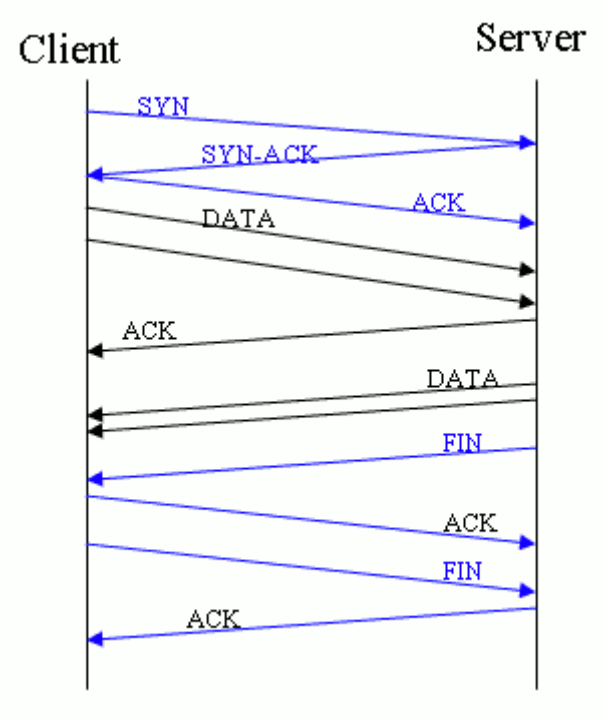
SSL 延时有多大

Netscape 公司当年设计 SSL 协议的时候，有人提过，将互联网所有链接都变成 HTTPs 开头的加密链接。这个建议没有得到采纳，原因之一是 HTTPs 链接比不加密的 HTTP 链接慢，因此 HTTPs 开头的加密链接只应用在有安全要求的场景。

首先解释一下，为什么 HTTPs 链接比 HTTP 链接慢。HTTPs 链接和 HTTP 链接都建立在 TCP 协议之上。HTTP 链接比较单纯，使用三个握手数据包建立连接之后，就可以发送内容数据了。



上图中，客户端首先发送 SYN 数据包，然后服务器发送 SYN+ACK 数据包，最后客户端发送 ACK 数据包，接下来就可以发送内容了。这三个数据包的发送过程，叫做 TCP 握手。

再来看 HTTPs 链接，它也采用 TCP 协议发送数据，所以它也需要上面的这

三步握手过程。而且，在这三步结束以后，它还有一个 SSL 握手。

总结一下，就是下面这两个式子：

HTTP 耗时 = TCP 握手

HTTPs 耗时 = TCP 握手 + SSL 握手

所以，HTTPs 肯定比 HTTP 耗时，这就叫 SSL 延迟。

命令行工具 curl 有一个 w 参数 ,可以用来测量 TCP 握手和 SSL 握手的具体耗时，以访问支付宝为例。

curl -w "TCP handshake: %{time_connect}, SSL handshake: %{time_appconnect}\n" -so /dev/null https://www.alipay.com

TCP handshake: 0.022, SSL handshake: 0.064

上面命令中的 w 参数表示指定输出格式，time_connect 变量表示 TCP 握手的耗时，time_appconnect 变量表示 SSL 握手的耗时（更多变量请查看文档和实例），s 参数和 o 参数用来关闭标准输出。

从运行结果可以看到，SSL 握手的耗时（64 毫秒）大概是 TCP 握手（22 毫秒）的三倍。也就是说，在建立连接的阶段，HTTPs 链接比 HTTP 链接要长 3 倍的时间，具体数字取决于 CPU 的快慢和网络状况。

所以，如果是对安全性要求不高的场合，为了提高网页性能，建议不要采用保密强度很高的数字证书。一般场合下，1024 位的证书已经足够了，2048 位和 4096 位的证书将进一步延长 SSL 握手的耗时。