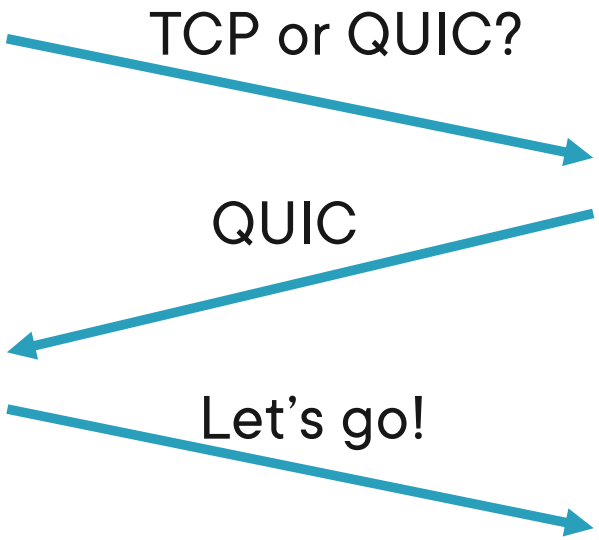
Analyzing QUIC with Wireshark

Module Overview

- TCP to QUIC Handoff
- The QUIC Handshake
  - TLS 1.3 Handshake
- QUIC Connections and Streams
- Packets and Frames
- QUIC Analysis with Wireshark

The QUIC Handoff

TCP to QUIC Handoff



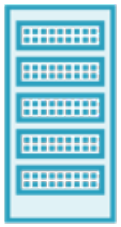
Before initiating QUIC, most clients check-in with TCP first

In future straight to QUIC (some do this now)

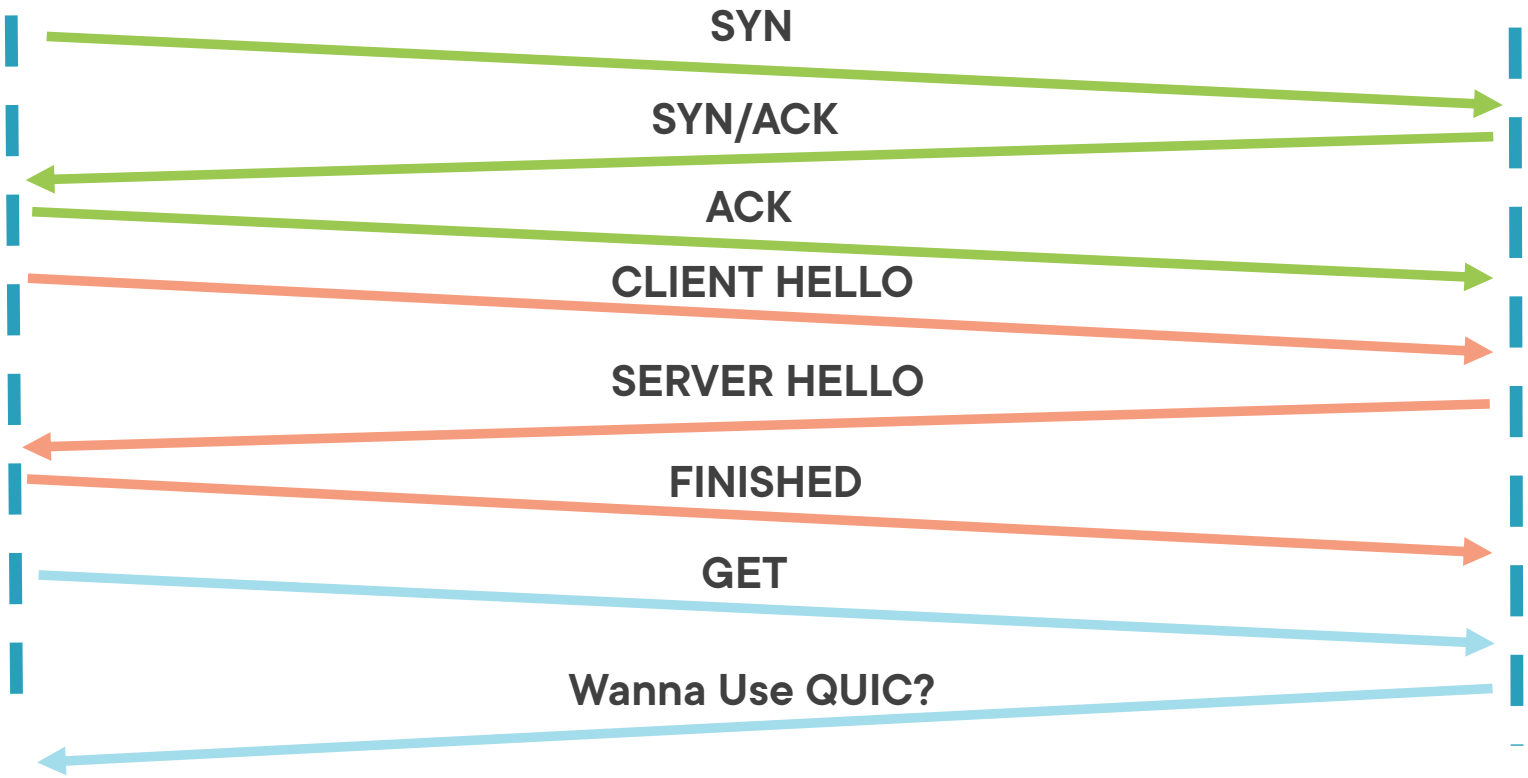
Uses an HTTP Redirect (302)

