

WEB加速 协议先行

罗成

腾讯高级工程师



CNUTCon 2017

全球运维技术大会

上海·光大会展中心大酒店 | 2017.9.10-11

智能时代的新运维

大数据运维
安全
SRE
DevOps
Kubernetes
Serverless
游戏运维
AI Ops
智能化运维
基础架构
监控
互联网金融



StuQ

斯达克学院

实践驱动的IT教育



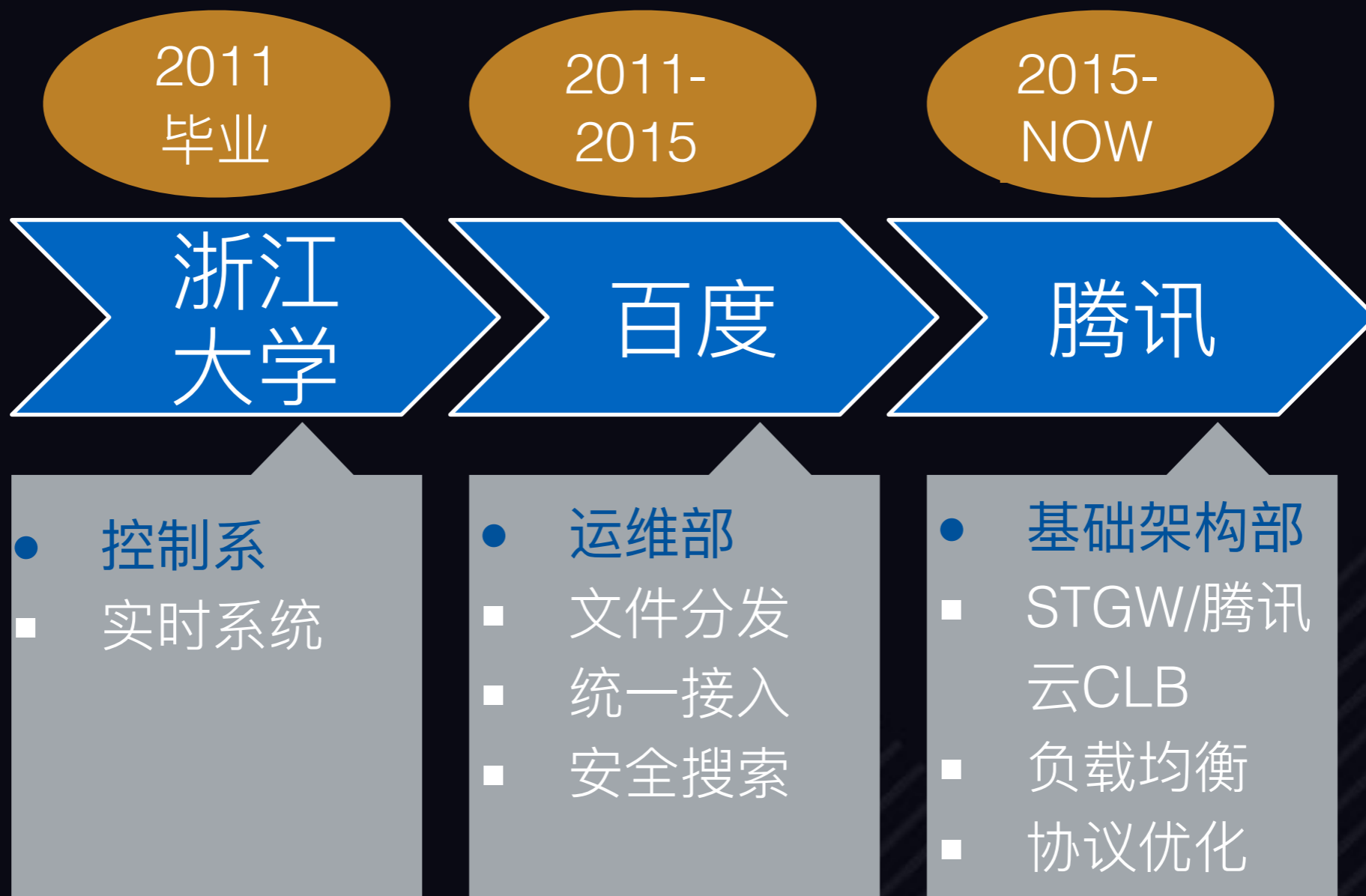
斯达克学院(StuQ)，极客邦旗下实践驱动的IT教育平台。通过线下和线上多种形式的综合学习解决方案，帮助IT从业者和研发团队提升技能水平。



10大职业技术领域课程

<http://www.stuq.org>

个人简介



访问Web经常遇到的问题



Unable to access the network

ERR_NETWORK_CHANGED

Refresh



LOADING

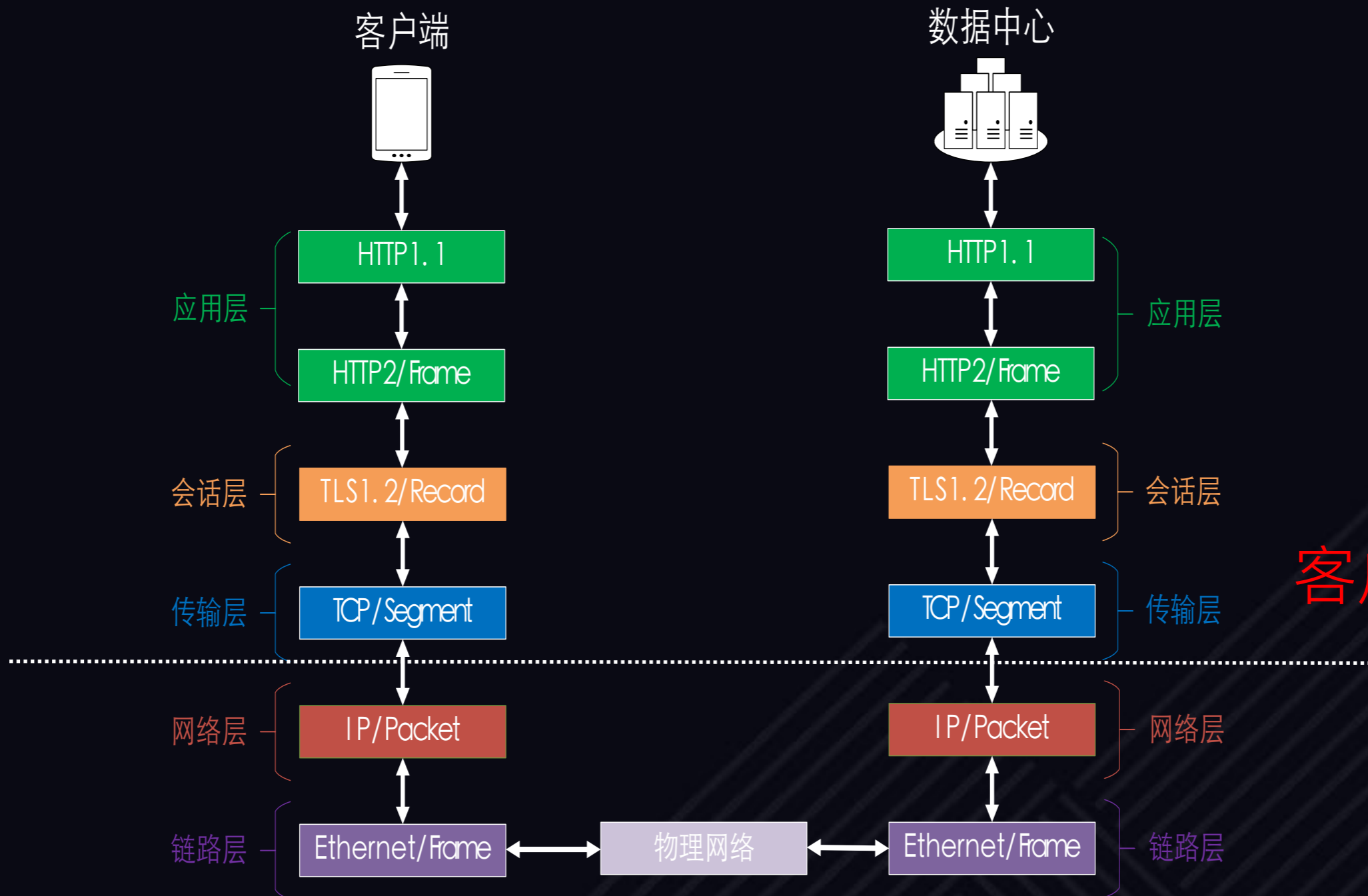
Please feel free to wait forever.

