Invariants - Connection ID

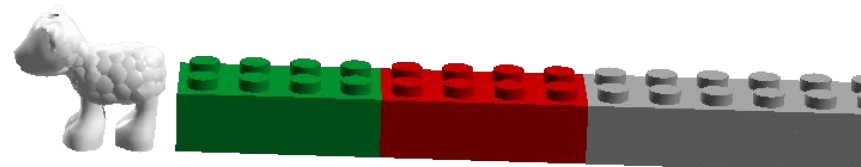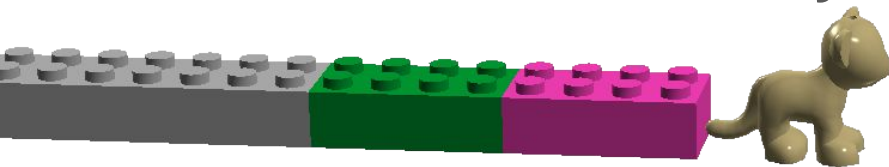IETF 101 London

Connection ID Protocol

Long headers have two connection IDs:

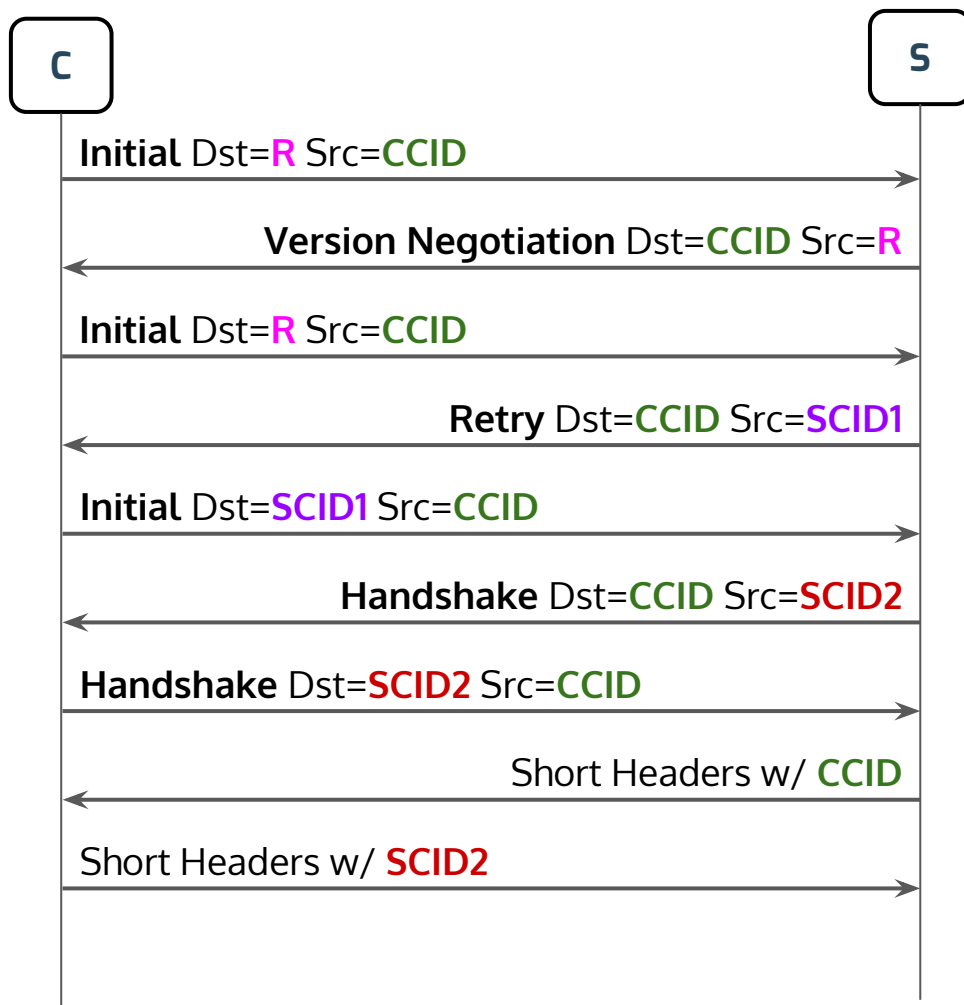One for the recipient, one for the sender