QUIC Handoff

192.168.1.100 : 1000



10.1.1.100 : 443



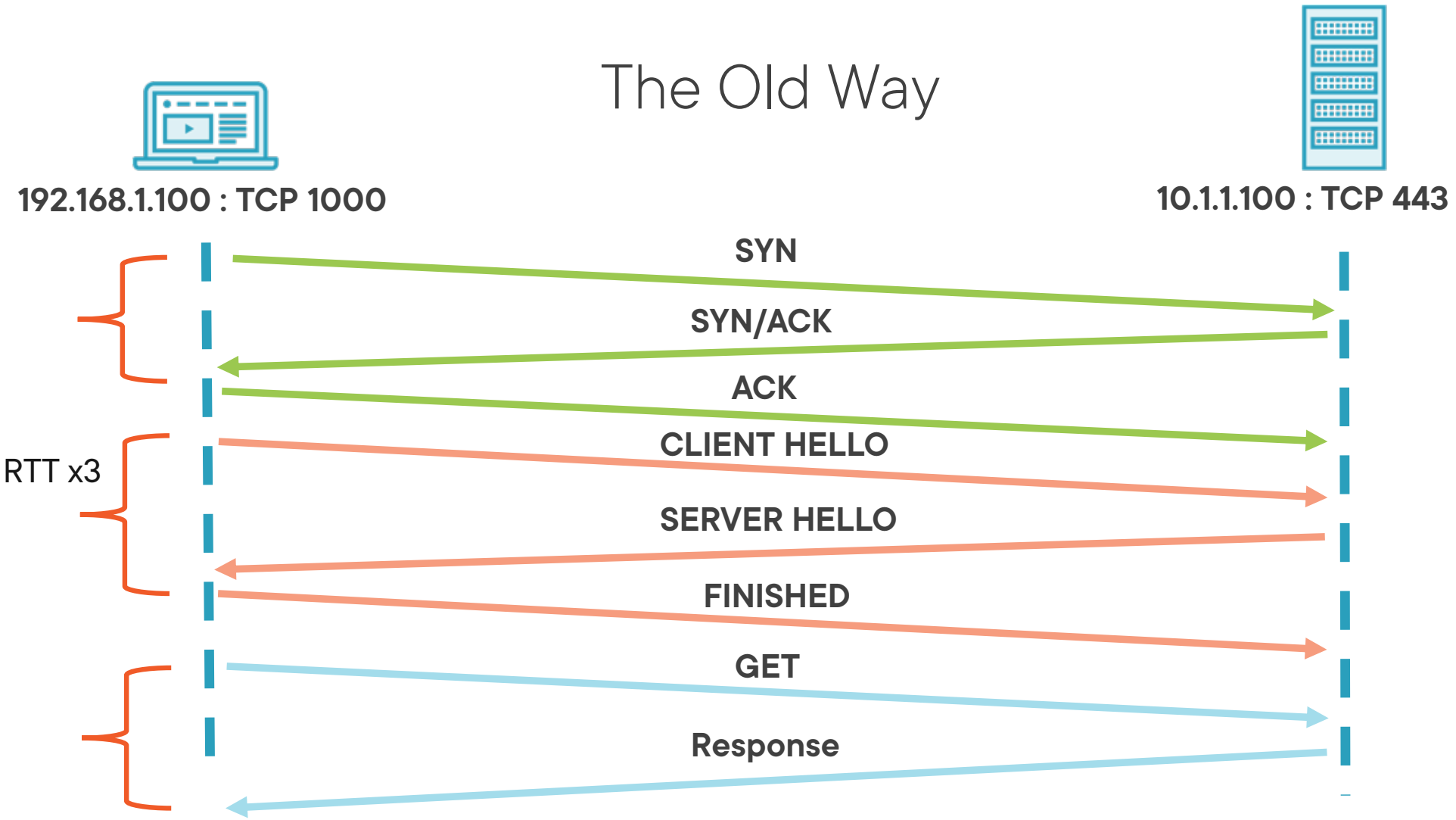
Demo

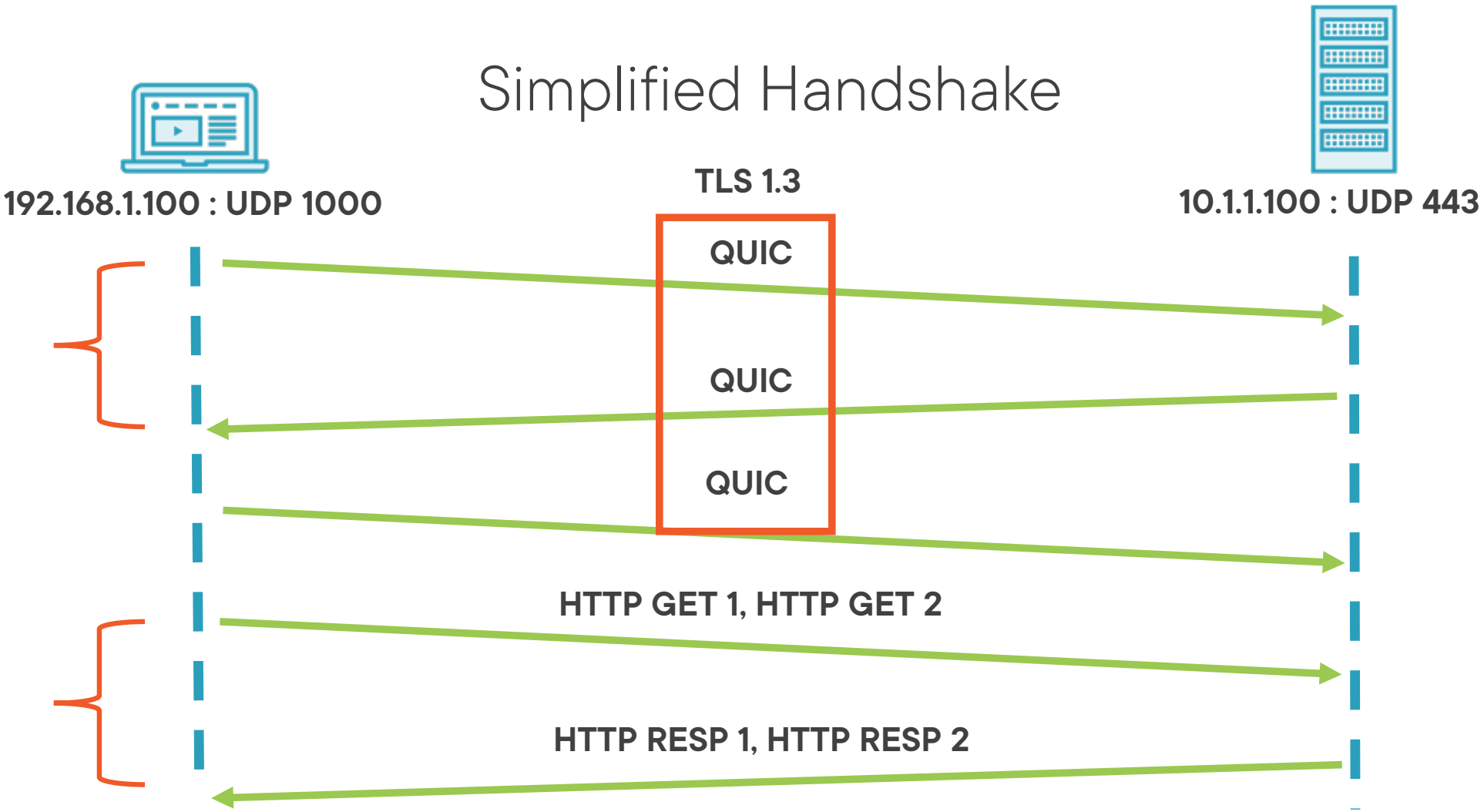
QUIC Handoff Demo

- **Use Lab 1 Trace File**

The QUIC Handshake

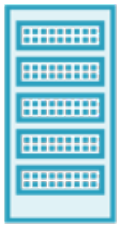
The Old Way


