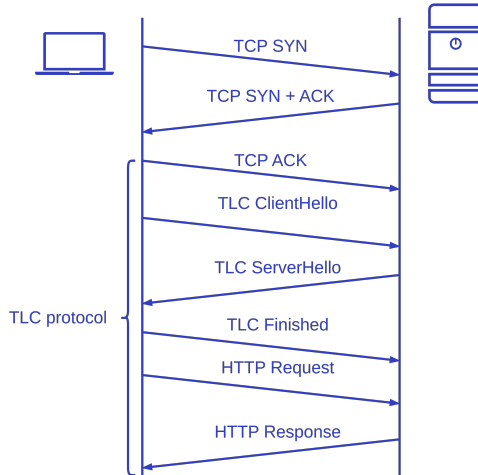


# HTTP3 y QUIC

ComSoc Icesi

Nicolás J. Salazar E.

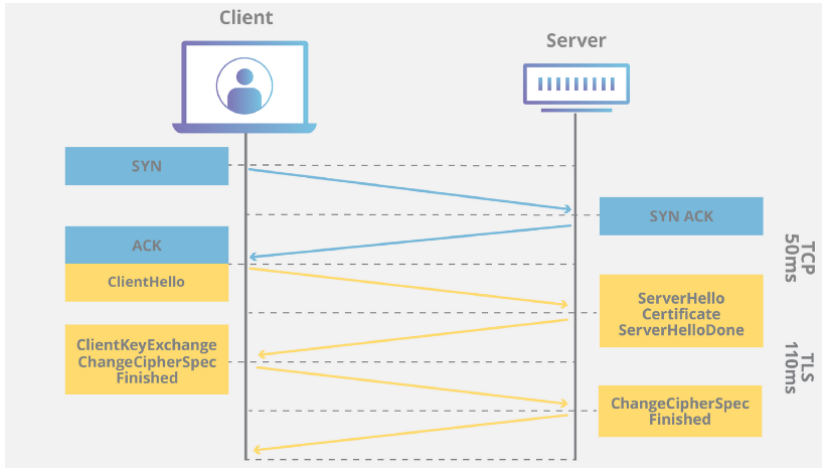
# HTTP Request Over TCP + TLS



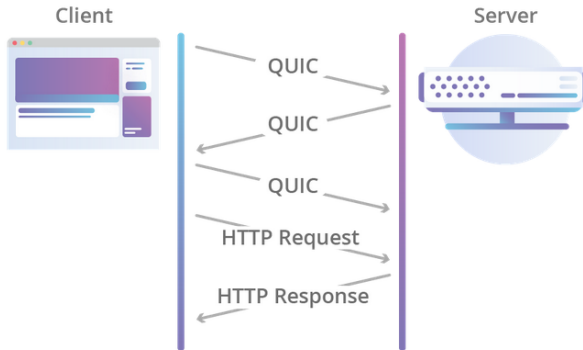
- Client Hello
  - TLS version the client supports.
  - Cipher suites supported.
  - Random string (client random)
- Server Hello
  - Server's SSL certificate
  - the server's chosen cipher suite.
  - Random string (server random)

- 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

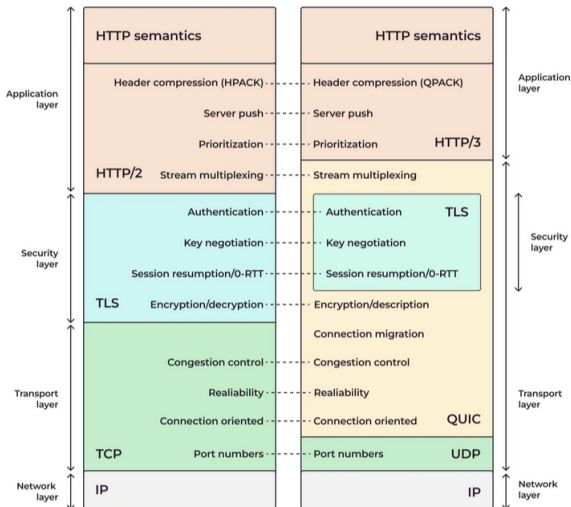
- Does not support RSA
- Client Hello: assuming server's preferred method, send data for premaster
- Server Generates master secret
- Server send Finish (Server Ready)
- Client send Finish (Client Ready)
- Secure Symmetric Encryption Achieved



## HTTP Request Over QUIC

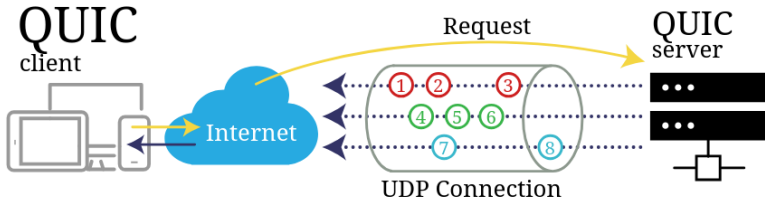
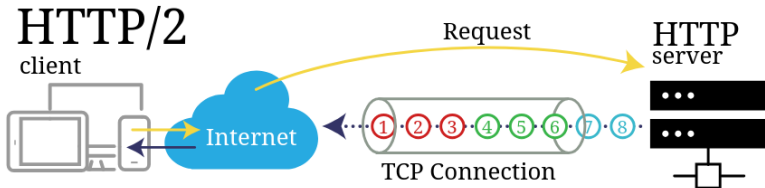


# HTTP2 vs HTTP3





# HTTP2 vs HTTP3





DEMO

- quic work groud
- RFC 9000
- RFC 9001



**Gracias**