GOPS 2020
Shanghai

GOPS

GOPS 全球运维大会

2020
-AIOps 风向标

上海站

指导单位：

主办单位：

大会时间：2020年11月27日-28日

大会地点：上海中庚聚龙酒店

GOPS 2020
Shanghai

HTTP3，为IoT时代保驾护航

陶辉

陶辉

智链达CTO

《深入理解Nginx》作者，极客时间《系统性能优化必知必会》专栏作者，视频课《Web协议详解与抓包实战》

《Nginx核心知识100讲》讲师，腾讯云TVP

目录

CONTENTS

HTTP2的遗留问题

HTTP/0.9 -1991

$> telnet ashenlive.com 80

(Connection 1 Establishment - TCP Three-Way Handshake)
Connected to xxx.xxx.xxx.xxx

(Request)
GET /my-page.html

(Response in hypertext)
<HTML>
A very simple HTML page
</HTML>

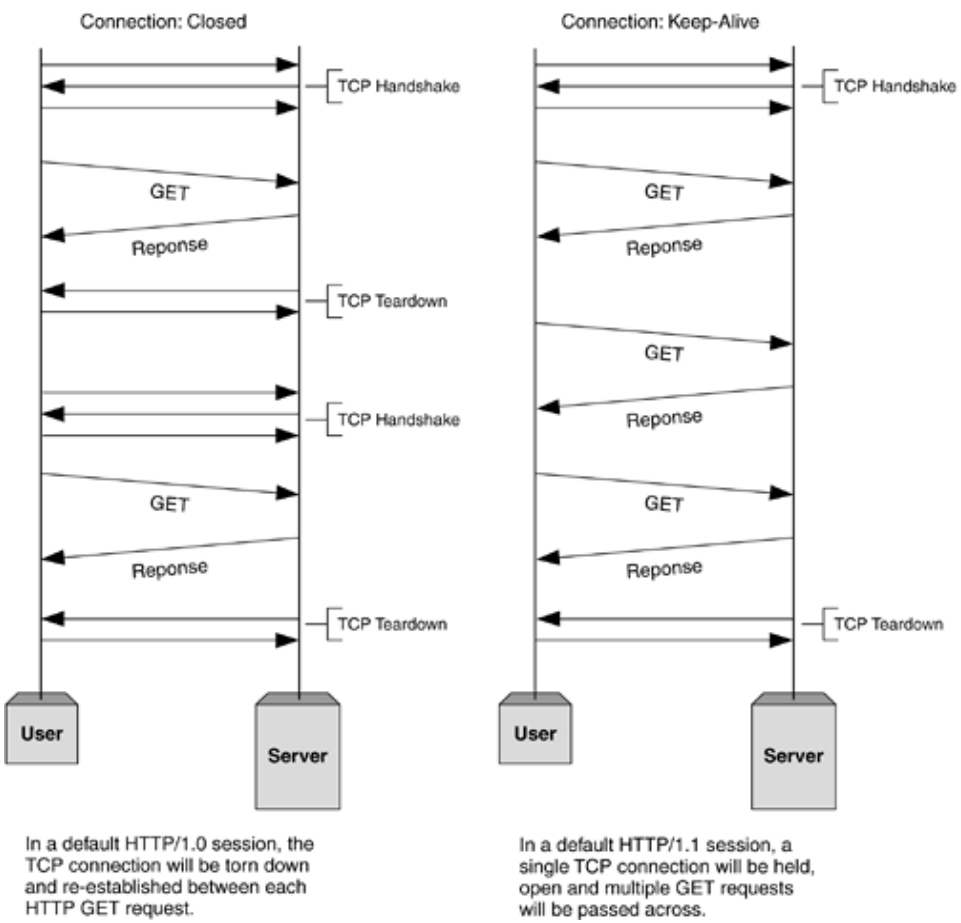
(Connection 1 Closed - TCP Teardown)

HTTP/1.0的改进　-1996

- HTTP Header头部
  - 通过Content-Type可以传输各类文件
- Status Code响应码
- HTTP Version版本号
- Method方法扩展