192.168.1.100 : TCP 1000
10.1.1.100 : TCP 443
SYN
SYN/ACK
ACK
RTT x3
CLIENT HELLO
SERVER HELLO
FINISHED
GET
Response

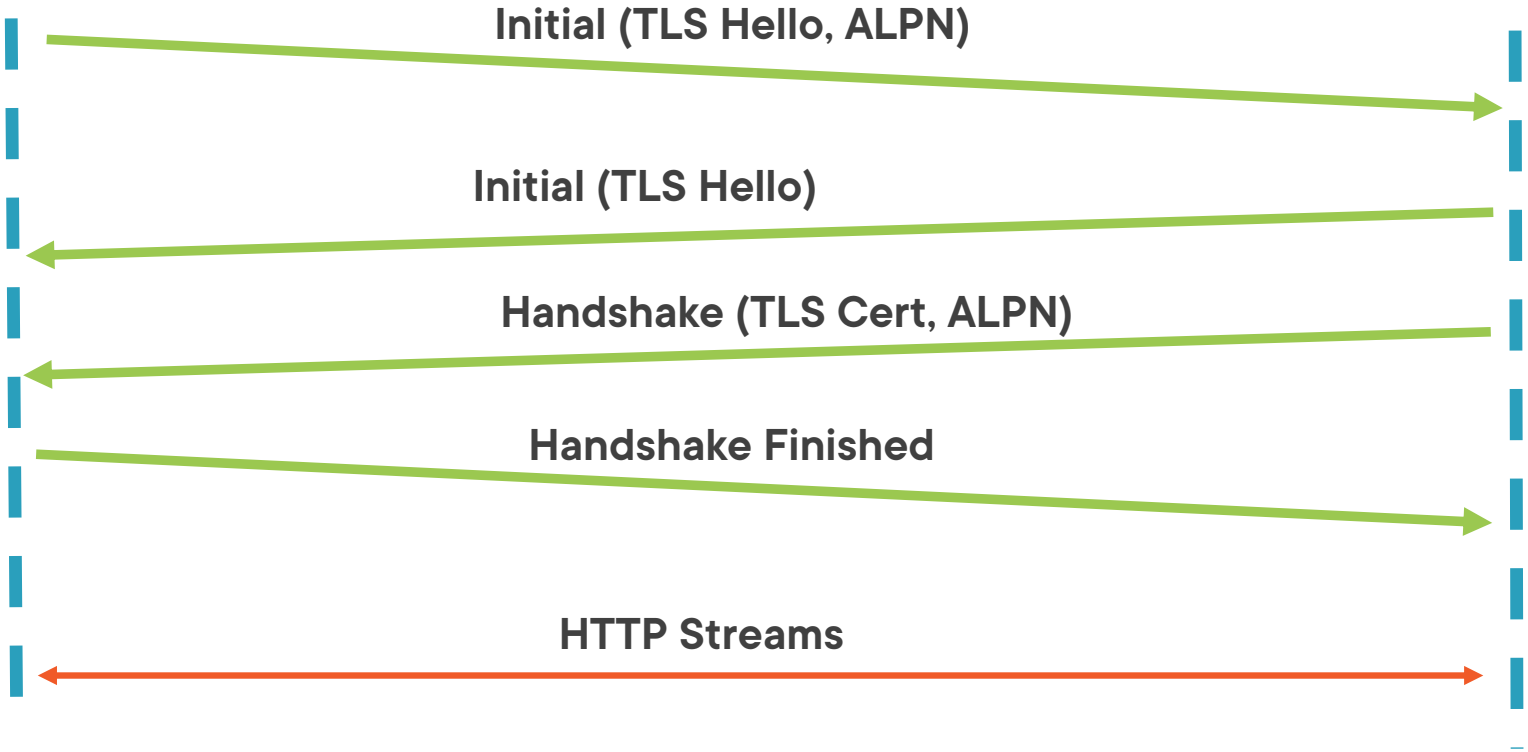

Simplified Handshake
192.168.1.100 : UDP 1000
TLS 1.3
10.1.1.100 : UDP 443
QUIC
QUIC
QUIC
HTTP GET 1, HTTP GET 2
HTTP RESP 1, HTTP RESP 2

QUIC Handshake Detail

192.168.1.100 : UDP 1000



10.1.1.100 : UDP 443



Demo

Demo the QUIC Handshake

- **Lab 2-QUIC Handshake**

QUIC Connections and Streams

QUIC Connections

192.168.1.100 : UDP 1000

Shared Secret (TLS)

