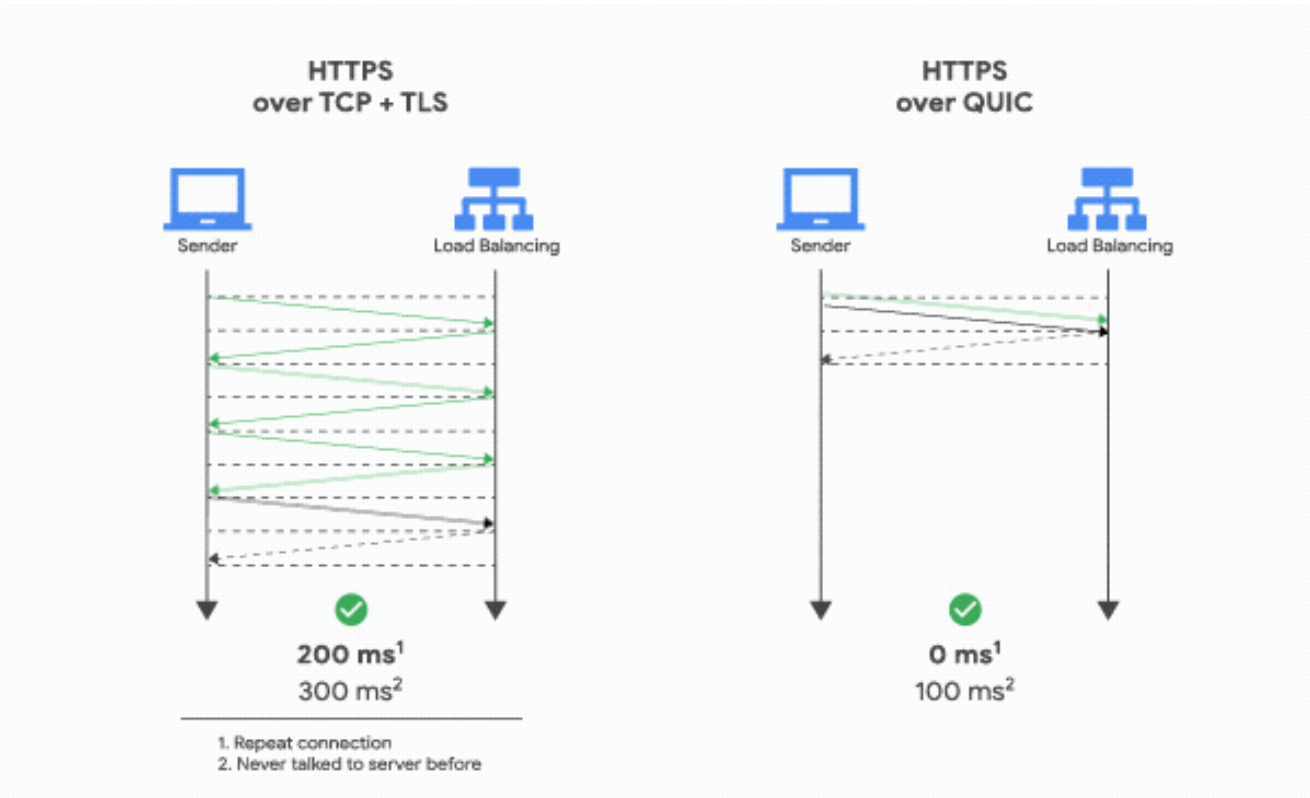
1. 降低 RTT 次数
2. HTTP/3 over QUIC

QUIC 是新一代的传输协议，基于 UDP 协议，降低 RTT 主要是通过减少握手次数。

我们知道 TCP 建立连接需要 3 次握手，这需要 1.5-RTT，如果再加上 TLS 的握手时间，总共需要 3-RTT 。QUIC 把传输和加密握手合并成一个，以最小化延迟（1-RTT）建立连接。如果复用连接的话，后续可以达到 0-RTT 。

