MEASUREMENTS IN THE ERA OF ENCRYPTION

END OF MEASUREMENTS, CLOSE WG?

RIPE MAT WG, May 2019

Jari Arkko and Marcus Ihlar, Ericsson
Brian Trammell, Google

Some material from a presentation by Mirja Kühlewind and Brian Trammell; as well as a tech talk by Gonzalo Camarillo and Jari Arkko

MEASUREMENTS IN THE ERA OF ENCRYPTION

OR NOT? CASE OF THE QUIC SPIN BIT

RIPE MAT WG, May 2019

Jari Arkko and Marcus Ihlar, Ericsson
Brian Trammell, Google

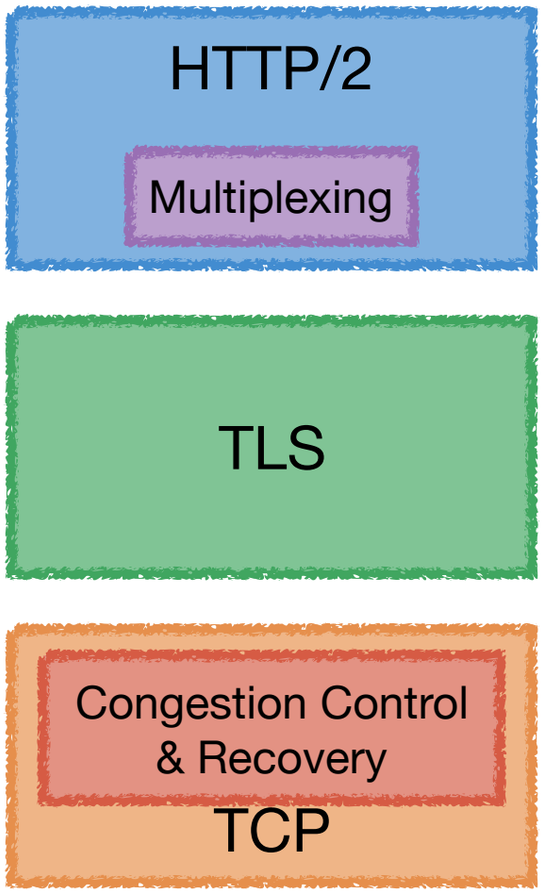
Some material from a presentation by Mirja Kühlewind and Brian Trammell; as well as a tech talk by Gonzalo Camarillo and Jari Arkko

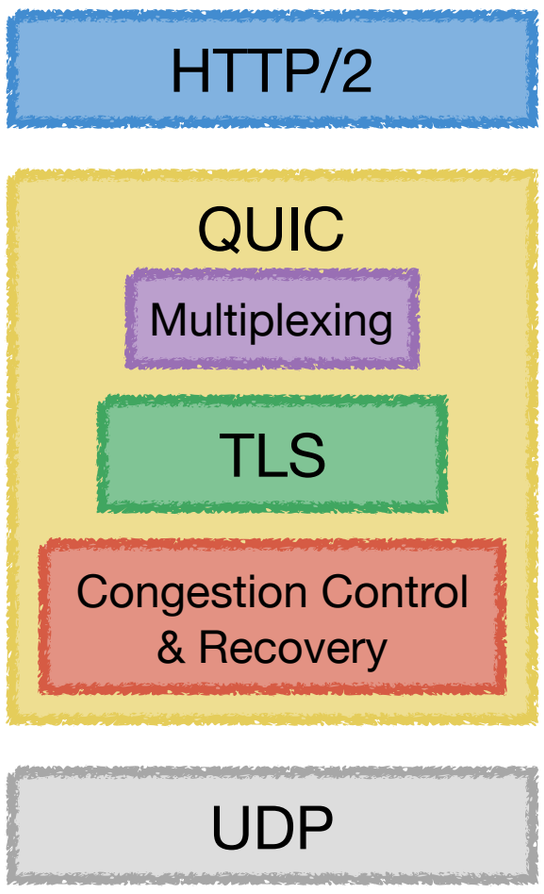
QUIC & WHAT IT GIVES

- Better security
- Deployability via user space implementations and UDP
- Extensibility; avoid ossification
- Reduced latency for connection setup
- Avoids head-of-the-line blocking

QUIC & WHAT IT GIVES

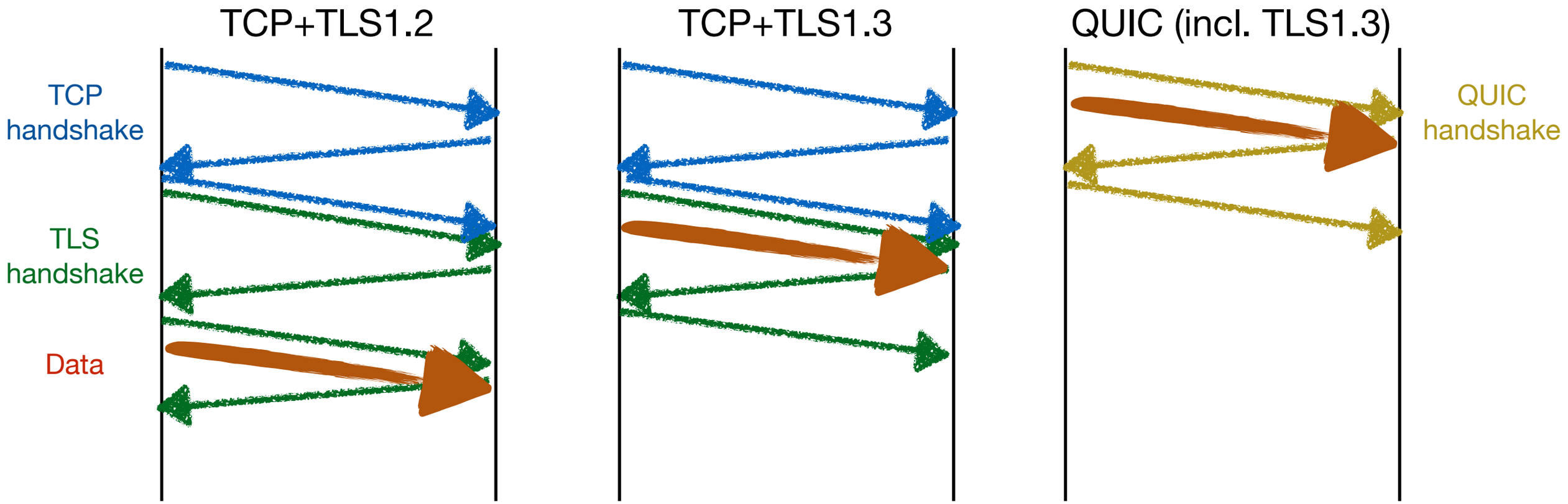
- Better security
- Deployability via user space implementations and UDP
- Extensibility; avoid ossification
- Reduced latency for connection setup
- Avoids head-of-the-line blocking





