



Operations



“秒开” 体验背后的CDN优化之路

新浪内容加速平台 - 徐永健

2018年5月



目录

01

SinaEdge 架构介绍

02

CDN 服务优化要点

03

特殊服务场景与优化

04

HTTPS 优化实践



Operations



SinaEdge 架构介绍

01



什么是CDN?



Operations



3556
关注

880690
粉丝

68930
微博

全部

热门

更多

搜索他的微博



最近

2018

2017

2016

2015

2014

2013

2012

2011

2010

2009

查看更多微博

内容

- html
- js
- jpg
- mp4
- ...

分发

- 代理
- 缓存
- ...

网络

- 多地域
- 多运营商
- 大带宽
- 低延迟
- 调度系统
- ...

Resources Network Performance Memory Application Security Audits AdBlock

☐ Group by frame ☐ Preserve log ☐ Offline Online

data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other

60000 ms

80000 ms

100000 ms

120000 ms

140000 ms

160000 ms

180000 ms

200000 ms

220000 ms

240000 ms

260000 ms

Headers Preview Response Timing

x-cache: HIT TCP MEM HIT dirn:0:80163231 mlen:-1

x-debug-hit: sto(30795,0.303)

x-request-id: g63.138-1510762419.318000-3198714620

x-swift-cachetime: 7775680

x-swift-savetime: Tue, 15 May 2018 06:00:34 GMT

x-via-cdn: f=alicdn,s=cache2.cn211,c=61.135.152.133;f=alicdn,s=cache19.12nu20-3,c=202.108.250.203 f=edge,s=cnc.guangzhou.ha2ts4.41.nb.sinaedge.com,c=27.221.6.36;f=Edge,s=cnc.guangzhou.ha2ts4.59,c=1

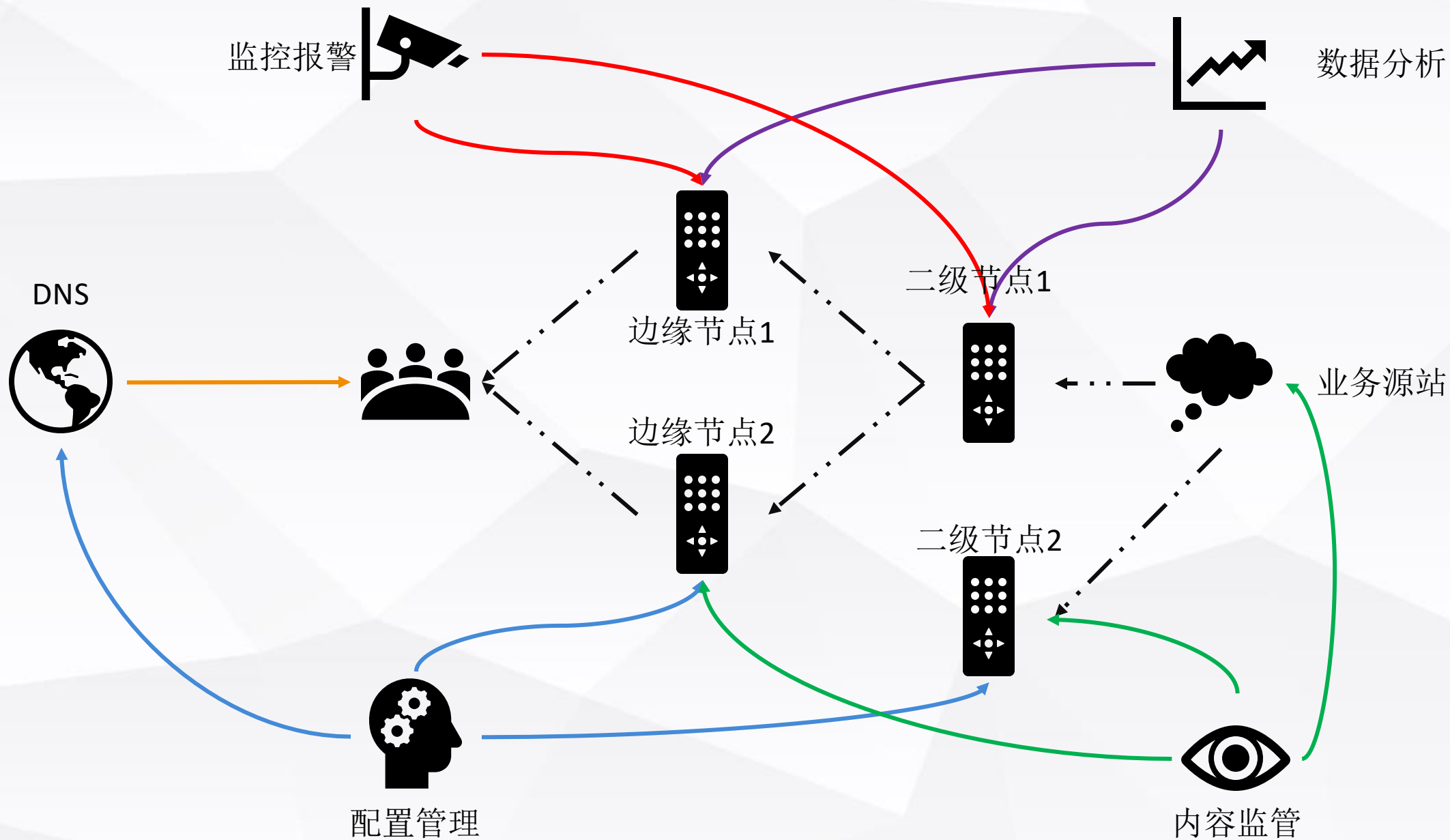
x-via-edge: 15263637146172406dd1bee065a7018c3514b



