

# EVALUATION OF MASQUE-PROXYING

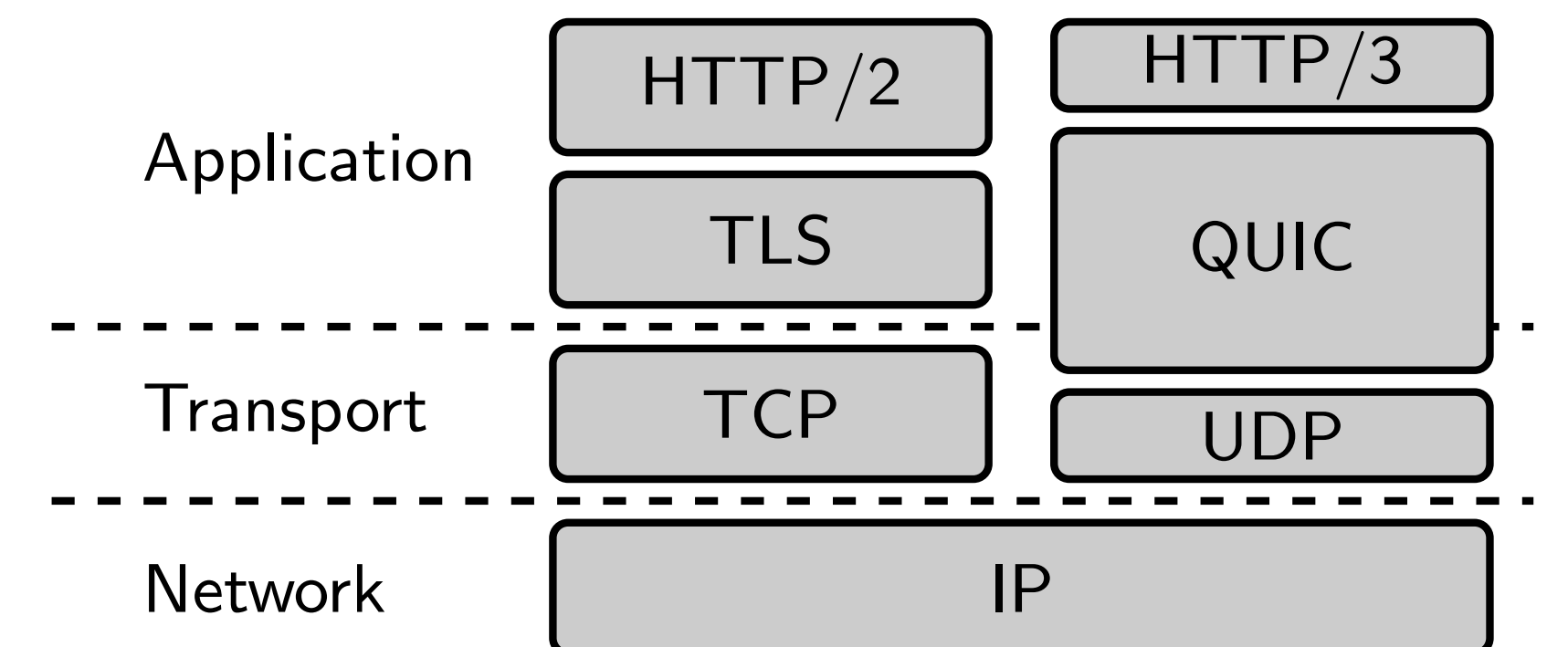
## Introduction

### QUIC

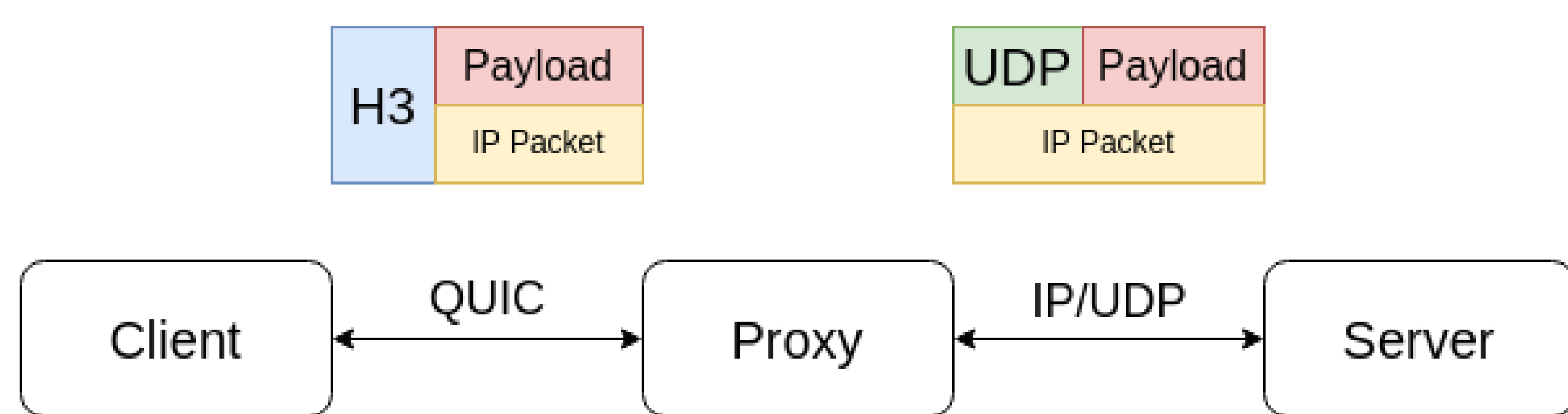
- ▶ Transport protocol on top of UDP
- ▶ Standardized in 2021
- ▶ Implemented in Userspace
- ▶ Built-in encryption
