# HTTPS最佳实践

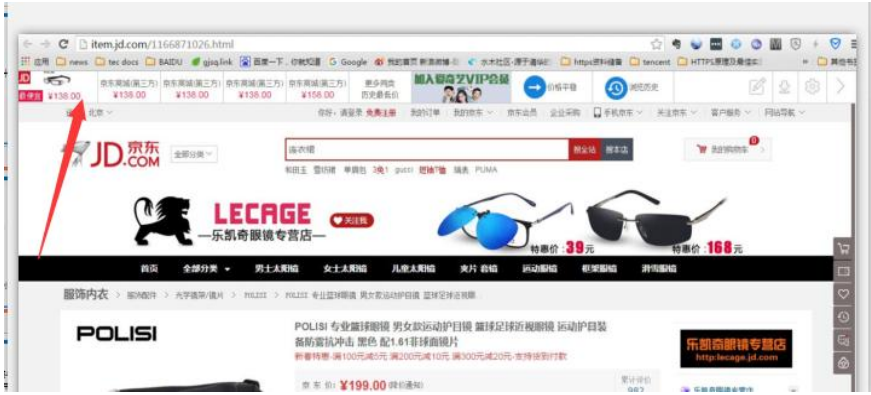
罗成
2016.09.10

# 个人介绍

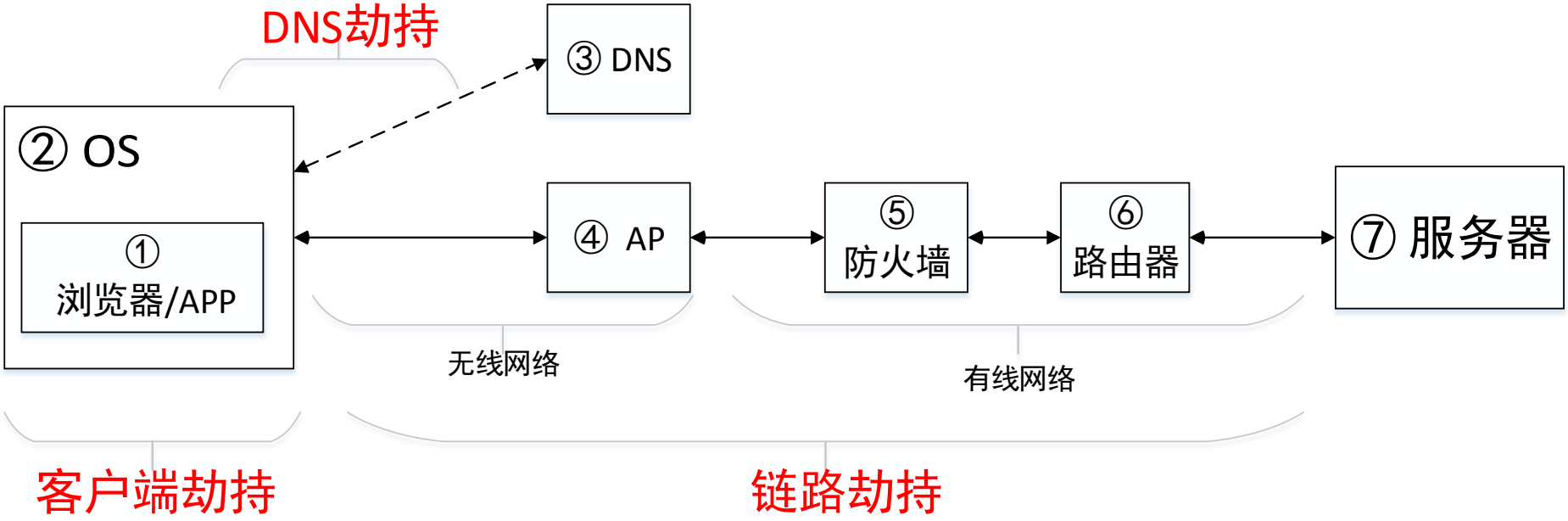
- 2011.03
  - 硕士 毕业于浙江大学 控制系
- 2011.04 ~ 2012.11 百度 广告检索系统运维
  - 百度最早的持续部署系统、分布式文件传输系统
- 2012.11 ~ 2015.07 百度 统一前端（BFE）
  - 性能优化，搜索访问速度优化
  - 百度安全搜索
- 2015.07 ~ now 腾讯 基础架构部 云网关组
  - STGW，腾讯安全云网关

# HTTPS背景

- 安全问题
  - 隐私泄露
    - 登陆态窃取
    - 骚扰电话
  - 内容劫持
    - 广告
    - 不良内容
- iOS ATS
  - 2017.1.1 强制使用HTTPS




# 劫持路径




- DNS劫持
- 客户端劫持
  - 插件、木马
- 链路劫持

# HTTPS访问速度优化

# HTTPS影响速度的因素

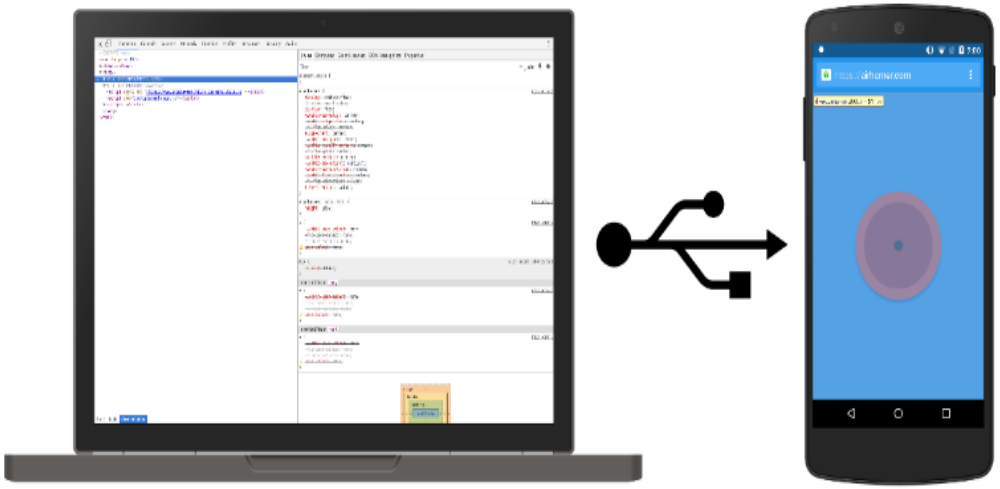
- 网络耗时
  - 最坏情况下增加7个RTT
  - Round trip time
- 计算耗时
  - 客户端，50ms以上
    - 证书校验、密钥交换
  - 服务端，15ms以上