QUIC & WHAT IT GIVES

- Better Security
- Deployability via user space implementations and UDP
- Extensibility; avoid ossification
- Reduced latency for connection setup
- Avoids head-of-the-line blocking



QUIC AND MEASUREMENTS

OK… but what about measurements?

- **Problem 1**: Round-Trip Time (RTT) can be estimated during the handshake but no easy way to correlate other packets
- **Problem 2**: Packet numbers are now encrypted and cannot be utilised
- **Problem 3**: Retransmissions and ECN congestion reactions are not visible

Can we do anything else than measure traffic volume or where it is going to?

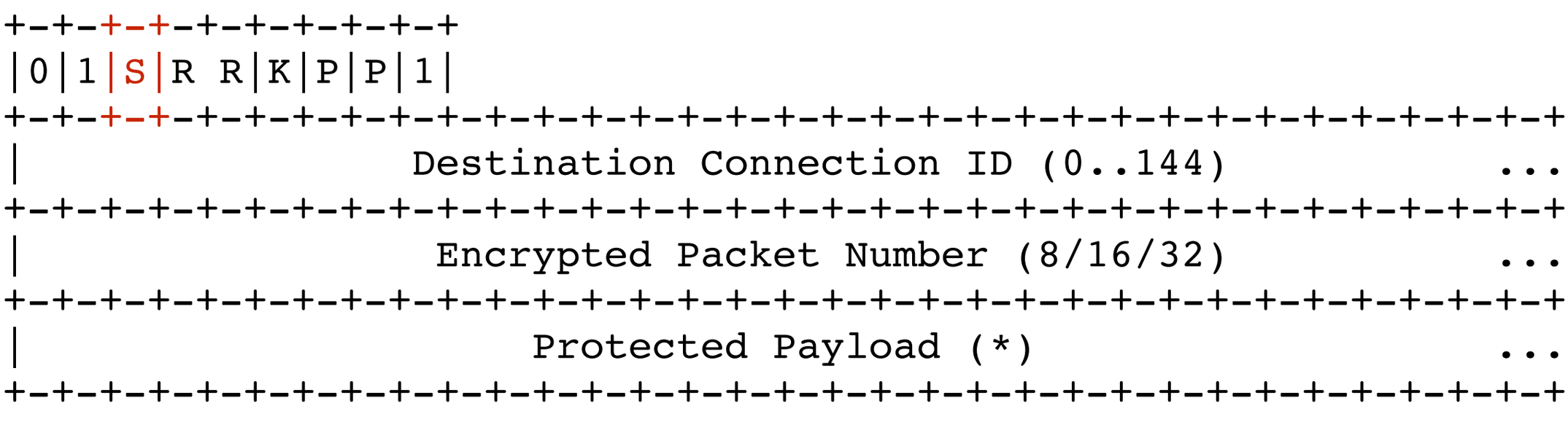
THE QUIC “SPIN” BIT

The IETF has chosen to only provide three pieces of information for on-path elements in QUIC (explicit, not accidental exposure of information):

- IP headers & addresses

- Connection ID:s are visible in packet headers

- **Spin Bit** is a mechanism for passive latency measurement

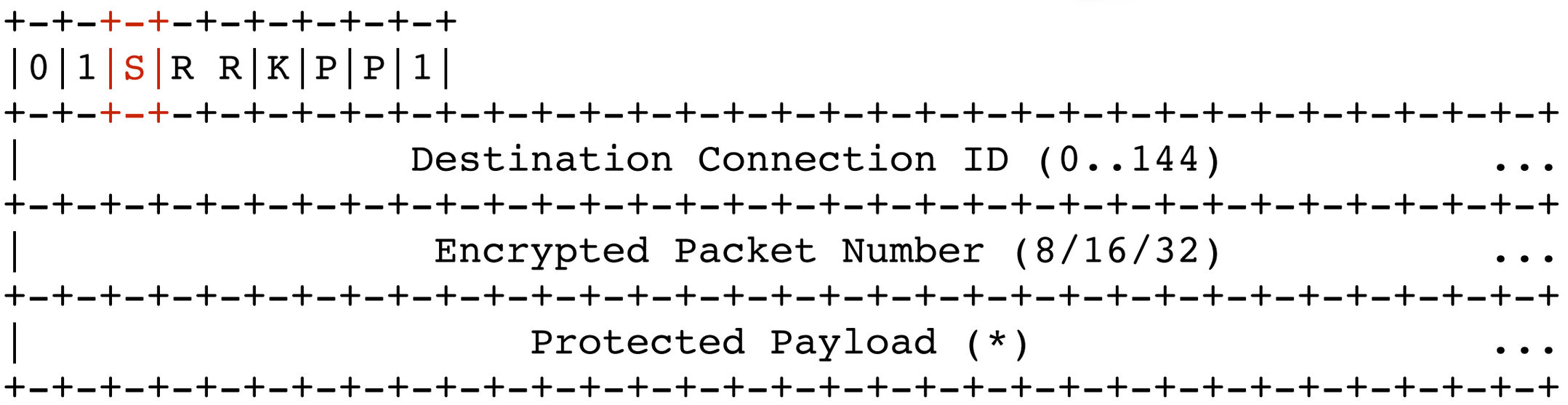


THE QUIC “SPIN” BIT

The IETF has chosen to only provide three pieces of information for on-path elements in QUIC (explicit, not accidental exposure of information):