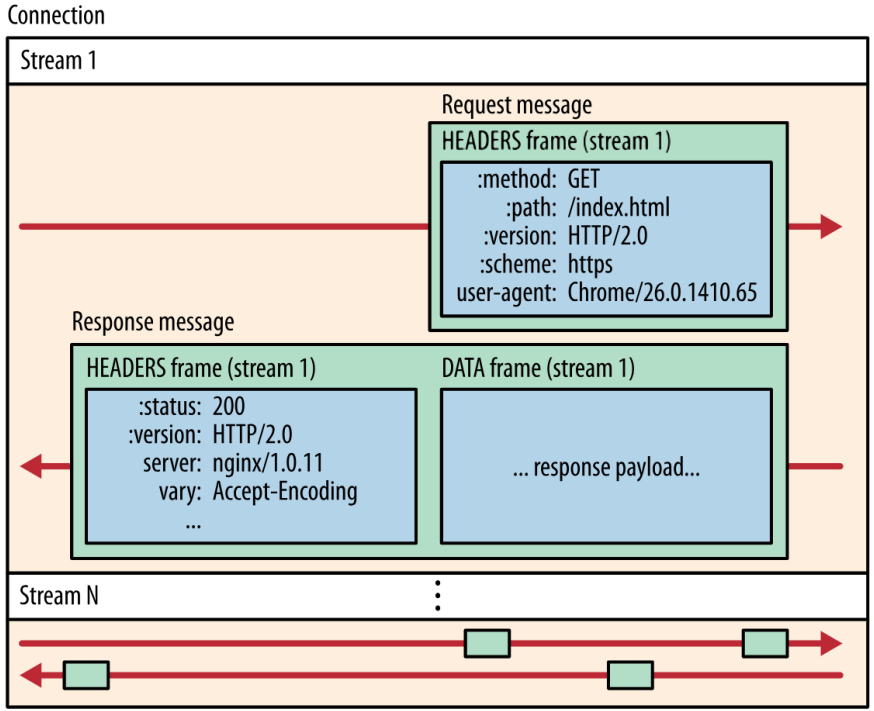
HTTP/1.1的改进-1997

- 增加Host头部
- KeepAlive长连接
- Chunk包体
- 增强内容协商范围
- 增加cache-control

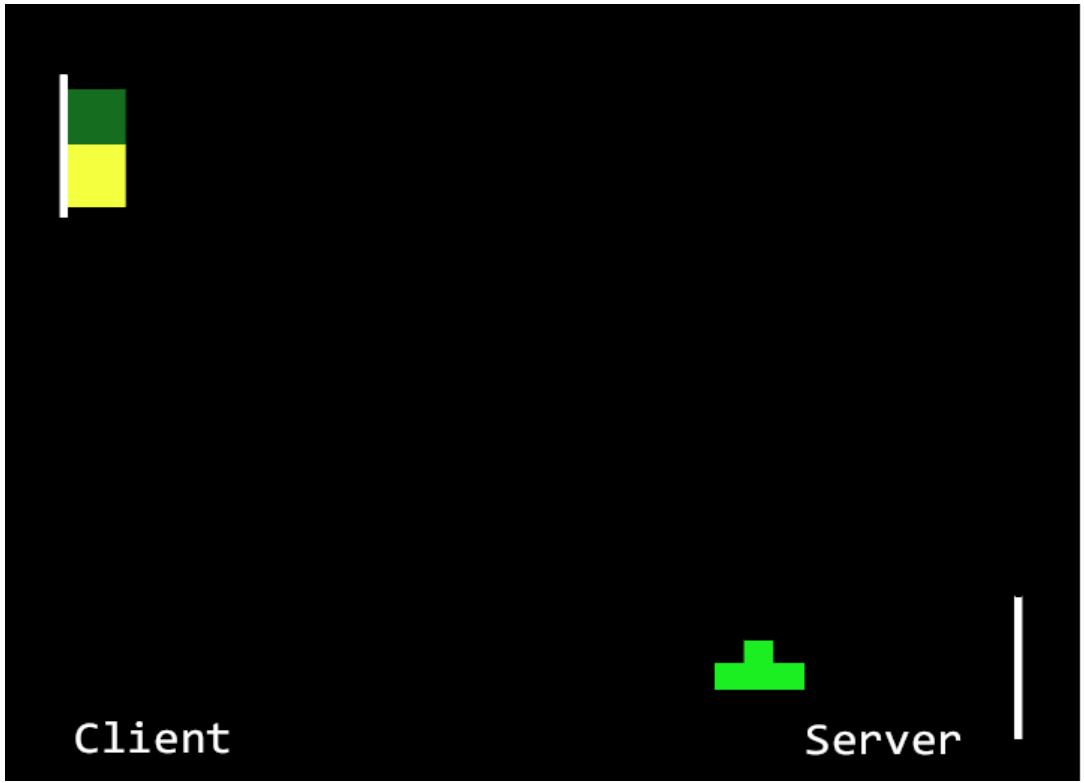


HTTP/2的改进　-2015

- HTTP层的多路复用
  - 资源优先级控制
- 提升编码效率
- 支持服务器推送

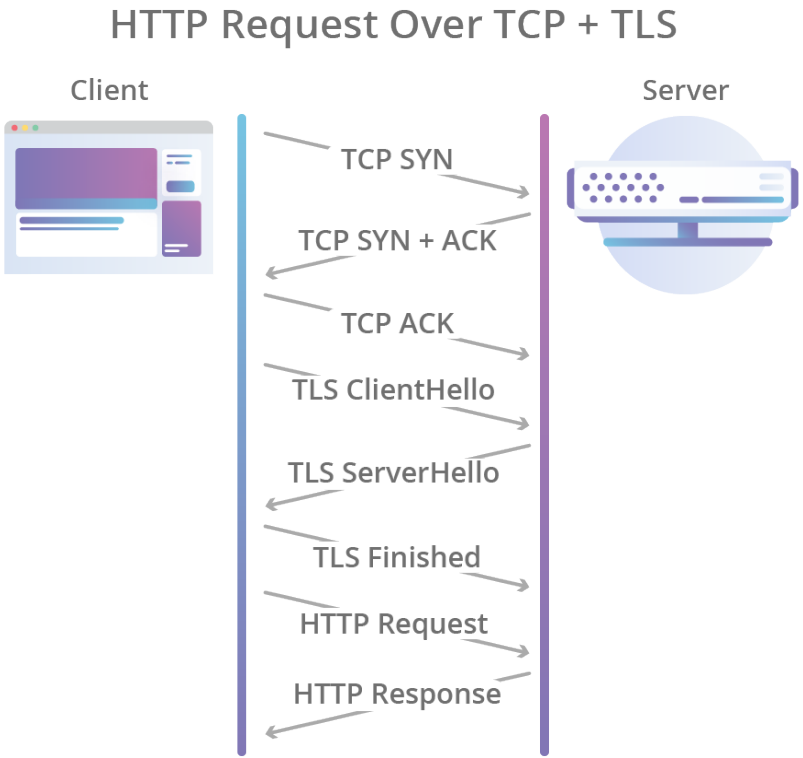


队头阻塞问题



建立连接成本过高

- 2重握手
  - TCP握手
  - TLS握手