系统架构



Operations

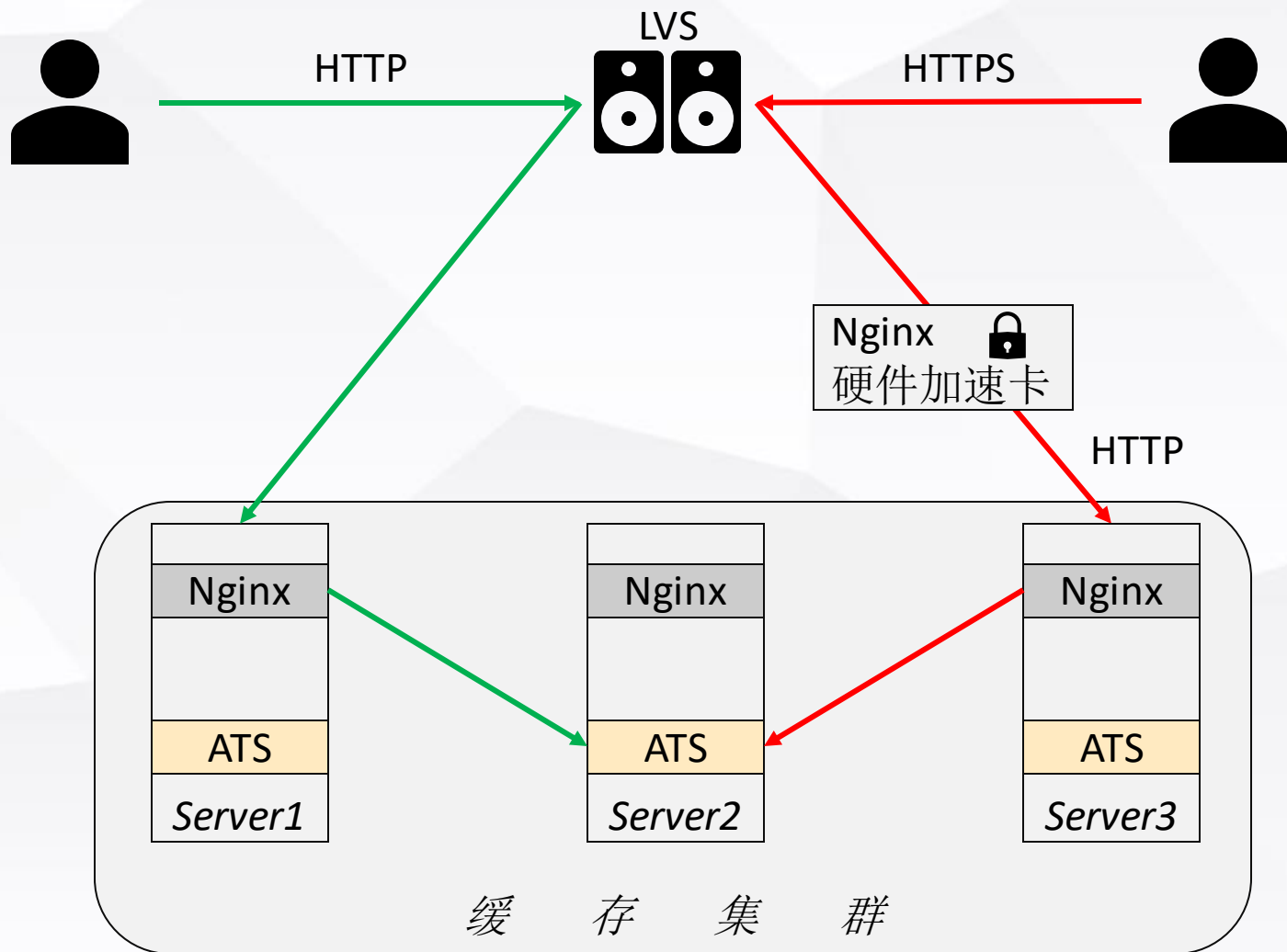




缓存节点架构



Operations





CDN 服务优化要点

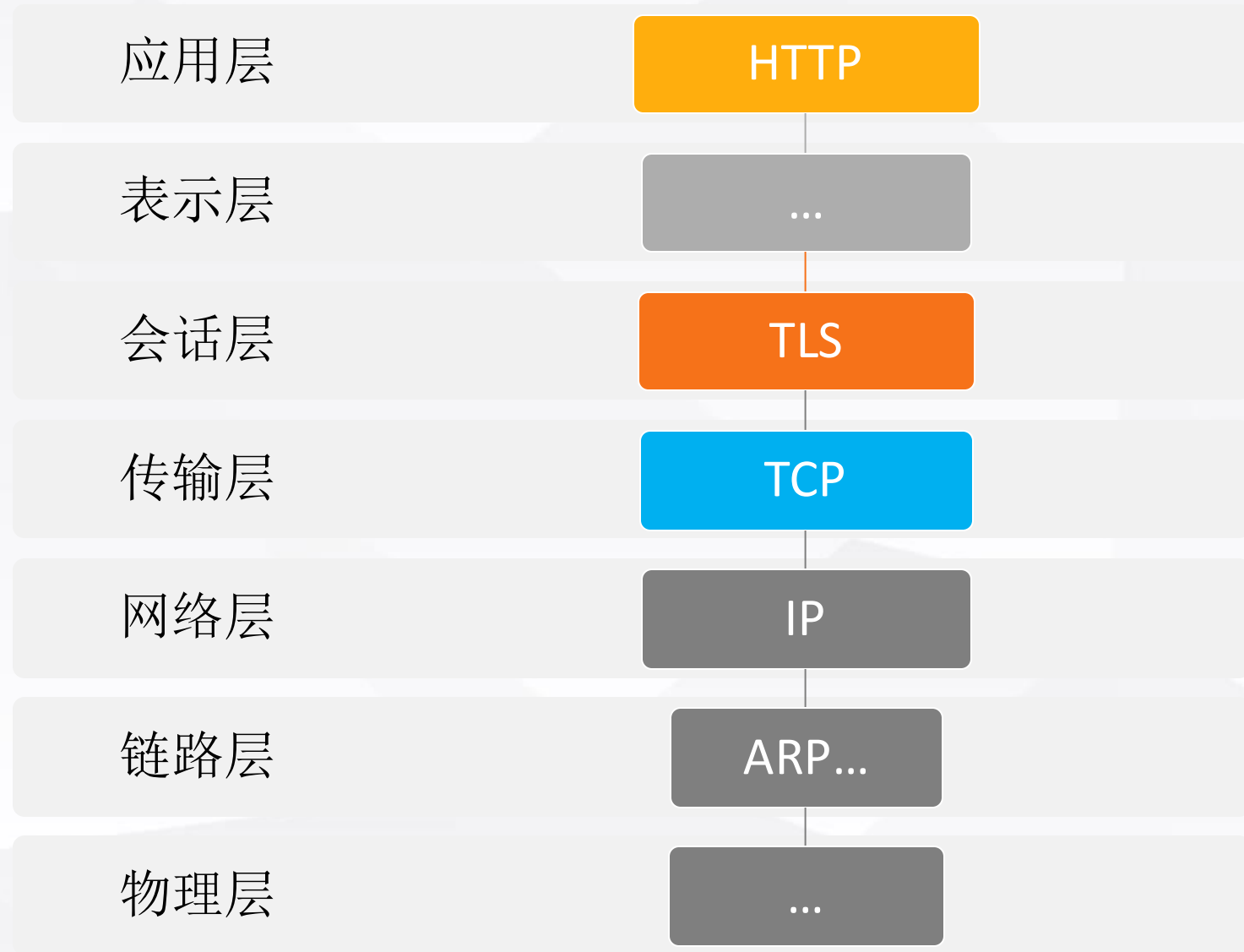
02



CDN 基础技术栈



Operations

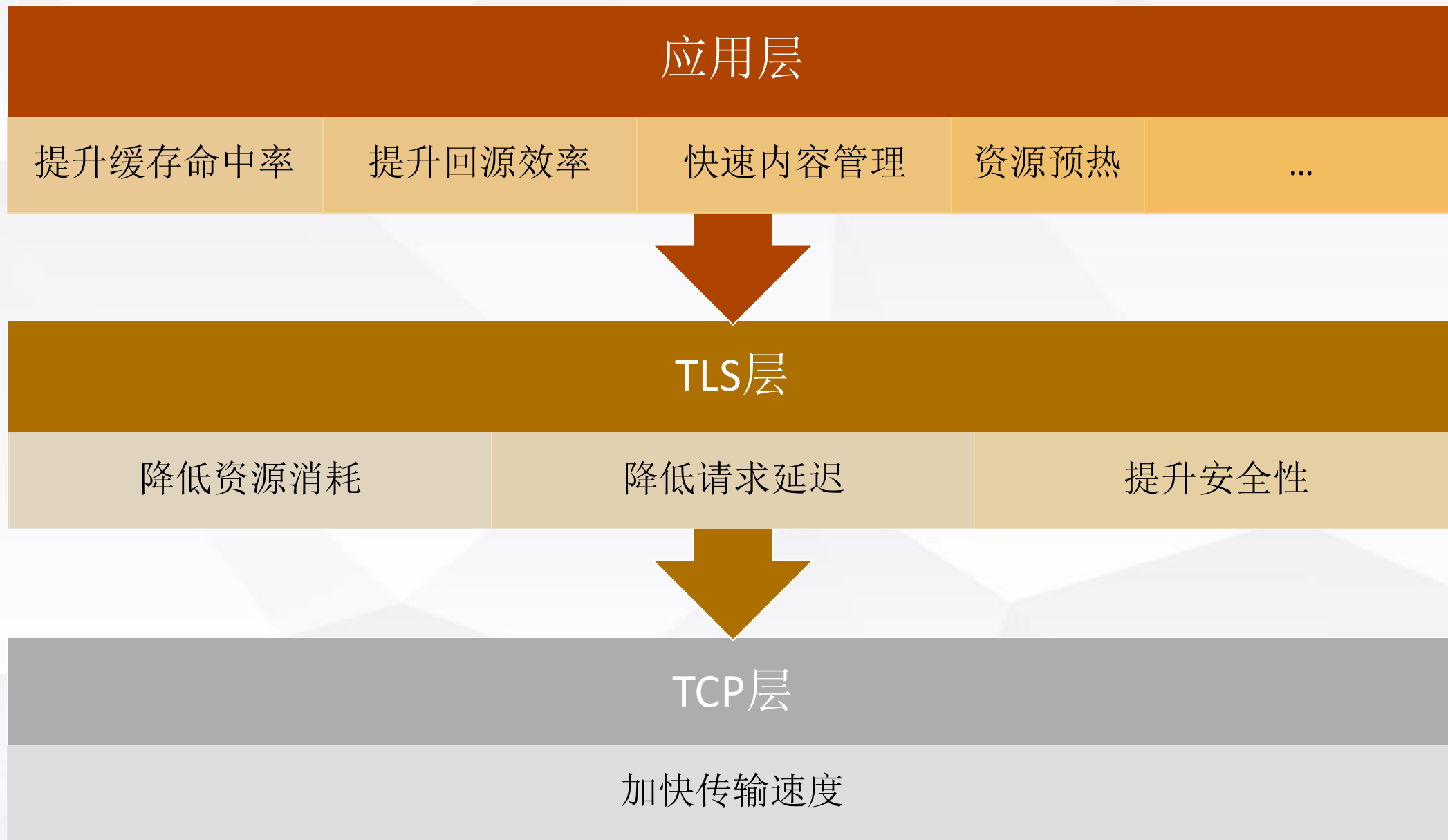




CDN 服务分层优化要点



Operations





特殊服务场景与优化

03



用户**A**: **xx**视频特别火，你看了没？