10%

影响WEB性能的主要因素

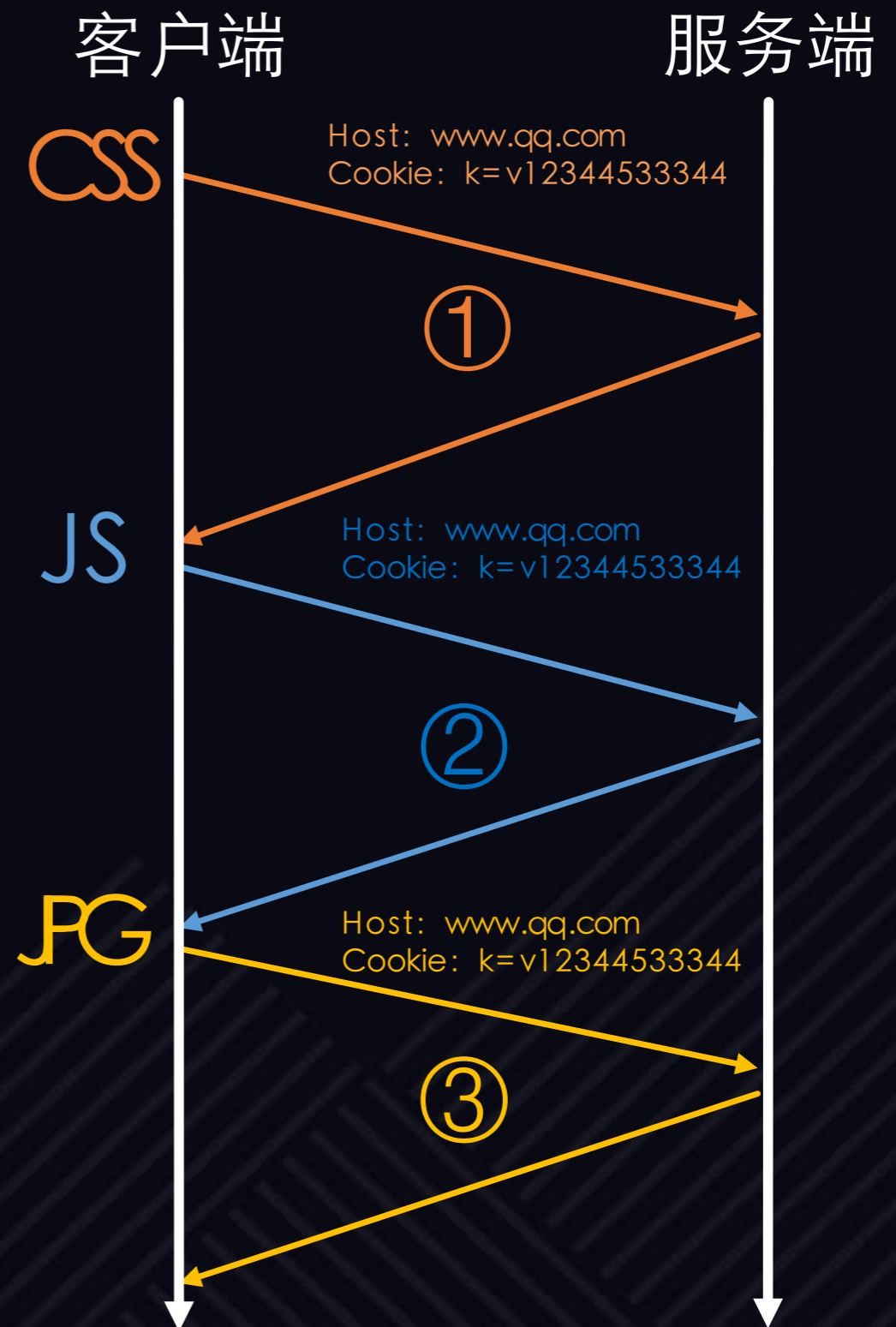


一条HTTP2 请求经过的协议栈



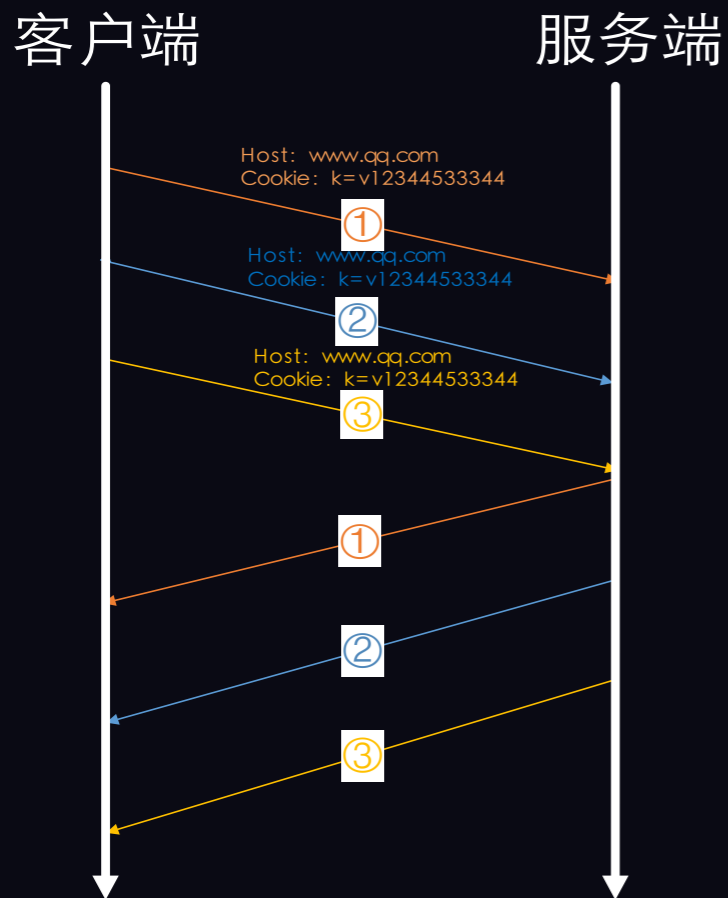
HTTP1.1的性能问题

- 单链接串行
 - 效率低下
- 头部未压缩
 - 冗余
 - 上下行带宽不对称
 - 头部平均大小超过 1500B
- ASCII明文
 - 解析慢

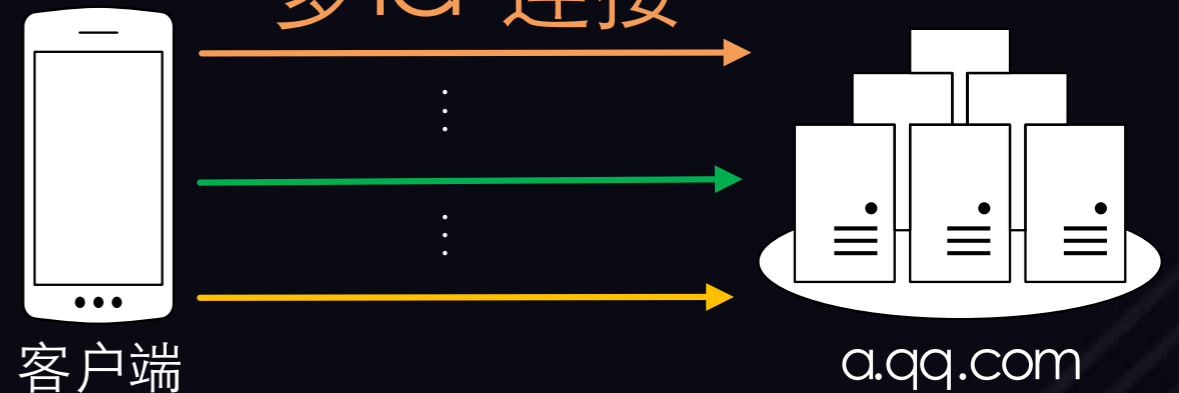


HTTP1.1的优化---增加连接, 减少请求

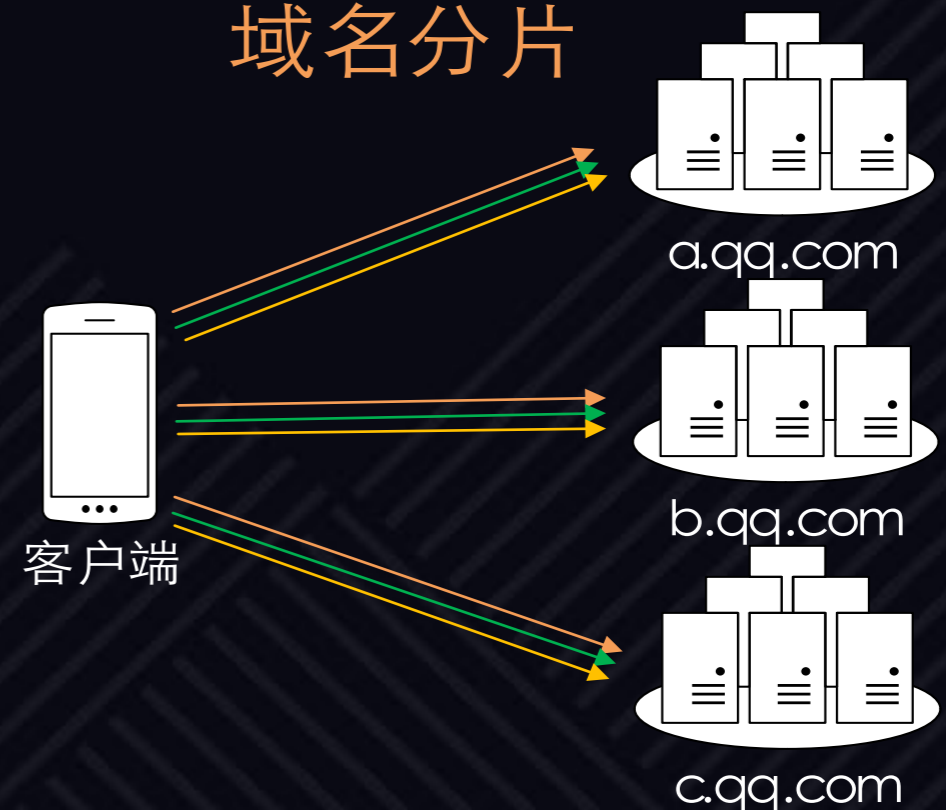
pipelining



单域名 多TCP连接



域名分片



其他WEB优化策略

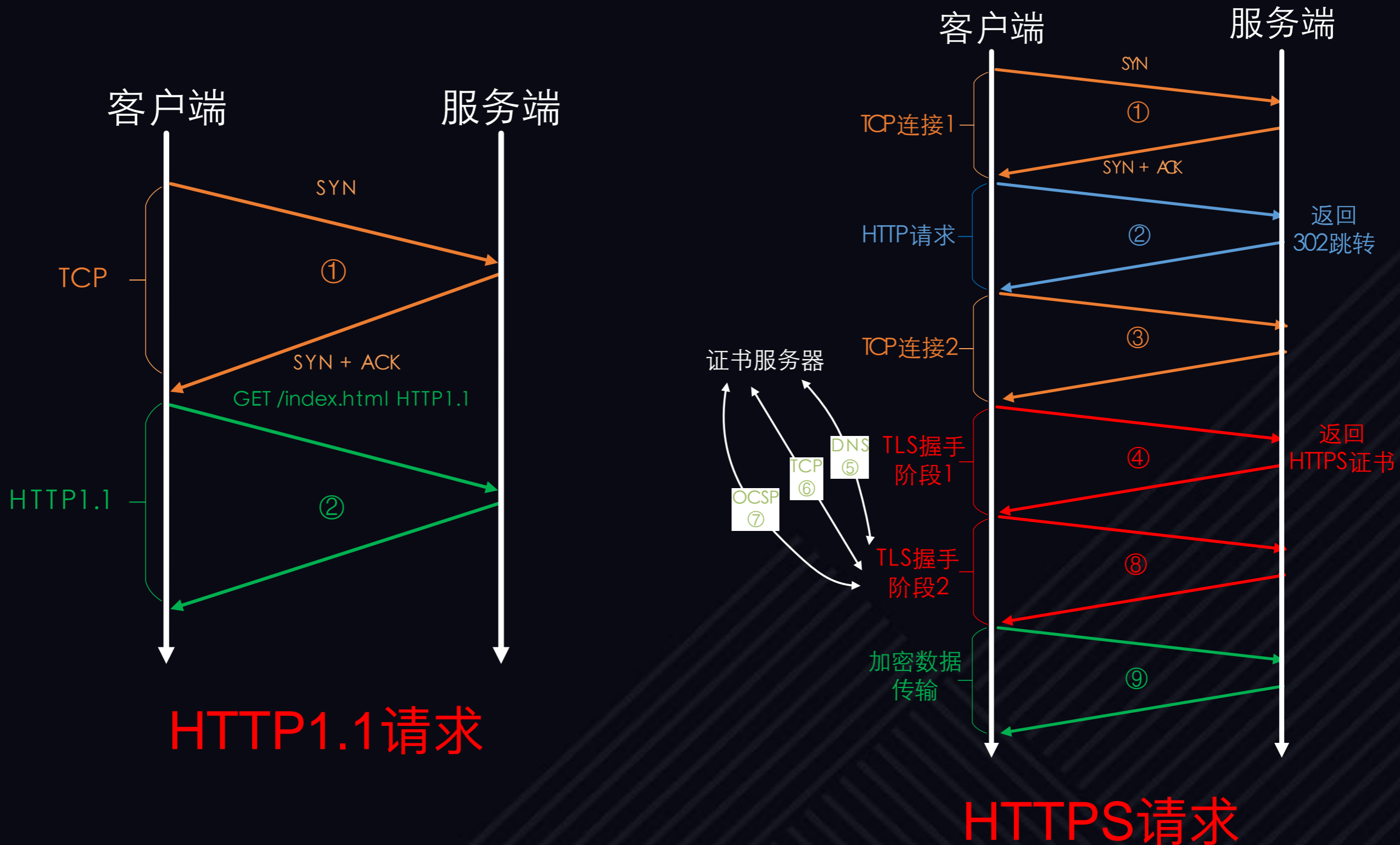
- 缓存
- CSS Sprites
- data uri, Inline Images

HTTPS/HTTP2加速HTTP1.1的淘汰

- 全站HTTPS快速普及
 - 46%的网站支持HTTPS