- 更换IP后断链重连
  - TCP四元组

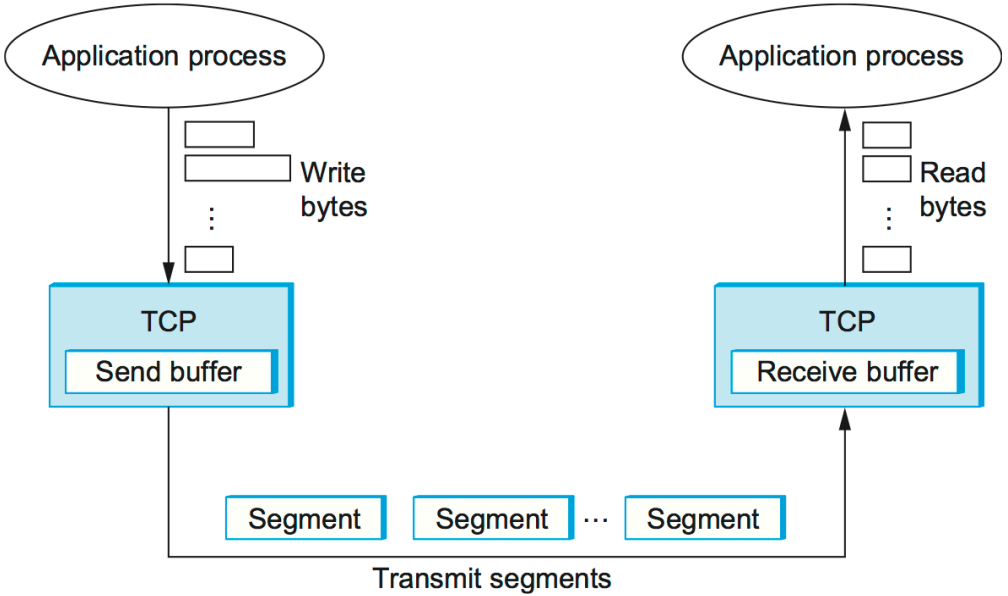


2

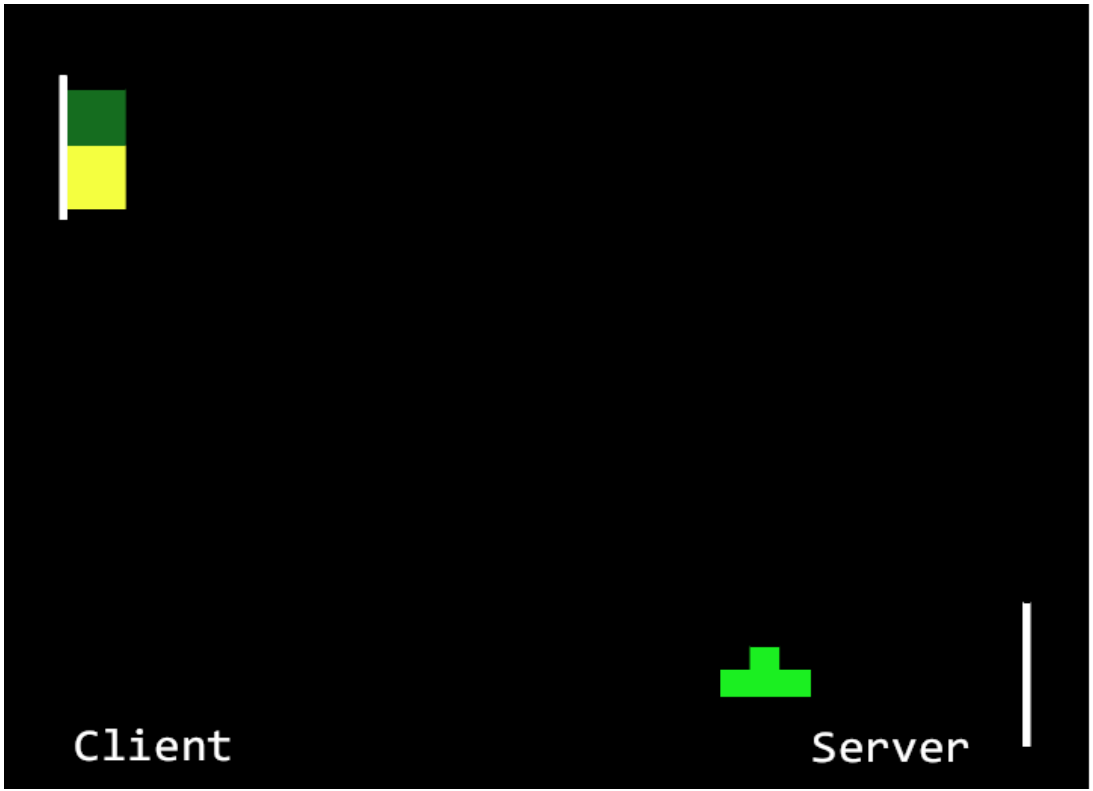
HTTP3协议概览

TCP引入的问题

- 有序字符流
- 协议分层
- IP、端口四元组

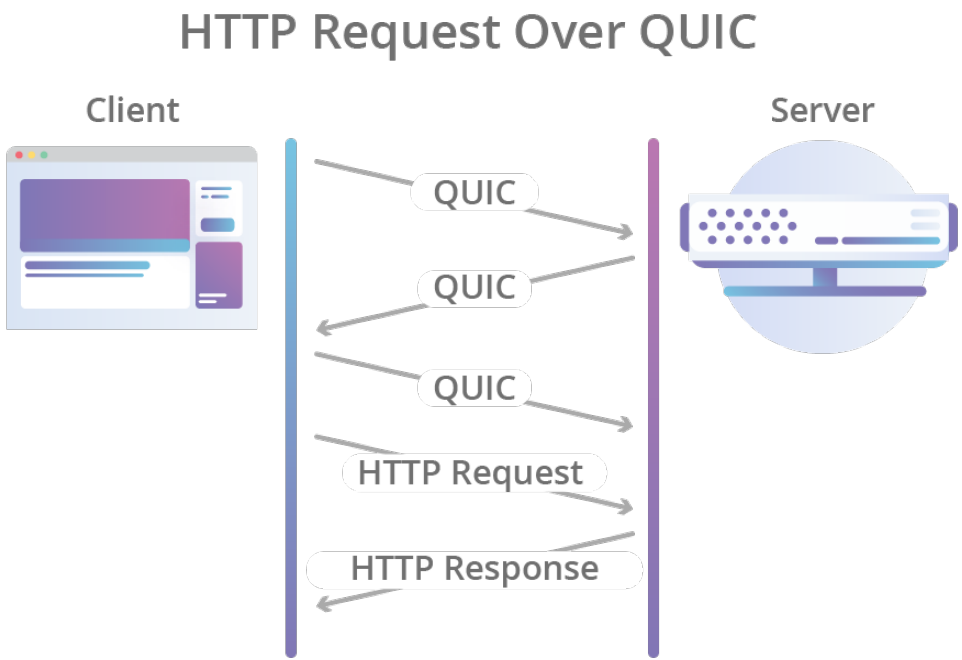


队头阻塞的解决

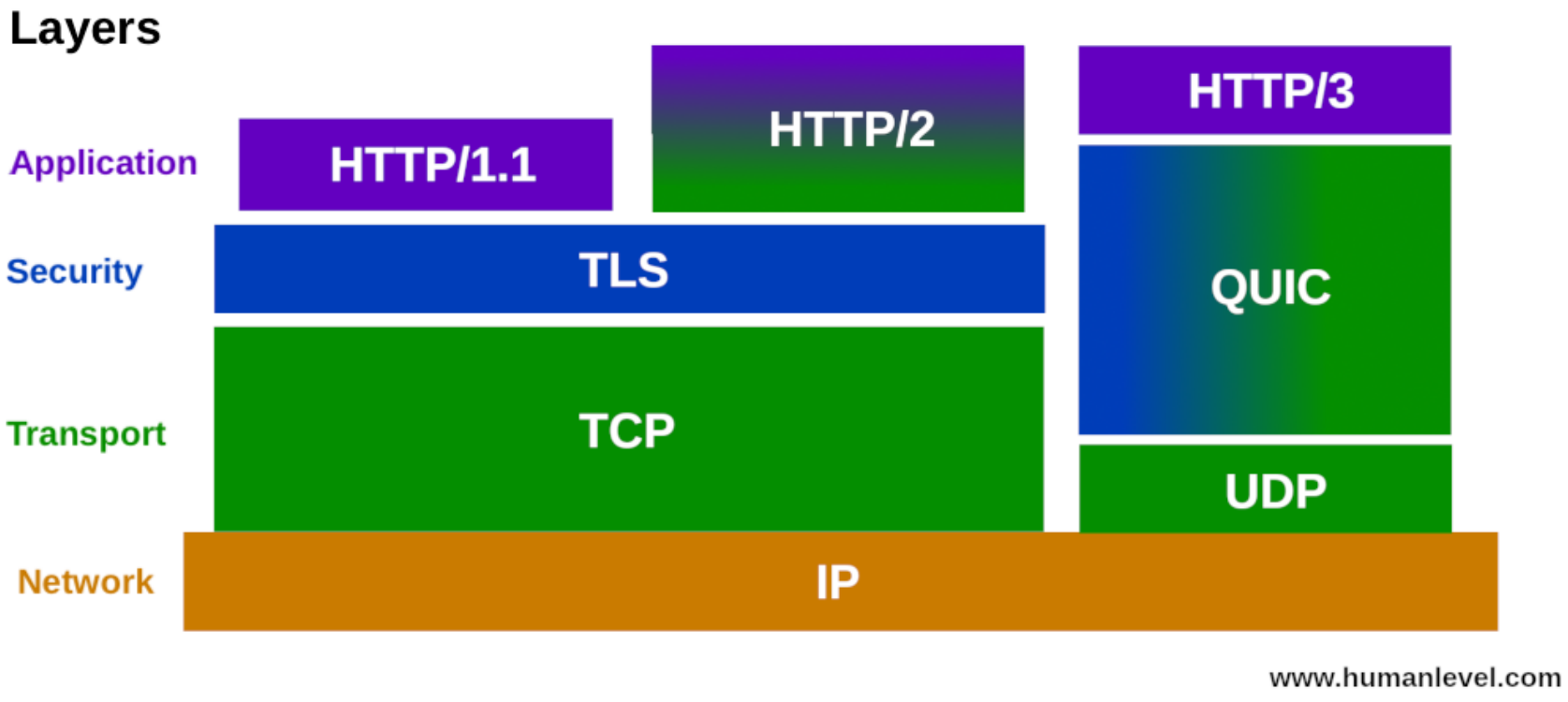


连接成本的降低

- 基于ConnectionID的连接迁移
- 握手合并



HTTP3与UDP协议



5个RFC

1. QUIC: https://tools.ietf.org/html/draft-ietf-quic-transport-32
2. QUIC+TLS: https://tools.ietf.org/html/draft-ietf-quic-tls-32
3. 丢包重传: https://tools.ietf.org/html/draft-ietf-quic-recovery-32
4. QPACK: https://tools.ietf.org/html/draft-ietf-quic-qpack-19
5. HTTP3: https://tools.ietf.org/html/draft-ietf-quic-http-32

