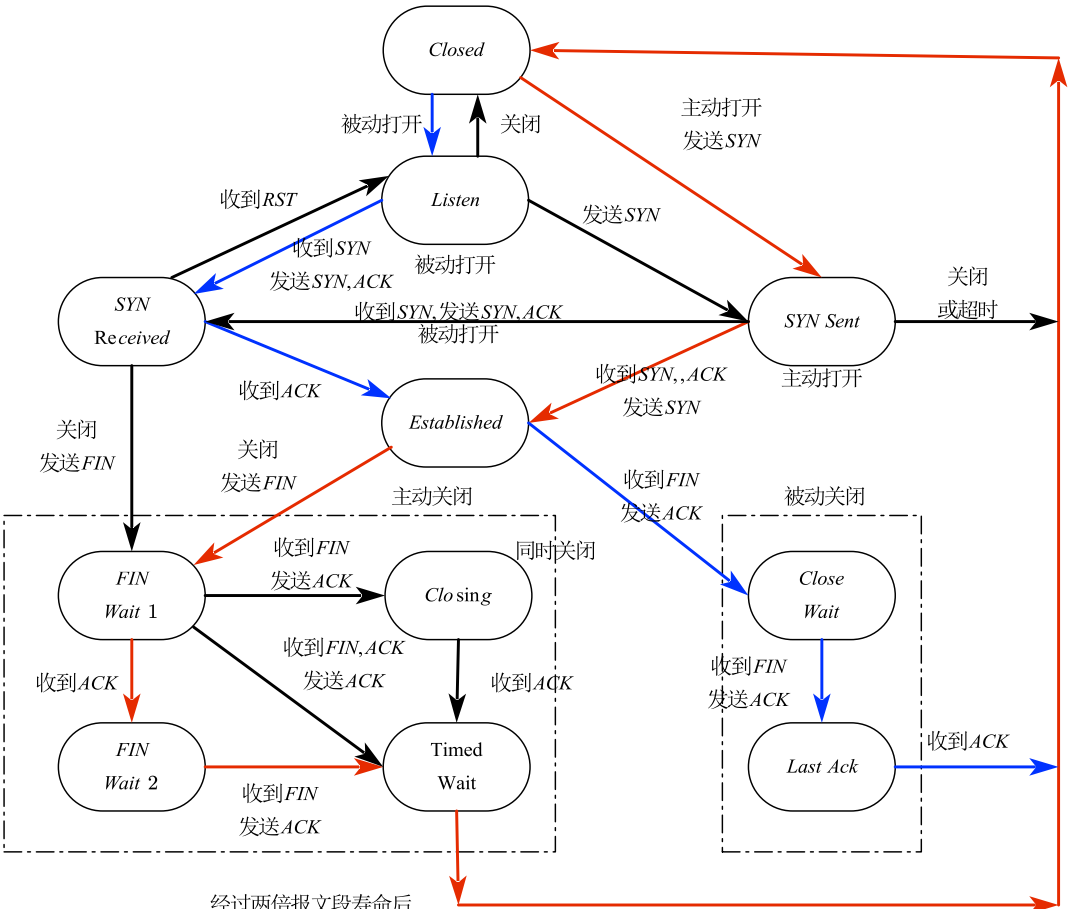

图 3.1 TCP 状态机

图中的各种状态如下表 A.1所示：

状态	负责内容
LISTEN	等待来自远程 TCP 应用程序的请求
SYN-SENT	发送连接请求后等待来自远程端点的确认。TCP 第一次握手后客户端所处的状态

续表

状态	负责内容
SYN-RECEIVED	该端点已经接收到连接请求并发送确认，该端点正在等待最终确认。TCP 第二次握手后服务端所处的状态
ESTABLISHED	代表连接已经建立起来了。这是连接数据传输阶段的正常状态
FIN-WAIT-1	等待来自远程 TCP 的终止连接请求或终止请求的确认
FIN-WAIT-2	在此端点发送终止连接请求后，等待来自远程 TCP 的连接终止请求
CLOSE-WAIT	该端点已经收到来自远程端点的关闭请求，此 TCP 正在等待本地应用程序的连接终止请求
CLOSING	等待来自远程 TCP 的连接终止请求确认
LAST-ACK	等待先前发送到远程 TCP 的连接终止请求的确认
TIME-WAIT	等待足够的时间来确保远程 TCP 接收到其连接终止请求的确认

表 3.1　TCP **状态表**

由于丢失报文会在重传计时器结束后被重传，且出错报文会被校验机制拒绝。因此丢失报文和出错报文并不会导致连接被异常释放。因此我们仅需讨论延迟，失序和重复等情况下的异常报文是否会导致连接被异常释放。

