iCloud Private Relay

Tommy Pauly
PEARG
IETF 111, July 2021, Virtual

What is Private Relay?

Solution for user privacy that separates client IPs from origin servers

- Multi-hop MASQUE proxy for fully-protected traffic
- Oblivious DoH for other traffic
- Proxies authenticated with TLS 1.3 raw public keys
- Clients authenticated with RSA blind signatures

What is Private Relay?

iOS 15 and macOS Monterey

- All Safari traffic
- All DNS traffic
- All unencrypted HTTP traffic
- *Also used for Mail pixel trackers*

Goals

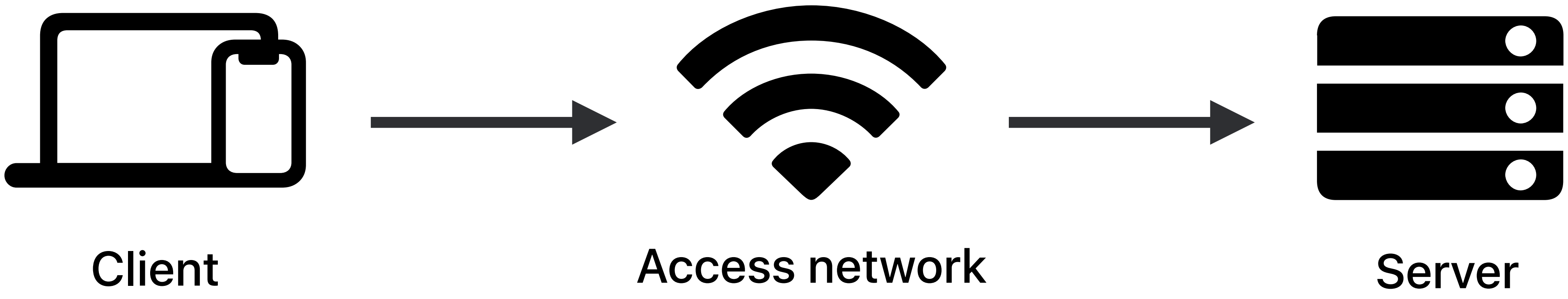
No one entity can see both who a user is (IP address) and what they are accessing (origin server)