Connection

1 RTT握手
0 RTT握手
连接迁移

Frame

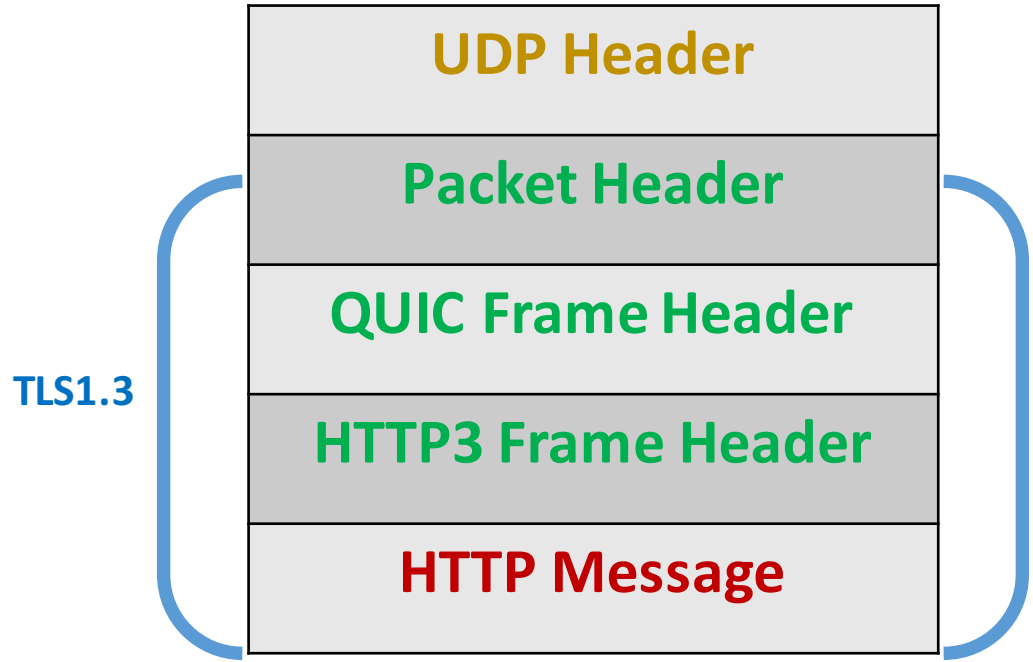
packet
QUIC Frame
HTTP3 Frame

Stream

双向Stream
单向Stream

HTTP3报文

- Packet头部
- TLS头部
- QUIC Frame头部
- HTTP3 Frame头部
- HTTP消息

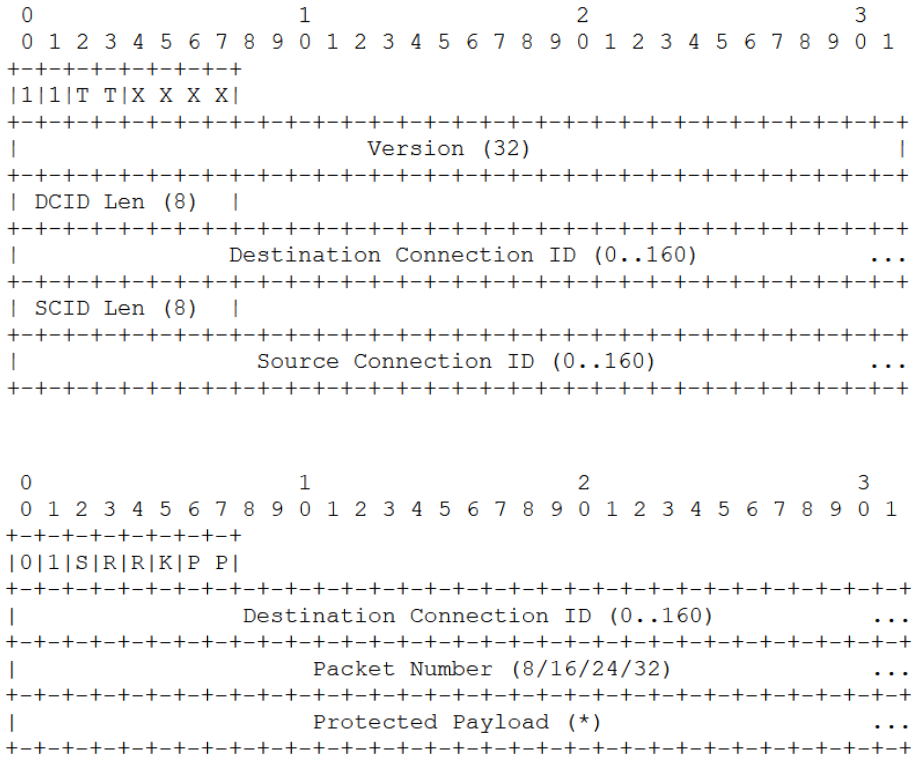


3

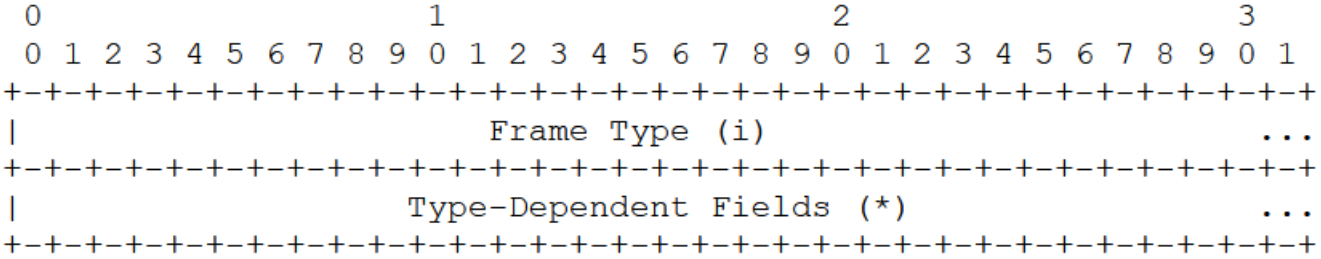
QUIC层的实现

Packet头部

- Long Packet Header
- Short Packet Header

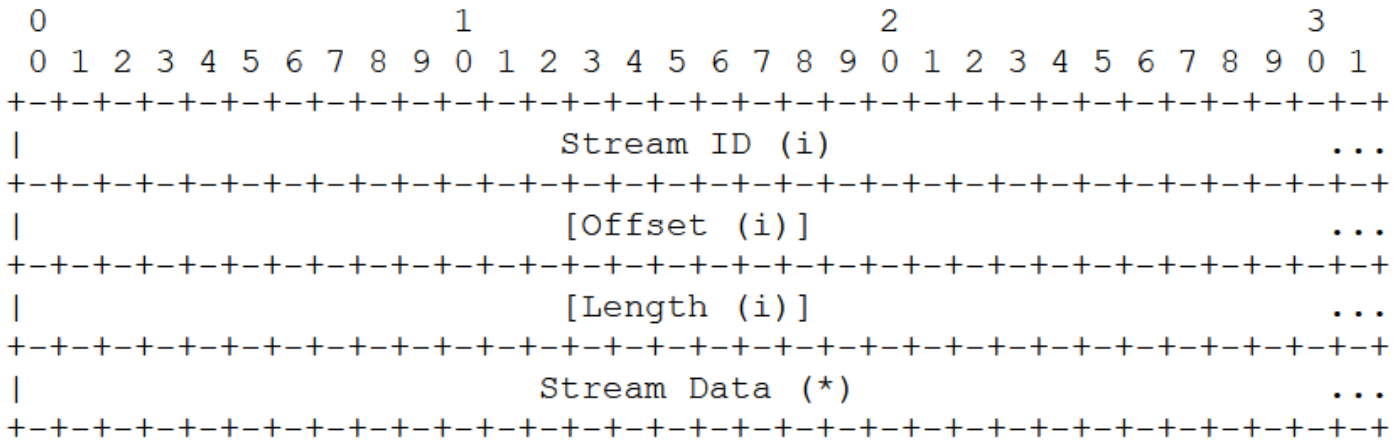


QUIC Frame头部



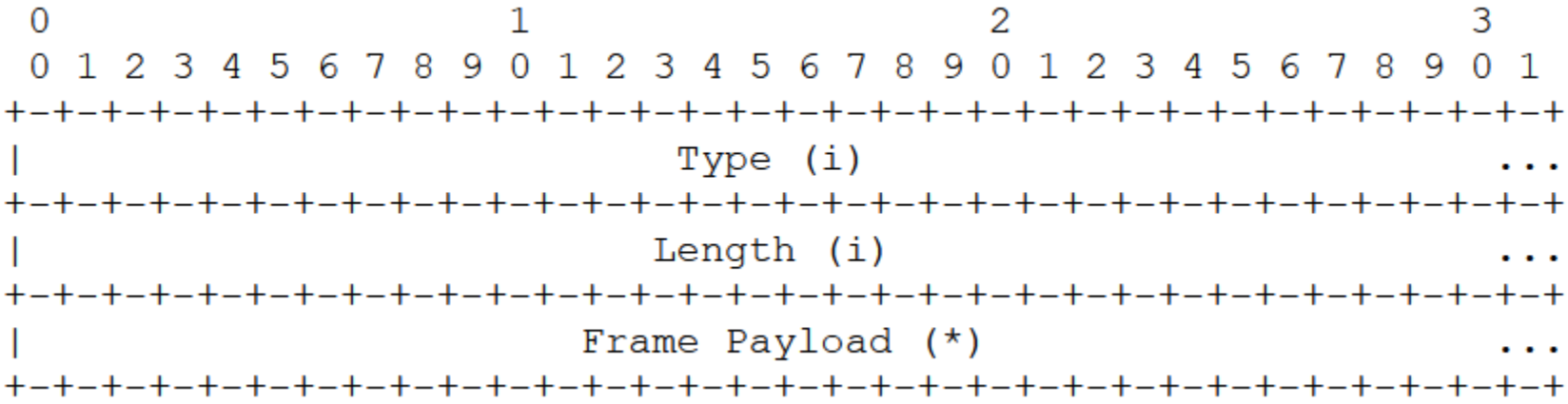
Value	Name	Value	Name		
0x00	PADDING	0x02 – 0x03	ACK	0x15	STREAM_DATA_BLOCKED
0x01	PING	0x08 – 0x0f	STREAM	0x18	NEW_CONNECTION_ID
0x04	RESET_STREAM	0x12-0x13	MAX_STREAMS	0x19	RETRY_CONNECTION_ID
0x05	STOP_SENDING	0x16-0x17	STREAM_BLOCKED	0x1a	PATH_CHALLENGE
0x06	CRYPTO	0x1c-0x1d	CONNECTION_CLOSE	0x1b	PATH_RESPONSE
0x07	NEW_TOKEN	0x11	MAX_STREAM_DATA	0x1e	HANDSHAKE_DONE
0x10	MAX_DATA	0x14	DATA_BLOCKED		