下文中出现的 DR,DC 等缩写来源于运输协议数据单元 (TPDU)，见附录一

3.1　双方同时发出释放请求，又同时发出同步确认

这种情况虽然发生的可能性极小，但是是确实存在的，TCP 也特意设计了相关机制，使得在这种情况下双方能正常释放连接。

双方同时发出连接释放报文 DR x、DR y，并进入 FIN-WAIT-1 状态；假设实体 A 先收到 DR 报文，在收到对方的报文之后，发送 DC 确认报文，并进入 CLOSING 状态；实体 B 后受到 DR 报文，同样进入 CLOSING 状态，发送 DC 确认报文。假设实

体 A 先收到对方的 DC 报文，在收到对方的确认报文后，进入 TIME-WAIT 状态，等待 2MSL 之后关闭 A 到 B 方向连接。后收到 DC 报文的实体 B，同理，等待 2MSL 之后关闭 B 到 A 方向连接。过程如图 3.2所示：

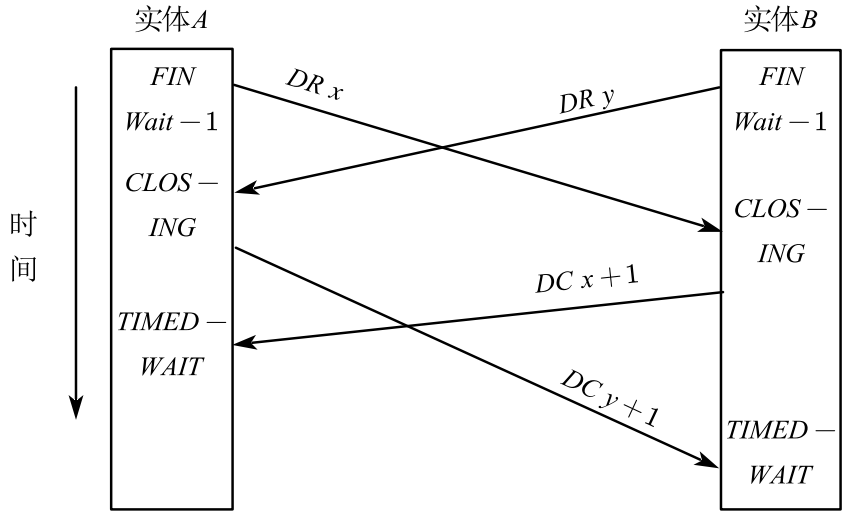

图 3.2　同时释放连接

需要注意的是，这个时候虽然不用再次发送确认报文并确认对方收到，双方仍需等待 2MSL 之后再关闭连接，是为了防止“已失效的连接请求报文段”的影响。

3.2　A/B 连接已连接，B 又收到 A 迟到的释放请求

假设实体 A 有一个 DR x, 由于延迟，在连接建立后达到实体 B。由于运输实体 B 没有收到确认报文，此时仍然处于 ESTABLISHED 状态。在收到 DR x 报文后，运输实体 B 即用 DC y 给出确认，运输实体 A 在检查时发现，自己并没有申请连接释放，判定该报文为非法报文，发出 REJ y 报文拒绝该确认报文。运输实体 B 在收到来自 A 的拒绝报文后，发出 REJ x 报文表明拒绝异常的连接释放请求。过程如图 3.3所示。

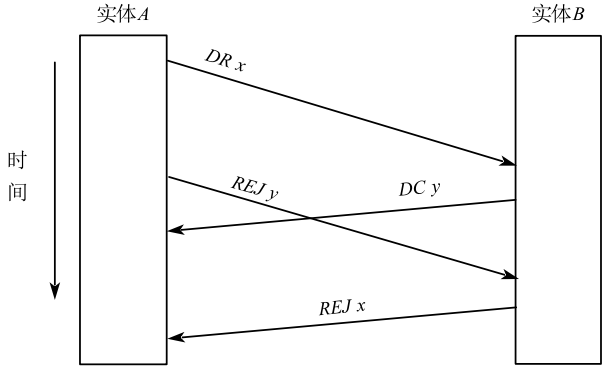

图 3.3　迟来连接释放请求

3.3 A/B 连接已连接，B 又收到 A 迟到的释放确认

假设实体 A 有一个 DC x+1, 由于延迟，在连接建立后达到实体 B。运输实体 B 在检查顺序号时发现，这是由于延迟而引起的，发出 REJ x+1 报文拒绝该确认报文。过程如图 3.4所示。