Application Protocol

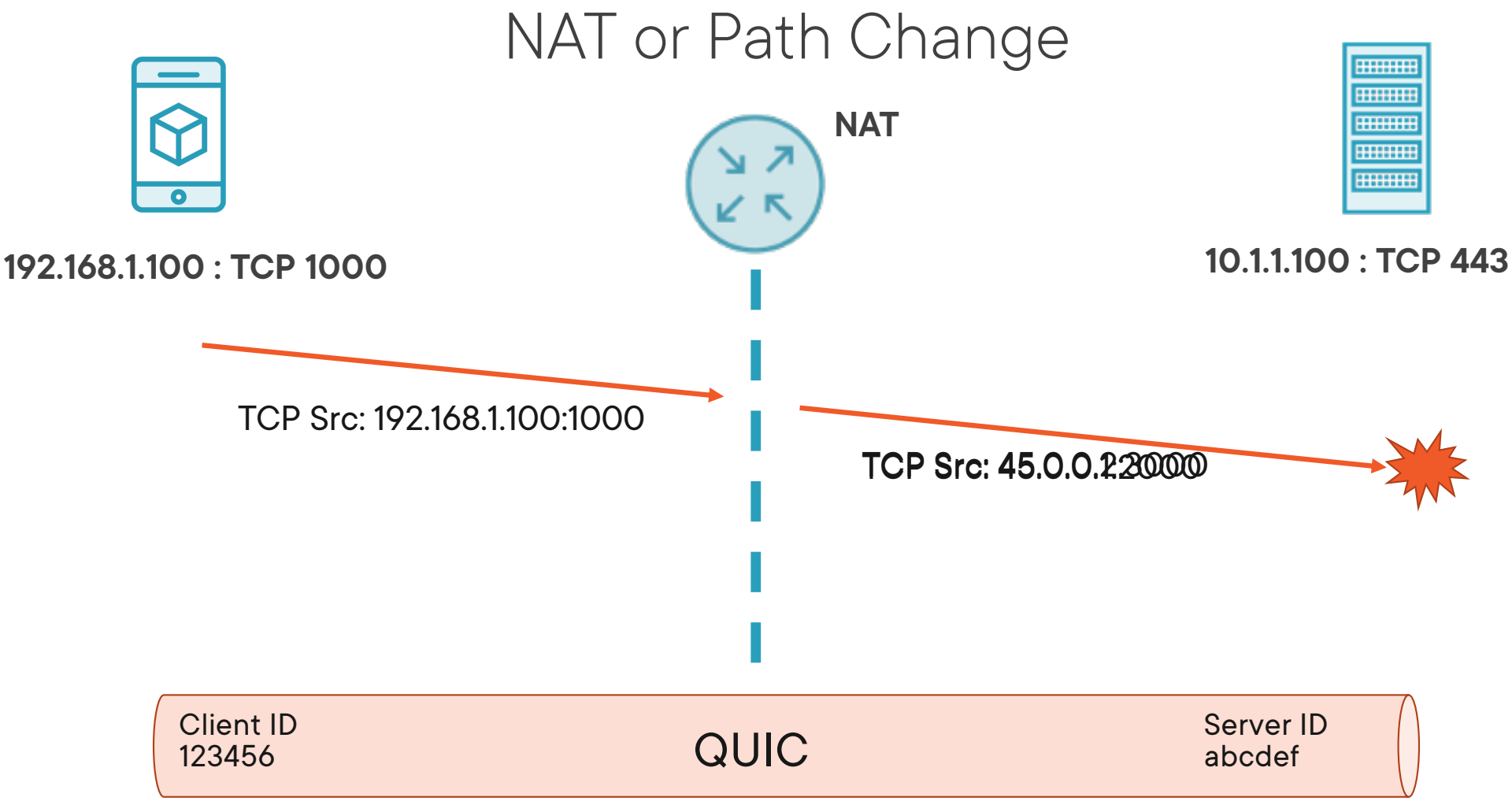
Parameters for Connection

10.1.1.100 : UDP 443

QUIC Connection ID's

192.168.1.100 : UDP 1000

10.1.1.100 : UDP 443

