QUIC E HTTP3

Eduardo Braga, Henrique Franca, Isabela Medeiros, Júlia Vilela

O QUE É O QUIC

- Protocolo de transporte confiável baseado em UDP.
- Desenvolvido pelo Google e padronizado pela IETF em 2021.
- Combina: transporte, multiplexação e segurança.
- Recursos TCP sobre um protocolo minimizado e mais flexível.
- É a base do HTTP/3, sucessor do HTTP/2.

POR QUE SURGIU O QUIC?

Web moderna exige menor latência, mais segurança e resiliência.

TCP + TLS + HTTP/2 possuem limitações:

- Lento no início da conexão (várias etapas).
- Head-of-Line Blocking (HOL) no TCP.
- Não lida bem com mudança de rede/IP (mobilidade).

HTTP/2 X HTTP/3

Característica	HTTP/2 (TCP)	HTTP/3 (QUIC)
Transporte	TCP	UDP (com QUIC)
Multiplexação	Sim, mas com HOL	Sim, sem HOL
Latência de Conexão	Alta (3-RTT)	Baixa (1-RTT ou 0-RTT)
Suporte a Mobilidade	Não (quebra IP)	Sim (Connection ID)
Criptografia	TLS 1.2 (opcional)	TLS 1.3 (obrigatória)
Confiabilidade	Via TCP	Gerenciada pelo QUIC

TCP X UDP

Característica	TCP	UDP
Confiável?	Sim (ordem e entrega)	Não (sem garantias)
Controle de fluxo?	Sim	Não
Ordem garantida?	Sim	Não
Velocidade	Mais lento	Mais rápido
Conexão persistente?	Sim (handshake 3 vias)	Não (sem conexão)
Flexível?	Não (difícil atualizar)	Sim (usado como base para QUIC)

O QUIC usa o UDP por ser leve e flexível, e implementa confiabilidade por conta própria.

COMO FUNCIONA O UDP?

- Protocolo de transporte sem conexão.

- Envia pacotes chamados datagramas, sem garantir:
  - Entrega
  - Ordem
  - Retransmissão

- Muito usado em streaming, VoIP e jogos online, onde a velocidade é prioridade.

- QUIC aproveita essa base para implementar seu próprio sistema de controle confiável.

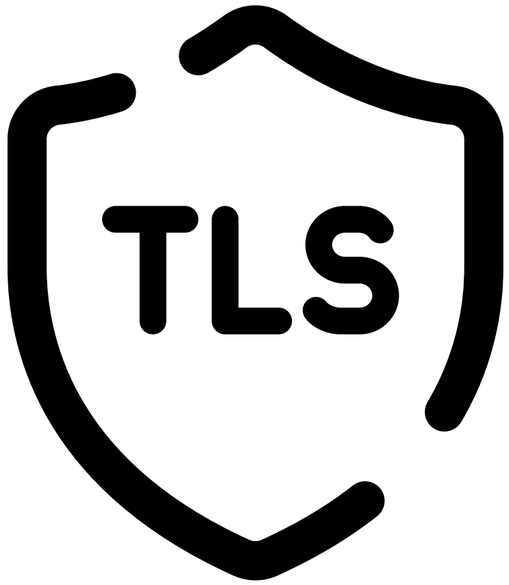
SSL (Secure Sockets Layer)

- Protocolo de criptografia
- Principal objetivo de proteger a comunicação entre CLI X SERV

Versões

- SSL 1.0 (nunca lançada)
- SSL 2.0 (1995, mas insegura)
- SSL 3.0 (1996, mais estável mas ao longo do tempo ficou vulnerável)