| 网络制式 | WIFI | 4G | 3G | 2G |
|---|---|---|---|---|
| RTT | 70ms | 100ms | 200ms | 400ms |
| 7*RTT | 490ms | 700ms | 1.4s | 2.8s |

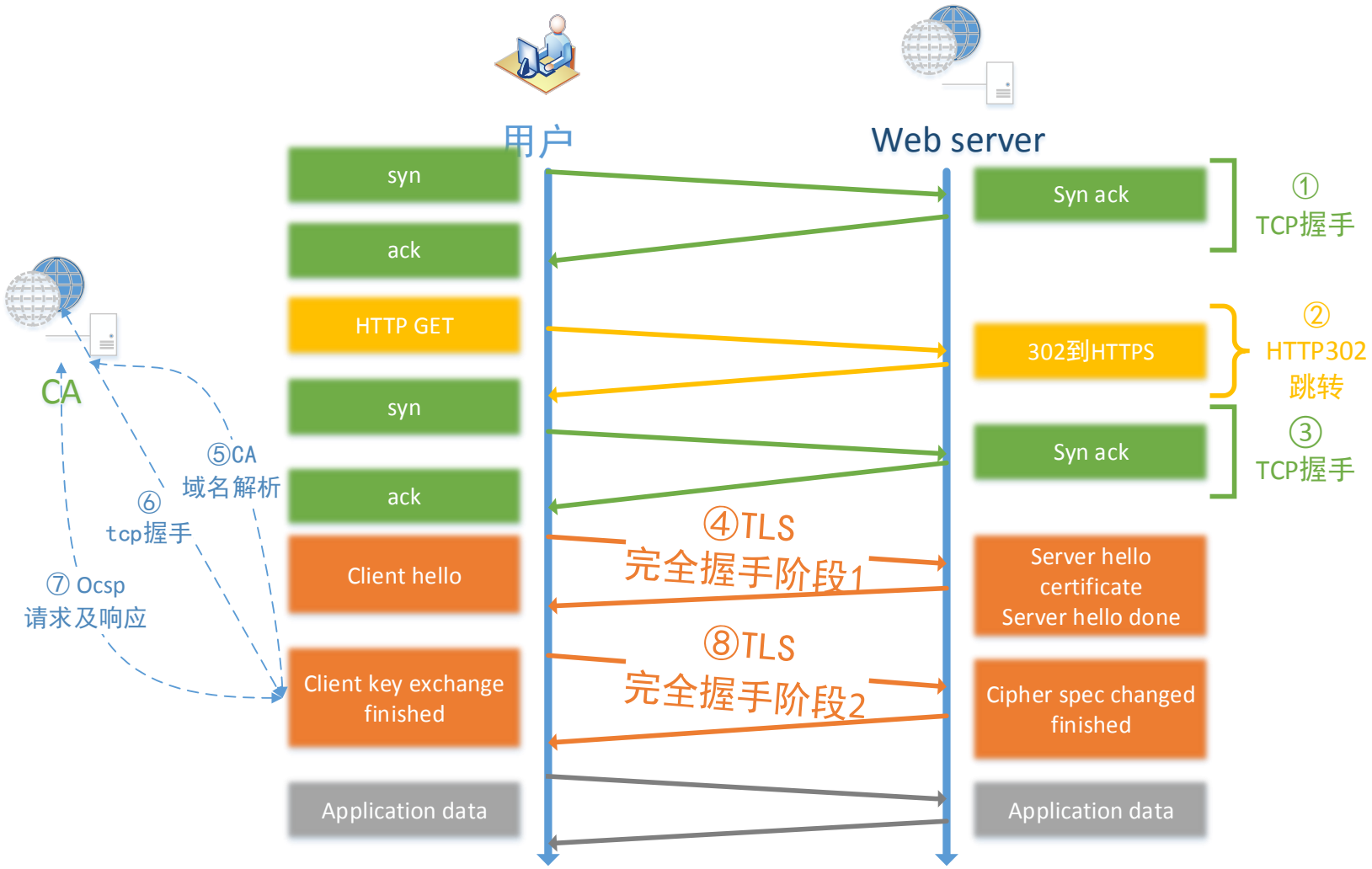
不同网络下的RTT参考值

# 性能分析技术

- 服务端耗时
  - Openssl speed, wrk
  - 握手时间计算
- 客户端耗时
  - Chrome Remote debug
  - Performance timing api
- 环境模拟
  - Linux traffic control
  - atc(facebook)