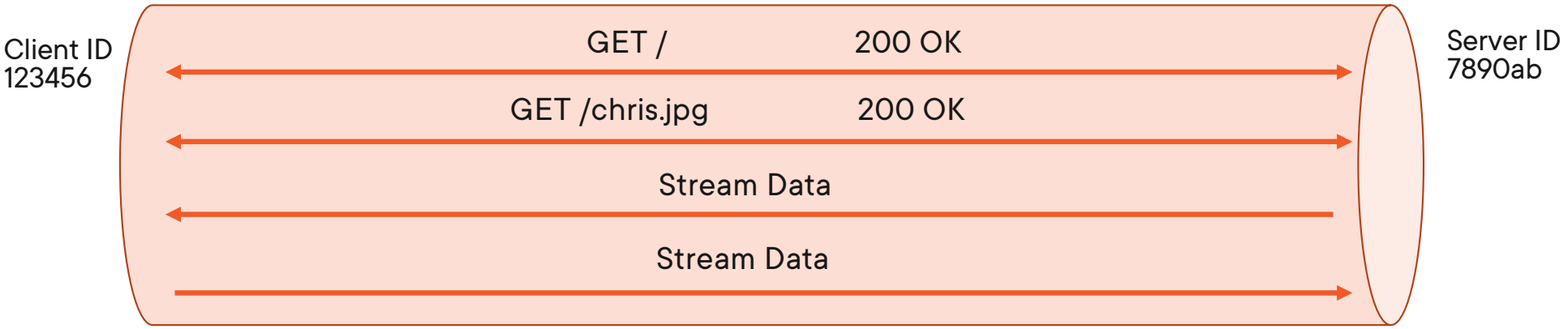

NAT or Path Change
NAT
192.168.1.100 : TCP 1000
10.1.1.100 : TCP 443
TCP Src: 192.168.1.100:1000
TCP Src: 45.0.0.1:20000
Client ID
123456
QUIC
Server ID
abcdef