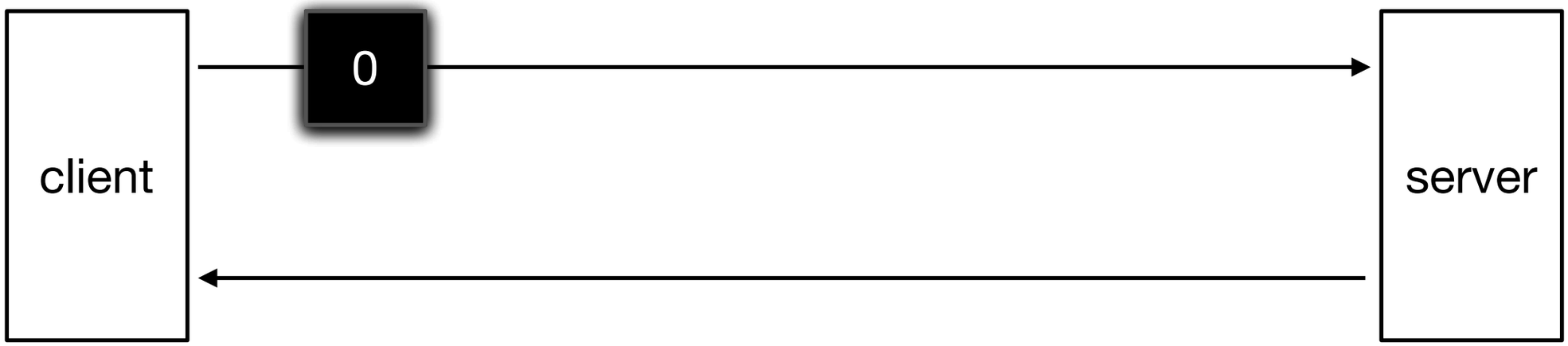
- IP headers & addresses
- Connection ID:s are visible in packet headers
- **Spin Bit** for passive latency measurement

- **Troubleshooting**
- **Congestion detection**
- **Quality monitoring**
- **Research**