Performance must be good enough for generic web browsing, for any user

Built to be left on, not flipped on and off like many VPNs

Two hops is a minimum for separation of connection data

Status Quo



Client

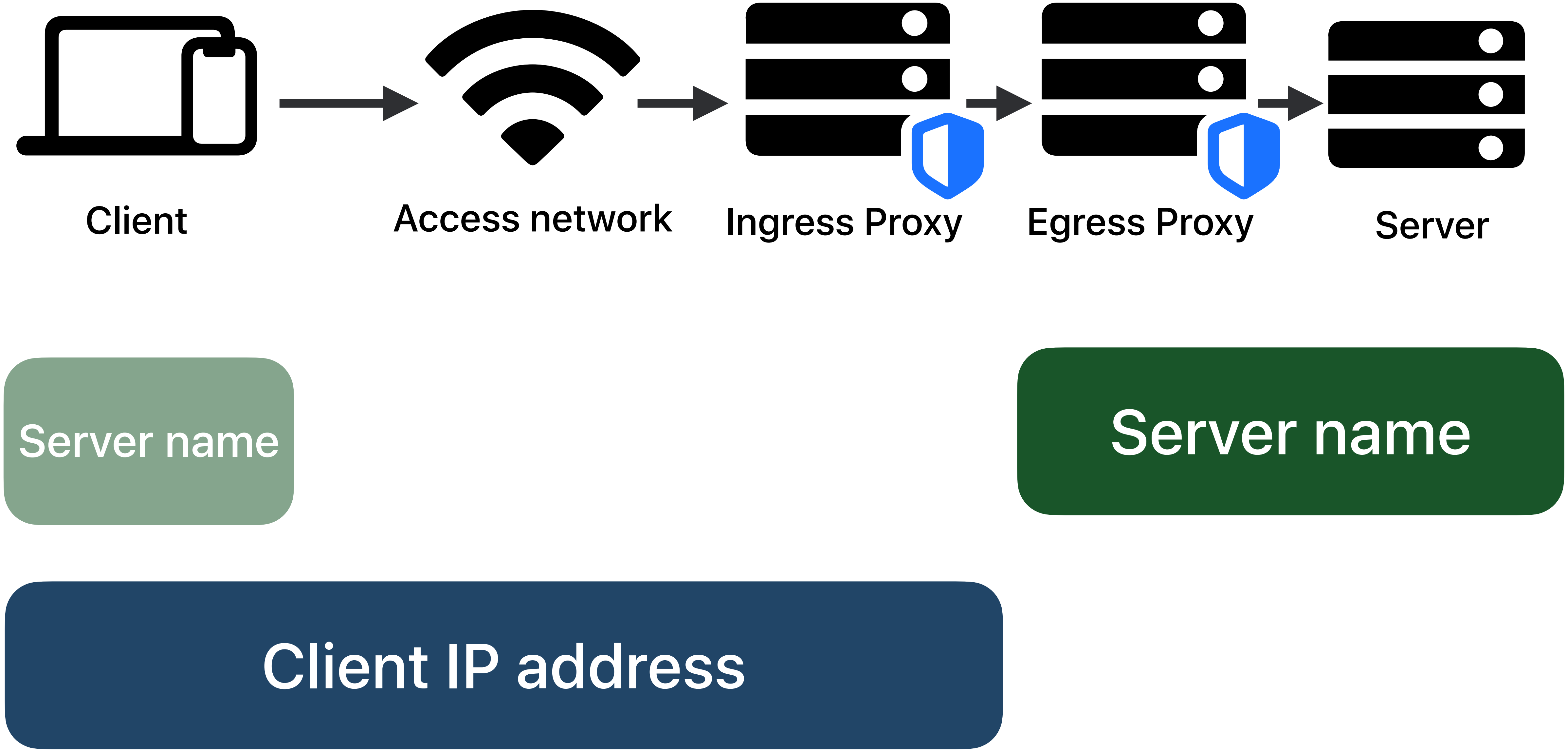
Access network

Server

Server name

Client IP address

Private Relay



Client

Access network

Ingress Proxy

Egress Proxy

Server

Server name

Server name

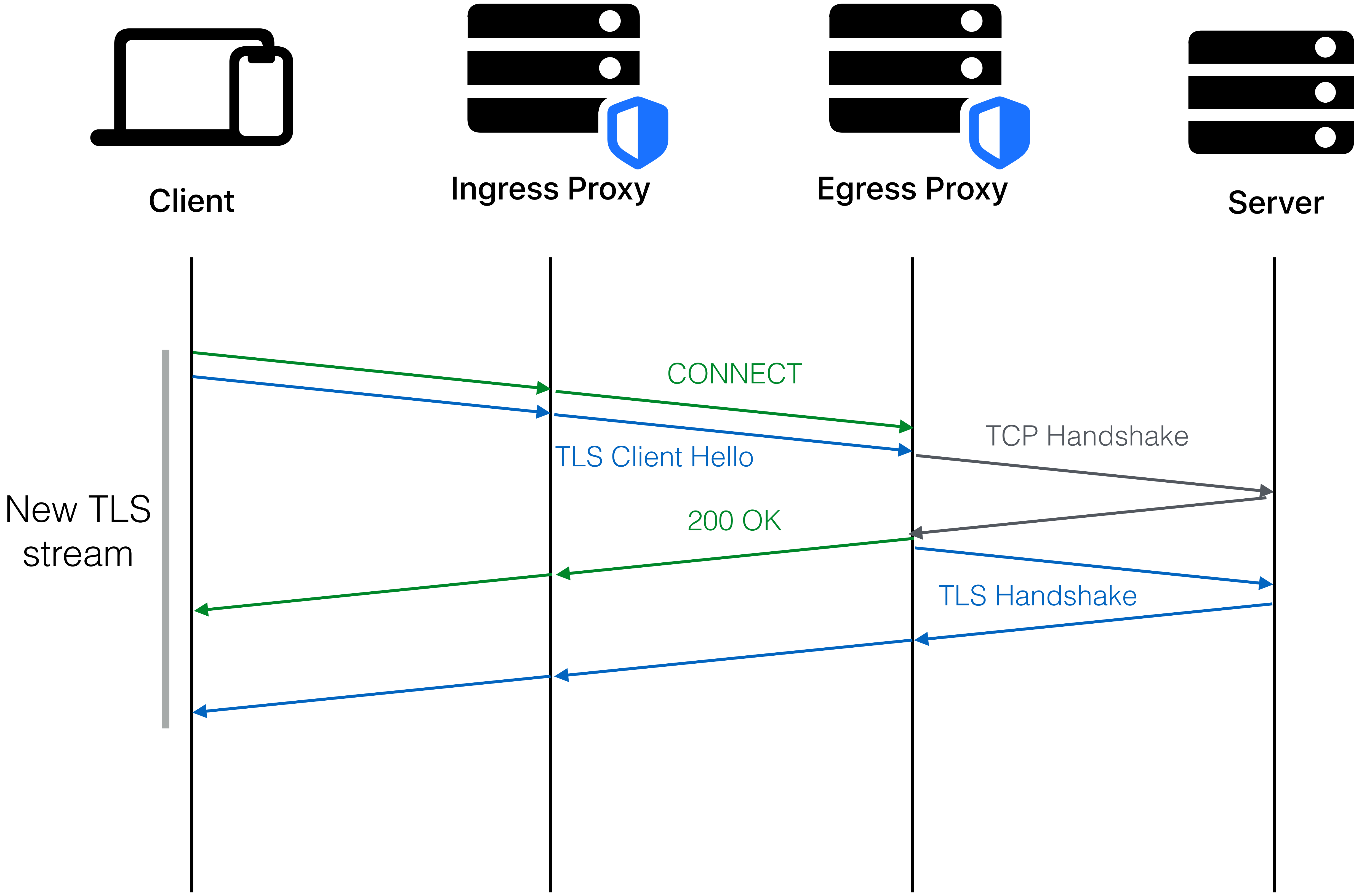
Client IP address

Clients select the hops, and have nested encryption for handshakes to the next hop

The hops are chosen to be run by separate entities

Collusion across entities would be required to track user activity; currently handled by not allowing sharing of this data by policy

Privacy ≠ slow


Client
Ingress Proxy
Egress Proxy
Server
CONNECT
TCP Handshake
TLS Client Hello
New TLS stream
200 OK
TLS Handshake

Always able to do “fast open” for TLS handshakes

Clients can use QUIC on last mile regardless of origin server support

Clients can use IPv6 regardless of server support; servers see IPv6 regardless of last mile support

Metrics from seed users indicates that web browsing is on par with non-proxied, and sometimes even faster

Focus on breaking as little as possible,
to maximize who can benefit from privacy

Network compatibility

No impact on local network routes

Failover for private hostnames and addresses

Not used if VPNs or other proxies are installed

Website/server compatibility

Rough geolocation preserved, when user wants it

Geohash client hint provided to egress proxy

Selects an appropriate egress IP

Further standards work needs to be done to replace IP for geolocation and fraud prevention

Where do we go from here?

Future possibilities

Expand support for MASQUE proxies

Let's make an open, interoperable network for privacy

Ingress proxies in ISPs and carriers

Egress proxies located within content providers

Clients should be able to select the combination of hops, discover hops, and choose the number of hops

Questions?