- ▶ Per-stream congestion control

### HTTP/3

- ▶ New HTTP version after HTTP/2
- ▶ Runs on top of QUIC
- ▶ CONNECT method transforms web server into TCP proxy



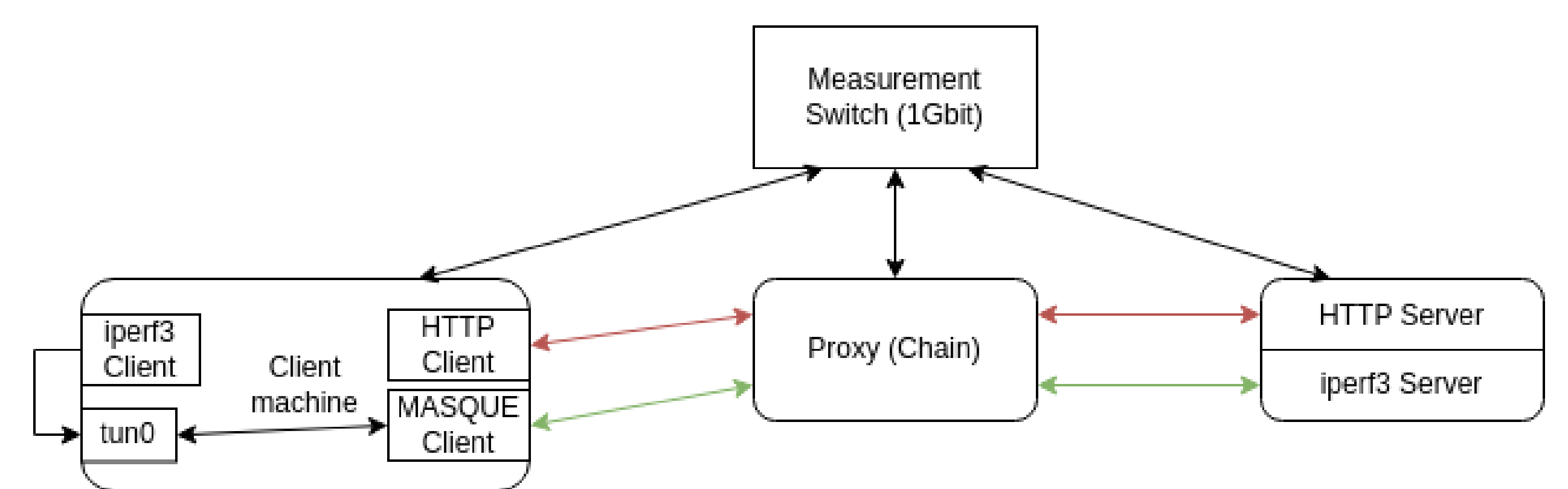
## MASQUE



CONNECT-UDP (top) and -IP (bottom)