- HTTP2 渐成主流
 - 2015.5 发布
 - 2017.05, 使用率13.7%
- 高连接成本+多路复用+server push
 - HTTP1.1优化策略失效



HTTP vs HTTPS连接成本



未经优化的HTTPS速度明显慢于HTTP

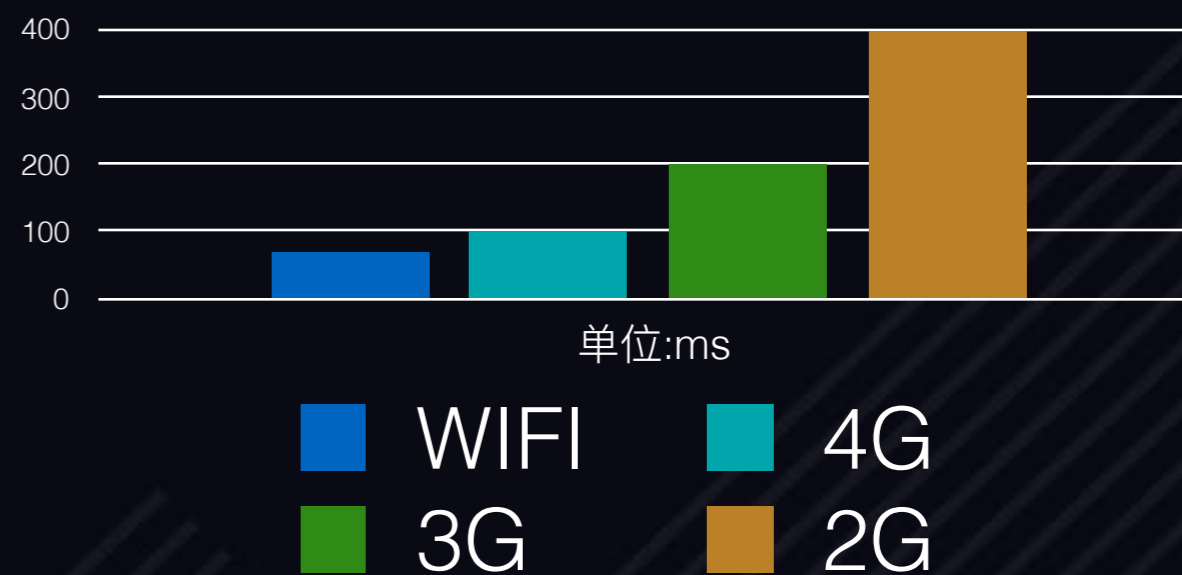
- 网络耗时

- 最坏情况下增加7个RTT
- 500ms以上

- 计算耗时

- 客户端，50ms以上
 - ◆ 证书校验、密钥交换
- 服务端，15ms以上

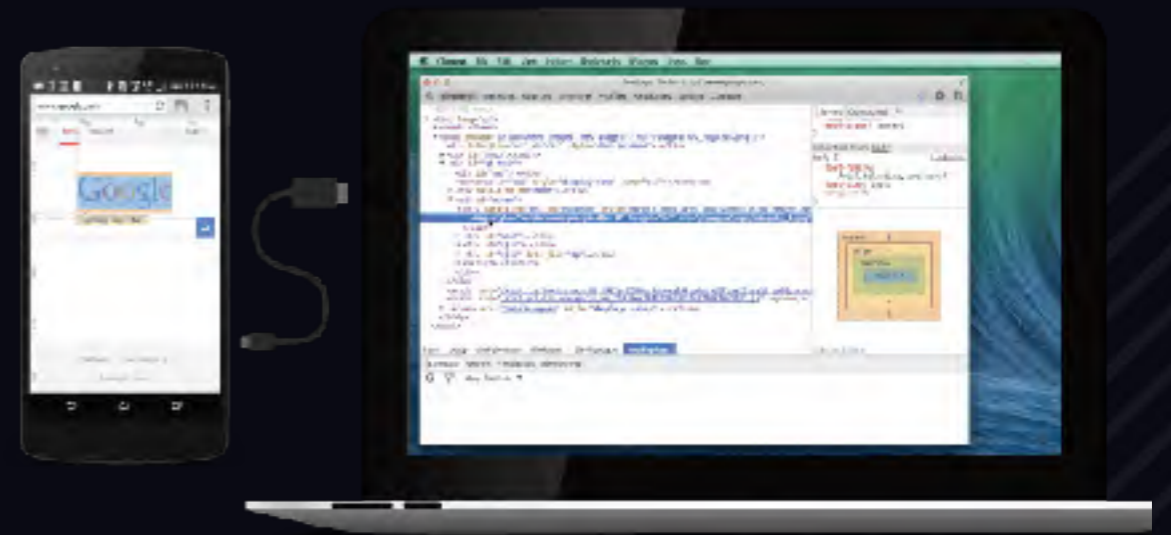
RTT参考值



HTTPS = HTTP + SLOW ?

Why Slow? 线下模拟测试

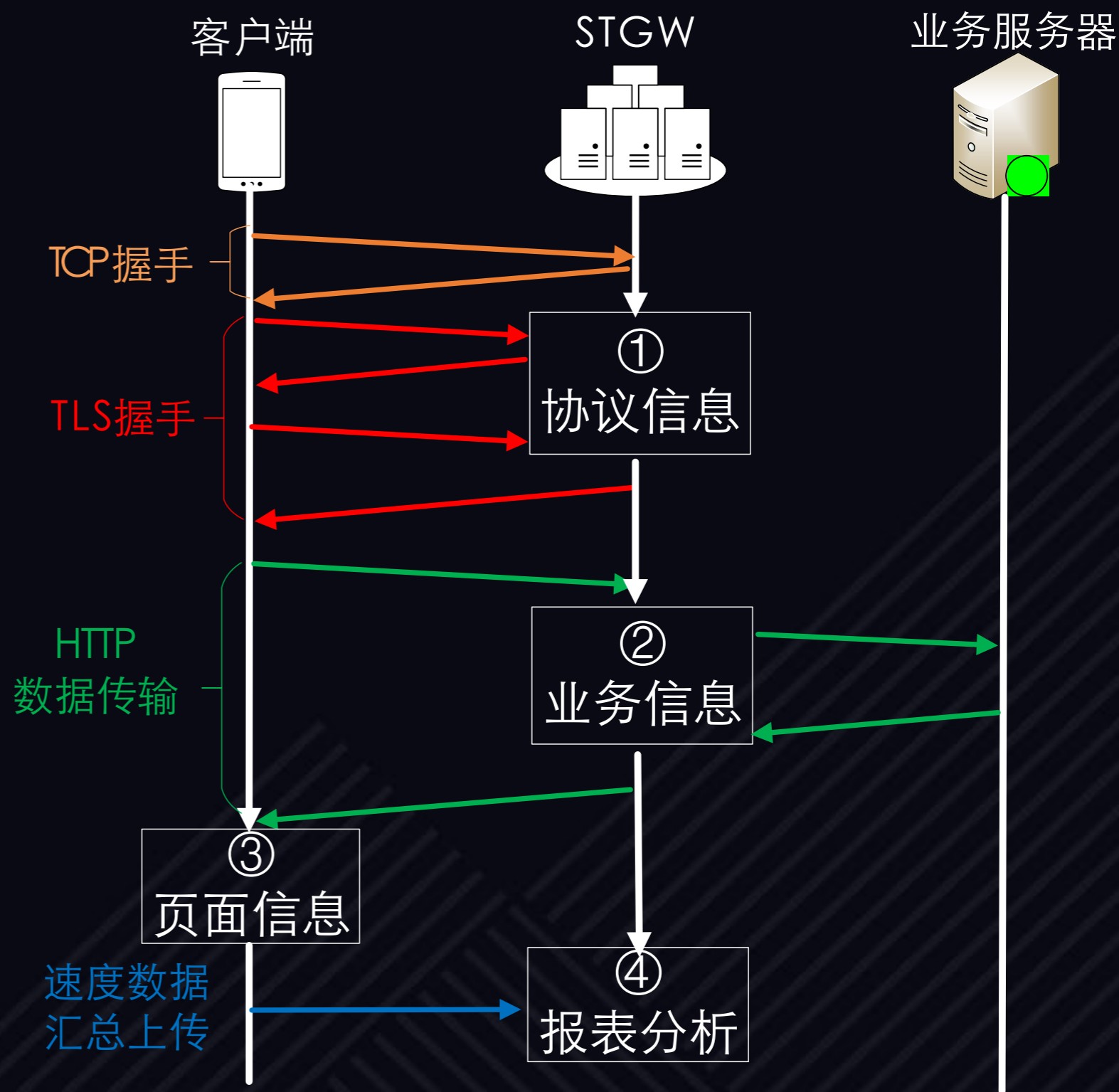
- 自动化
- 消除误差
 - 📁 同比, 环比, 10000条
- 工具
 - 📁 Chrome Remote debug
 - 📁 Linux traffic control
 - 📁 performance timing api