# HTTPS增加7个RTT

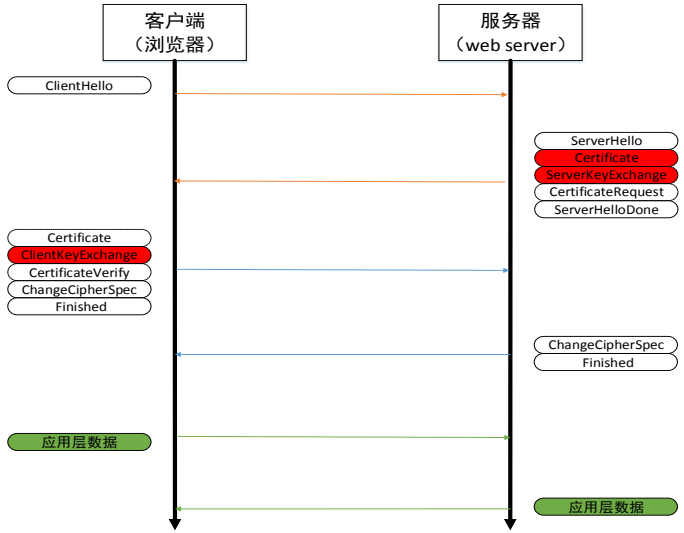


# HTTPS速度优化---TCP连接层面

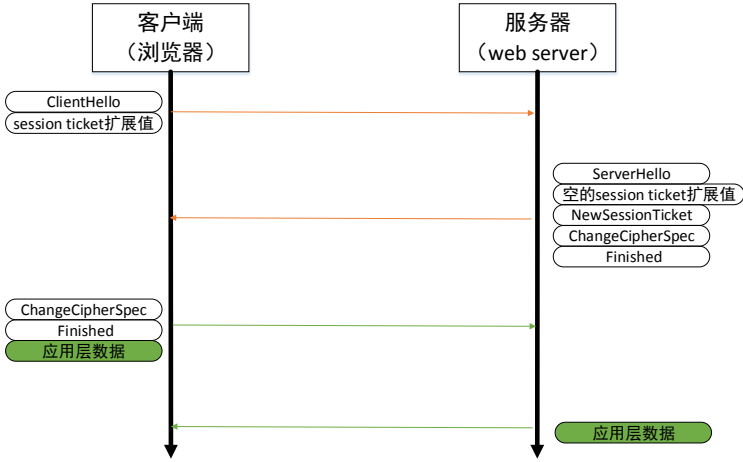
- 提升初始拥塞窗口
  - 3 → 10
- 节省TCP连接
  - Tcp fast open(缺乏支持）
- 提前建立连接，减少用户可感知的延迟
  - 预连接 400ms以上
    - 首页提前预建子页面连接
  - 长连接维持(stgw_precon.html)
    - 后台JS秒级别维持长连接

# HTTPS速度优化---SSL协议层面

- SSL握手时间优化
  - 提升简化握手，节省1RTT
    - 全局session cache
    - 全局session ticket
  - 完全握手
    - False start，节省 1 RTT
  - Tls 1.3(draft)
- SSL 动态record size
- 证书状态查询
  - ocsp stapling



