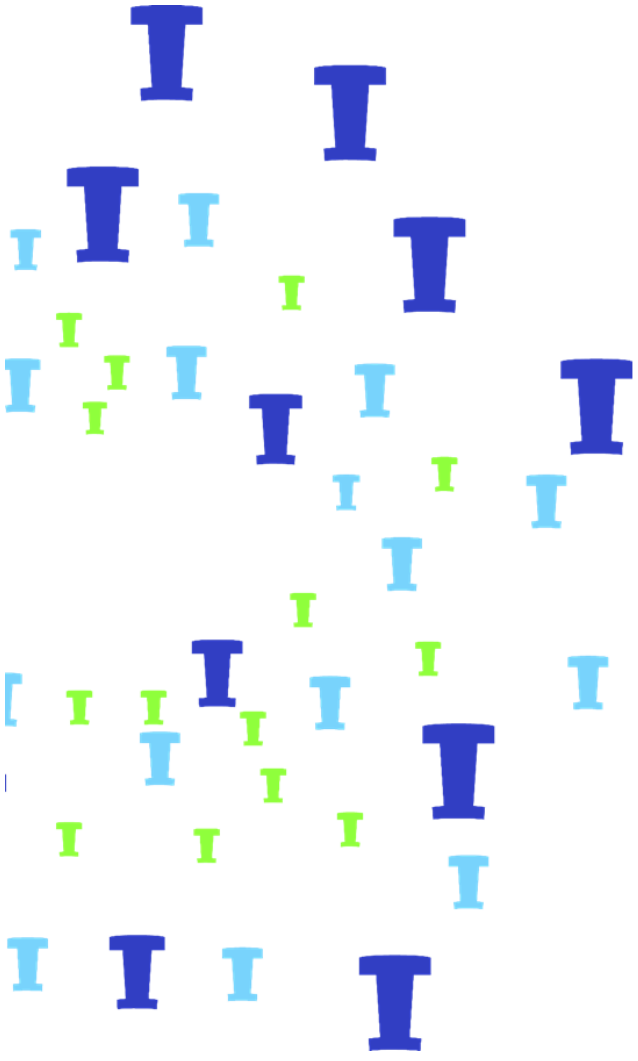


UNIVERSIDAD ICESI

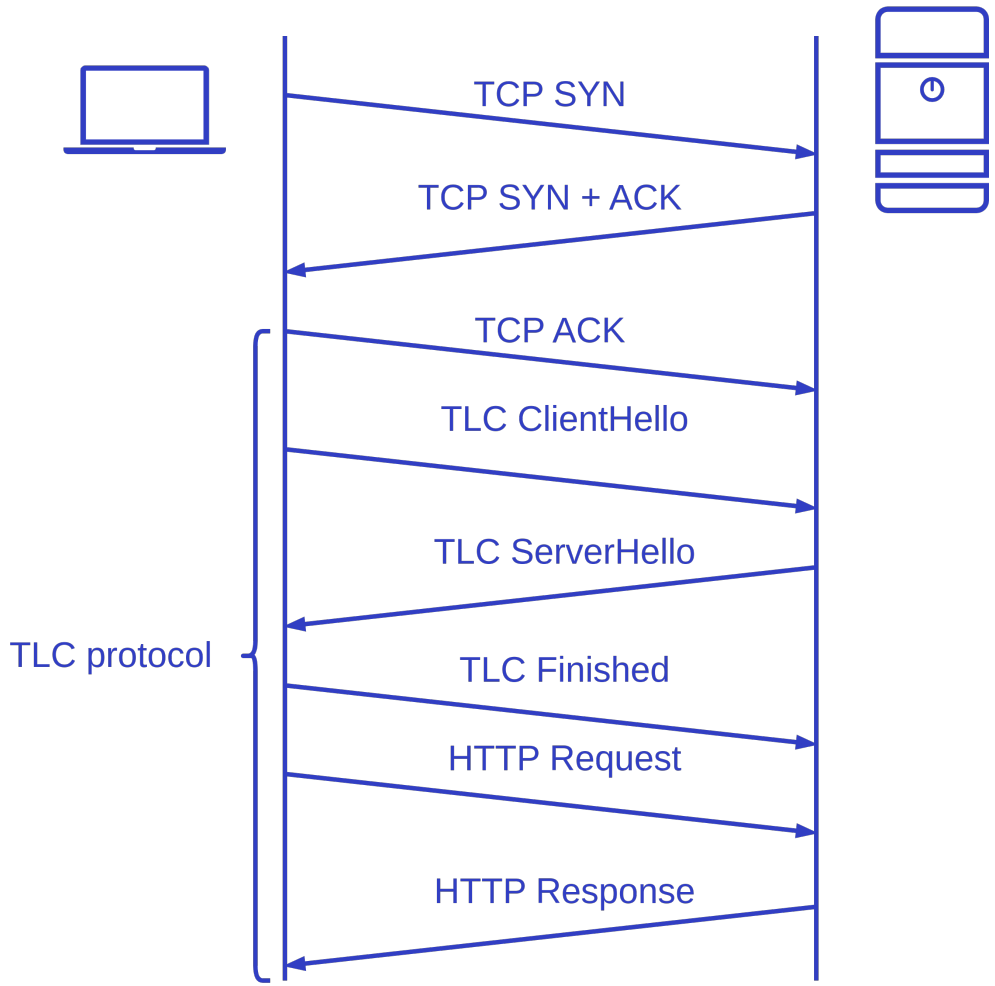
TU FUTURO A OTRO NIVEL

UNIVERSIDAD ICESI
TU FUTURO A OTRO NIVEL

Infraestructura II
QUIC

Nicolás J. Salazar E.

HTTP Request Over TCP + TLS



TLS handshake

- Client Hello

  TLS version the client supports.

  Cipher suites supported.

  Random string (client random)

- Server Hello

  Server's SSL certificate

  the server's chosen cipher suite.

  Random string (server random)