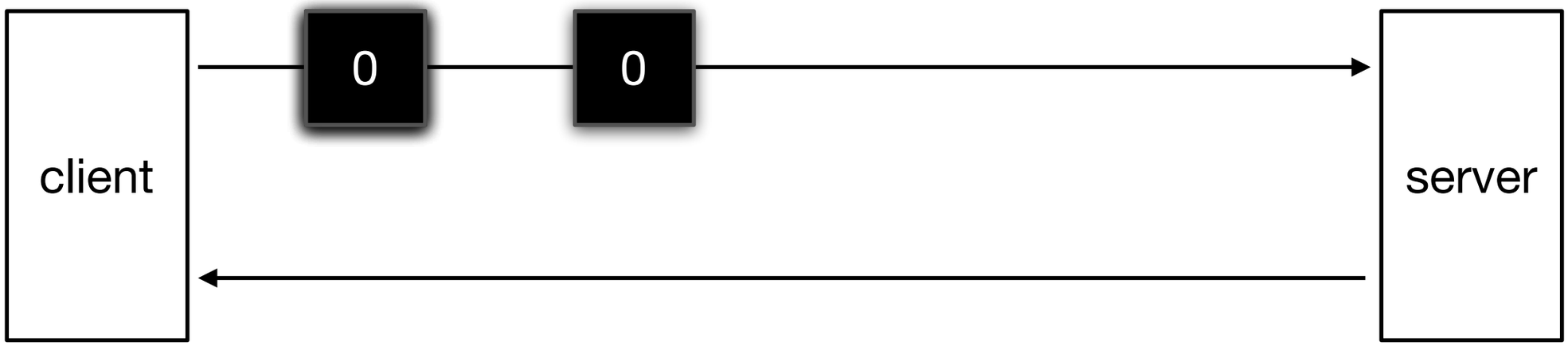


HOW SPIN BIT WORKS

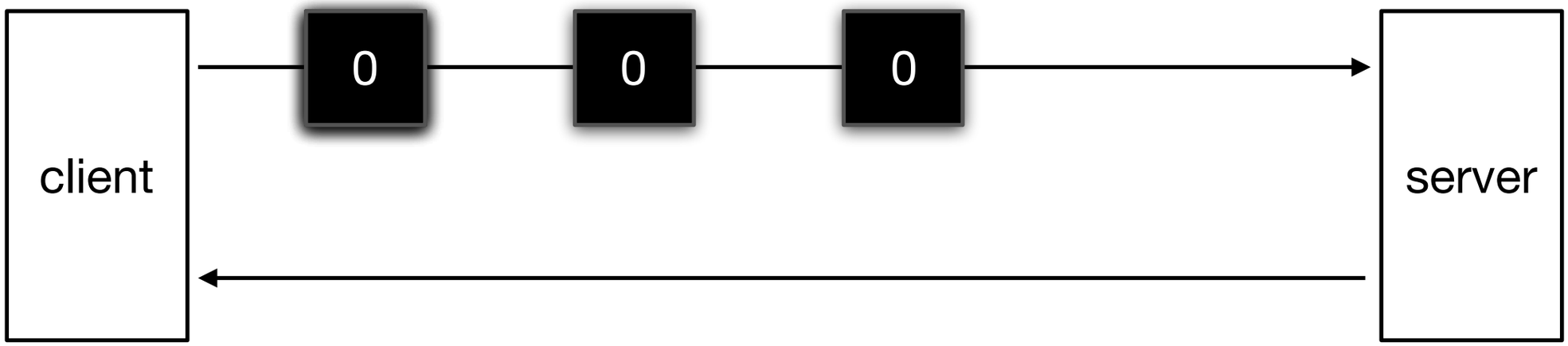
HOW SPIN BIT WORKS



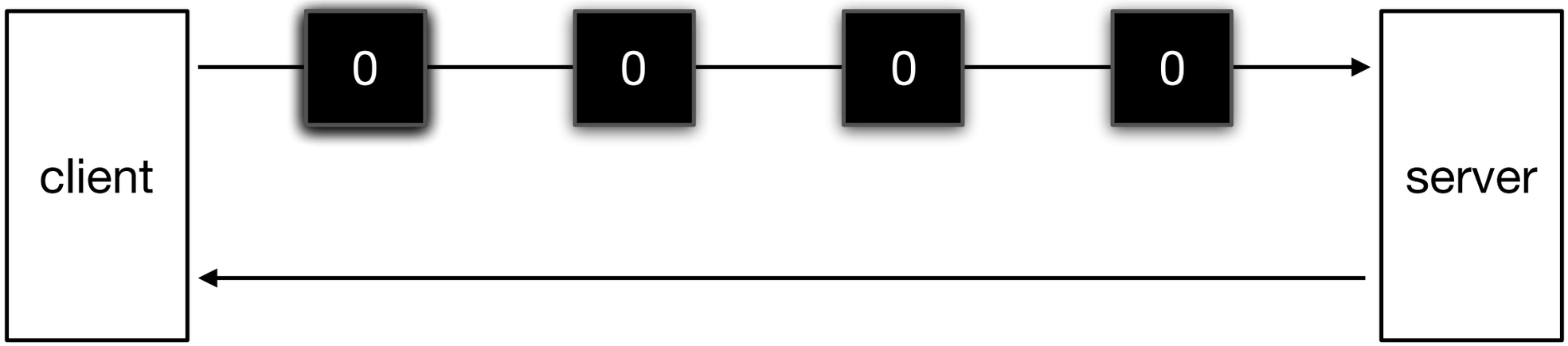
HOW SPIN BIT WORKS



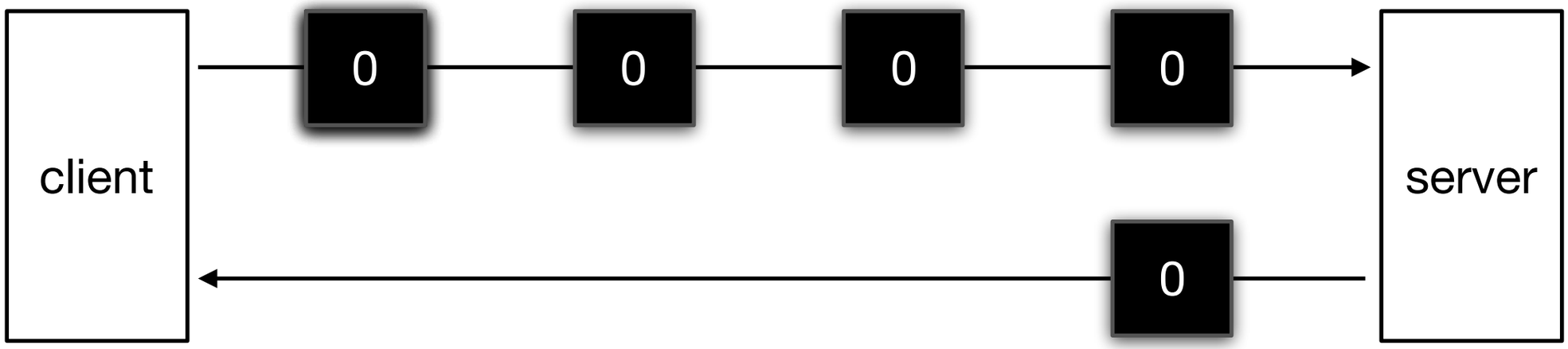
HOW SPIN BIT WORKS



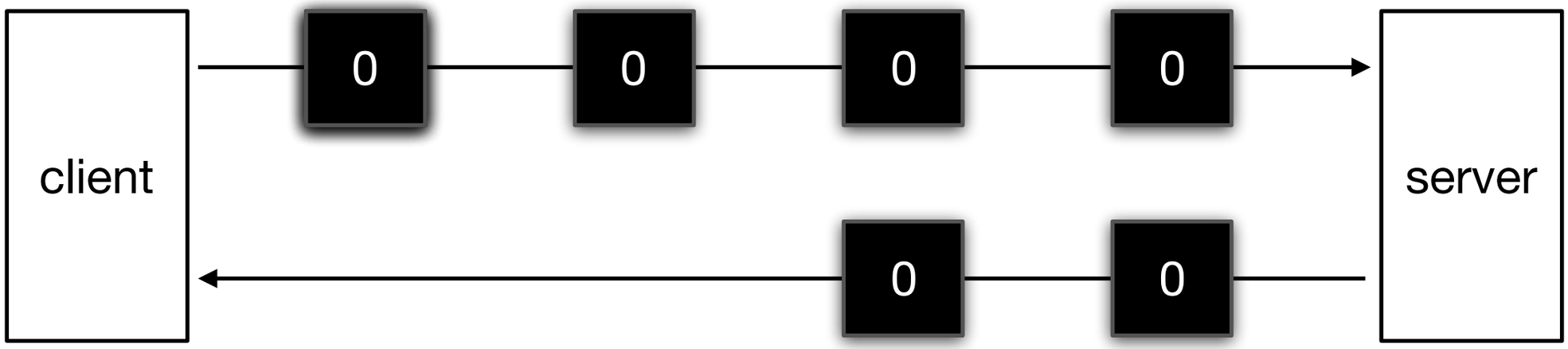
HOW SPIN BIT WORKS



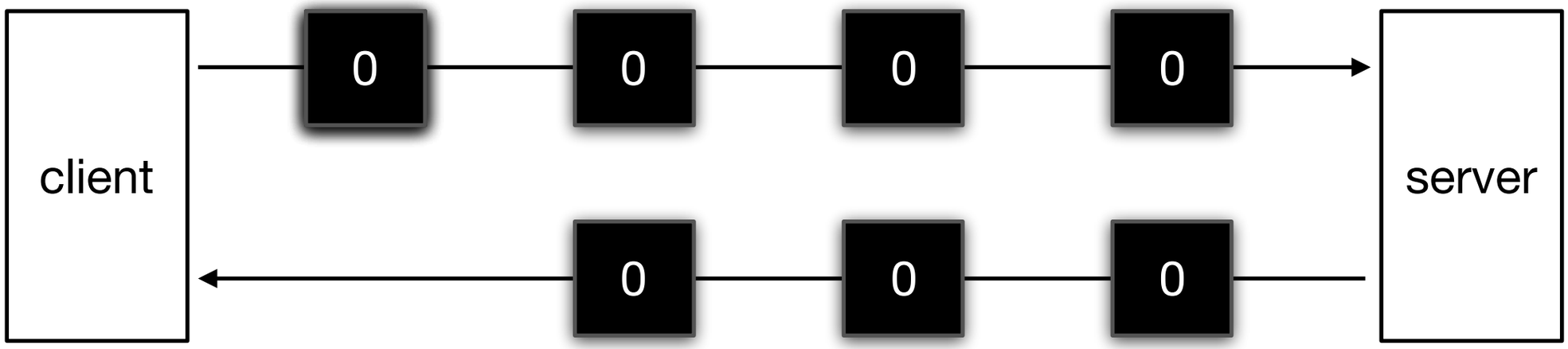
HOW SPIN BIT WORKS



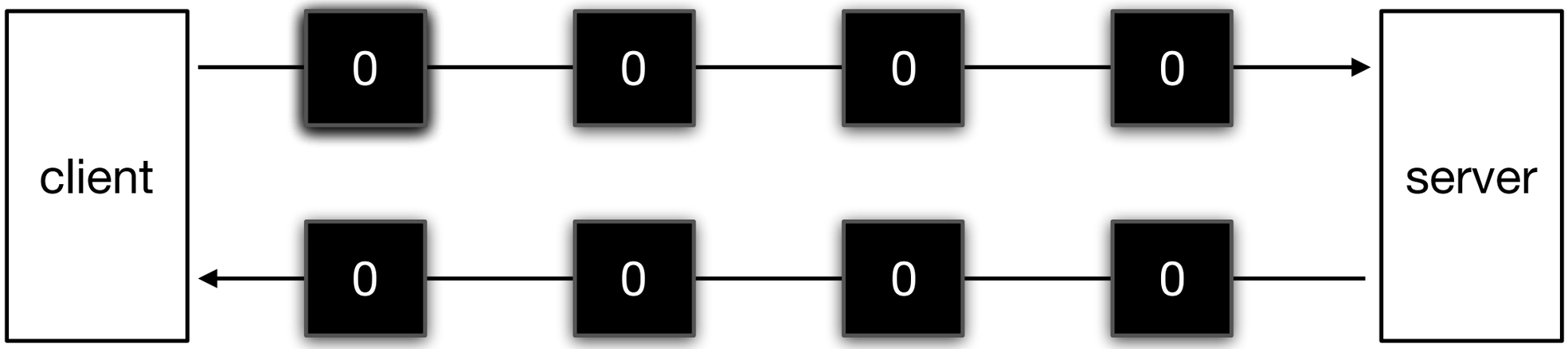