QUIC Stream Frame头部

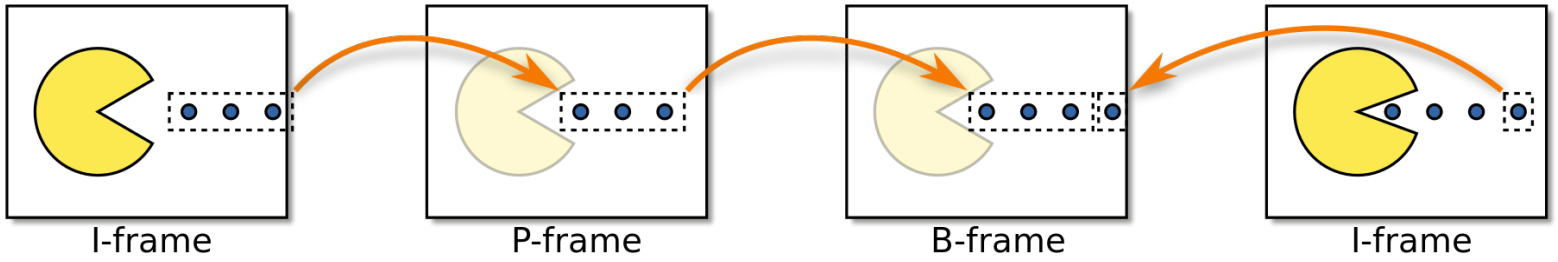


HTTP3 Frame头部

Type	意义	Type	意义	Type	意义
0x00	DATA	0x04	SETTINGS	0x0d	MAX_PUSH_ID
0x01	HEADERS	0x05	PUSH_PROMISE		
0x03	CANCEL_PUSH	0x07	GOAWAY		

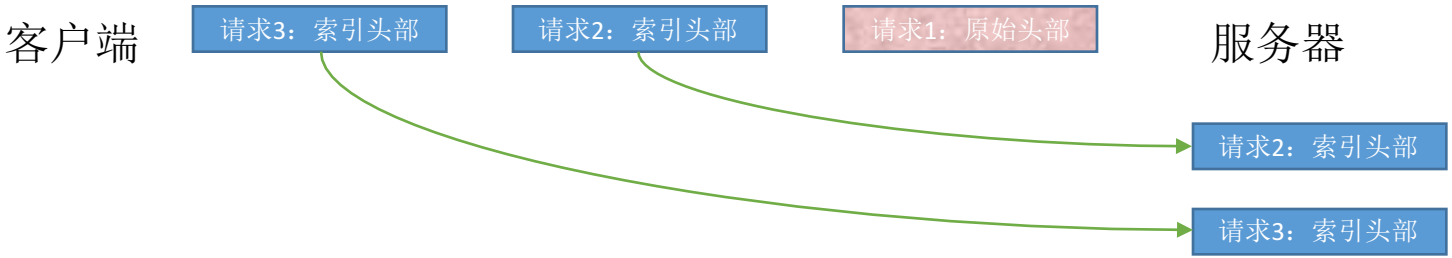


QPACK与视频压缩



QPACK编码

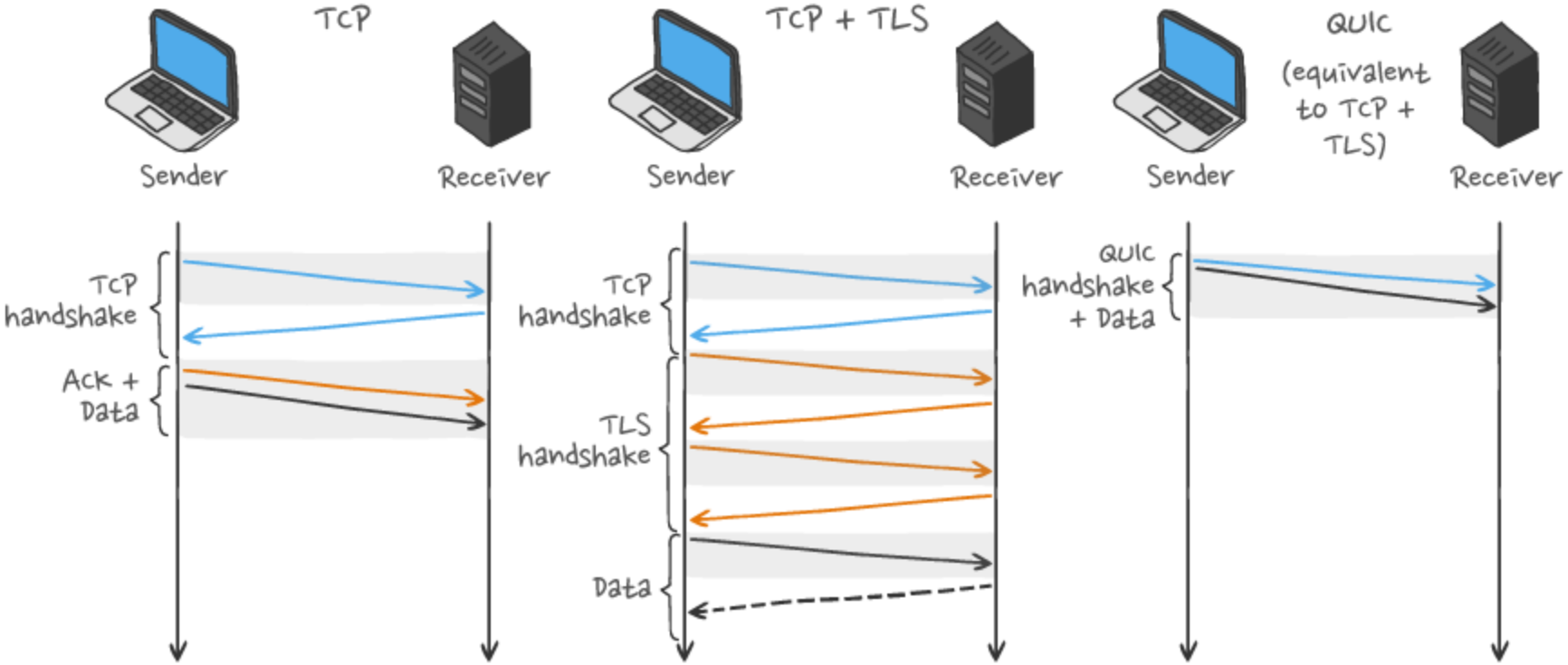
- 99项静态表
- 解决HOL的动态表：编码效率VS阻塞容忍
- 静态Huffman编码



TLS1.2到TLS1.3

- 密钥交换（移除静态密码，支持前向保密性）
  - DHE / ECDHE(Elliptic-curve Diffie–Hellman)：X25519，X448
  - PSK-only
  - PSK with ECDHE/DHE
- 身份验证算法
  - RSA
  - 椭圆曲线
    - ECDSA
    - EdDSA
  - PSK（TLS Pre-Shared Key）
- 对称加密算法
  - AEAD算法