下图展示了 TCP + TLS 和 QUIC 建立连接的区别：



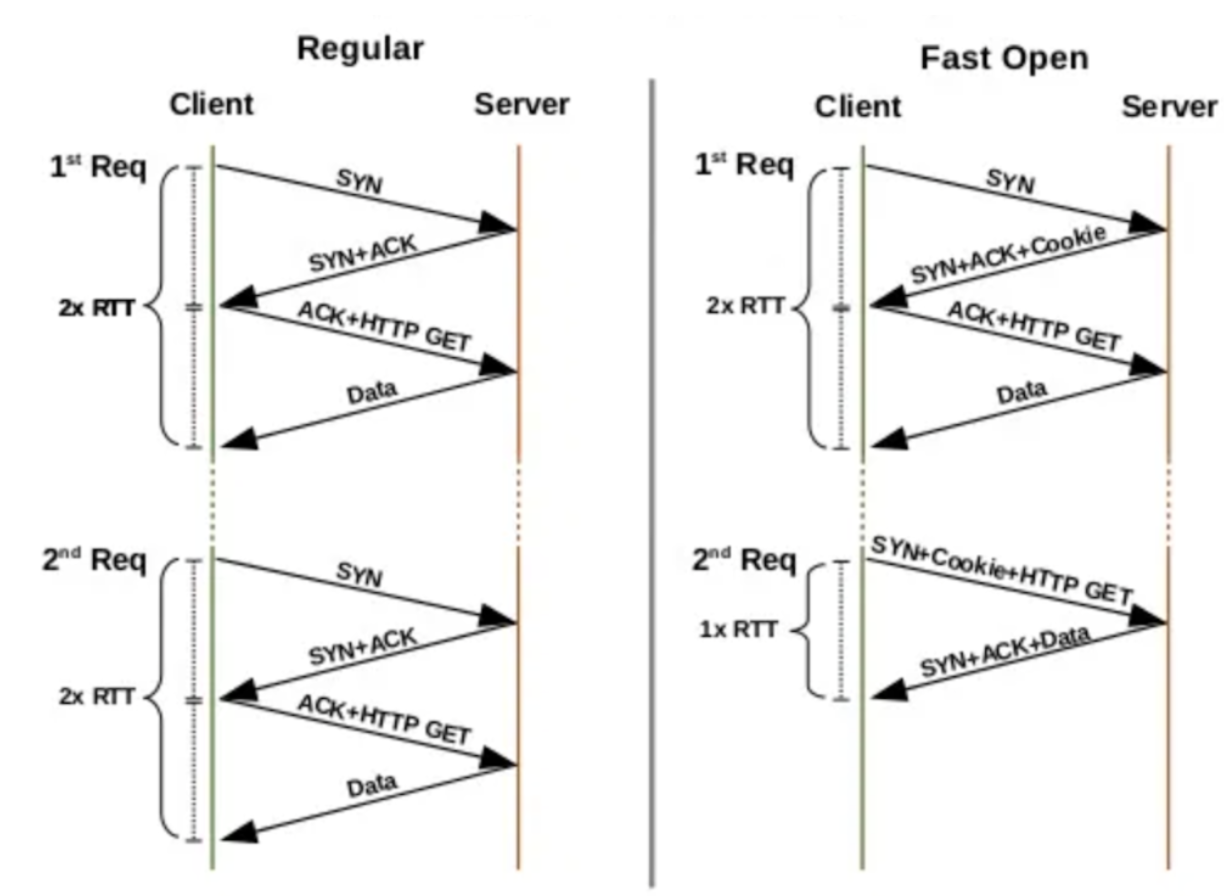
QUIC 建立连接的过程如下：1.当客户端首次发起 QUIC 连接时，客户端向服务器发送一个 client hello 消息，服务器回复一个 server reject 消息。该消息中有包括 server config ，类似于 TLS1.3 中的 key\_share 交换。这需要产生 1-RTT. 事实上，QUIC 加密协议的作者也明确指出当前的 QUIC 加密协议是「注定要死掉的」(destined to die), 未来将会被 TLS1.3 代替。只是在 QUIC 提出来的时候，TLS1.3 还没出生，这只是一个临时的加密方案。2.当客户端获取到 server config 以后，就可以直接计算出密钥，发送应用数据了，可以认为是 0-RTT。

因此，QUIC 握手除去首次连接需要产生 1-RTT，理论上，后续握手都是 0-RTT的。假设 1-RTT = 100ms, QUIC 建立安全连接连接的握手开销为 0ms, 功能上等价于 TCP+TLS , 但是握手开销比建立普通的 TCP 连接延迟都低。

1. TCP fast open

TCP fast open 简称 TFO，TFO 允许在 TCP 握手期间发送和接收初始 SYN 分组中的数据。如果客户端和服务器都支持 TFO 功能，则可以减少建立到同一服务器的多个 TCP 连接的延迟。这是通过在初始 TCP 握手之后在客户端上存储 TFO cookie 来实现的。如果客户端稍后重新连接，则此 TFO cookie 将发送到服务器，从而允许连续的 TCP 握手跳过一个往返延迟，从而减少延迟。