用户**B**: 快发给我！

10秒钟后... 视频还没有打开



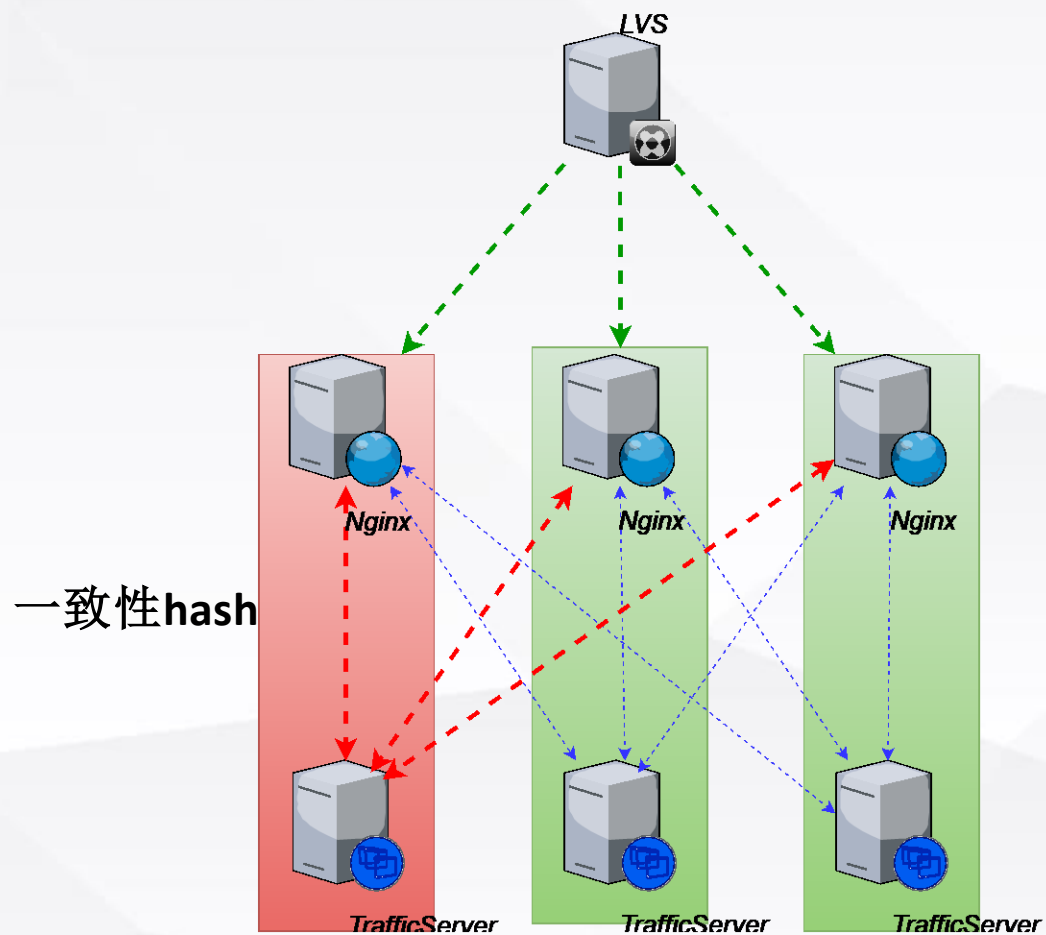
热点文件问题与解决方案



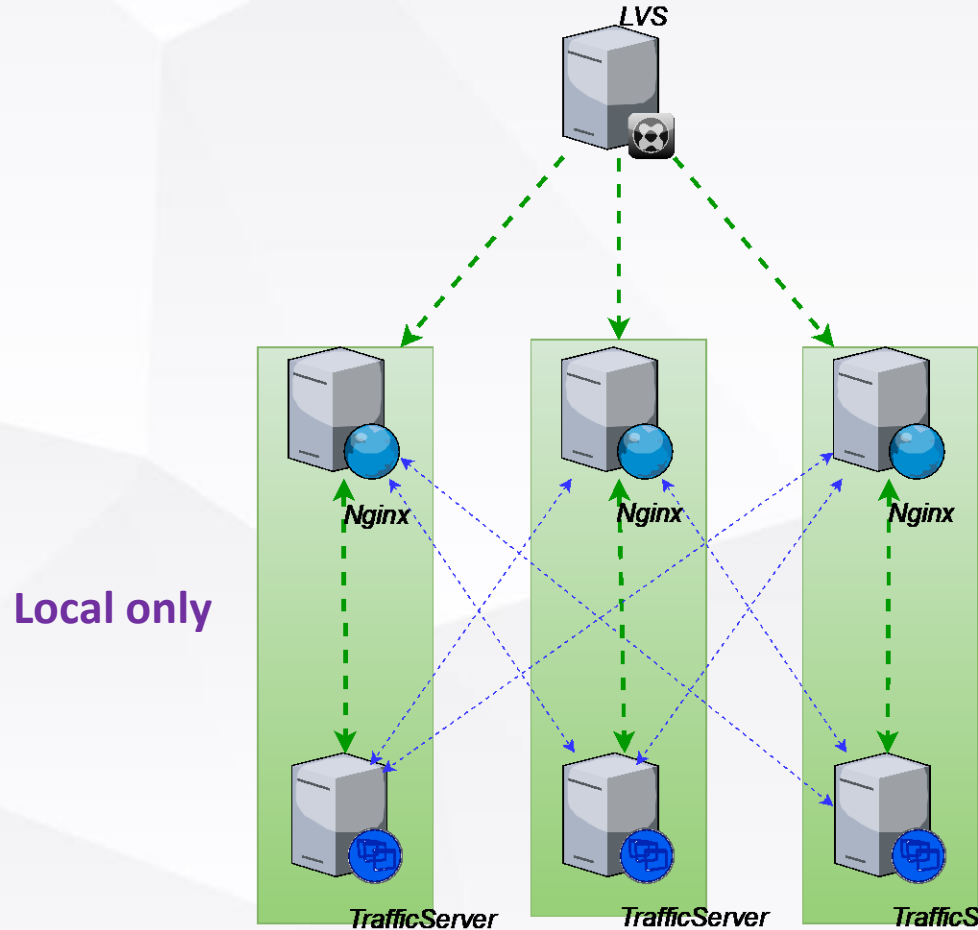
Operations



热点文件导致某缓存过载



发现热点文件后直接本地服务





小猿：老板，业务上线了！

老板：干的漂亮，晚餐加鸡腿！

1分钟后...服务器瘫痪



应对情况

秒杀等活动页面资源

定时更新或发布的资源

准备新上业务

...

预热等级