更快的握手


TCP
Sender
Receiver
TCP handshake
Ack + Data
TCP + TLS
Sender
Receiver
TCP handshake
TLS handshake
Data
QUIC (equivalent to TCP + TLS)
Sender
Receiver
QUIC handshake + Data

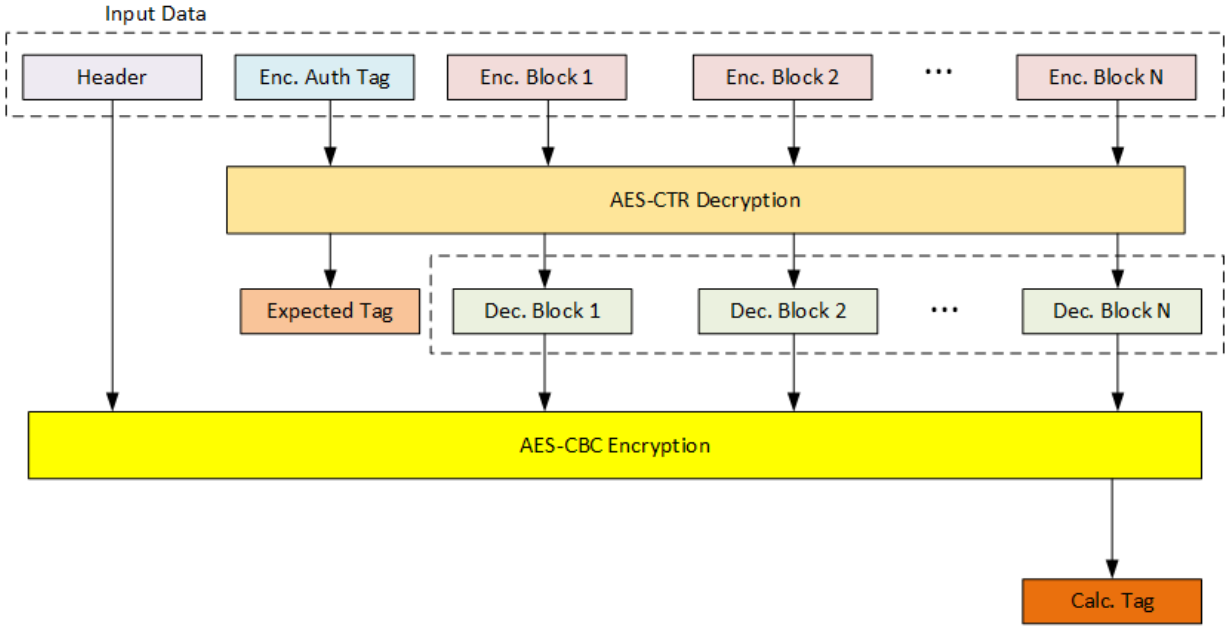
AEAD算法

- Authenticated Encryption with Associated Data
  - 完整性
  - 机密性
  - 不可篡改
- 块加密
  - AES-GCM
  - AES-CCM
- 流加密
  - ChaCha20-Poly1305