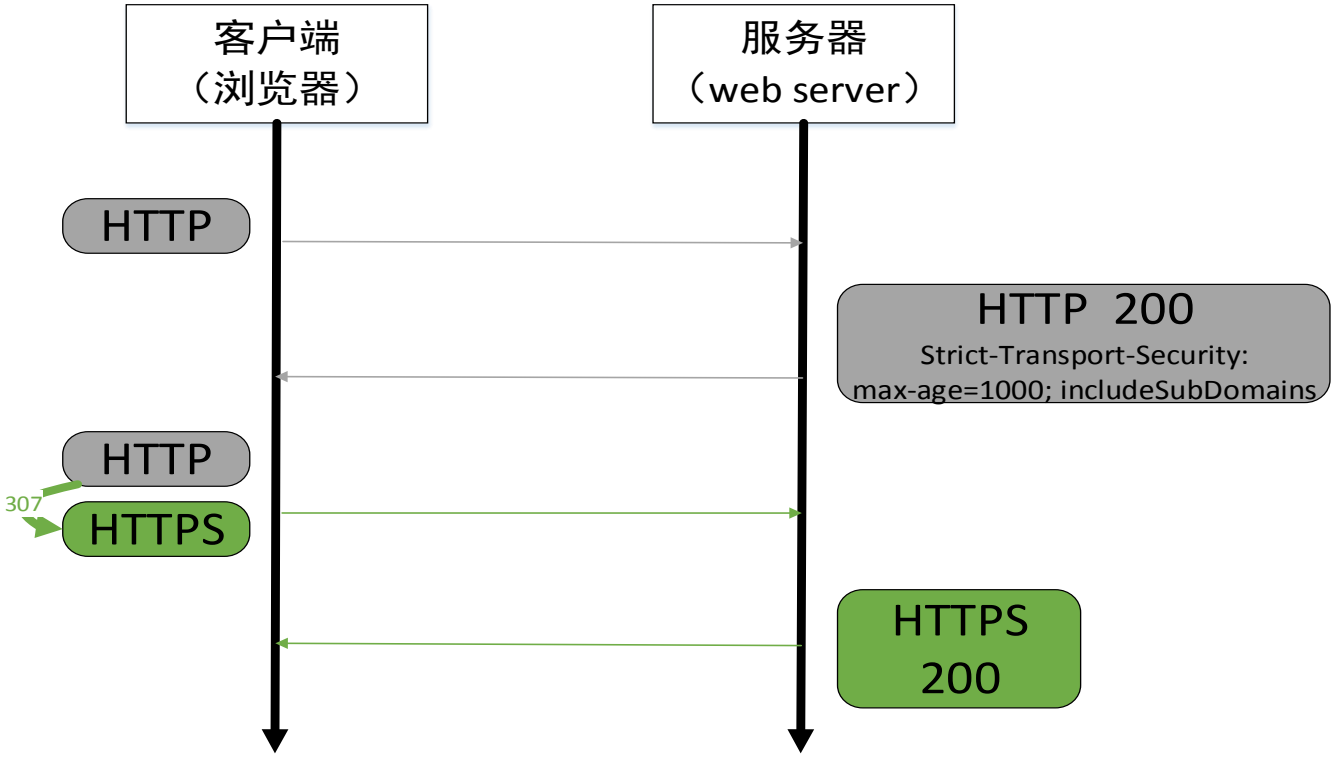

完全握手




简化握手

# HTTPS速度优化---应用层协议层面

## HSTS减少302跳转

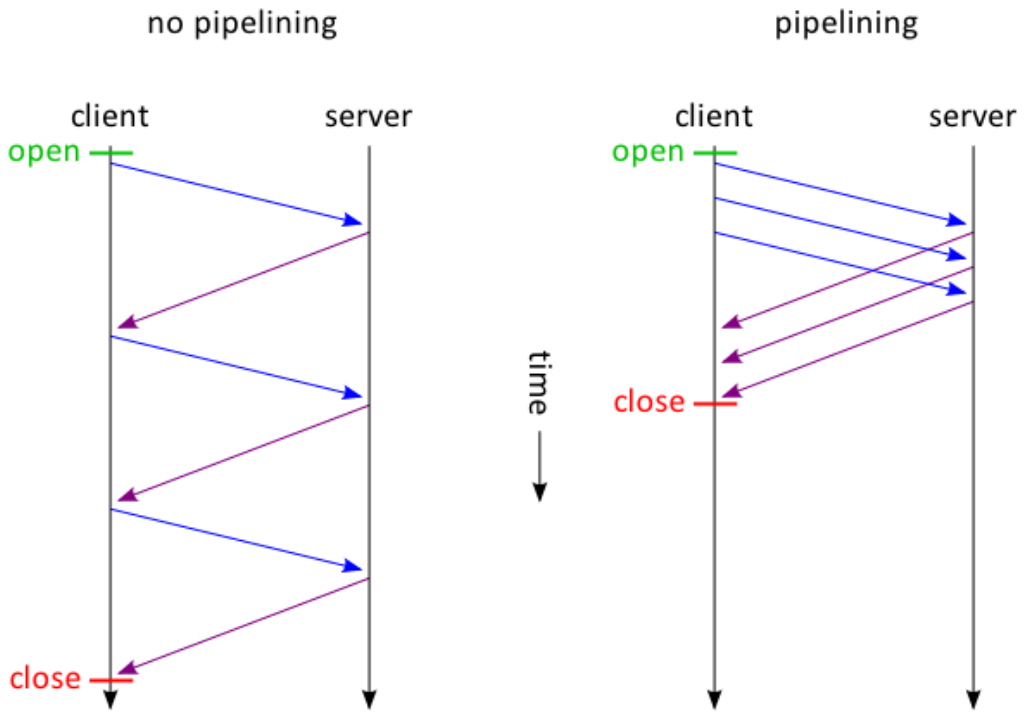



- HTTP Strict Transport Security(HSTS)
  - Strict-Transport-Security: max-age=0; includeSubDomains
- Preload list
  - https://hstspreload.appspot.com

# HTTPS速度优化---应用层协议层面

## HTTP1.X协议的问题

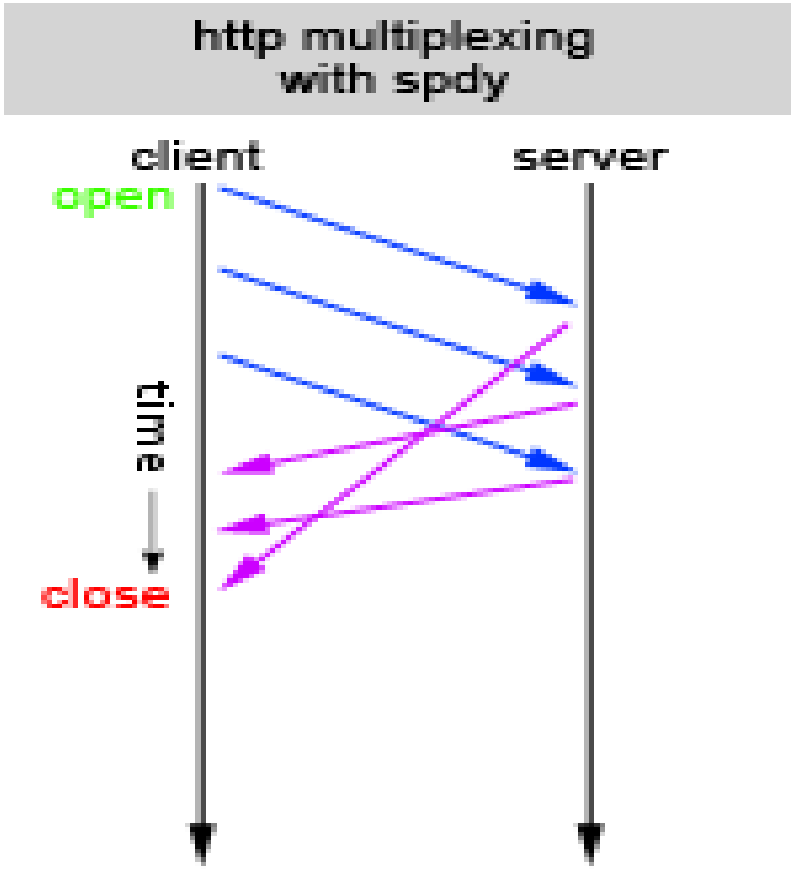
- 串行
- Pipelining
  - head of line blocking
  - 实现上的BUG
- 单域名多连接
  - 影响TCP特性
- 多域名
  - HTTPS建连消耗时间
  - 建议3个域名



# HTTPS速度优化---应用层协议层面

## HTTP2X的优点

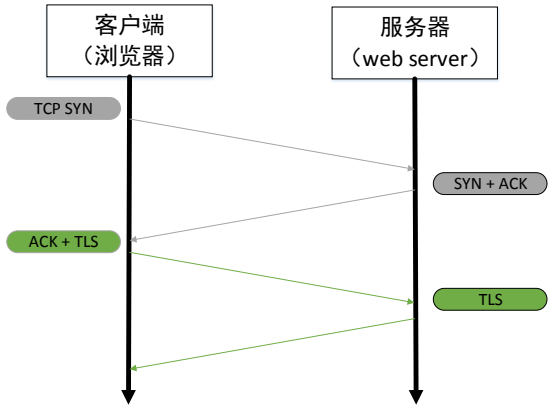
- 二进制
  - 方便解析
- 多路复用
- 头部压缩
  - 90%压缩率
- 优先级
- Server push