仿真预热（边缘节点）

普通预热（二级节点）



网监：这张图片社会影响很不好！

小猿：稍等，我清理一下

1分钟后...服务器IP被封



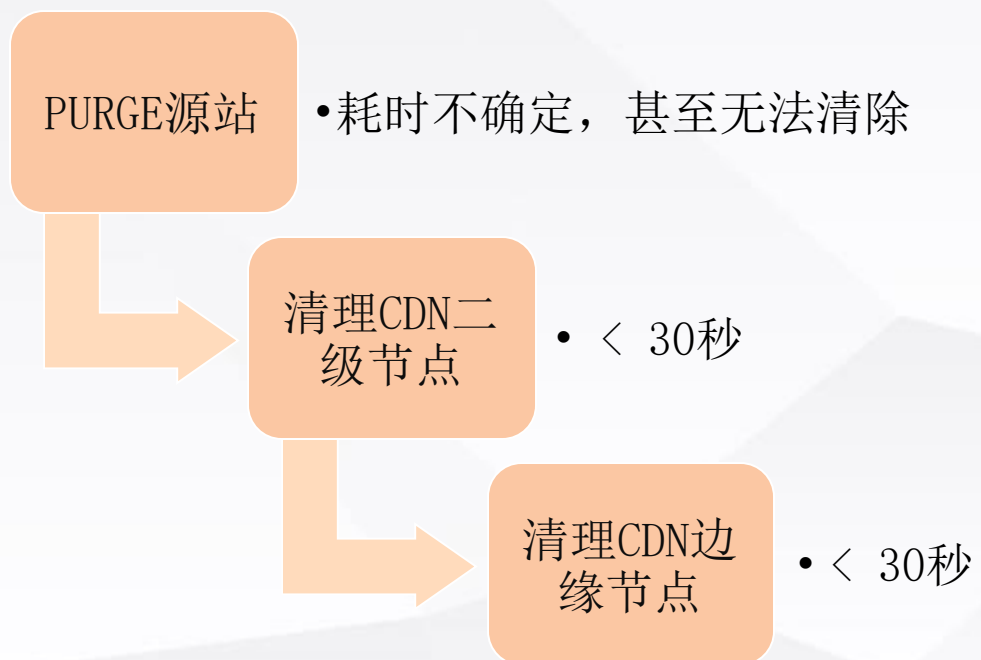
URL快速封禁



Operations



普通的缓存清除操作



快速封禁





Operations



HTTPS 优化实践

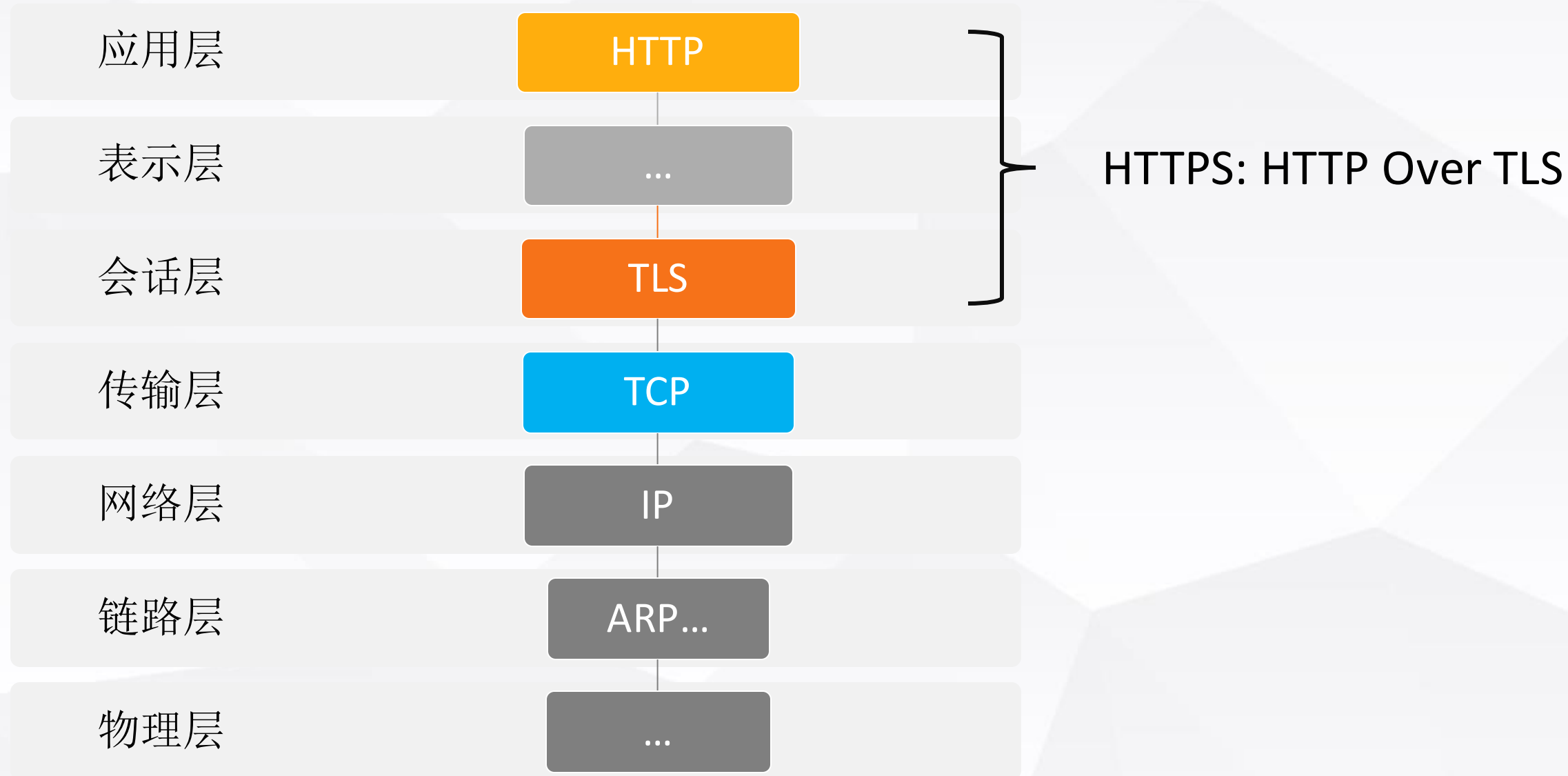
04



HTTPS



Operations





劫持

隐私泄露

钓鱼网站

...