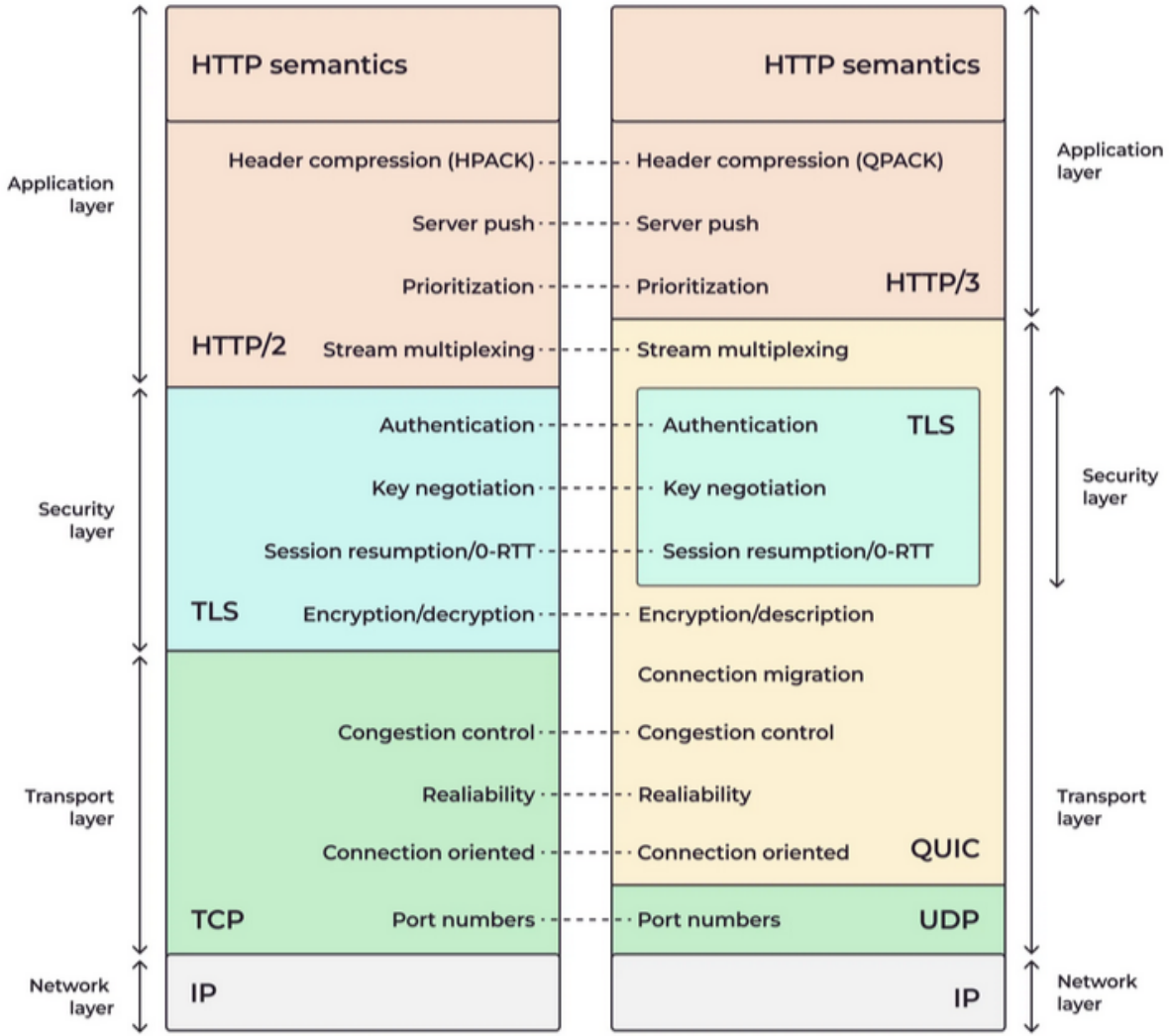
TLS handshake

- Authentication: Client verifies SSL certificate
- Premaster Secret: client sends other random string (encrypted with public key)
- Private Key: Server decrypts the premaster with private key
- Session Key: Both client and server generate session keys from the client random, the server random, and the premaster secret.
- Client Ready
- Server Ready
- Secure Symmetric Encryption Achieved

TLS 1.3

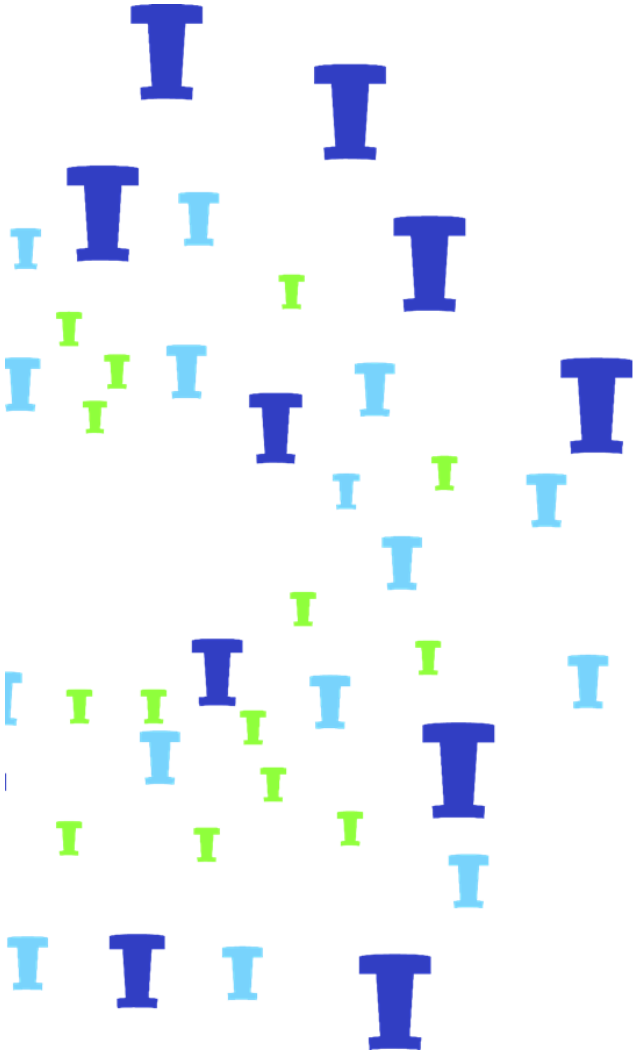
- Does not support RSA
- Client Hello: assuming server's preferred method, send data for premaster
- Server Generates master secret
- Server send Finish (Server Ready)
- Client send Finish (Client Ready)
- Secure Symmetric Encryption Achieved

HTTP3


HTTP semantics
HTTP semantics
Application layer
Header compression (HPACK)
Header compression (QPACK)
Application layer
Server push
Server push
Prioritization
Prioritization
HTTP/3
HTTP/2
Stream multiplexing
Stream multiplexing
Authentication
Authentication
TLS
Security layer
Key negotiation
Key negotiation
Session resumption/0-RTT
Session resumption/0-RTT
TLS
Encryption/decryption
Encryption/description
Connection migration
Congestion control
Congestion control
Transport layer
Realiability
Realiability
Transport layer
Connection oriented
Connection oriented
QUIC
TCP
Port numbers
Port numbers
UDP
Network layer
IP
IP
Network layer

Referencias

- quic-go
- RFC 9000
- RFC 9001



UNIVERSIDAD ICESI

TU FUTURO A OTRO NIVEL

¡Gracias!

UNIVERSIDAD ICESI
TU FUTURO A OTRO NIVEL