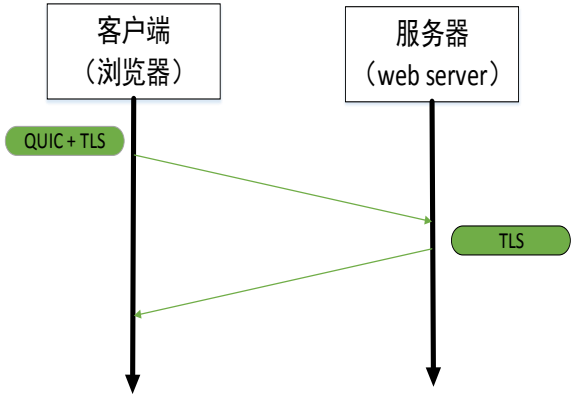


# HTTPS速度优化---应用层协议层面

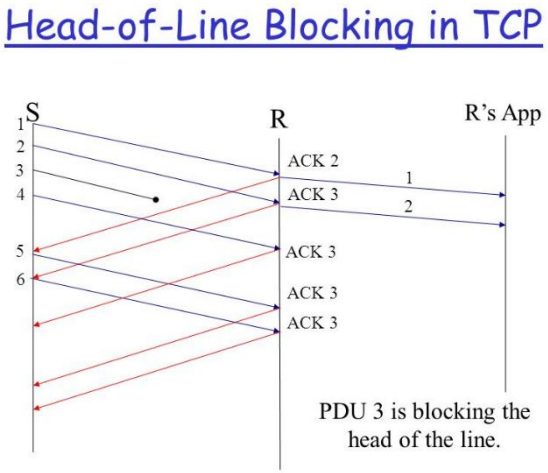
## QUIC

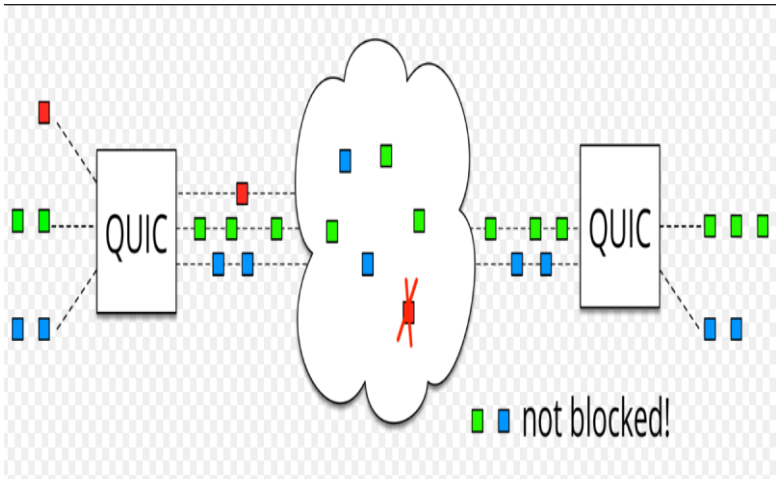
- 0 RTT 建连



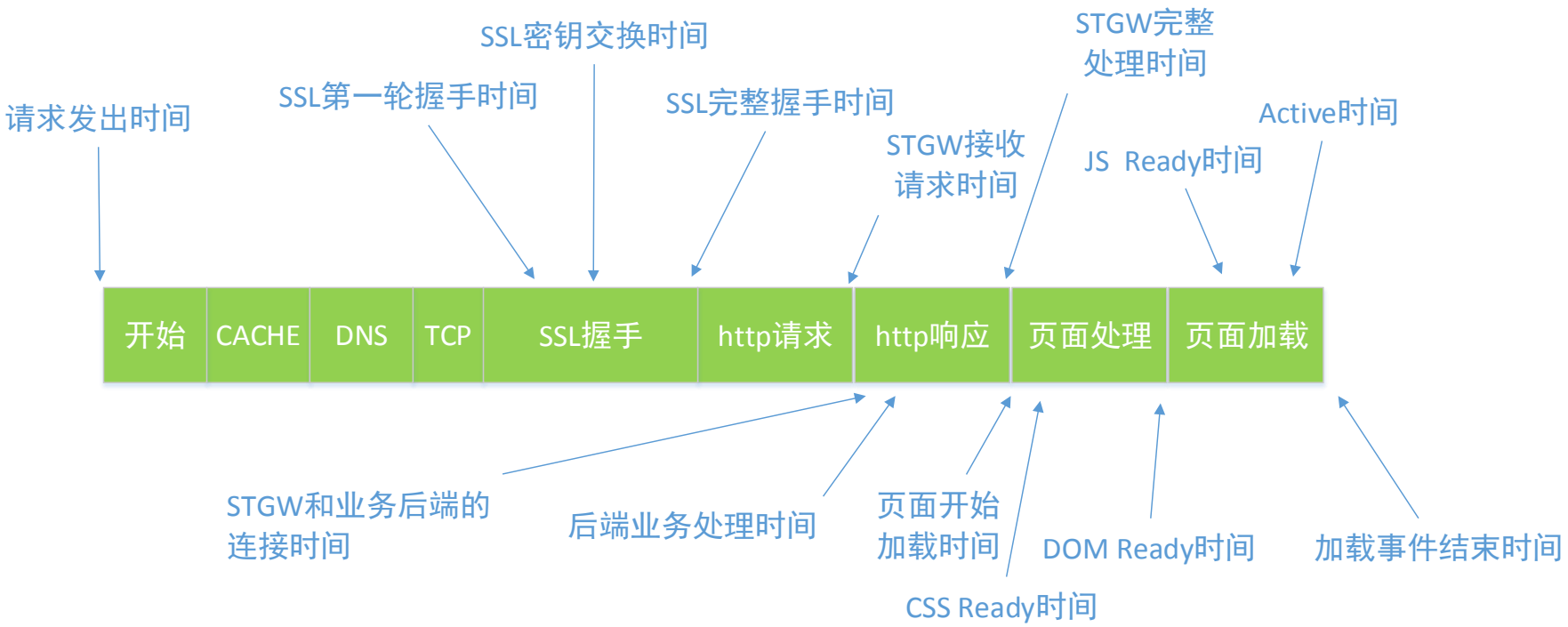




- 没有TCP的队头阻塞