响应慢

服务器压力大

证书管理麻烦

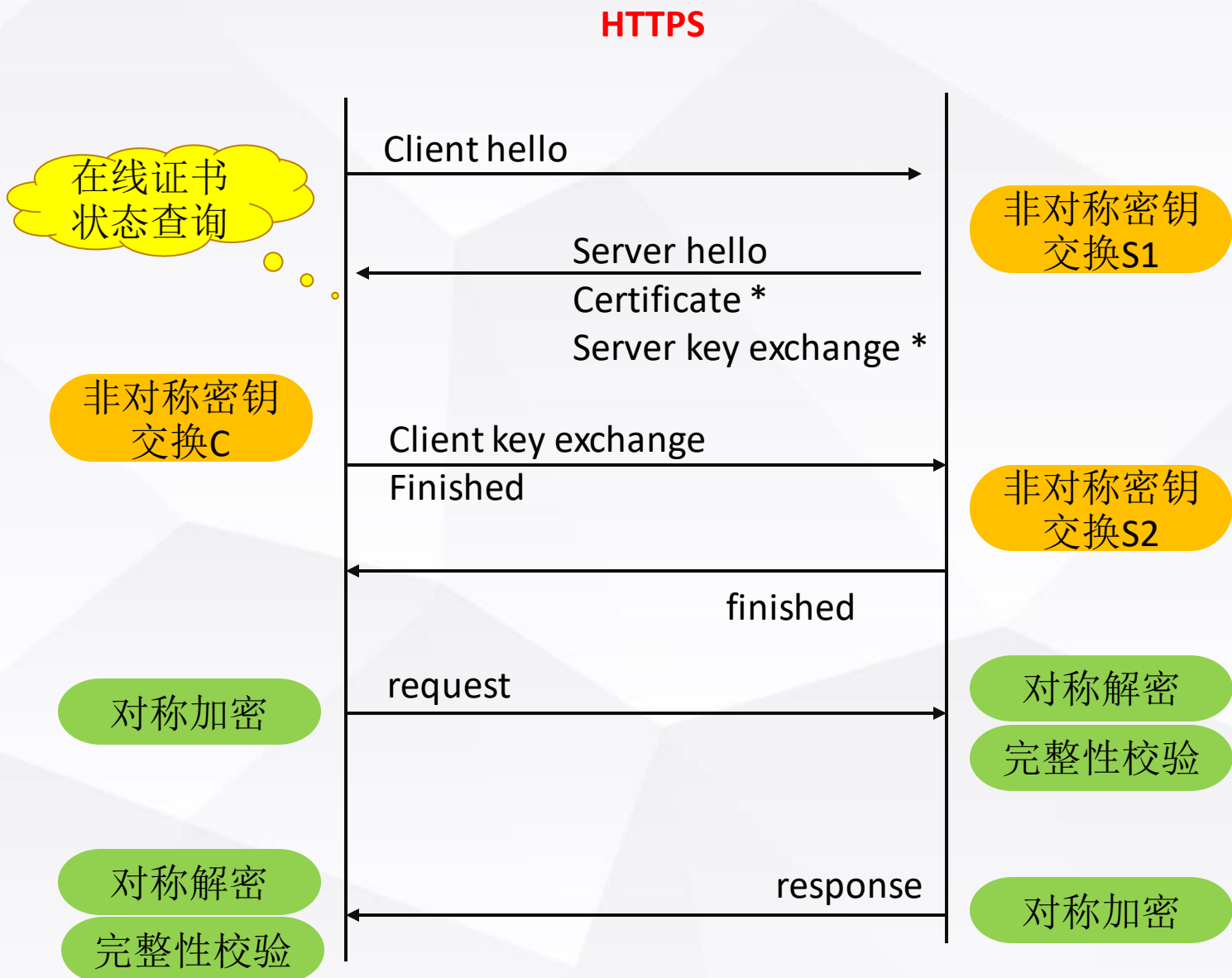
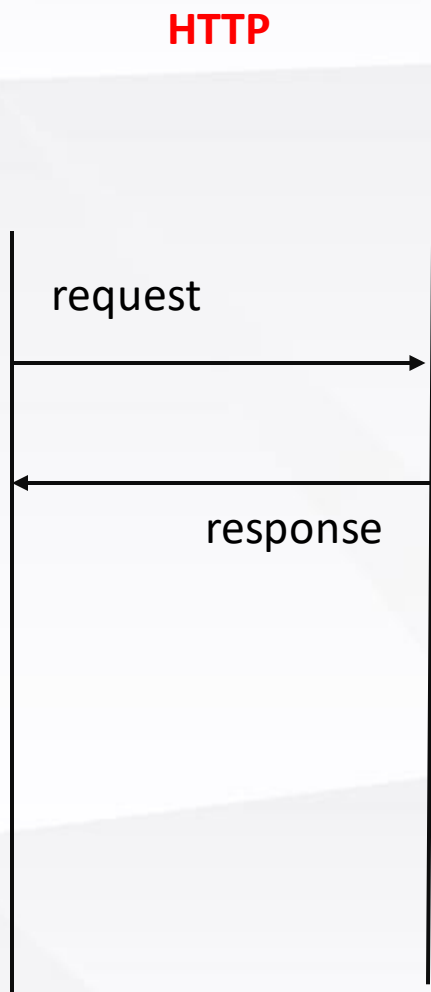
...



HTTPS 慢且耗能



Operations





HTTPS 现有解决方案



Operations



在边缘节点中加入专门的HTTPS代理集群（带SSL硬件加速卡）

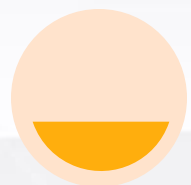




HTTPS 重点优化内容



Operations



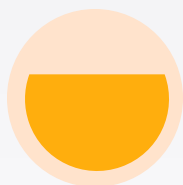
降低消耗

硬件加速卡

远程异步计算

加密套件选择

...



减少延迟

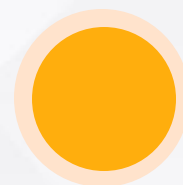
Keepalive

HTTP/2

TLS session 恢复

OCSP Stapling

...



安全增强

私钥安全

session ticket key

自动更换

HTTP强制跳转

...