Why Slow? 线上业务速度数据采集

- 服务端采集优势

- 底层信息丰富，RTT，协议版本，连接信息，session，密码套件，握手时间，头部压缩比
- 跨平台，开发成本低



Why Slow? 多维数据分析

item	start_load	css_load	js_load	dom_ready	active	req_time
tcp_reuse	705	719	1541	858	2120	147
TLSv1.2	966	982	1982	1132	2591	165
tcp_first_use	1422	1430	2856	1618	3594	138
ecdhe-rsa-aes128-gcm-sha256	975	994	1973	1140	2568	163
android_wifi_spdy_tcp_first_use	1574	1594	2924	1772	3618	147
android5_tcp_first_use(http)	999	1046	2048	1217	2461	86
ios8_tcp_reuse(http)	349	382	737	441	893	100

腾讯X5内核浏览器在4G网络下使用HTTP2并且是TLS1.2协议并且使用ECDHE并且没有复用tls session的首屏时间是多少？

WEB访问速度优化方向

- 协议
 - TCP, TLS, HTTP2
- 资源
 - CDN, 域名, 页面元素
- 用户行为
 - 预建连接

TCP速度优化

- TFO(tcp fast open)

- 80分位 **487ms->390ms**
- iOS9+, kernel v3.7+

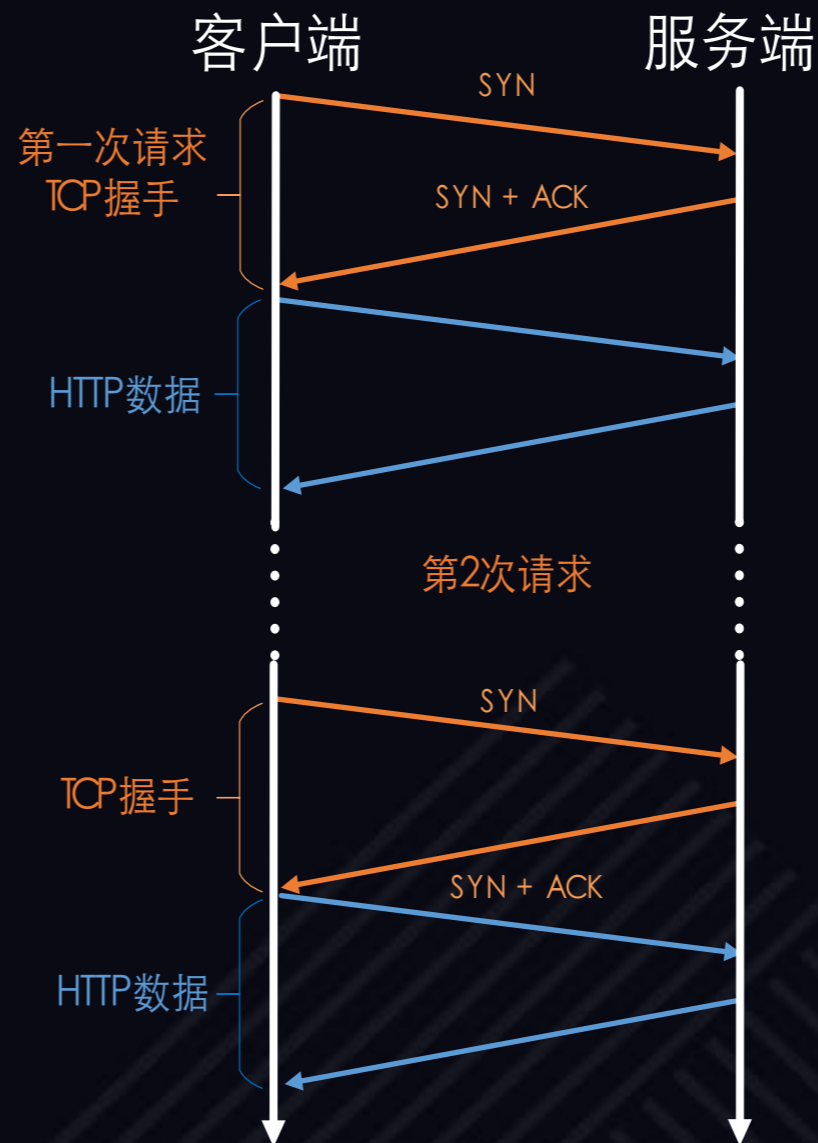
- 拥塞控制

- 增大拥塞窗口 3 ->10
- BBR

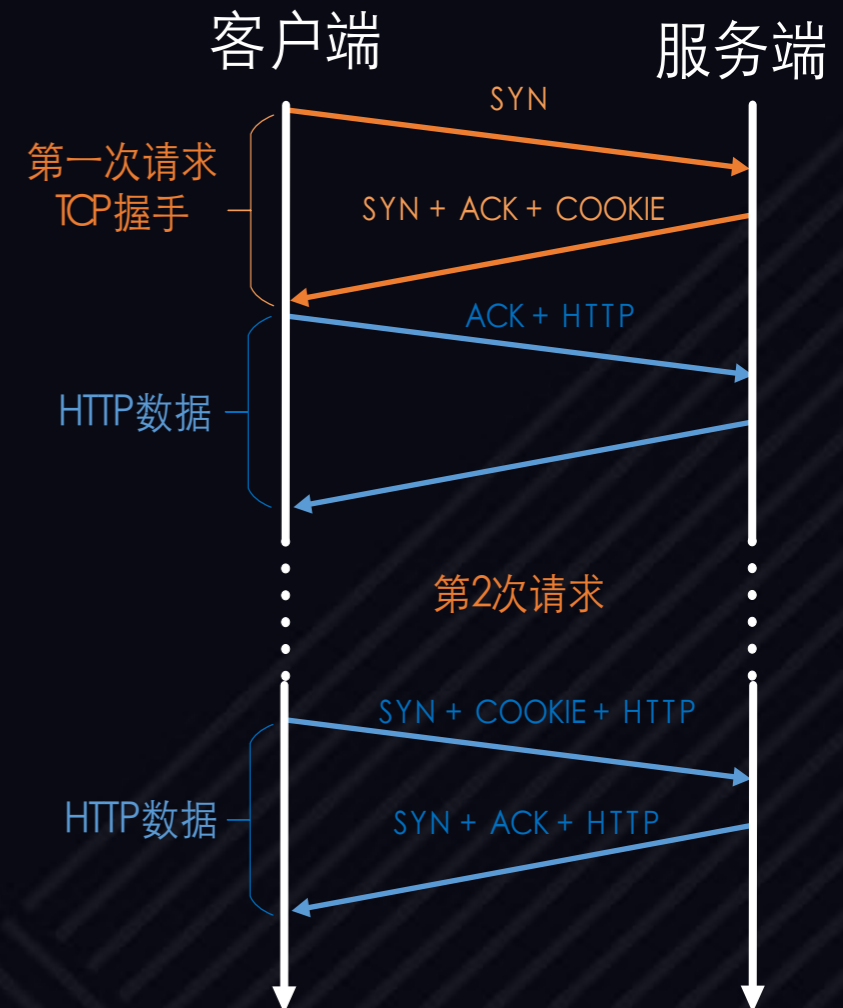
- 优化成本高

- 需要操作系统支持

普通握手

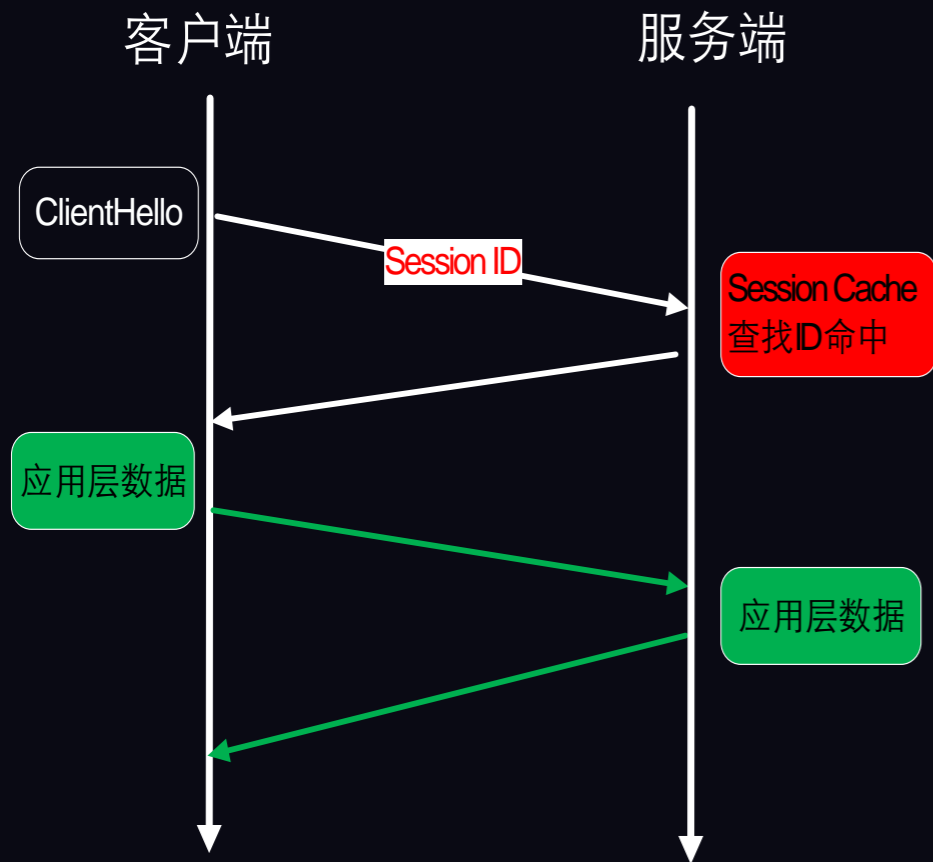


TFO

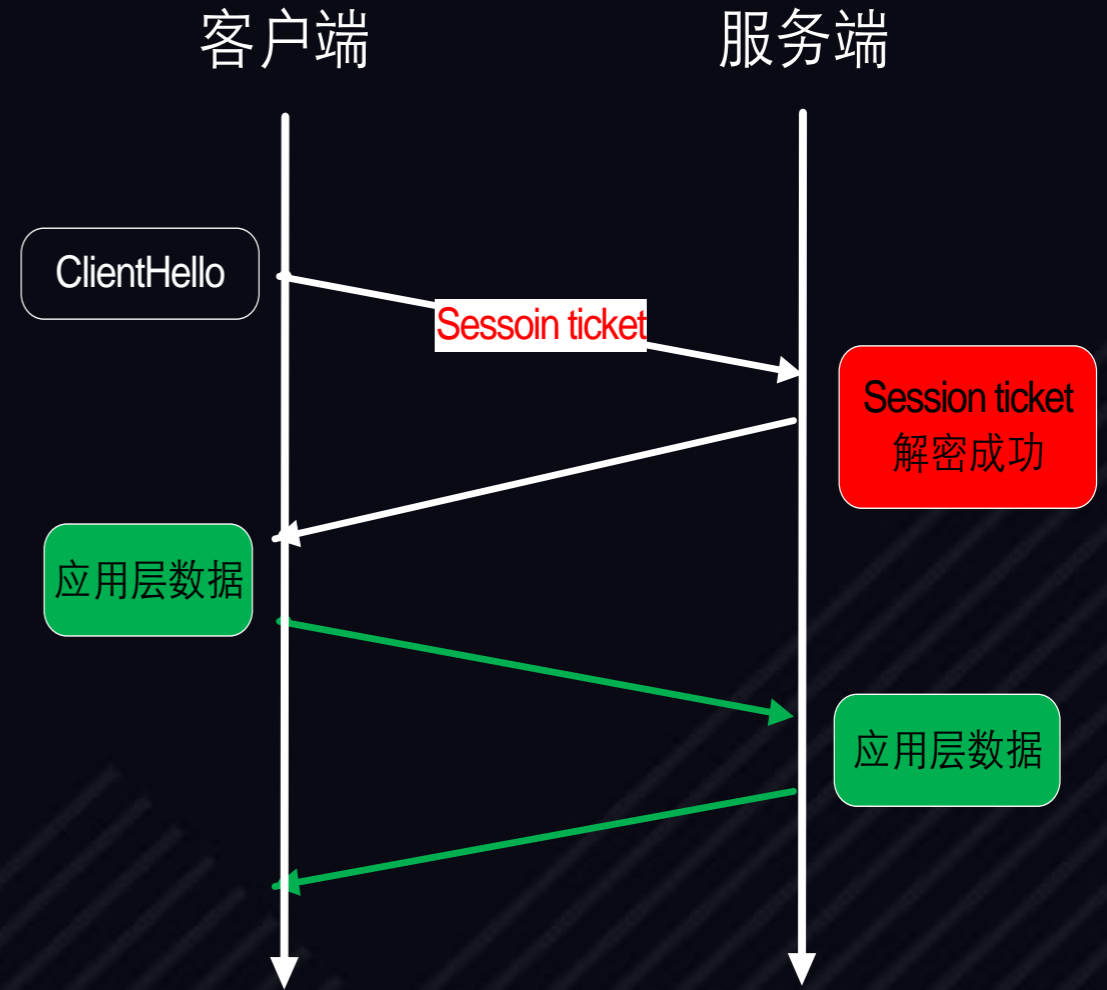


TLS速度优化—session resumption

Session id



Session ticket