One for routing, one for the routing value on the reverse path

Connection IDs are variable length

Short headers include only the recipient's connection ID

Connection ID Protocol

C → S: **Initial** Dst=**R** Src=**CCID**

S → C: **Version Negotiation** Dst=**CCID** Src=**R**

C → S: **Initial** Dst=**R** Src=**CCID**

S → C: **Retry** Dst=**CCID** Src=**SCID1**

C → S: **Initial** Dst=**SCID1** Src=**CCID**

S → C: **Handshake** Dst=**CCID** Src=**SCID2**

C → S: **Handshake** Dst=**SCID2** Src=**CCID**

S → C: Short Headers w/ **CCID**

C → S: Short Headers w/ **SCID2**

R is random (8 octets+)
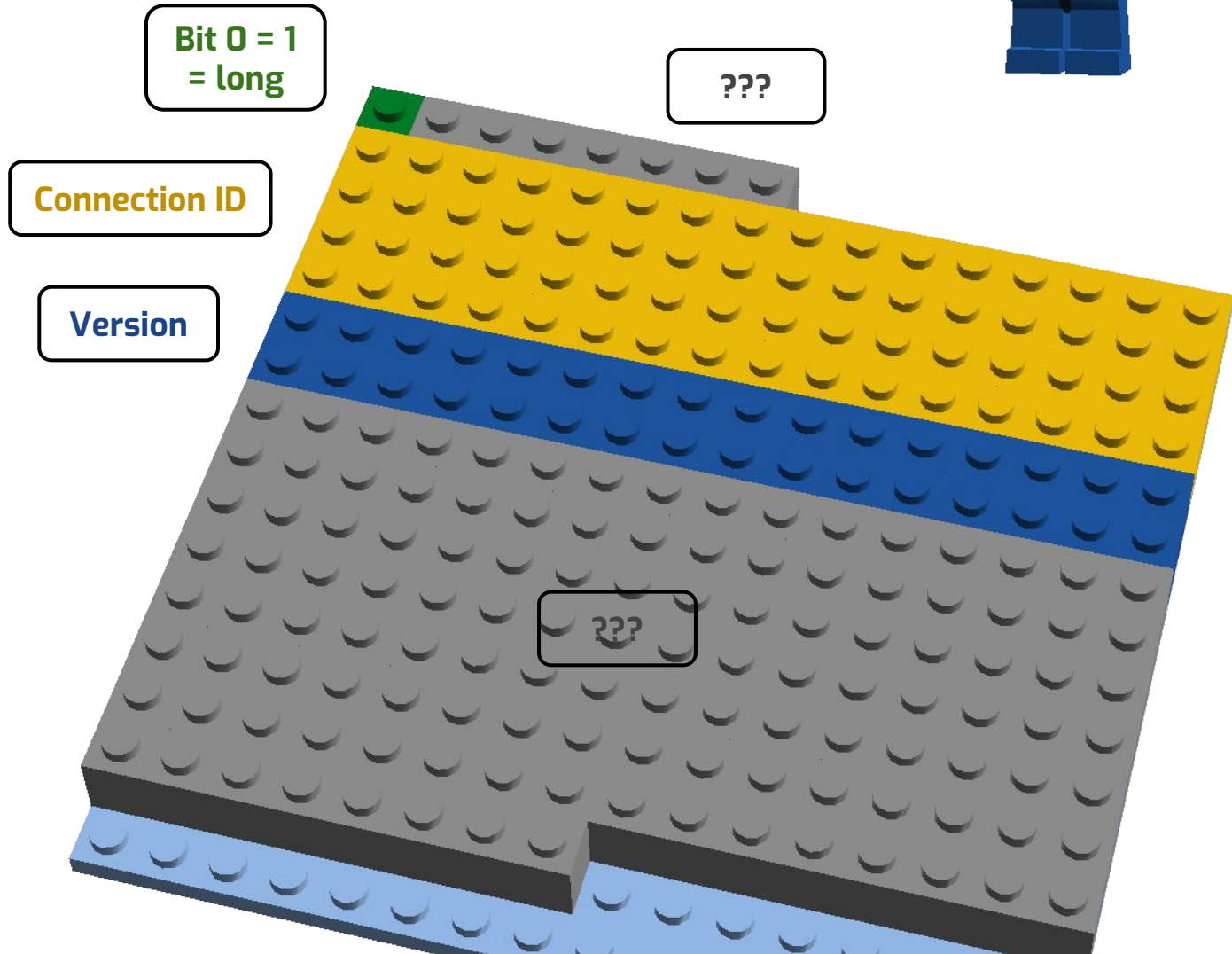Echoing **R** is used to demonstrate return routeability for Version Negotiation packets.