HOW SPIN BIT WORKS



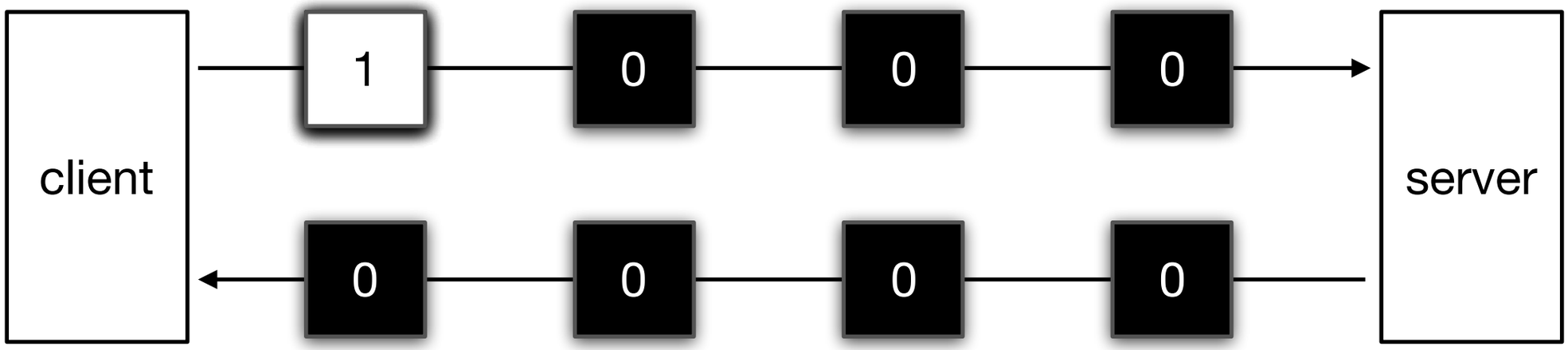
HOW SPIN BIT WORKS



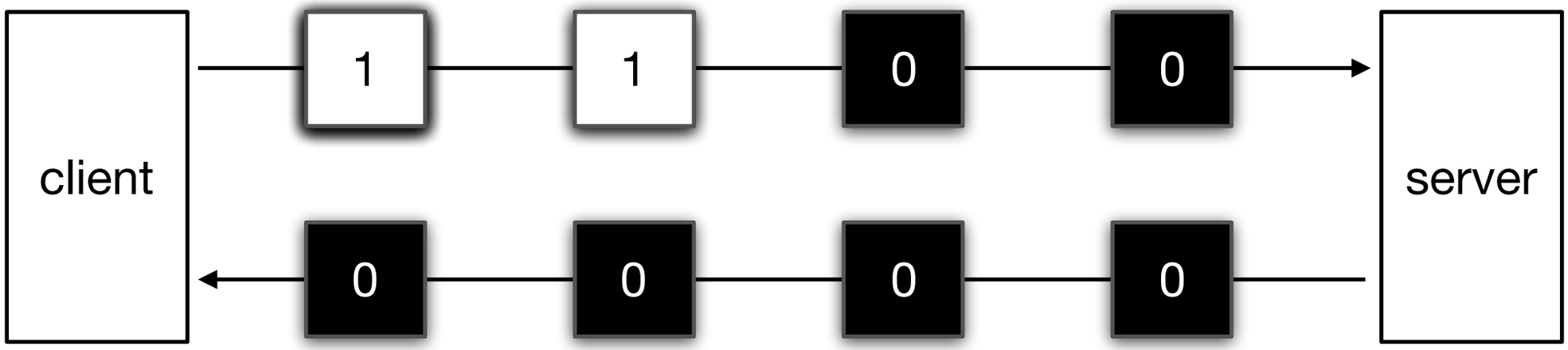
HOW SPIN BIT WORKS



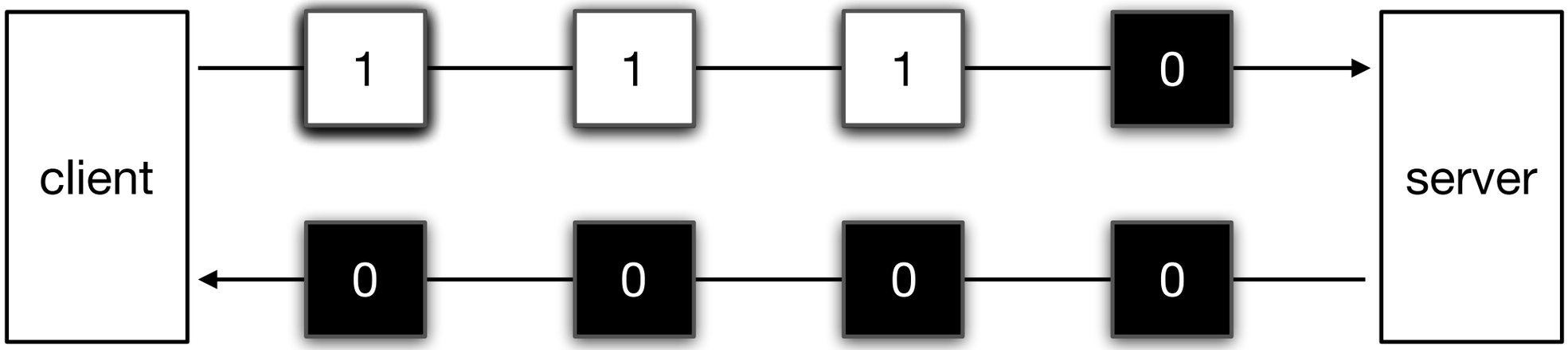
HOW SPIN BIT WORKS



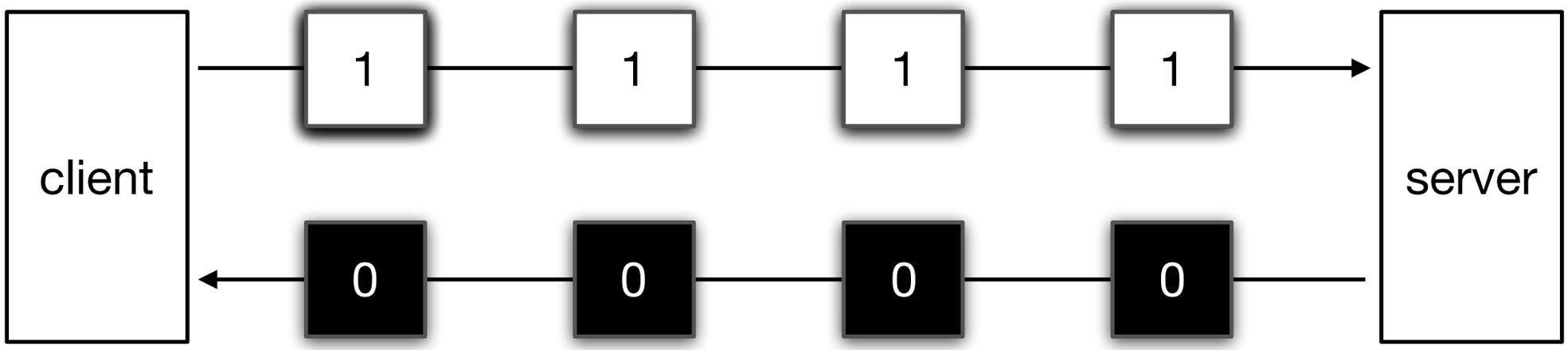
HOW SPIN BIT WORKS



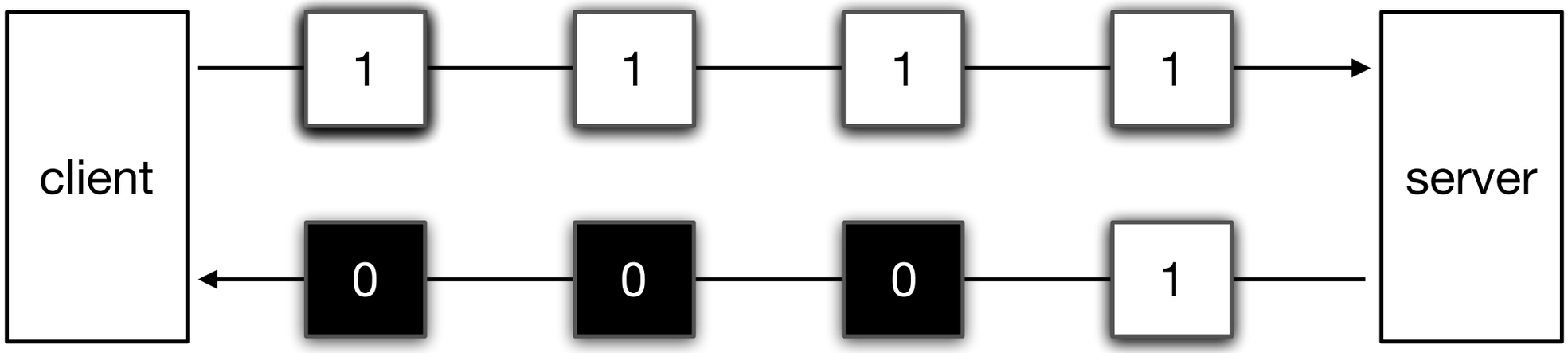
HOW SPIN BIT WORKS



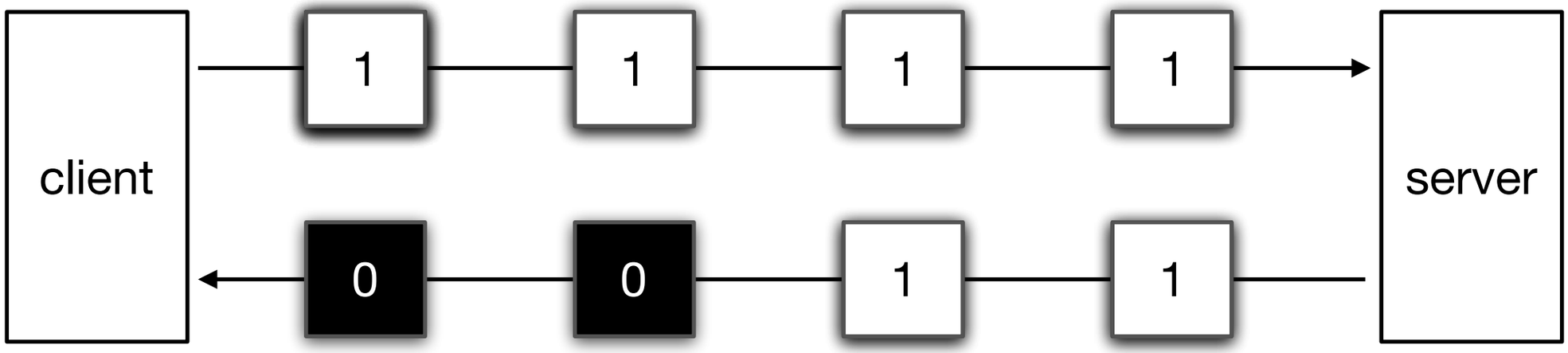
HOW SPIN BIT WORKS