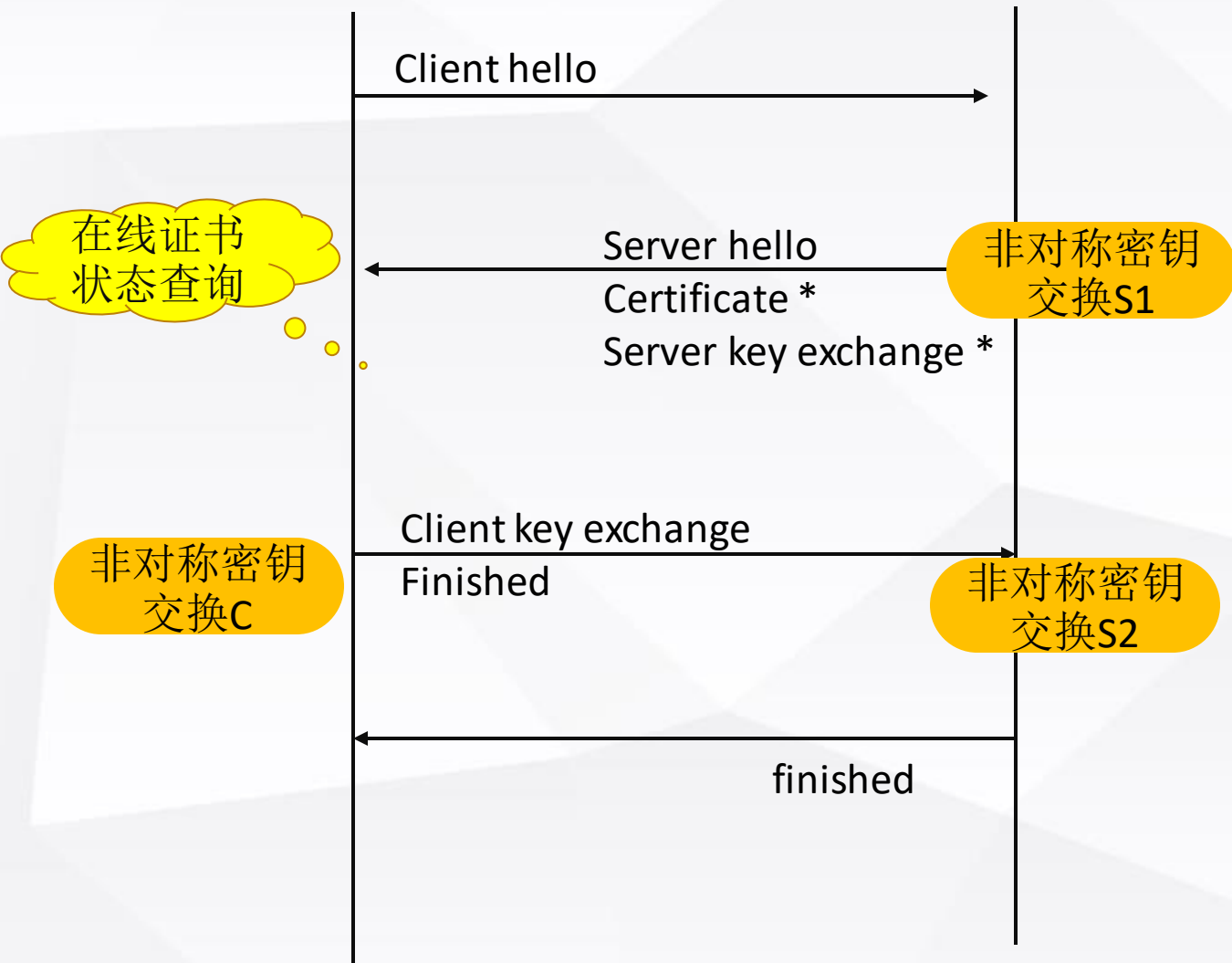
TLS session resume



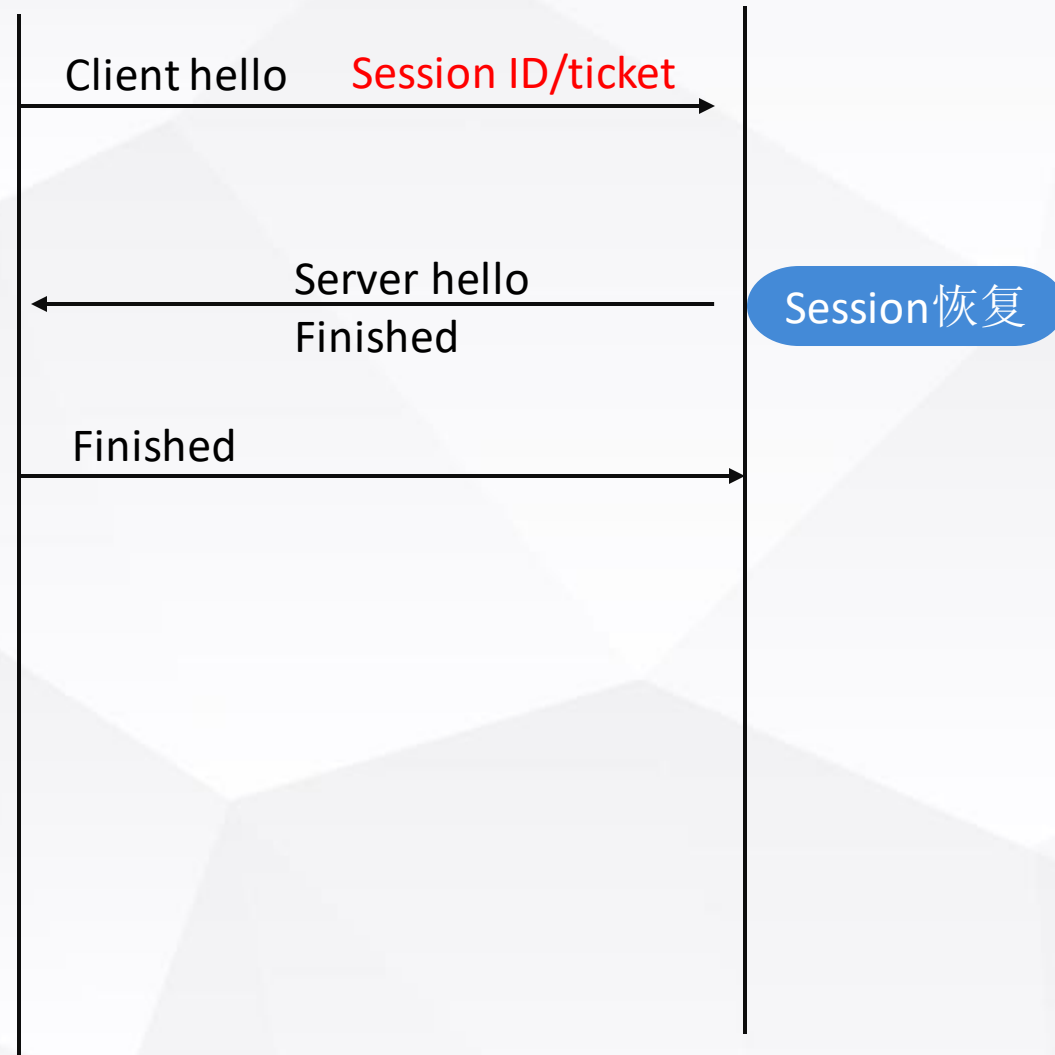
Operations



完全握手



简化握手 (Session resume)