Client picks **CCID**. Server adds **CCID** to all packets.

Server picks **SCID**. Client uses **SCID** for all subsequent packets.
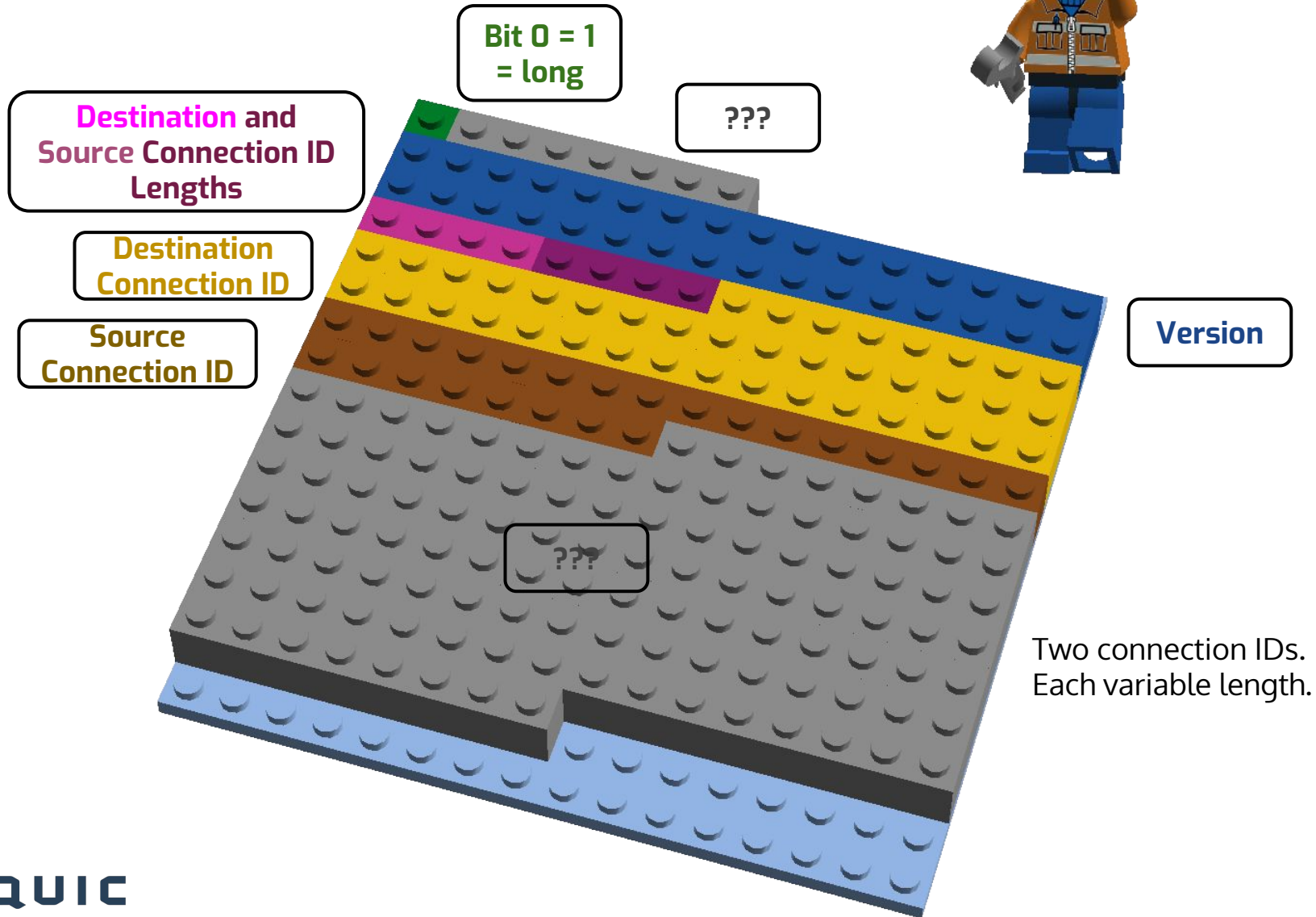
Server can send a different **SCID** value on Retry for re-routing the handshake

.