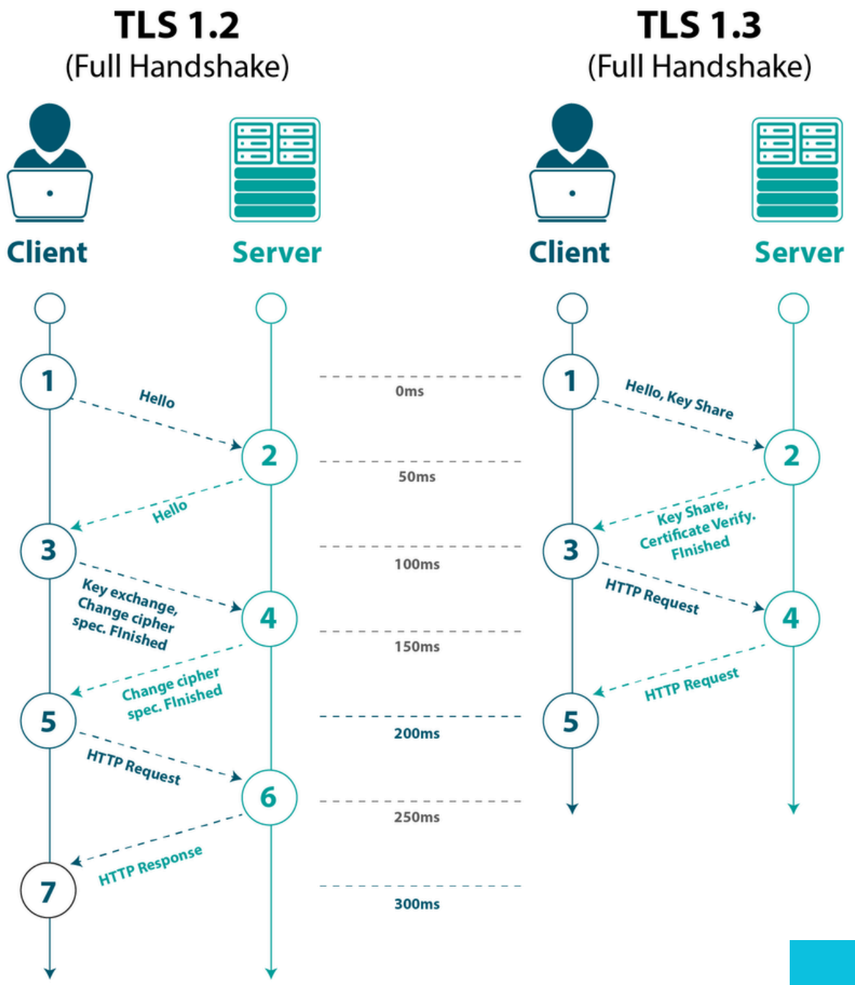
TLS(Transport Layer Security)



- Sucessor do SSL, com o TLS 1.0 (1999)
  - Corrigir vulnerabilidades que existiam no SSL 3.0
- Garante confidencialidade, integridade e autenticação.
- Versões (TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3)
- QUIC usa TLS 1.3 nativamente e obrigatoriamente.
- Handshake mais robusto por conta da criptografia

POR QUE O TLS 1.3 É MELHOR QUE O TLS 1.2

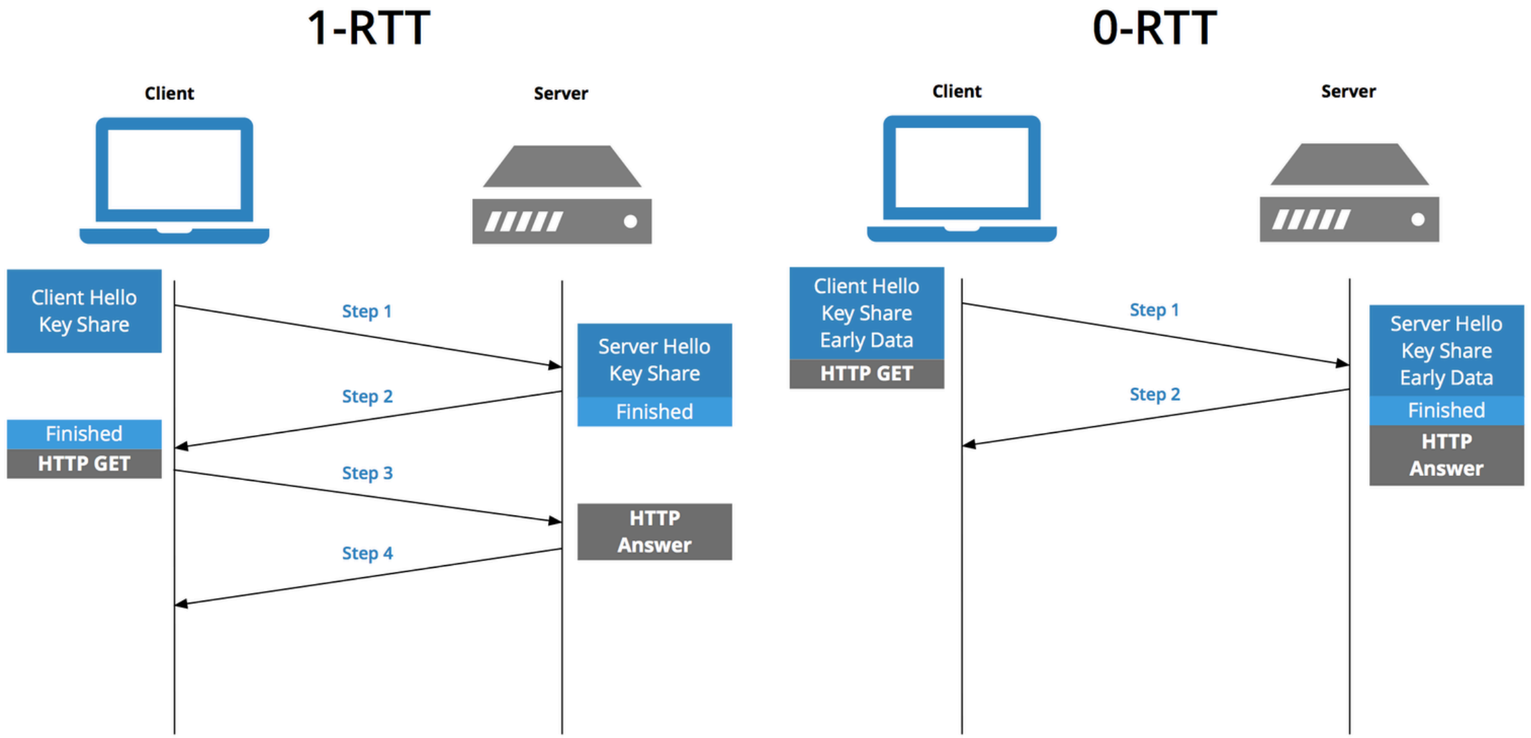
- Handshake mais rápido
- Suporte a 0-RTT
- Fim da renegociação
- Cifras mais modernas e simples
- Menor latência e menos uso de CPU