# HTTPS访问速度优化---数据分析

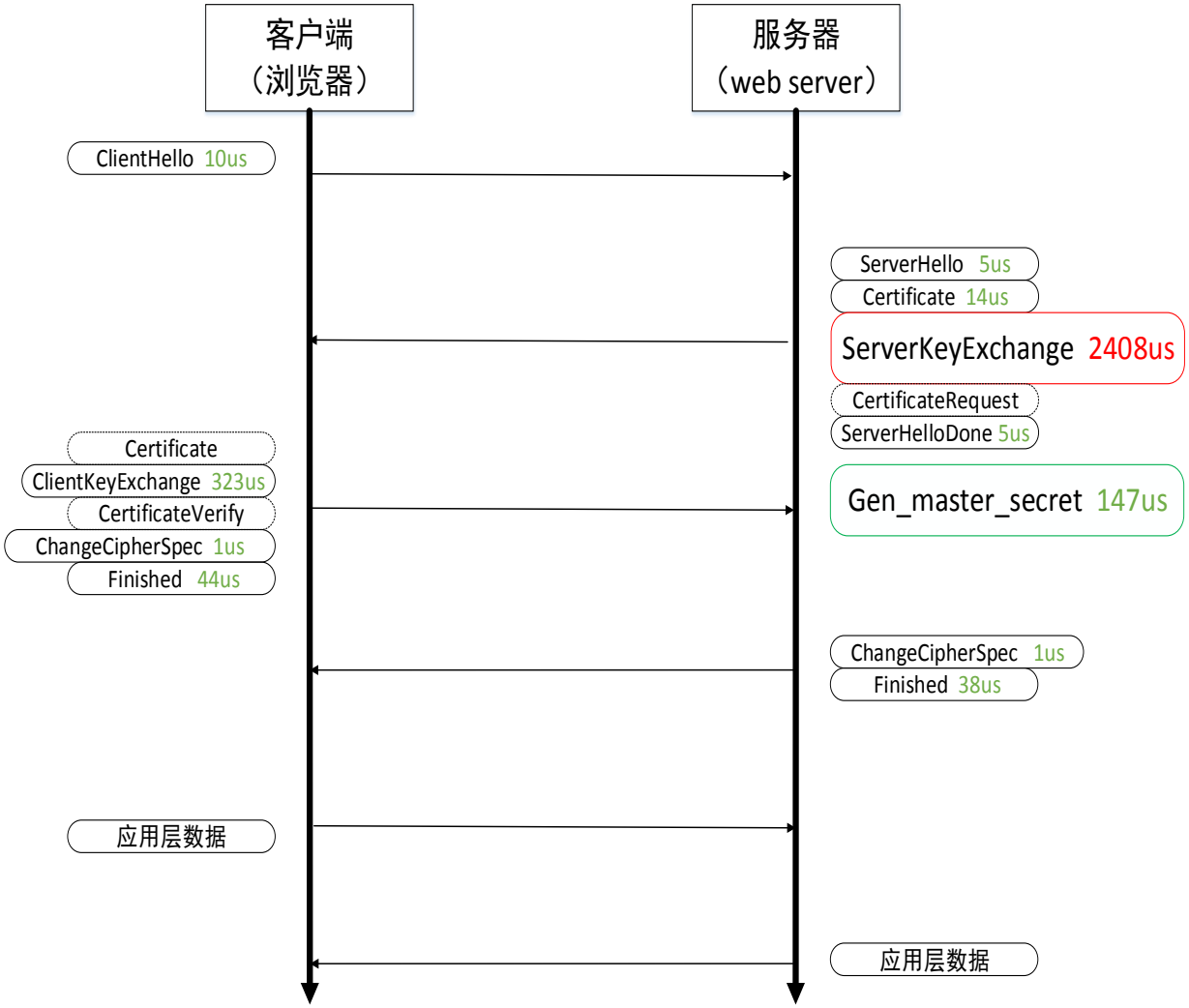


# HTTPS计算性能优化

# HTTPS主要计算环节及分析

算法→协议→系统

- 非对称密钥交换
  - RSA消耗80%以上
  - $c \equiv m^e (mod\ n)$
- 证书签名校验
  - 微秒级
- 对称加解密
  - 内容相关
- 内容一致性校验
  - 微秒 级