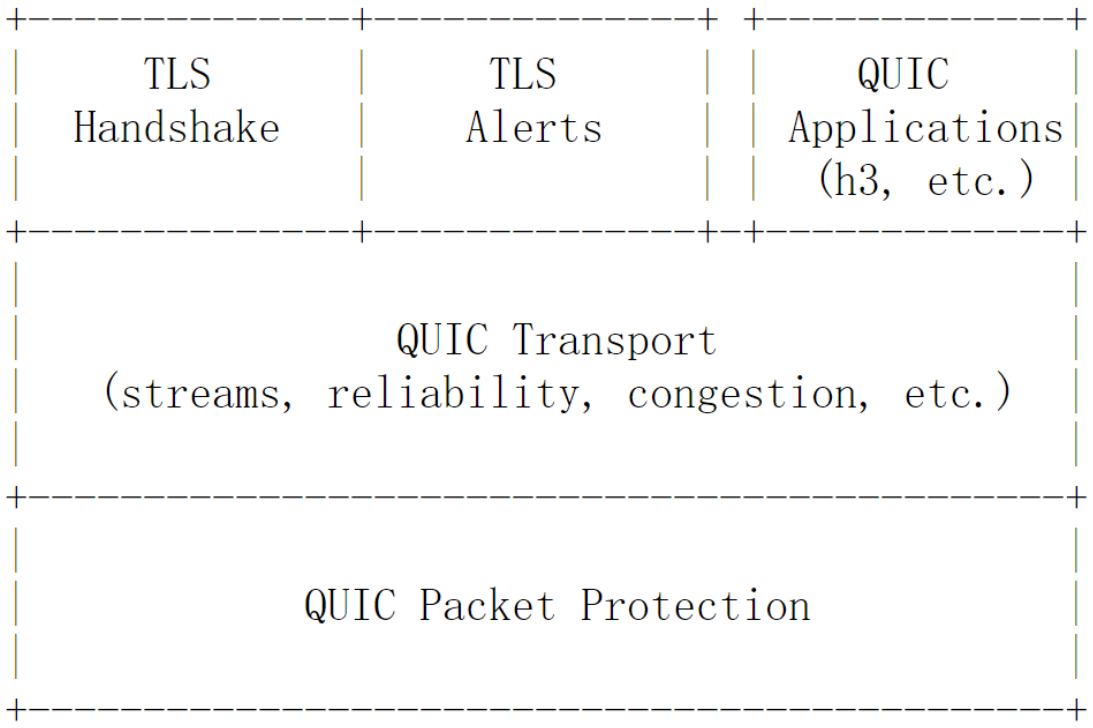
CCM模式

counter with cipher block chaining message authentication code

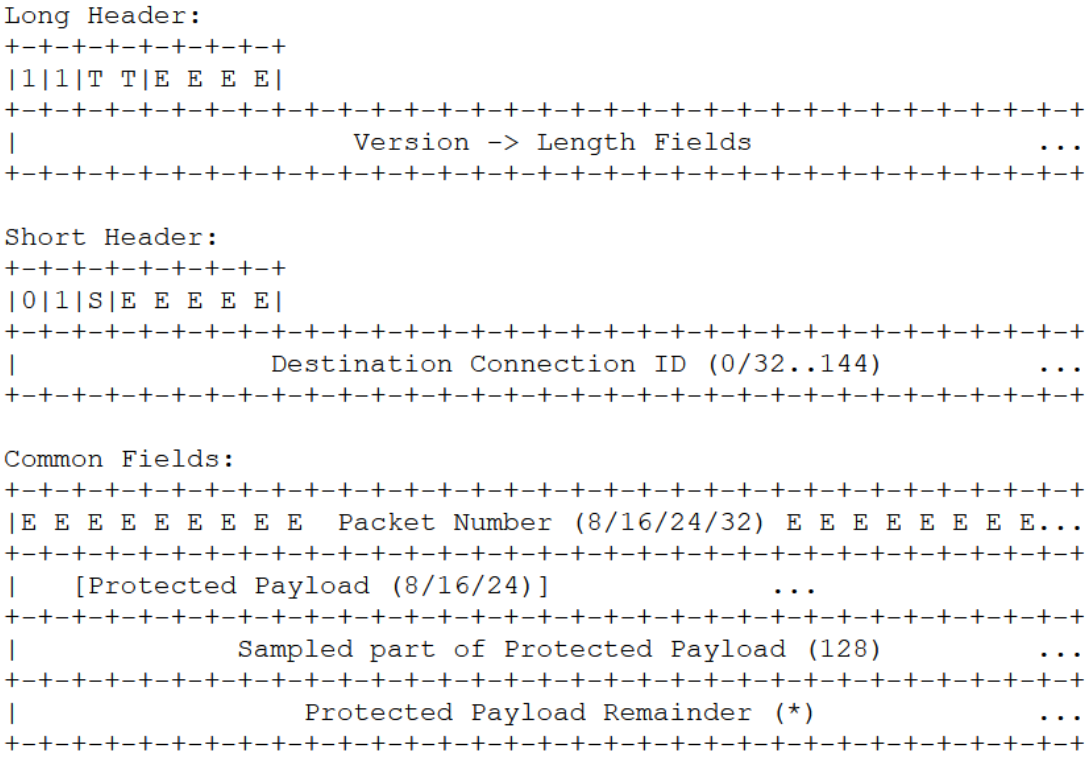
1. CBC：Auth Tag加密（authenticate-then-encrypt）
2. CTR：消息加密



TLS1.3与QUIC的耦合



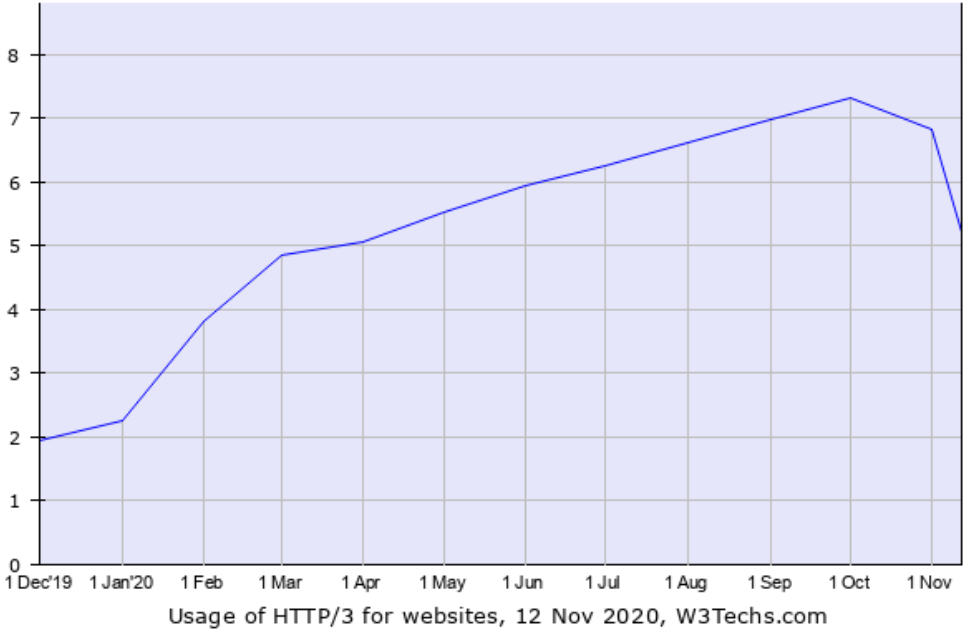
TLS头部


Long Header:
|1|1|T T|E E E E|
Version -> Length Fields
Short Header:
|0|1|S|E E E E E|
Destination Connection ID (0/32..144)
Common Fields:
|E E E E E E E E E Packet Number (8/16/24/32) E E E E E E E E...
[Protected Payload (8/16/24)]
Sampled part of Protected Payload (128)
Protected Payload Remainder (*)

HTTP3协议应用

HTTP3应用情况

- 截止2020.10.20号，已发布32个草案
- W3Techs近1年HTTP3站点统计
- 协议升级
  - Alt-Svc: h3=":50781"
- chrome启用http3
  - --enable-quic --quic-version=h3-29
- firefox启用http3
  - network.http.http3.enabled



Nginx流控指令（1）- http{} server{}

- quic_initial_max_data
  - 连接上飞行中的报文数量，默认为16*65536，可以由MAX_DATA帧改变
- quic_initial_max_stream_data_bidi_local
  - 双向stream本地端的初始流控值，默认65536
- quic_initial_max_stream_data_bidi_remote
  - 双向Stream远端的初始流控值，默认65536
- quic_initial_max_stream_data_uni
  - 单向Stream的初始流控值，默认65536
- quic_initial_max_streams_bidi
  - 双向Stream的最大并发数，默认16，可以由MAX_STREAM帧改变
- quic_initial_max_streams_uni
  - 单向Stream的最大并发数，默认16

Nginx QUIC 指令（2）- http{} server{}

- quic_max_idle_timeout
  - 最大空闲时间，单位毫秒，Nginx默认60000，0表示关闭功能
- quic_max_ack_delay
  - 延迟确认的最大值，默认（也是RFC推荐）25毫秒
- quic_max_packet_size
  - 默认65527，不能小于1200字节
- quic_ack_delay_exponent
  - 将ACK确认帧中，将ACK时延按2的倍数扩大。默认值3（RFC推荐），不允许超过20
- quic_active_migration
  - 是否支持客户端迁移连接，默认为1表示开启
- quic_retry
  - 防止流量放大攻击时，可以通过retry功能强制要求客户端开启TOKEN地址验证功能。默认关闭off

Nginx指令（3）- http{} server{}

- http3_max_field_size
  - HTTP QPACK头部的大小限制
- http3_max_table_capacity
  - 设置动态表容量
  - SETTINGS_QPACK_MAX_TABLE_CAPACITY帧可以修改其值
    - 与HTTP2中的SETTINGS_HEADER_TABLE_SIZE帧功能一致
- http3_max_blocked_streams
  - QPACK动态表会阻塞Stream，该值可以定义允许最大阻塞住的Stream数量，一旦超出，会立刻向客户端返回QPACK解压失败错误

HTTP3普及面临的挑战

Thanks

高效运维社区

开放运维联盟

荣誉出品