TLS 1.3

[Transport Layer Security]

HANDSHAKE TLS 1.3



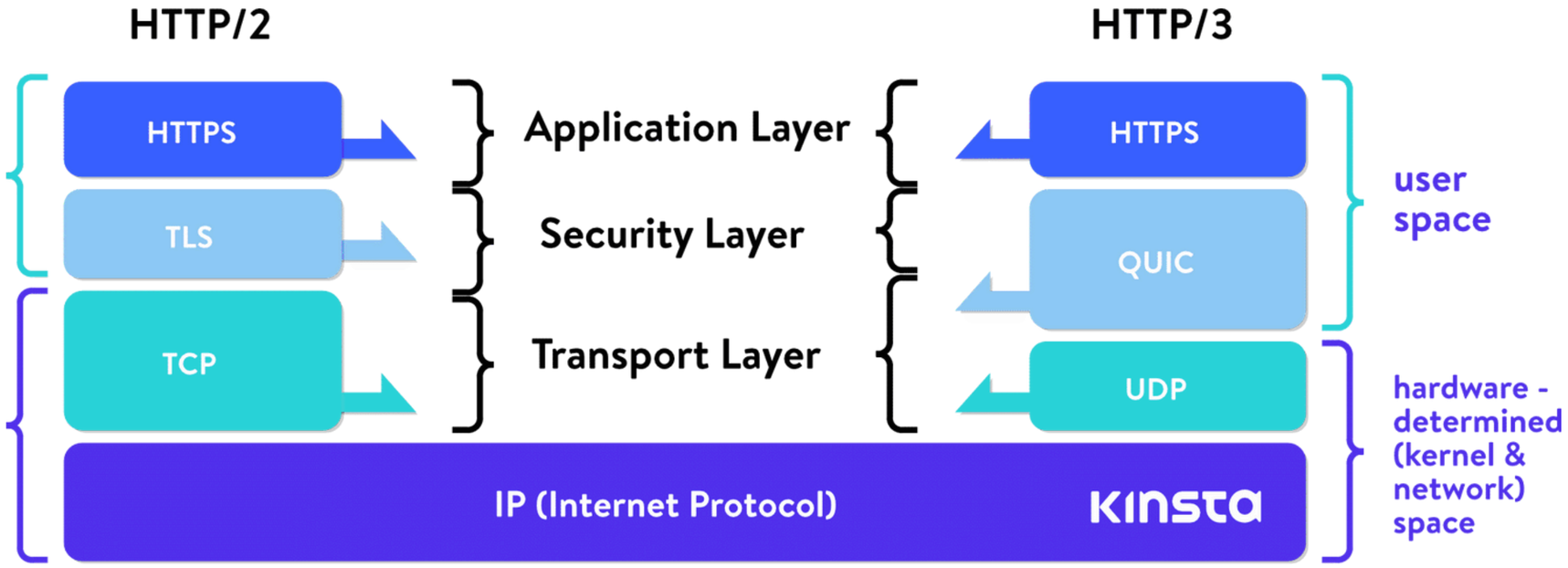
0-RTT é uma funcionalidade do TLS 1.3 que permite o envio de dados antes mesmo do handshake TLS terminar, aproveitando uma sessão já conhecida entre cliente e servidor.

QUIC = UDP + TLS

QUIC constrói uma camada de transporte confiável em cima do UDP.

- Handshake criptografado com TLS 1.3
- Controle de fluxo e congestionamento
- Correção de perdas
- Multiplexação de streams (arquivos podem ser enviados ao mesmo tempo pela mesma conexão, em frames, sem que um bloqueie o outro).