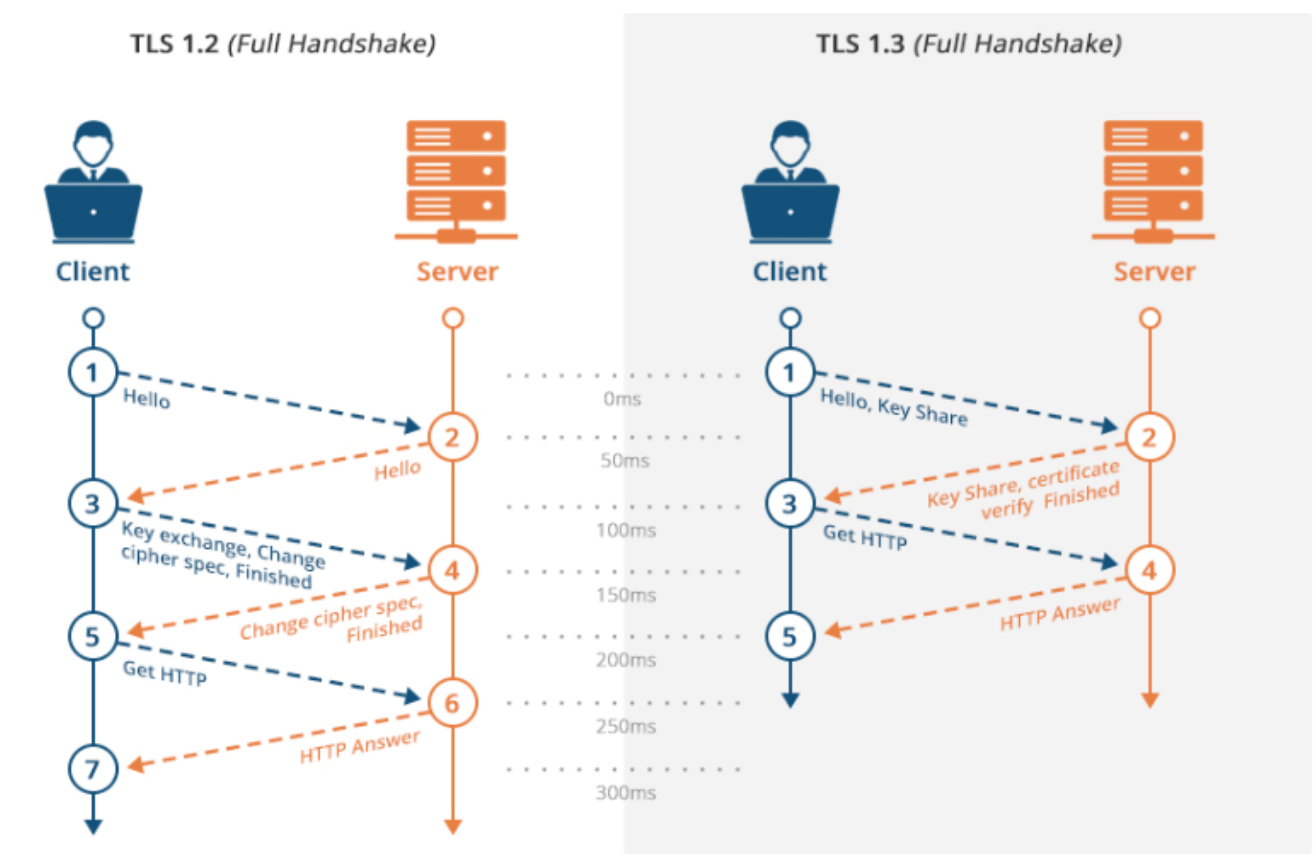
TFO 握手过程和普通 TCP 握手过程区别如下：



1. TLS1.3

传输层安全性协议（Transport Layer Security）及其前身安全套接层（英语：Secure Sockets Layer，缩写：SSL）是一种安全协议。目的是为互联网通信提供安全及数据完整性保障。TLS1.2 完成 TLS 密钥协商需要 2个 RTT 时间，TLS1.3 只需要1个 RTT时间。如果考虑重用的话，TLS1.2 session 重用需要1个 RTT 时间，TLS1.3 则因为在第一个包中携带数据，只需要0个 RTT。

TLS1.2 的握手过程和 TLS1.3 的过程区别如下：



可以看到在 TLS1.2 中，在第一个 RTT 需要协商算法版本等信息， 在第二个 RTT 才能完成对称密钥的协商。TLS 1.3 的区别在于，它在第一次 RTT 就进行了秘钥协商，TLS1.2 需要在双方明文交换了 key exchange 信息之后才会走加密通道，而 TLS1.3 在 sever 端发送完 ServerHello 信息之后就会走加密通道。基于此，TLS 1.3 能比 TLS 1.2 节省一个 RTT 时间。

发出请求到收到数据产生的 RTT 次数如下：

TLS1.2 over TCP ：4次

TLS1.3 over TCP ：4次

TLS1.3 over TCP Fast Open ：1-2 次

HTTP3/QUIC ：1-2次

其中 TLS 1.3 over TCP Fast Open 和 HTTP3/QUIC 效果最明显，相比 TLS 1.2 over TCP 可以节省一半以上的 RTT 次数。