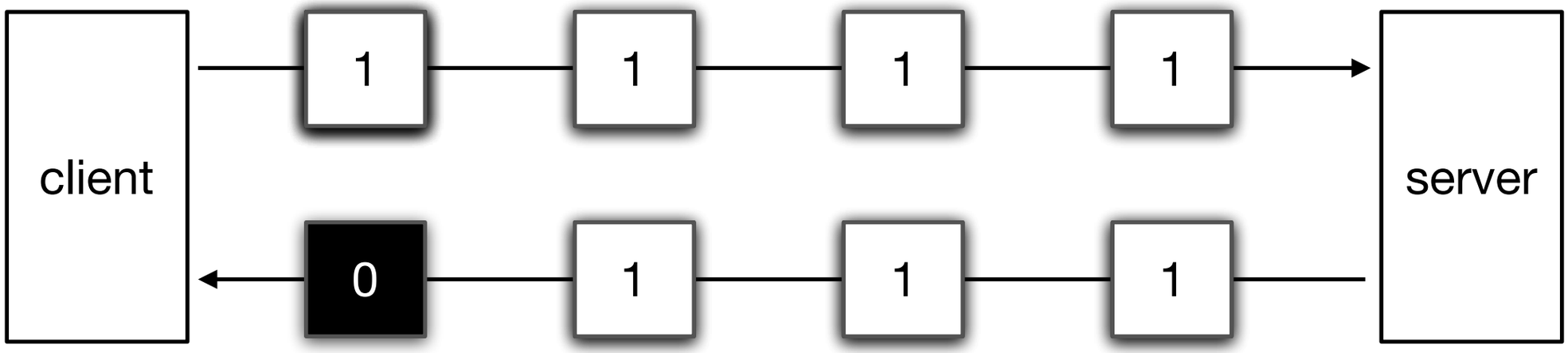
HOW SPIN BIT WORKS



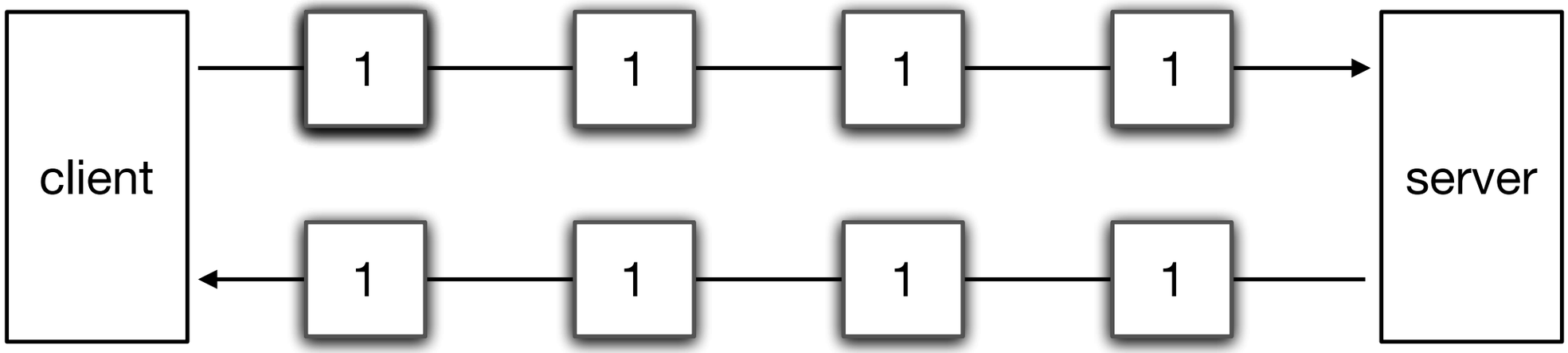
HOW SPIN BIT WORKS



HOW SPIN BIT WORKS



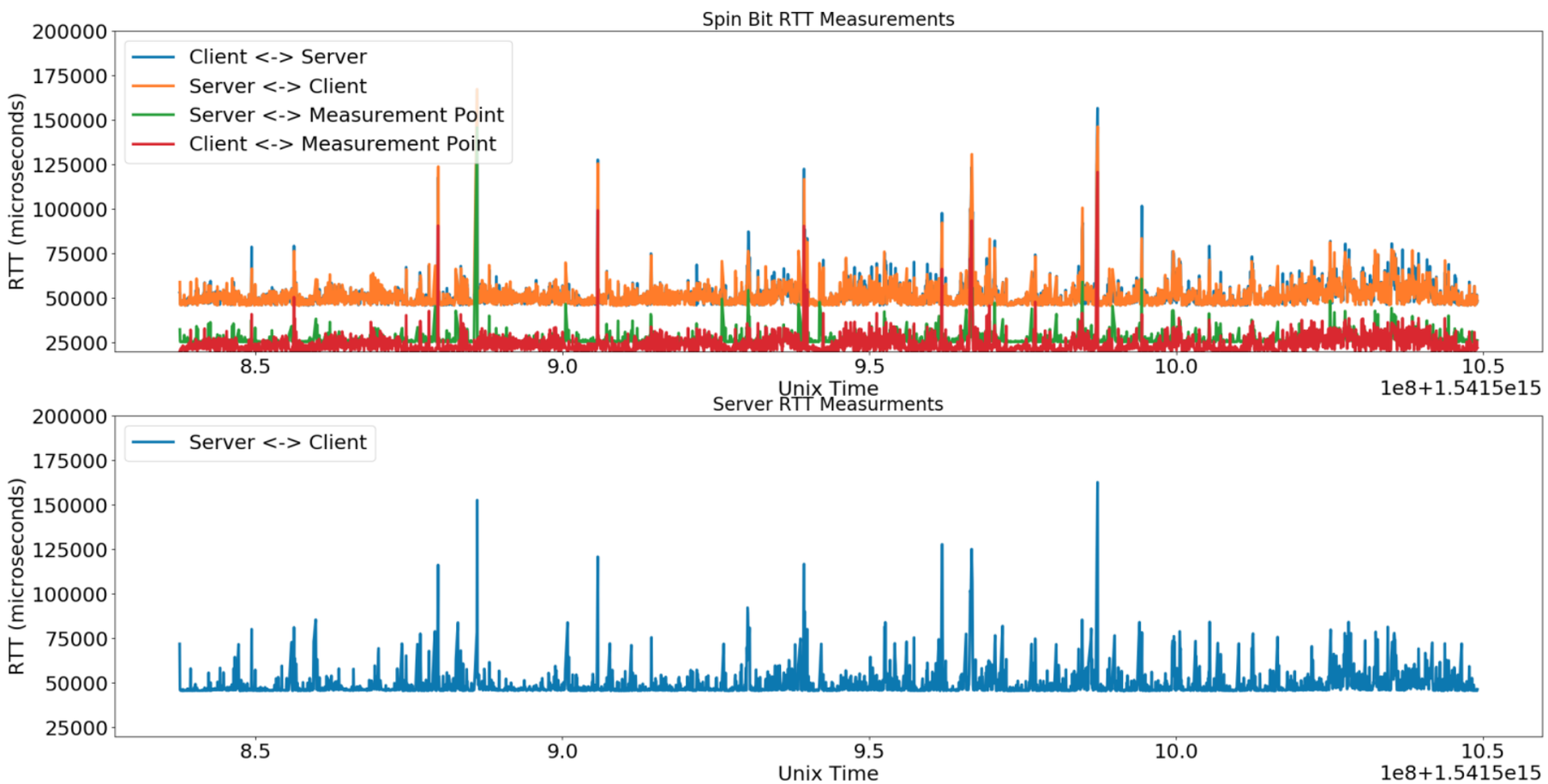
HOW SPIN BIT WORKS



MEASUREMENTS

- Can provide end-to-end RTT data similar to following TCP ACKs
- Results affected by loss, reorder, etc — but still relatively close to actual situation as seen by the endpoints

5% Packet loss