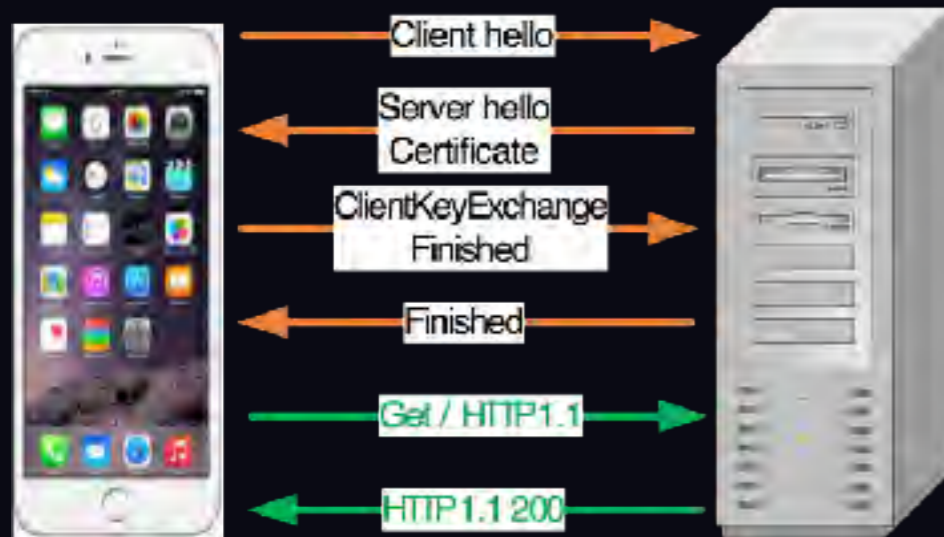


iOS Qzone SSL握手时间:
200ms -> 100ms 提升50%

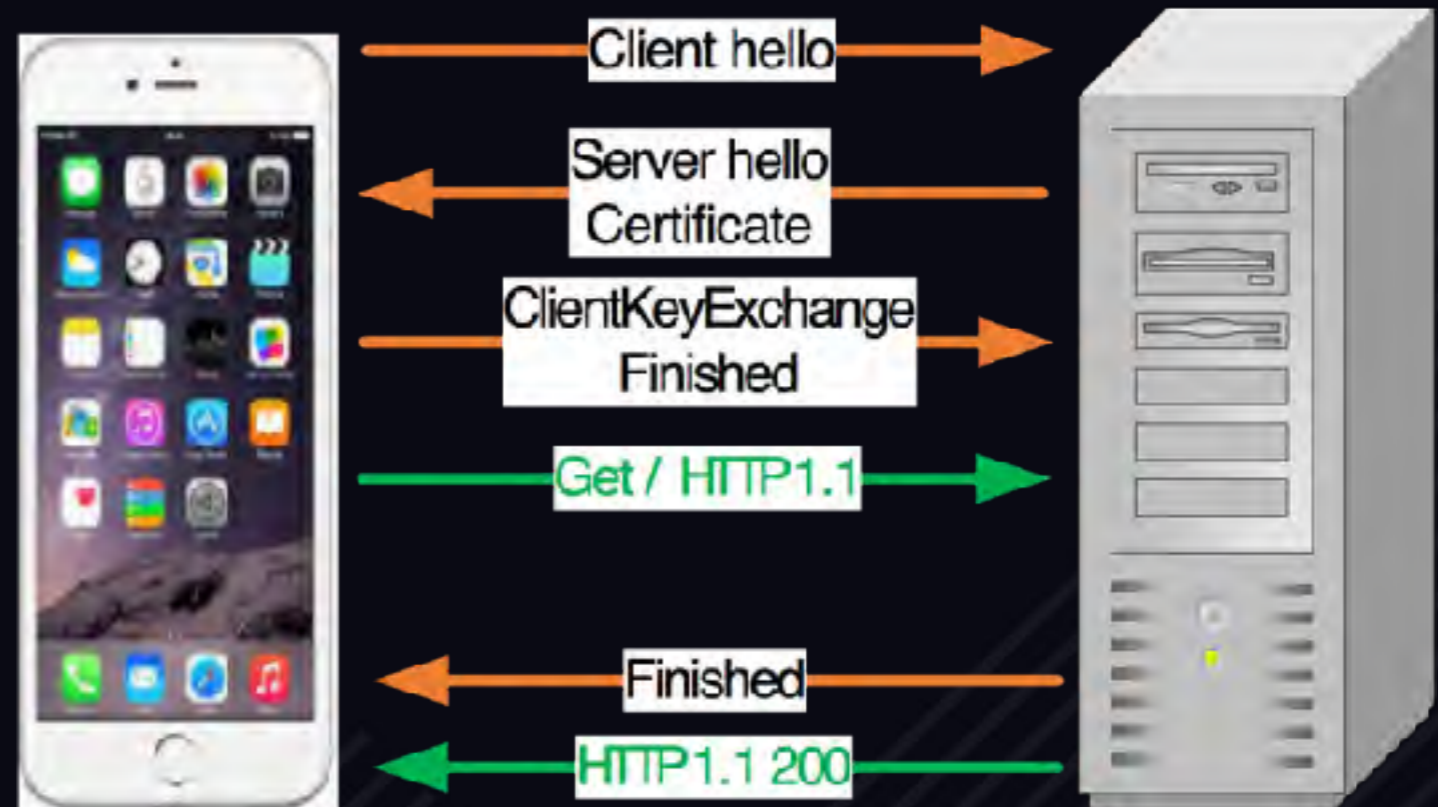
iOS 不支持

TLS速度优化---False Start

普通握手



False Start

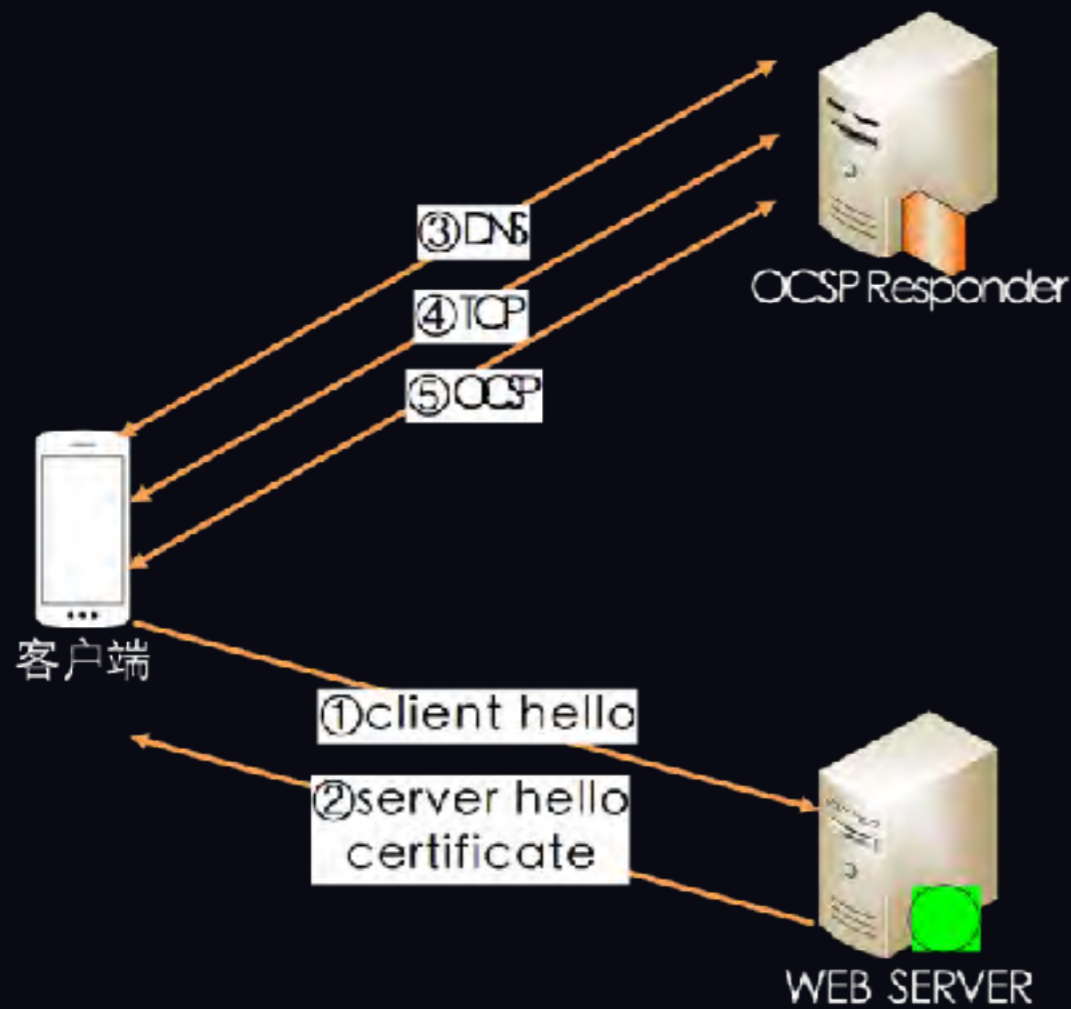


支持Perfect Forward Secret
ECDHE, DHE

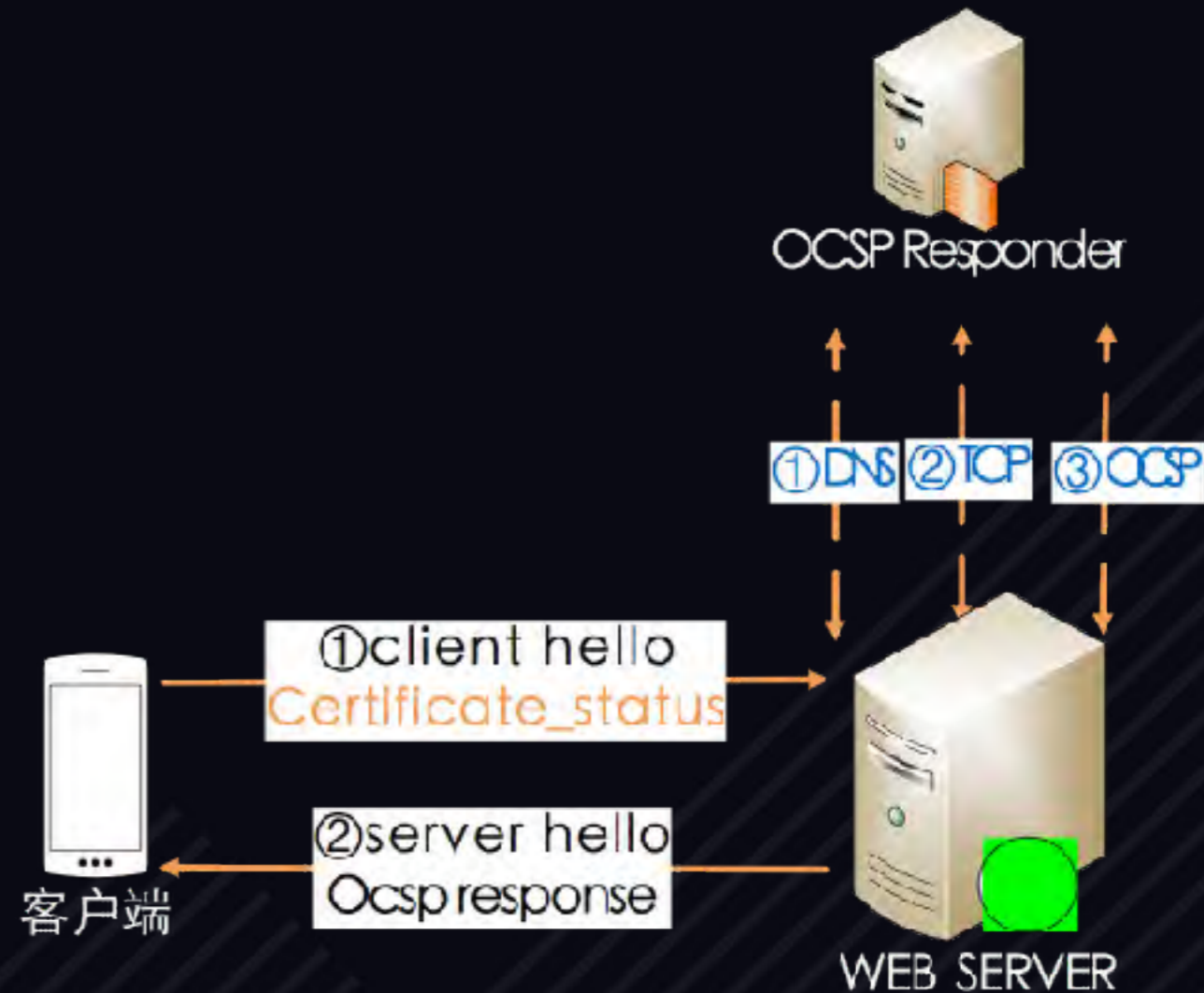
SSL 握手时间提升30%

TLS速度优化---OCSP Stapling

OCSP



OCSP Stapling



客户端缓存7天

TLS速度优化---dynamic record size

- 原因

- record是TLS处理的最小单位

- 解决方案

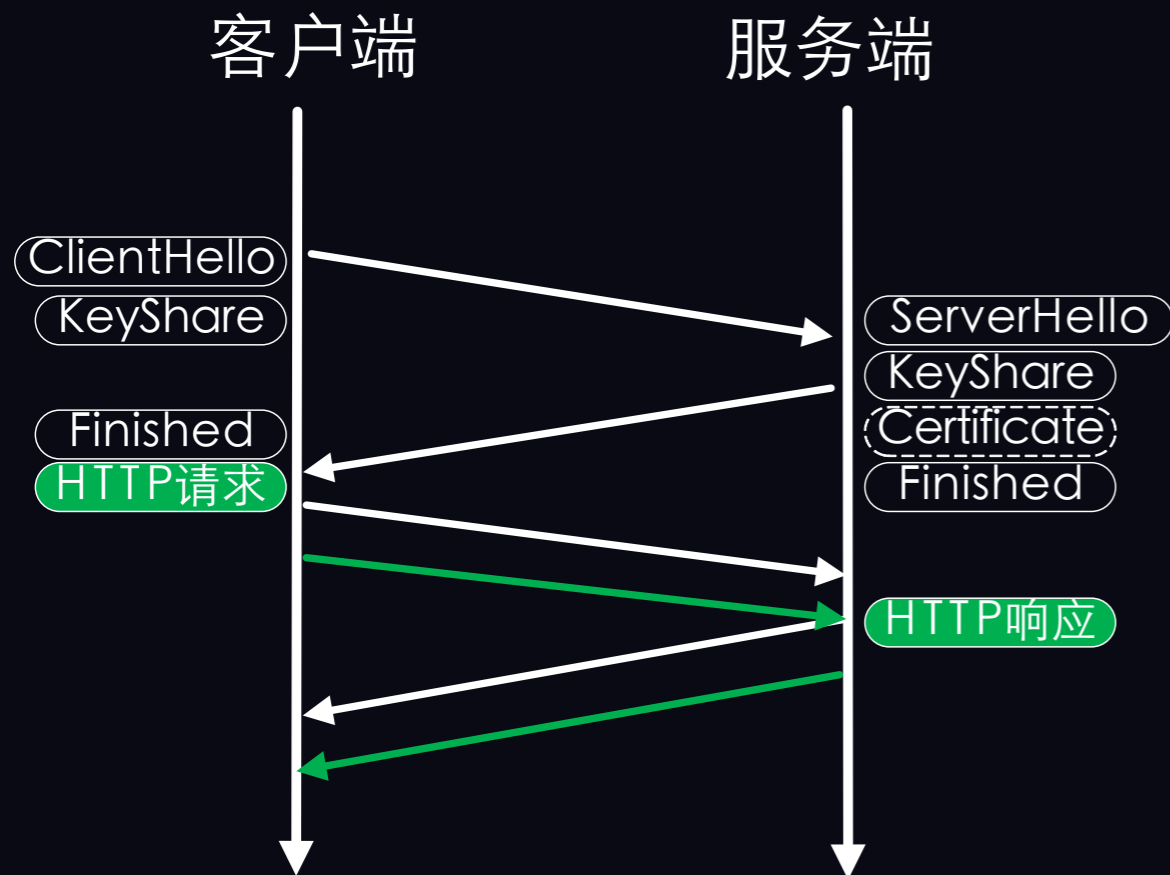
- ssl_buffer_size 4k
- [patch](#)