ARQUITETURA DO QUIC



QUADROS QUIC

- Mensagem Básica: A unidade fundamental de informação no QUIC.
- Conteúdo: Inclui tipo do quadro, ID do fluxo, deslocamento e dados do fluxo.
- Reunião de Dados: Os dados de um fluxo são distribuídos em múltiplos quadros e remontados usando:
  - ID da Conexão
  - ID do Fluxo
  - Deslocamento

CONEXÃO QUIC

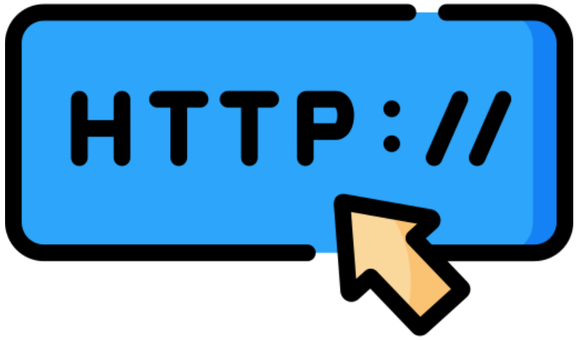
- Início com TLS embutido: O cliente envia um pacote Initial (contém os dados de handshake do TLS, incluindo a versão do QUIC e os algoritmos de criptografia).
- Resposta e Chave Inicial: O servidor responde com seu próprio pacote Initial, fornecendo um ID de conexão e uma chave inicial para a criptografia do handshake.
- Troca e Derivação de Chaves
- Negociação de Parâmetros
- Conexão Estabelecida
- 0-RTT (Opcional)

TÉRMINO DA CONEXÃO QUIC

- Tempo Limite de Inatividade
- Comando de Fechamento
- Violação de Protocolo: Em caso de comportamento inesperado ou malicioso, a conexão pode ser terminada para garantir a segurança e integridade.

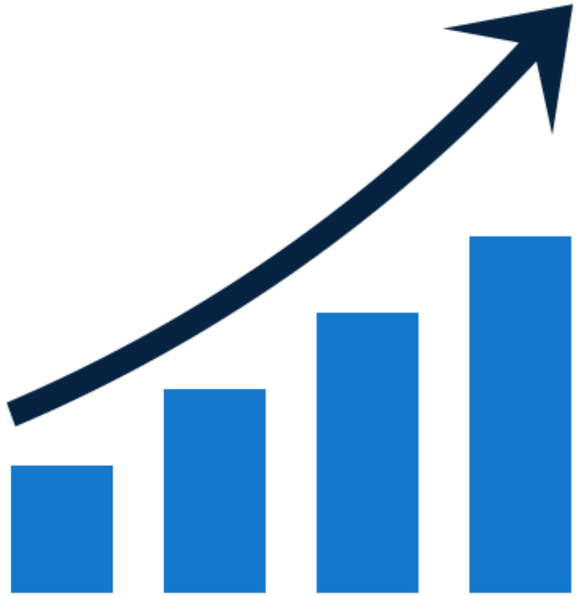
HTTP/3: A NOVA GERAÇÃO DO HTTP

- HTTP/3 é a versão mais recente do protocolo HTTP.
- Usa QUIC como transporte, substituindo o TCP do HTTP/1.1 e HTTP/2.
- Ganha:
  1. Conexões mais rápidas
  2. Maior confiabilidade em redes móveis
  3. Melhor desempenho geral



VANTAGENS DO HTTP/3 COM QUIC

- Handshake mais rápido
- Multiplexação real (sem HOL)
- Baixa latência
- Redução de uso de CPU e pacotes perdidos
- Sem Head-of-Line Blocking
- Usa Connection ID (Tolerância a mudanças de rede/IP)
- Segurança embutida com TLS 1.3
- Suporte a 0-RTT



EXEMPLOS REAIS DE USO

- Google: Gmail, YouTube, Chrome, usa QUIC por padrão.
- Meta: Facebook, Instagram, melhor performance em redes móveis.
- Cloudflare e Akamai: suporte completo ao HTTP/3.
- Navegadores: Chrome, Firefox, Safari, Edge já suportam HTTP/3.

DIFICULDADES NA ADOÇÃO DO HTTP/3 E QUIC

- UDP bloqueado por firewalls e middleboxes legados
- Infraestrutura de rede otimizada para TCP, não para QUIC
- Complexidade de implementação em comparação a TCP+TLS
- Ferramentas de análise e diagnóstico ainda limitadas para QUIC
- Desempenho instável em redes com alta perda de pacotes ou jitter
- Riscos com 0-RTT, como possibilidade de replay attacks
- Atualização de servidores e clientes necessária para adoção plena

DANOUSSE
É KENT🔥🔥🔥🔥🔥