Loss correlation 30%
Bi-dir measurement
Simple heuristics

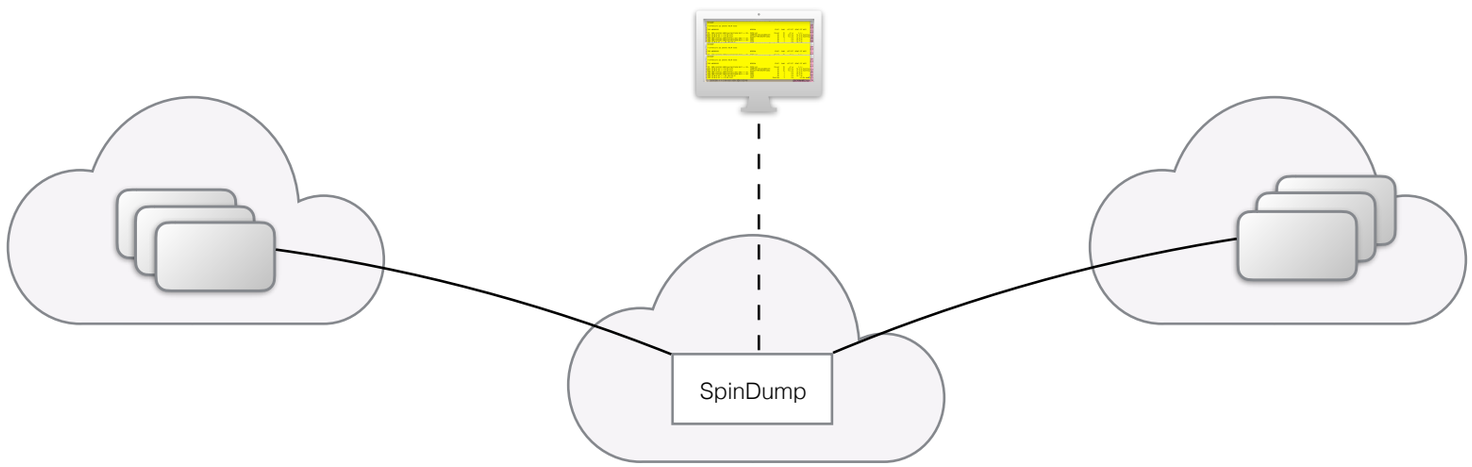


IMPLEMENTATIONS

Several QUIC client/server implementations that use the spin bit

One in-network tool, **Spindump**, analyses the information:

- Open source, https://github.com/EricssonResearch/spindump
- Supports measurements for TCP, QUIC (with or without spin bit), ICMP, DNS, COAP, …
- Measurements are either sent to a collection point or displayed visually
- Use cases range from debugging to operations, alarms, etc.



IMPLEMENTATIONS

Several QUIC client/server implementations that use the spin bit

One in-network tool, **Spindump**, analyses the information:

- Open source, https://github.com/EricssonResearch/spindump

- Supports measurements for TCP, QUIC (with or without spin bit), ICMP, DNS, COAP, …