TLS head of line blocking

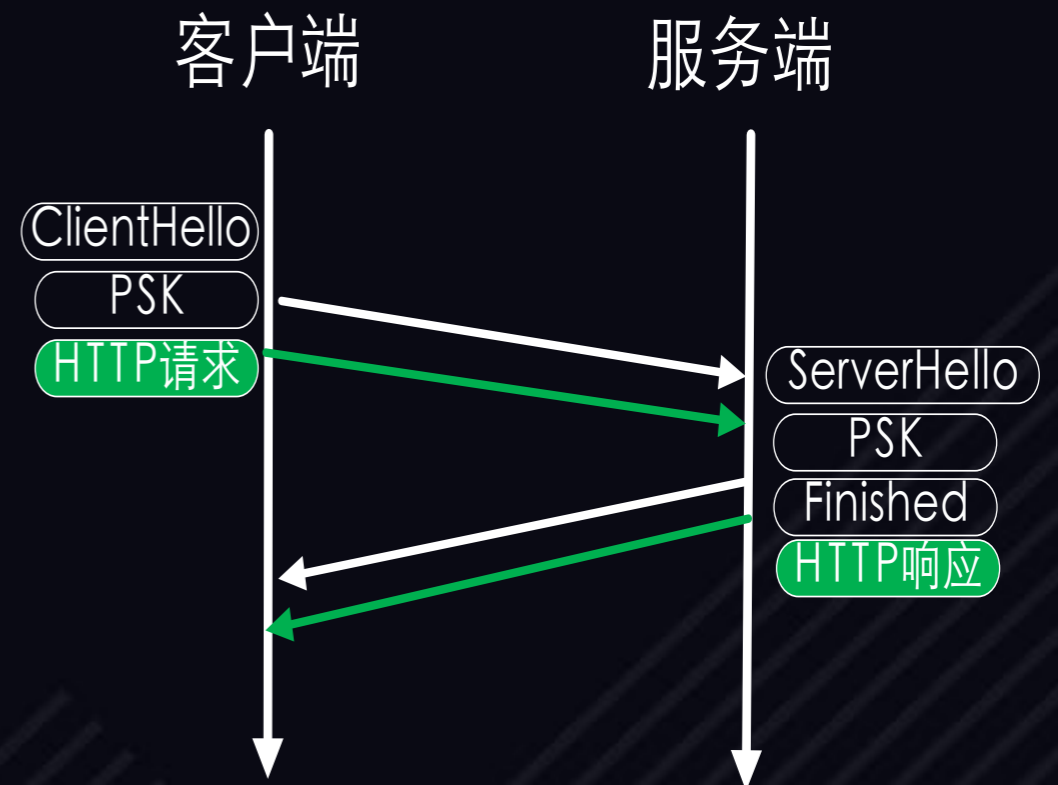


TLS1.3速度优化---0RTT Handshake

TLS1.3 1RTT full handshake



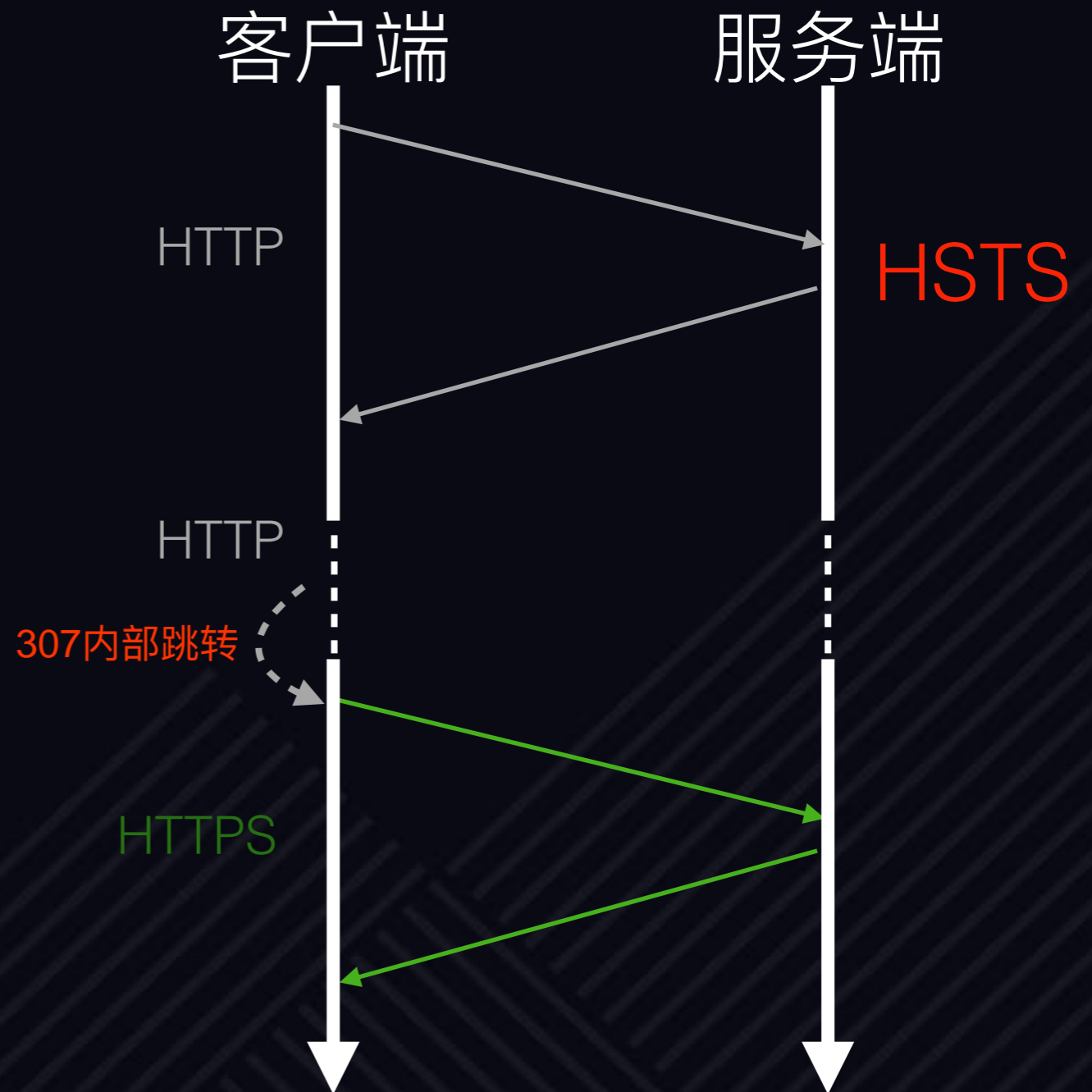
TLS 0RTT Preshared Key



- TLS1.3 预计于今年秋季正式发布
- Openssl 1.1.1, Nginx 1.13.0支持draft 20

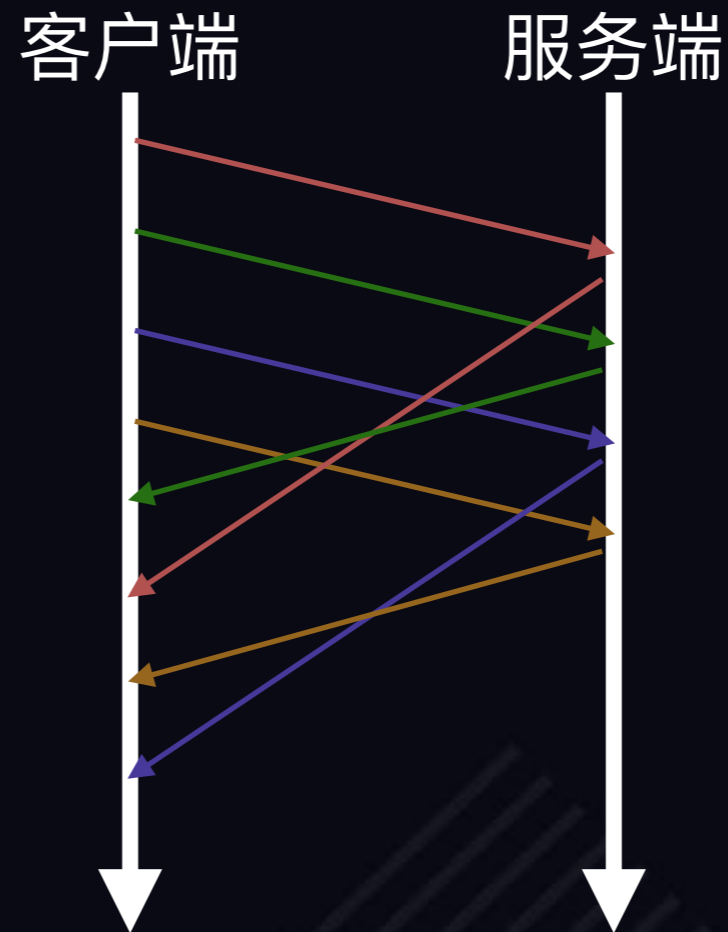
HTTPS速度优化---HSTS减少302跳转

- HTTP Strict Transport Security(HSTS)
 - Strict-Transport-Security: max-age=0; includeSubDomains
- Preload list
 - <https://hstspreload.appspot.com>