ECDHE_RSA密钥交换算法的握手耗时

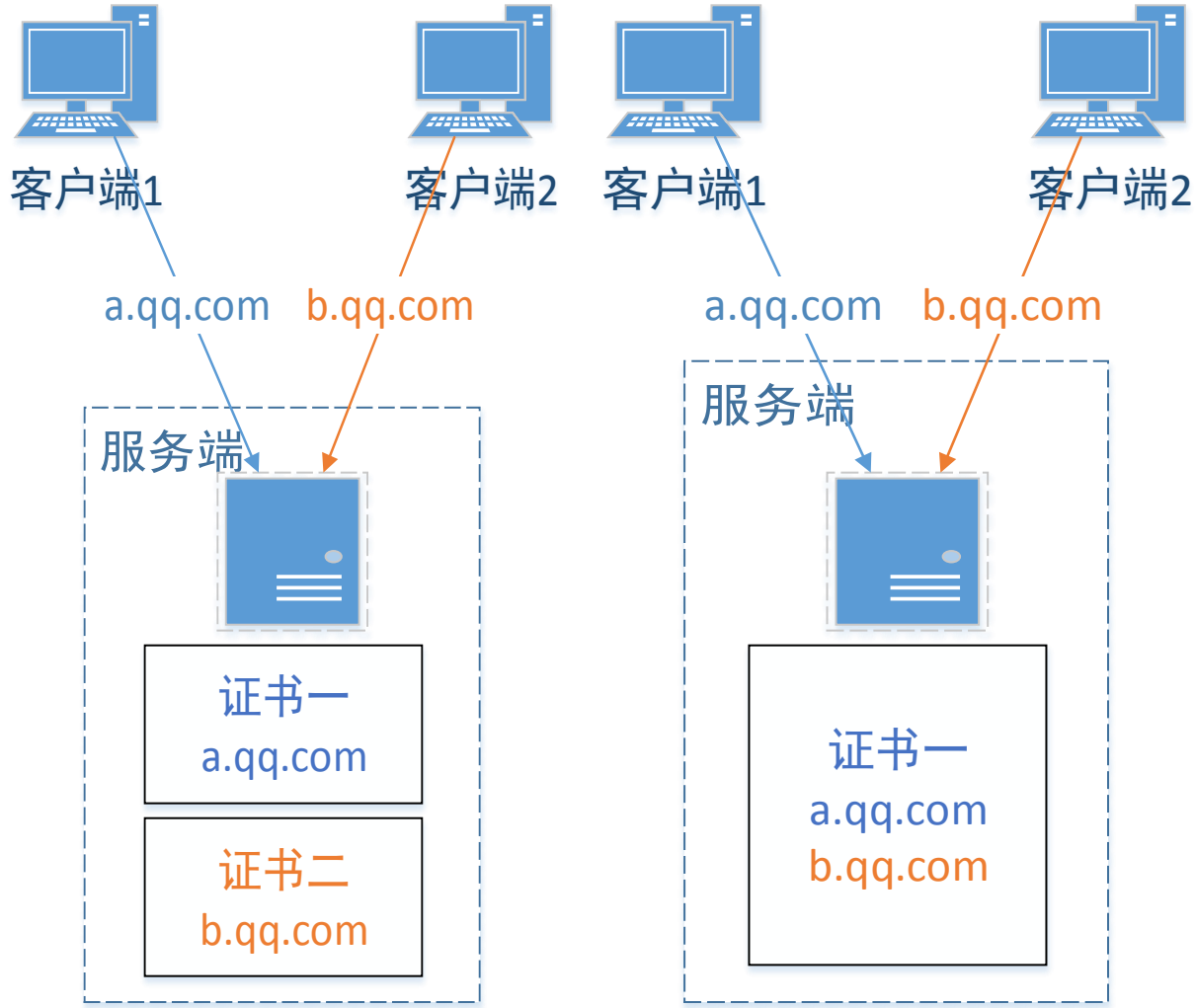
# HTTPS计算性能优化

- 优先使用ECC
  - P256
- 使用最新版openssl/libressl/boringssl
- 移动端使用 chacha20/poly1305
- TLS异步代理计算
  - 借助硬件加速卡

