## 一、各种非正常连接释放及可能引起的后果

1. 双方同时发出连接释放请求，又同时发送确认

在TCP连接释放的正常情况下，双方同时发出连接释放请求，并且同时发送确认（FIN/ACK）是一种合法的情况。这种情况通常是指两个端点（例如，两台计算机）准备关闭连接，彼此之间都发送了连接释放请求，并同时收到对方的释放请求，最后双方都发送了确认，完成连接的正常关闭。一方（主机A）发送连接释放请求（FIN）给另一方（主机B）。同时，另一方（主机B）也发送连接释放请求（FIN）给主机A。双方同时收到对方的连接释放请求，然后分别发送确认（ACK）给对方。双方都成功接收到对方的确认，连接正常释放。连接进入CLOSED状态。

这种情况下，双方的释放请求和确认交叉进行，确保彼此都知道对方希望关闭连接。这是TCP协议的设计考虑，以确保双方都有机会完成数据的传输和连接的正常释放。

在实际应用中，这种情况下的连接释放是常见的，而且是TCP协议设计的一部分，确保连接能够在双方都明确表达关闭意愿的情况下正常终止。

2.若是双方同时发出连接释放请求，同时发送的确认中发生丢失。

若只有一方丢失，则双方一定不是同时关闭。比如如果客户端发给服务器的确认报文丢失。首先不影响客户端收到服务器发送的确认报文，客户端在收到确认报文之后，会立即释放连接。而服务器虽然收不到确认报文，但是因为它发送过确认报文，他会在发送过确认报文之后的2MSL的时间后，释放连接。最终，客户机和服务器完成TCP连接的释放。

若双方均丢失确认报文。则服务器和客户端均会在发送过确认报文后，等待2MSL时间后，释放连接。最终，服务器和客户机完成TCP连接释放。

3. 若是双方同时发出连接释放请求，同时关闭后，收到确认报文

当双方同时发出连接释放请求且同时关闭后，如果双方都成功接收到对方的确认报文，那么连接正常释放，通信双方的连接进入CLOSED状态。这是正常的TCP连接释放过程，通常不会引起问题。一方（例如，主机A）发送连接释放请求（FIN）给另一方（主机B）。同时，另一方（主机B）也发送连接释放请求（FIN）给主机A。双方都接收到对方的连接释放请求，然后分别发送确认（ACK）给对方。双方都成功接收到对方的确认，连接正常释放。连接进入CLOSED状态。

4. 在B已经关闭连接，A还没有关闭连接，正处在TIME\_WAIT阶段，已失效的连接请求字段到达A。

此时特指A服务器，B特指客户机。此时服务器会拒绝，因为此刻还没有和客户机完全释放连接，服务器还没有释放连接。这里不能看seq的序号大小，因为也可能时新的连接请求，每一次建立连接请求的时候seq开始的值是随机的。如果是新的连接，超过设定等待时间后，客户机会重新发送连接请求，此时若服务器等待了2MSL后，已经释放了连接。可以再接受新的连接请求。总之，不会造成混乱。

5. 当客户端关闭并发送FIN报文的时候后，同收到FIN+ACK报文

由于报文的seq大小，因为v<w,拒收旧报文，并不影响客户机发送确认服务器释放的报文，当服务器收到确认报文，会释放连接。而服务器在等待一段时间后，也会释放连接。至此服务器和客户机间的连接得到释放。

当客户端关闭并发送FIN报文时，服务器端会收到这个FIN报文，并向客户端发送一个确认的FIN+ACK报文。这是TCP连接正常释放的一部分，通常包含以下步骤：

客户端发送FIN报文： 客户端在关闭连接时，发送一个带有FIN（Finish）标志的TCP报文给服务器端，表示客户端不再发送数据。

服务器端收到FIN报文： 服务器端接收到客户端的FIN报文后，意识到客户端不再发送数据，但服务器端仍可以向客户端发送数据。

服务器端发送FIN+ACK报文： 服务器端向客户端发送一个带有FIN和ACK标志的TCP报文，表示服务器端也准备关闭连接，并确认客户端的FIN请求。

客户端收到FIN+ACK报文： 客户端收到服务器端的FIN+ACK报文后，确认服务器端也希望关闭连接。

客户端发送ACK报文： 客户端发送一个带有ACK标志的TCP报文给服务器端，表示客户端确认接收到服务器端的FIN+ACK，连接正式关闭。

这个过程确保了双方都有机会完成数据的传输并安全地关闭连接。每个FIN报文和FIN+ACK报文都是一个单方向的操作，表示一方希望关闭连接。通过交换这些报文，双方都确认对方的关闭意愿，从而正常释放连接。

## 二、预防和应对措施

**2.1 足够的超时设置**

为连接释放过程设置合适的超时时间，以便在合理时间内检测到连接问题并采取相应的措施，防止超时释放的发生。

**2.2 使用心跳机制**

引入心跳机制，定期检测连接的状态。如果发现连接异常，可以及时采取措施，避免连接的非正常释放。

**2.3 错误处理和日志记录**

在应用程序中实现严格的错误处理机制，并记录连接释放过程中的关键信息。这有助于诊断问题并及时采取纠正措施。

**2.4 安全措施**

采取安全措施，如防火墙、入侵检测系统等，以减少异常关闭的可能性，防范攻击引起的非正常连接释放。