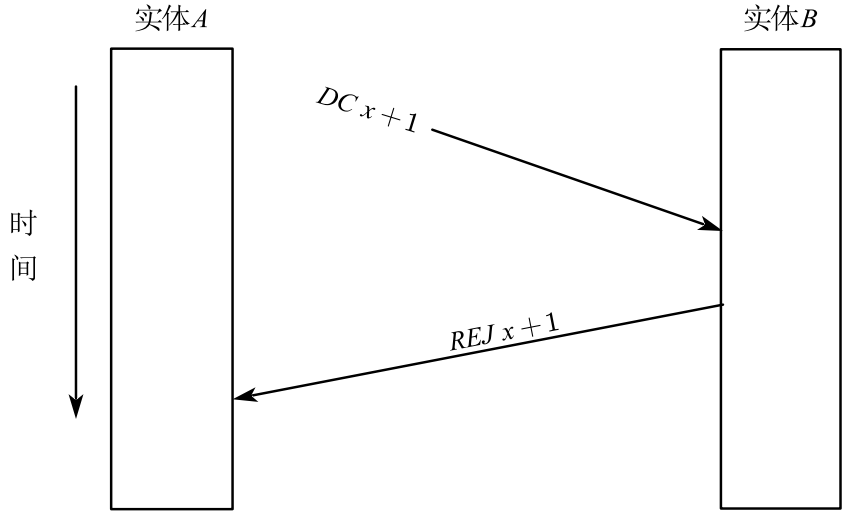

图 3.4 迟来释放确认请求

3.4 A/B 连接已连接，B 又收到 A 迟到的释放请求和释放确认

假设实体 A 有一个 DR x, 由于延迟，在连接建立后达到实体 B。由于运输实体 B 没有收到确认报文，此时仍然处于 ESTABLISHED 状态。在收到 DR x 报文后，运输实体 B 即用 DC y 给出确认。

然后实体 A 有一个 DC x+1 报文, 由于延迟，在此时达到实体 B。运输实体 B 在检查顺序号时发现，这是由于延迟而引起的，发出 REJ x+ 1 报文拒绝该确认报文。

当上述过程中所讲的 DC y 报文被 A 收到后，运输实体 A 在检查时发现，自己没有申请连接释放，判断该报文为非法报文，发出 REJ y 报文拒绝该确认报文，拒绝异常的连接释放请求。过程如图 3.5所示。

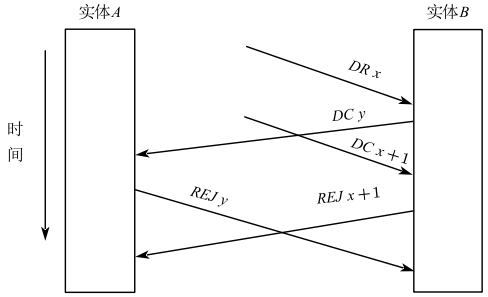

图 3.5 迟来释放请求和释放确认

4 总结

从讨论的结果上看，三次握手的 TCP 连接释放在不可靠的网络环境下同样具有强的健壮性。

在上述讨论中对于异常报文的检测，关键之处都在于对 ACK 报文的合法性识别。在 TCP 连接释放机制中，TCP 连接释放的 ACK 段就是为了实现连接“稳妥关闭”的目标, 但实际上这种稳妥性是不能仅通过 ACK 段来保证的。因此 TCP 连接释放进一步引入了超时机制，即在发送 FIN 段后即启动超时计时器，在超时时间间隔内如不能收到 ACK 段，则或重发 FIN 段，或强行释放连接。

此外, 为了防止连接释放后这次连接在网络中残留的 TCP 报文段 (可能是数据段、FIN 段或 ACK 段等) 对双方可能重新建立的连接造成干扰, 连接释放的主动方在完全释放连接前需要等待两倍最大报文段生命期 (maximumsegmentlifetime, MSL) 时间, 确保这次要释放的连接的 TCP 报文段 (特别是 FIN 段和对 FIN 段的 ACK 段) 完全从网络中消失, 才能最终释放连接。

A 附录一

状态	负责内容
CR	运输连接请求，要求与对等运输实体建立运输连接
CC	确认, 对 CR 的确认
DR	释放请求，要求释放与对等运输实体之间的运输连接
DC	确认，对 DR 的确认
DT, DATA	数据，一个运输实体向对等运输实体发送用户数据
AK, ACK	确认，对数据 TPDU 的认可
REJ, REJECT	拒绝，拒绝接受请求或数据 TPDU

表 A.1 **传输协议的** TPDU