# HTTPS部署过程中的问题

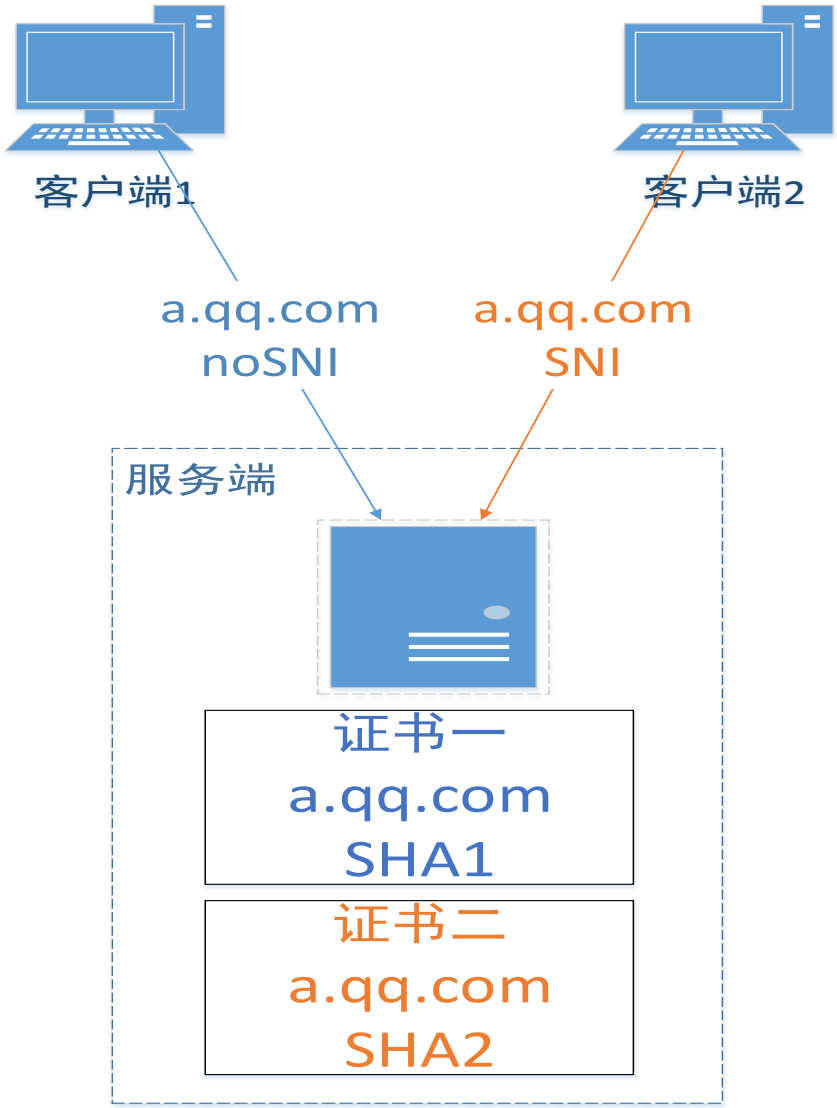
# 单IP使用多张证书/域名

- SNI
  - Server name indication
  - IE8，XP不支持
- 多域名证书
  - SAN
- 页面提示升级



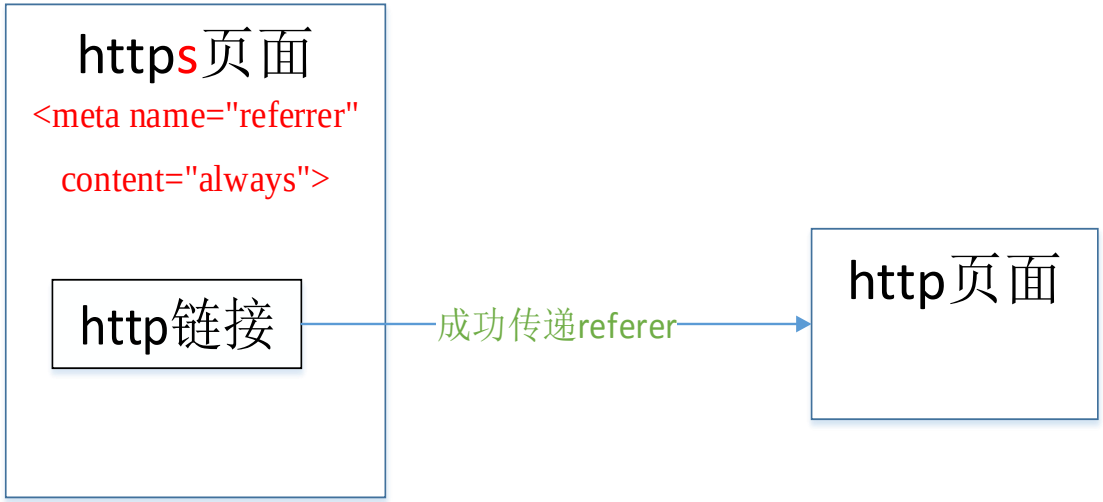
# 兼容SHA1、SHA256

- SHA1 or SHA256
  - SHA1不安全
  - SHA2兼容性差
- 不支持SNI = 不支持SHA2？
- Nginx配置
  - 证书一 server_name空

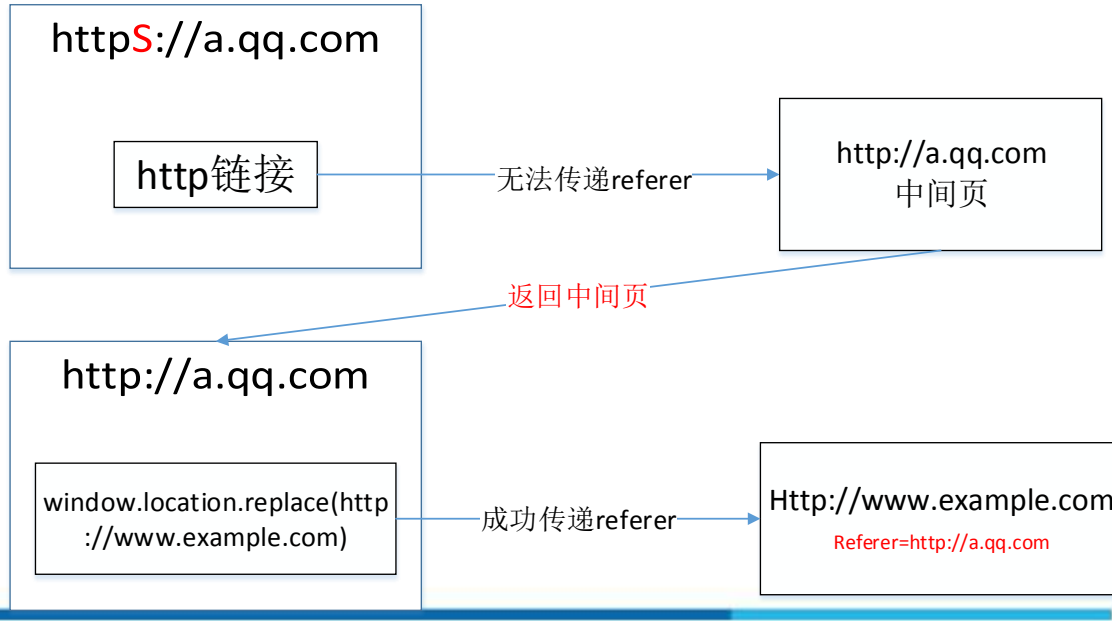


# HTTPS Referer传递

- Meta标签 referrer
  - <meta name="referrer“ content="always">




- 不支持meta标签
  - IE8
  - HTTP中间页跳转



# 其他问题

- 证书过期、监控
  - 系统时间错误
- 中间证书链
  - Android系统多
- 连通性问题
  - 小运营商
- Fiddler代理

# HTTPS发展趋势

- https everywhere
  - http1.1 -> http2
  - http2主流实现强制使用https
  - ATS 强制使用HTTPS
- 加密强度增加
  - Rsa 1024 -> 2048 -> 4096
  - Rsa -> ecc
- 证书开源免费
  - Let’s encrypt公测
- 速度提升
  - Tls1.3 减少握手

helloworlds

# THANKS