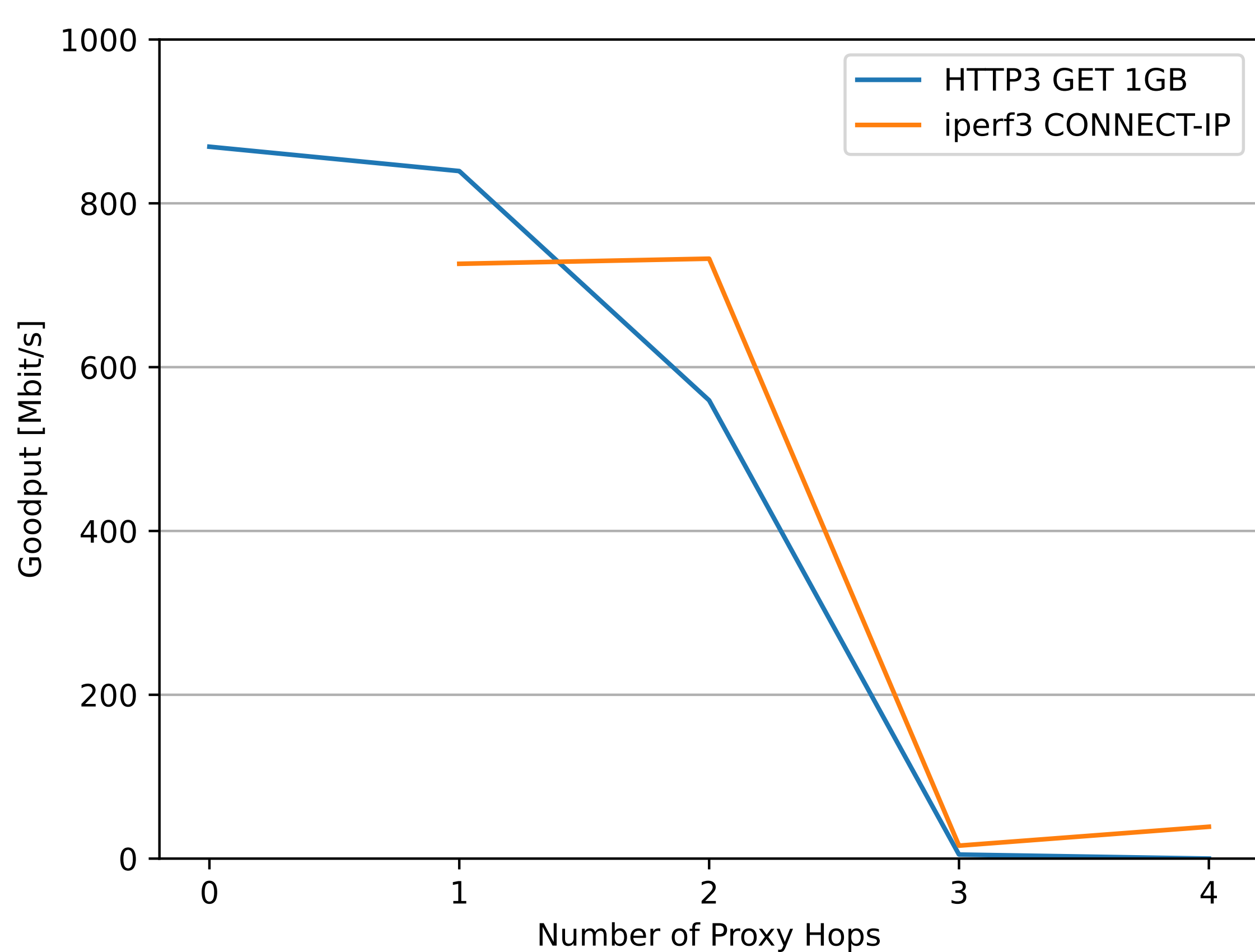
- ▶ Protocols to proxy UDP- and IP-based traffic over HTTP
- ▶ Standards are Active Internet Drafts CONNECT-UDP (RFC 9298) and CONNECT-IP (RFC 9484)
- ▶ Used by Apple in *iCloud Private Relay* service

## Test Setup



- ▶ Measuring throughput via HTTP/3 GET or iperf3
- ▶ iperf3 uses `tun` device to connect via MASQUE client
- ▶ Machines are connected via dedicated switch
- ▶ Multi-hop proxy chains use CONNECT-UDP mode for hops 1 to  $n - 1$  and desired mode for hop  $n$

## Evaluation



- ▶ More than two hops with encapsulated tunnels result in inefficient header overhead
- ▶ Up to two proxies are feasible in encapsulated mode

## Conclusion

### Current state:

- ▶ Scalable MASQUE proxies are feasible
- ▶ Implemented both CONNECT-UDP and -IP
- ▶ `tun` devices are a strong bottleneck
- ▶ Encapsulated tunnels reach a deterministic hop limit

### Limitations:

- ▶ Limited hardware for multi-hop setup
- ▶ All hosts share single switch

### Future work:

- ▶ QUIC-Aware proxying for proxy chains without overhead
- ▶ Encryption for QUIC-Aware proxying for TOR-like privacy and security properties
- ▶ Implement drafts such as CONNECT-ethernet