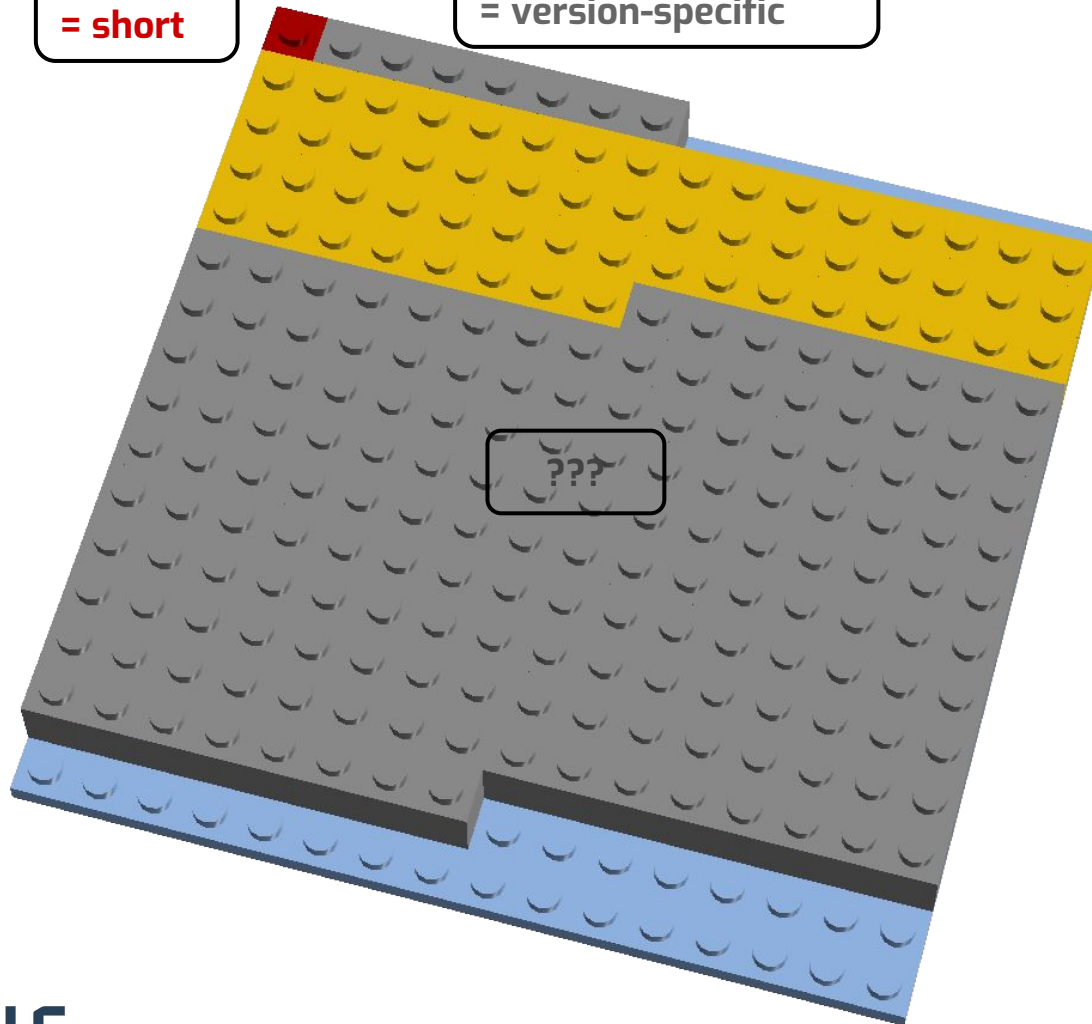**CCID** and **SCID** are variable length and may be 0 octets.

QUIC

Long Header Invariants (old)

Bit 0 = 1
= long

???

Connection ID

Version

???

QUIC

Long Header Invariants (proposed)

Bit 0 = 1
= long

???

Destination and
Source Connection ID
Lengths

Destination
Connection ID

Source
Connection ID

Version

???

Two connection IDs.
Each variable length.

QUIC

QUIC Short Header Changes

Bit 0 = 0
= short

Bit 1 = ?
= version-specific

Destination
Connection ID

???

Destination Connection ID is variable length, but **no explicit length** is included.

QUIC

6

Stateless Reset

Stateless reset breaks for clients that rely on connection ID

A server that loses state can't set the correct Destination Connection ID on the stateless reset packet

Advise setting a random connection ID, with two problems:

Stateless reset might be recognizable as such

Stateless reset might not arrive at the client

Proposal: stateless reset is only an optimization, so this is OK

Details and so forth

PR [#1151](#) creates two connection IDs

PR [#1167](#) moves the Version field

Version Negotiation changes too, but not fundamentally

    Still long w/ version=0

Handshake keys sometimes use zero-length inputs

    No server address validation on that round trip

    But that only happens after Retry, which can be validated