Streams

Bi-Directional or Unidirectional

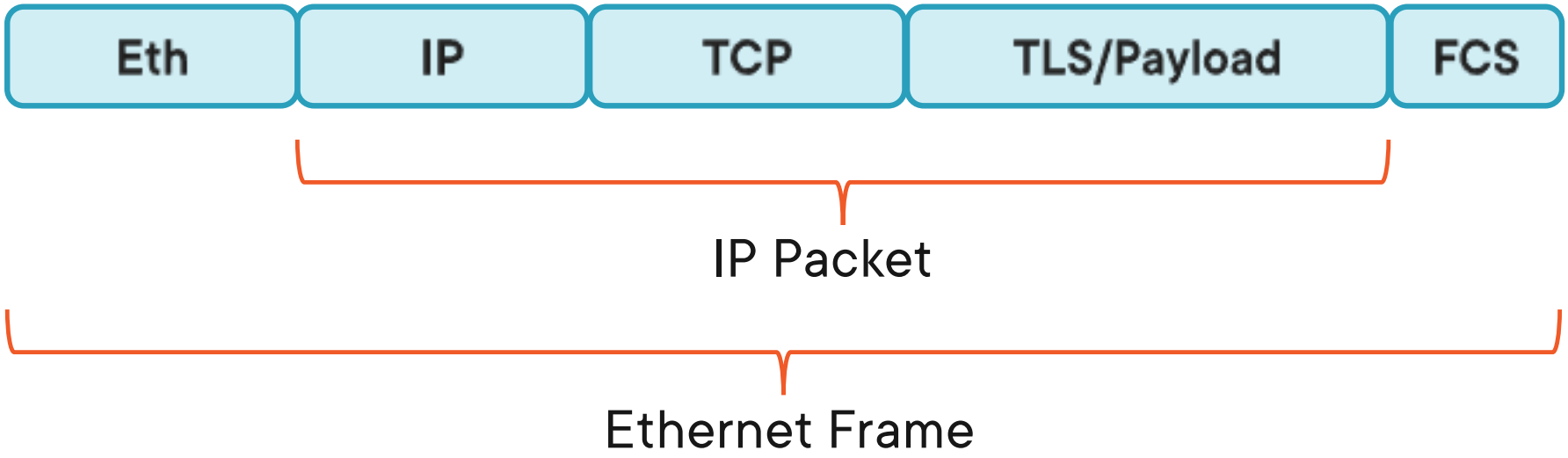
192.168.1.100 : UDP 1000

10.1.1.100 : UDP 443

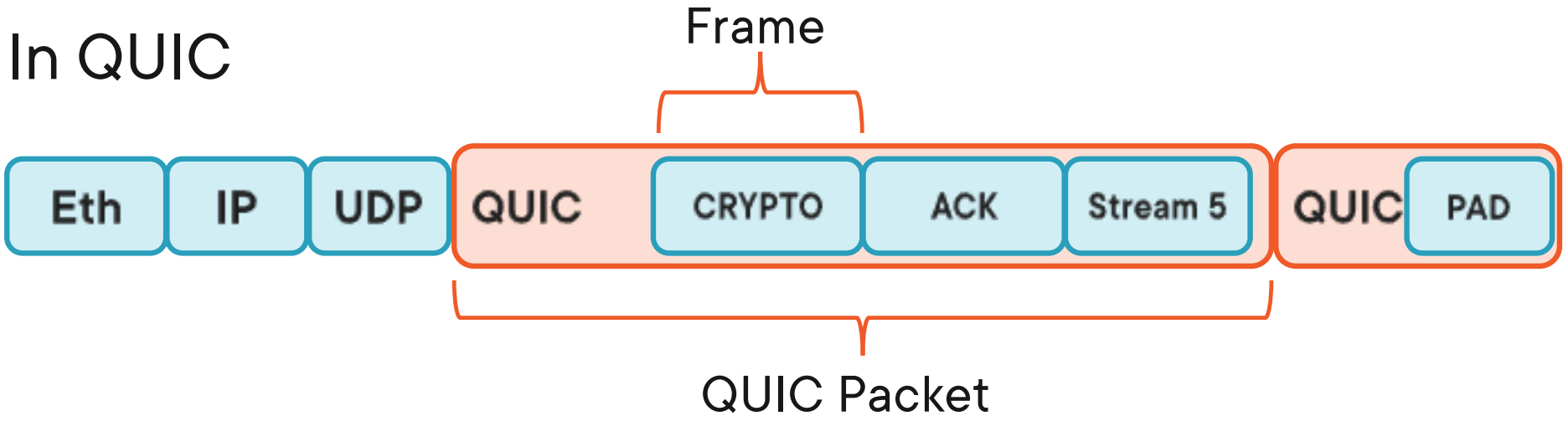


What is a Packet/Frame?

Until now...



What is a QUIC Packet/Frame?



Demo

QUIC Streams, Packets, and Frames