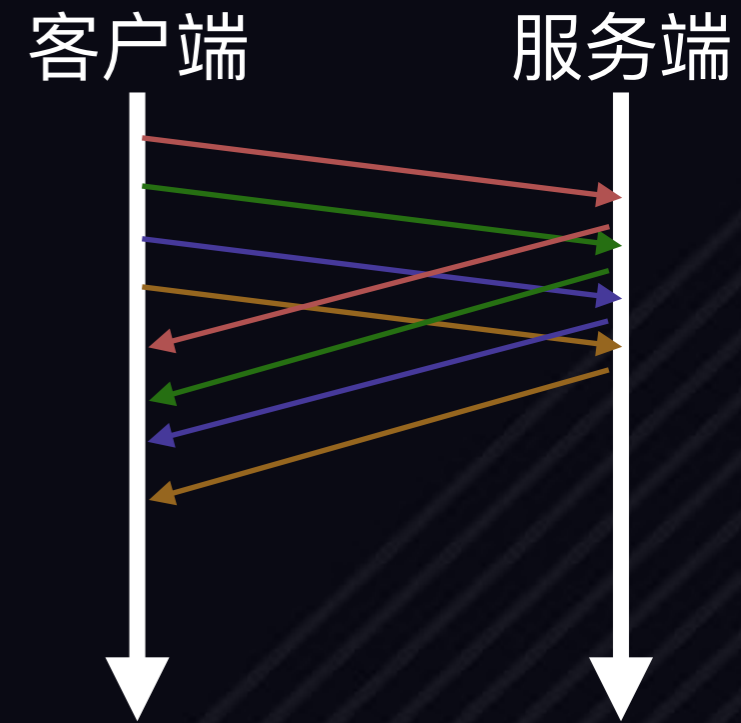


HTTPS速度优化---SPDY && HTTP2

- 二进制
- 多路复用
 - 单个连接，多个请求
- 优先级



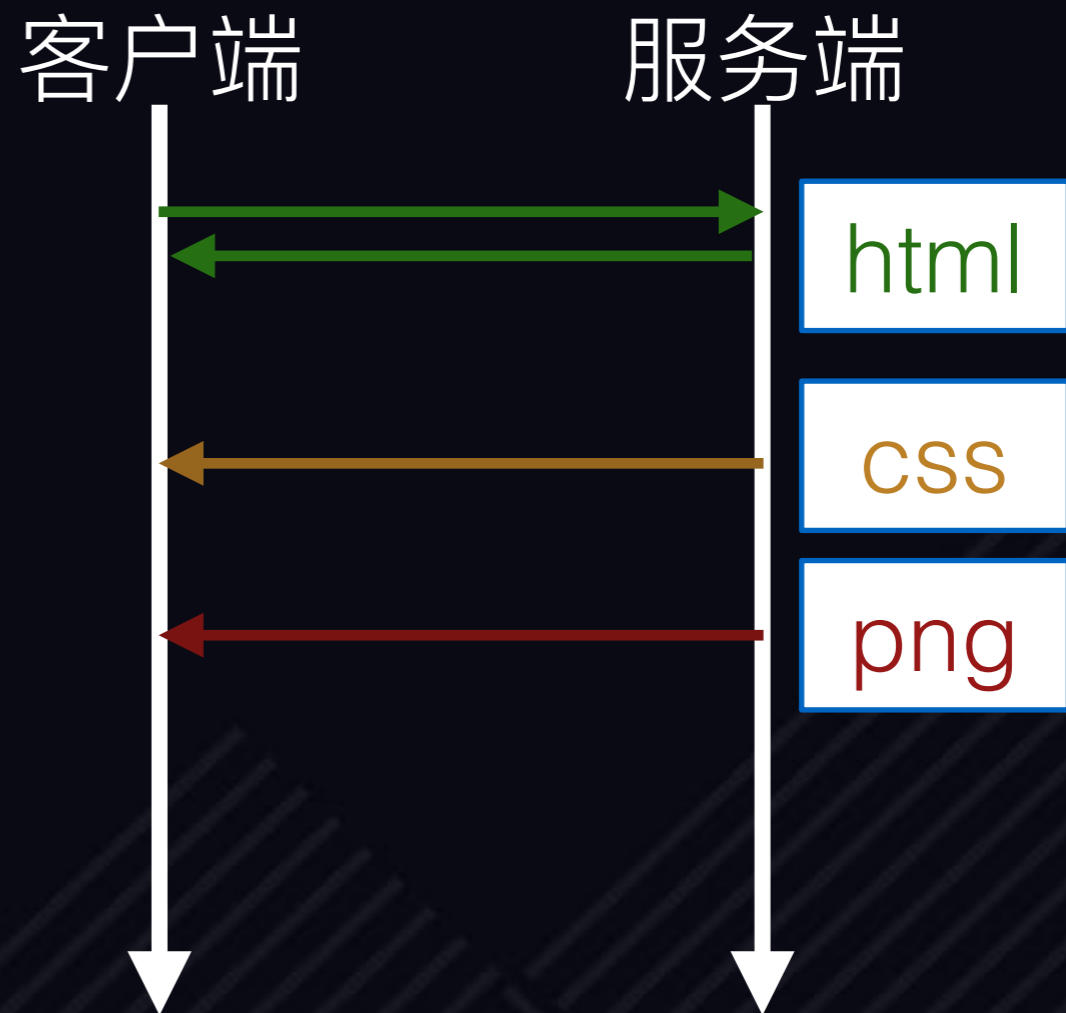
多路复用



pipelining

HTTPS速度优化—SPDY&&HTTP2

- 头部压缩
 - 90%压缩率
- Server push
 - 未发先至



HTTP2实践建议

- 使用一个连接
 - ◆ 握手少，压缩高，更好地利用TCP特性
- 使用更少的域名
 - ◆ 减少DNS解析时间
- 多域名复用相同IP，相同证书
 - ◆ 复用连接
- 灵活运用server push，代替inlining
- 使用TLS1.2
- HTTP2适用于多元素场景

WEB速度优化---预建连接

- 预建连接节省 **400ms以上**

- 📁 link 标签和头部

- 📁 首页提前预建子页面连接

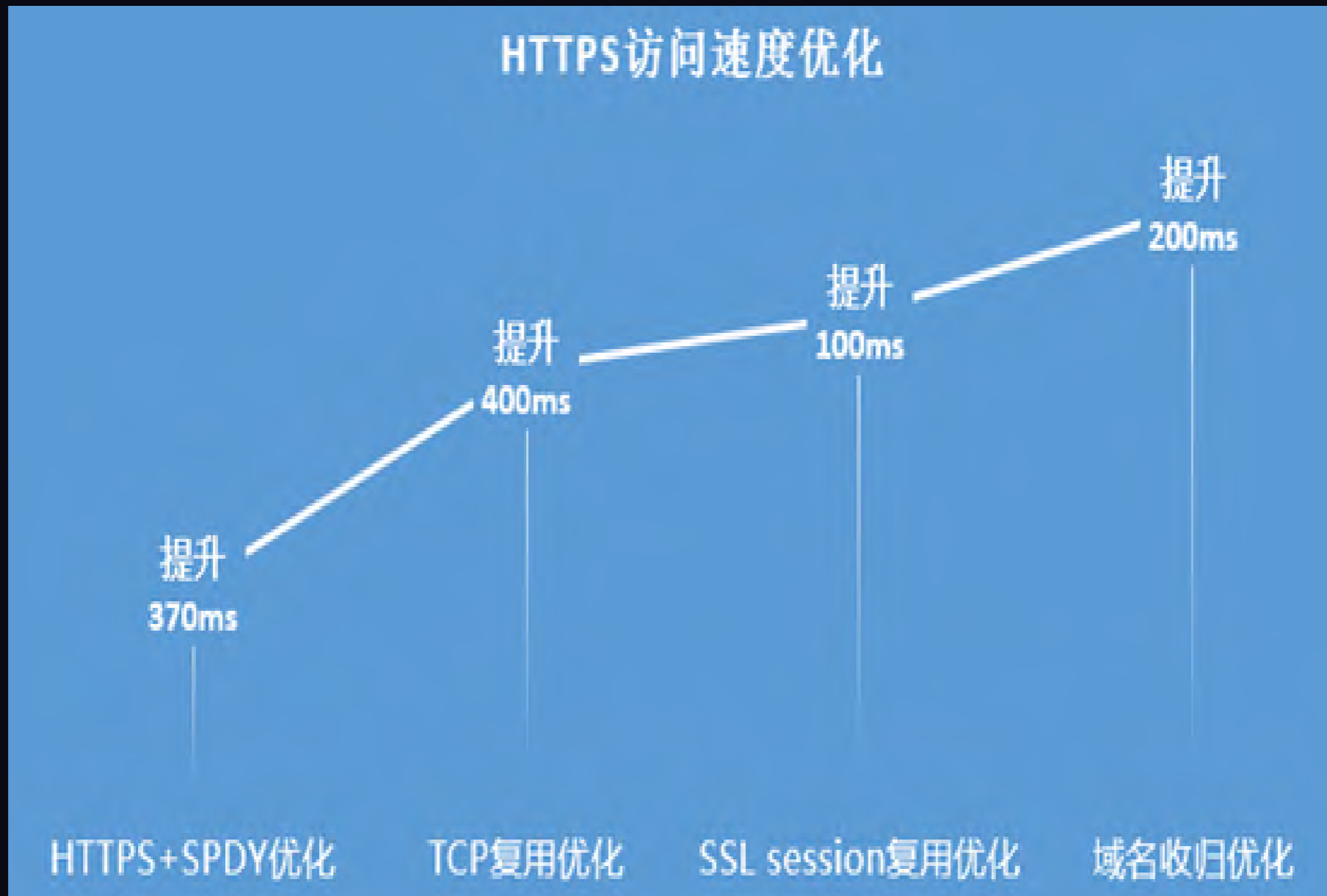
- 📁 用户行为预测

- 长连接维持

- 📁 stgw_precon.html

- 📁 后台JS秒级别维持长连接

HTTPS访问速度能够超越HTTP1.1



HTTP2是未来吗?

是!

- 多路复用
- 头部压缩
- server push
- 优先级

不是!

- TCP三次握手+TLS握手
- TCP头篡改
- Head of line blocking
- 重传
- 拥塞控制

拥抱QUIC

HTTP2特性 + TLS1.3 握手 + UDP传输 + 基于
packet的加密

欢迎体验腾讯云 + CLB负载均衡



腾讯云



CLB

欢迎关注



“腾讯架构师”

知乎ID: helloworlds
微博ID: 互联网罗成
知乎专栏:
HTTPS原理和实践

让创新技术推动社会进步

HELP TO BUILD A BETTER SOCIETY WITH
INNOVATIVE TECHNOLOGIES

Geekbang >

极客邦科技

InfoQ
ueue

专注中高端技术人员的技术媒体



EGO EXTRA GEEKS' ORGANIZATION
NETWORKS

高端技术人员学习型社交平台



StuQ
ueue

斯达克学院

实践驱动的 IT 教育平台