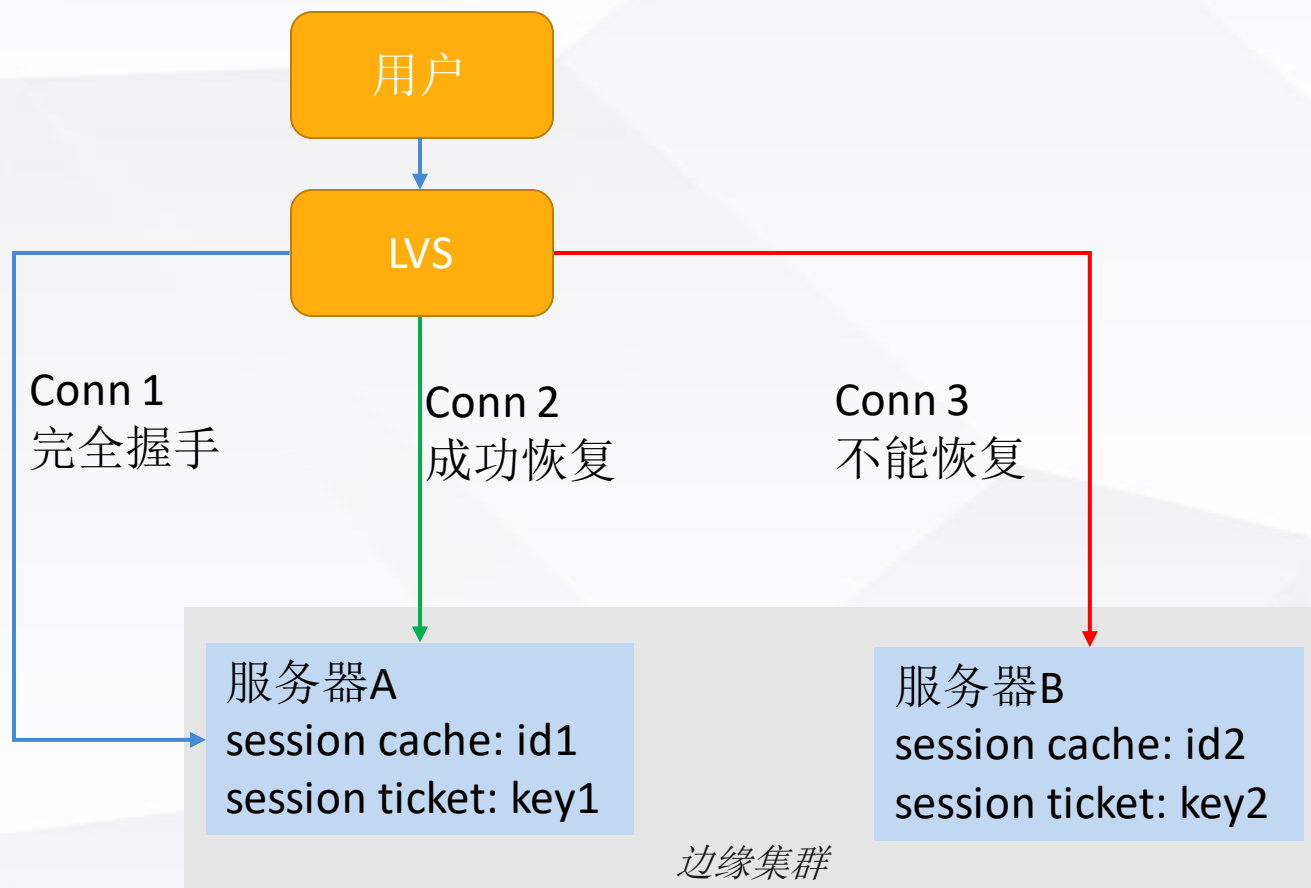
TLS session resume的障碍



Operations



Nginx仅支持单机的session cache



我们还需要:

- session **cache** 多机共享
- session **ticket key** 多机同步



TLS session cache 多机共享



Operations



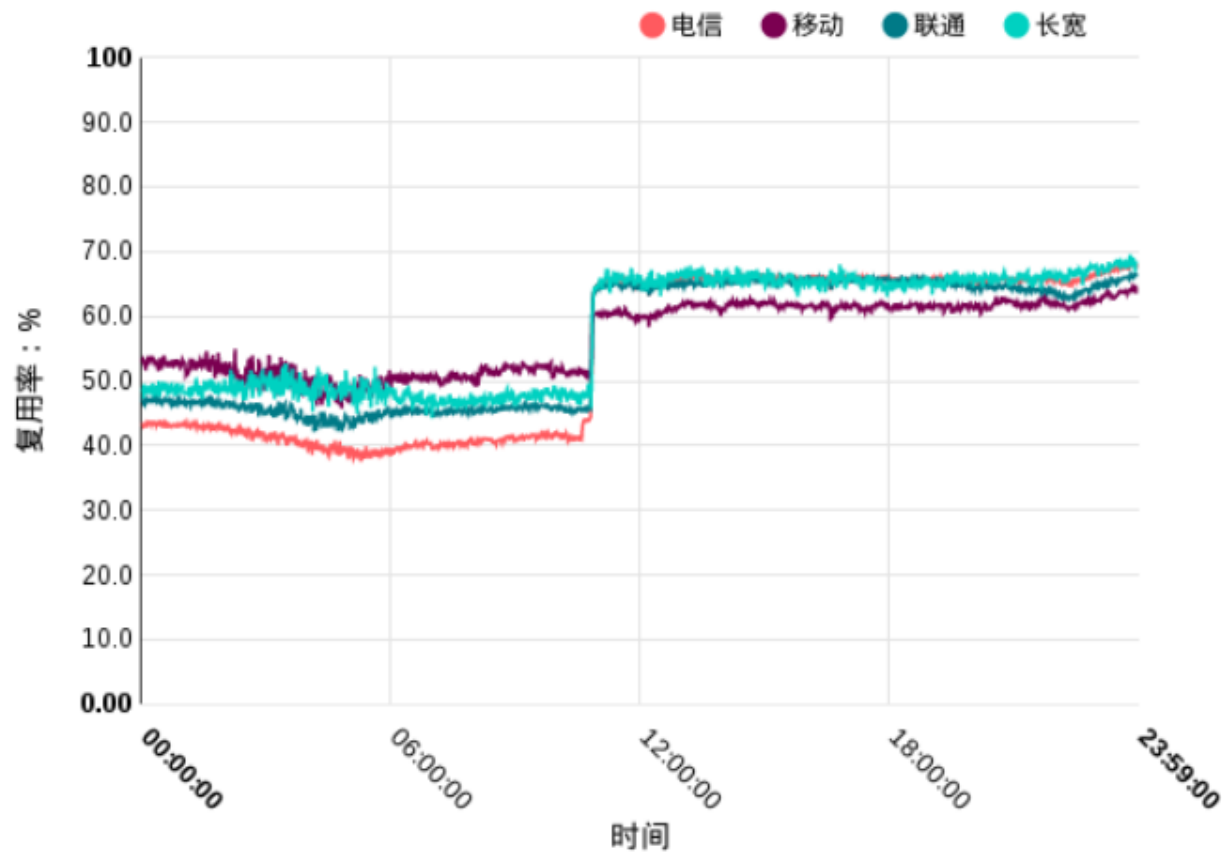
Nginx +
lua

不依赖其
他进程或
中心节点

一致性
hash

健康检查

各运营商session复用率趋势图

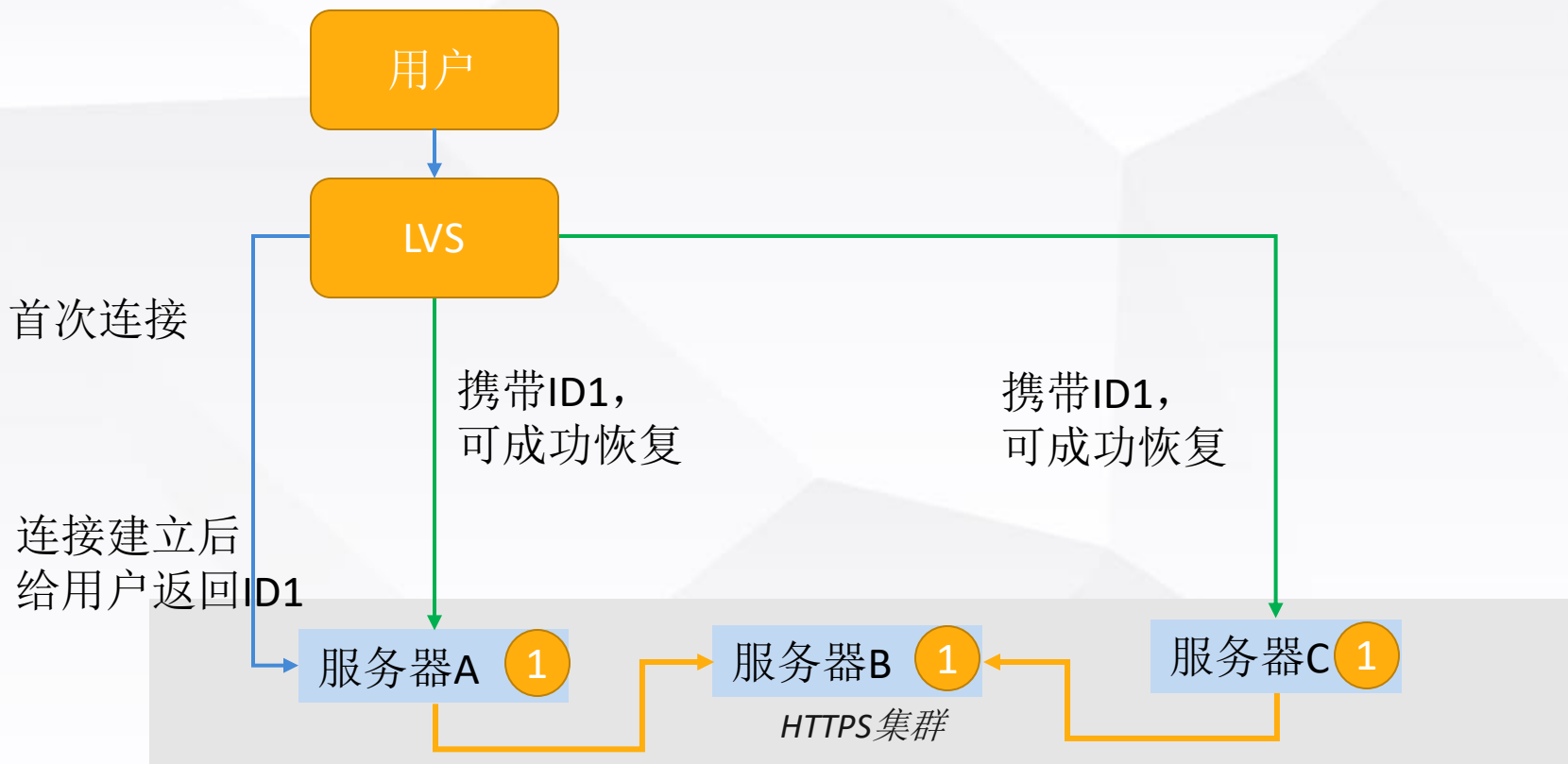




TLS session cache 多机共享



Operations



- 1 存储ID1到本机
- 2 通过一致性hash运算出应该同时存储到服务器B

- 1 本机查找失败
- 2 通过一致性hash运算出应该去服务器B查找
- 3 存储到本机



TLS session ticket key 多机同步与自动更新



Operations



配置灵活

安全性高

允许时钟不同步

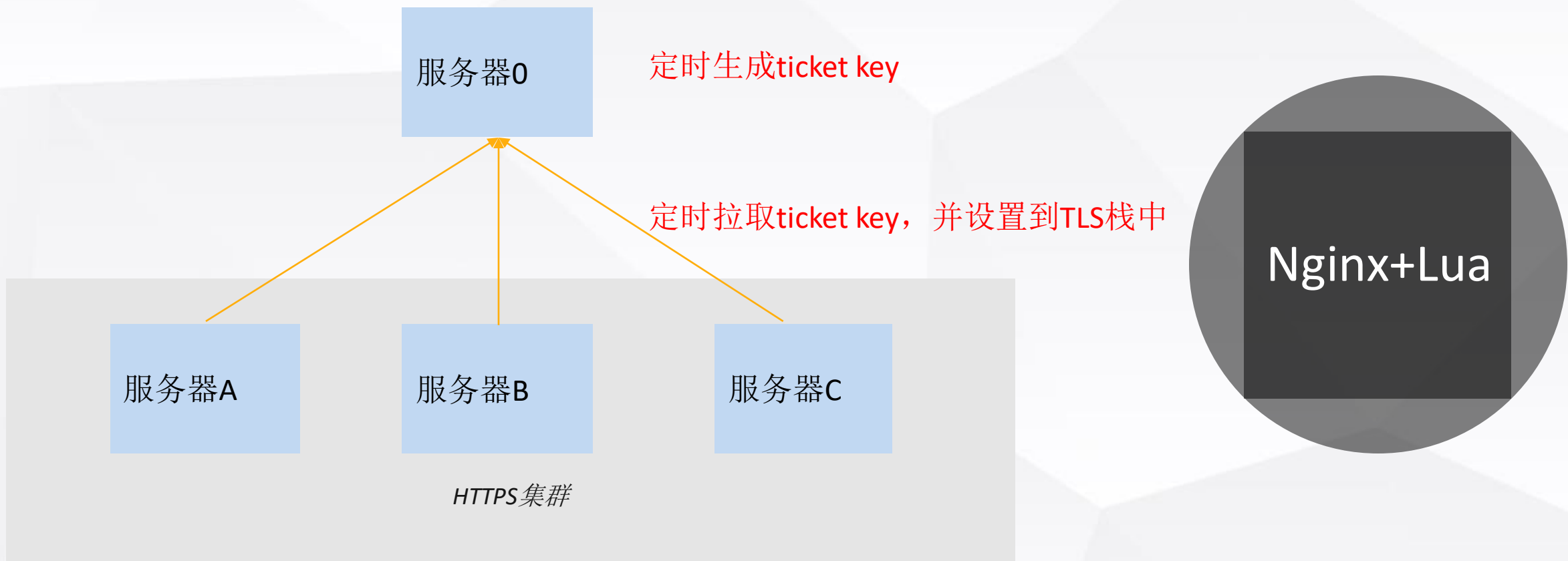
不依赖其他进程



TLS session ticket key 多机同步与自动更新



Operations





TLS session ticket key 兼容时钟不同步



Operations



Server A (时钟快)

Server B

仅链头Key用作生成Ticket

所有Key都可用来解密Ticket

预加载下一时刻Key到链尾
用于兼容时钟不同步

Key_20180531_15:00	Key_20180531_14:00
Key_20180531_14:00	Key_20180531_13:00
Key_20180531_13:00	Key_20180531_12:00
Key_20180531_12:00	Key_20180531_11:00
Key_20180531_11:00	Key_20180531_10:00
Key_20180531_10:00	Key_20180531_09:00
...	...
Key_20180531_16:00	Key_20180531_15:00



HTTPS

- OCSP Stapling
- 远程异步计算（已有初版）
- Keyless（开发中）
- ...

TCP

- fasttcp（自研TCP加速）
- BBR（已开始大规模部署）
- ...



yongjian3@staff.sina.com.cn

徐永健 @ SINAEDGE



Operations

