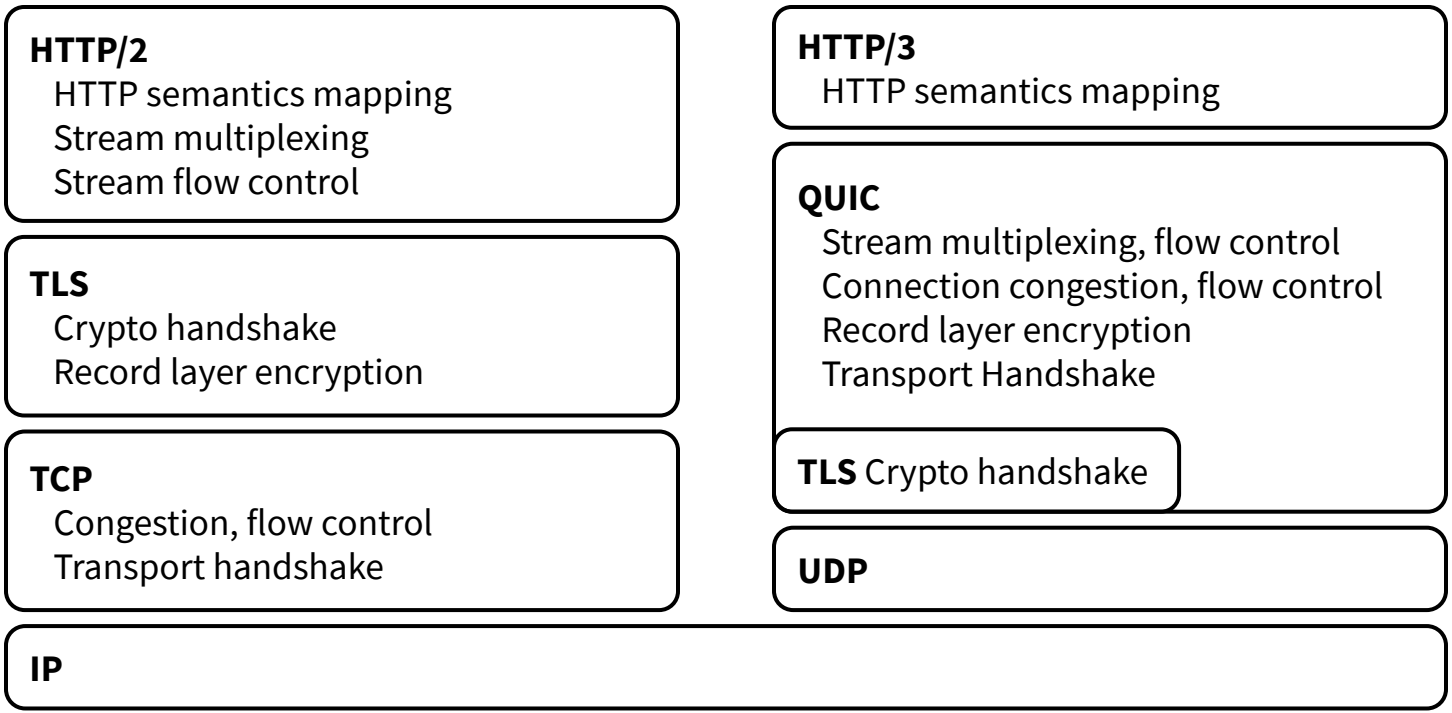
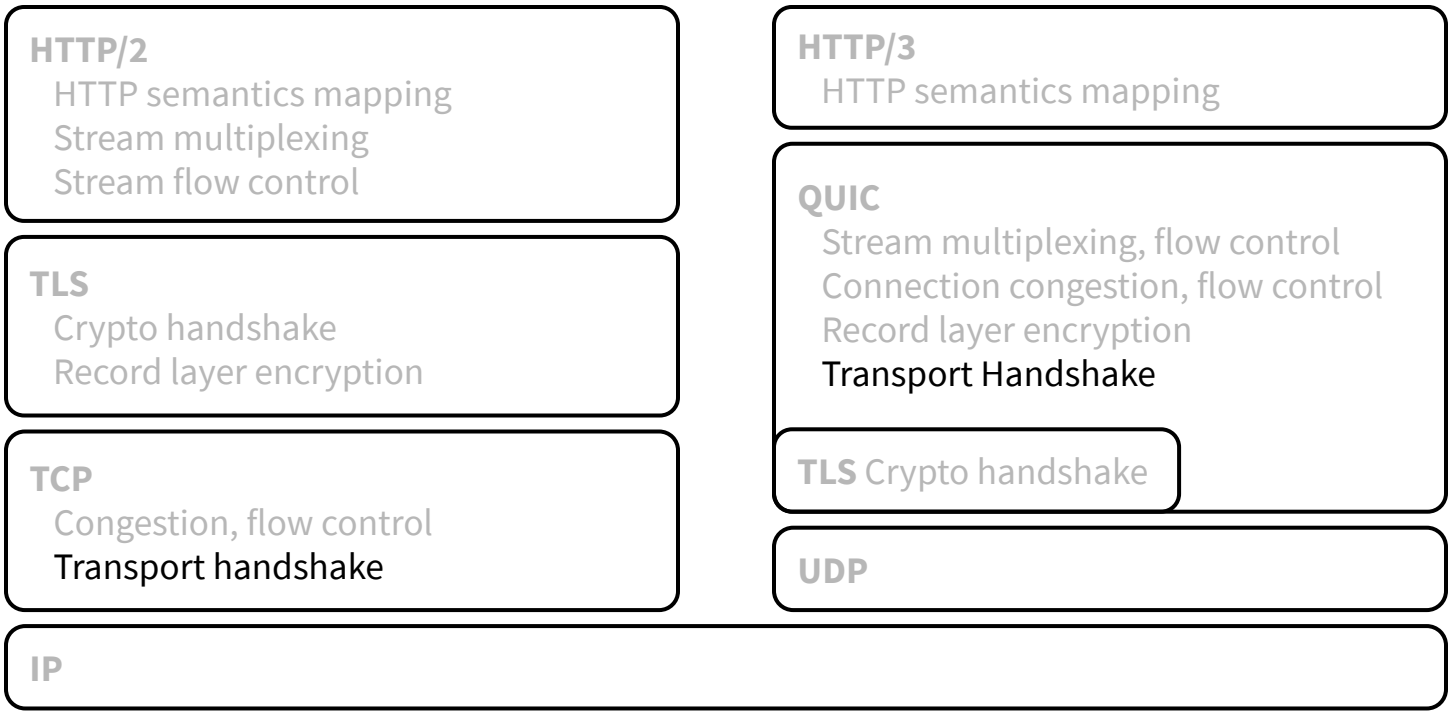
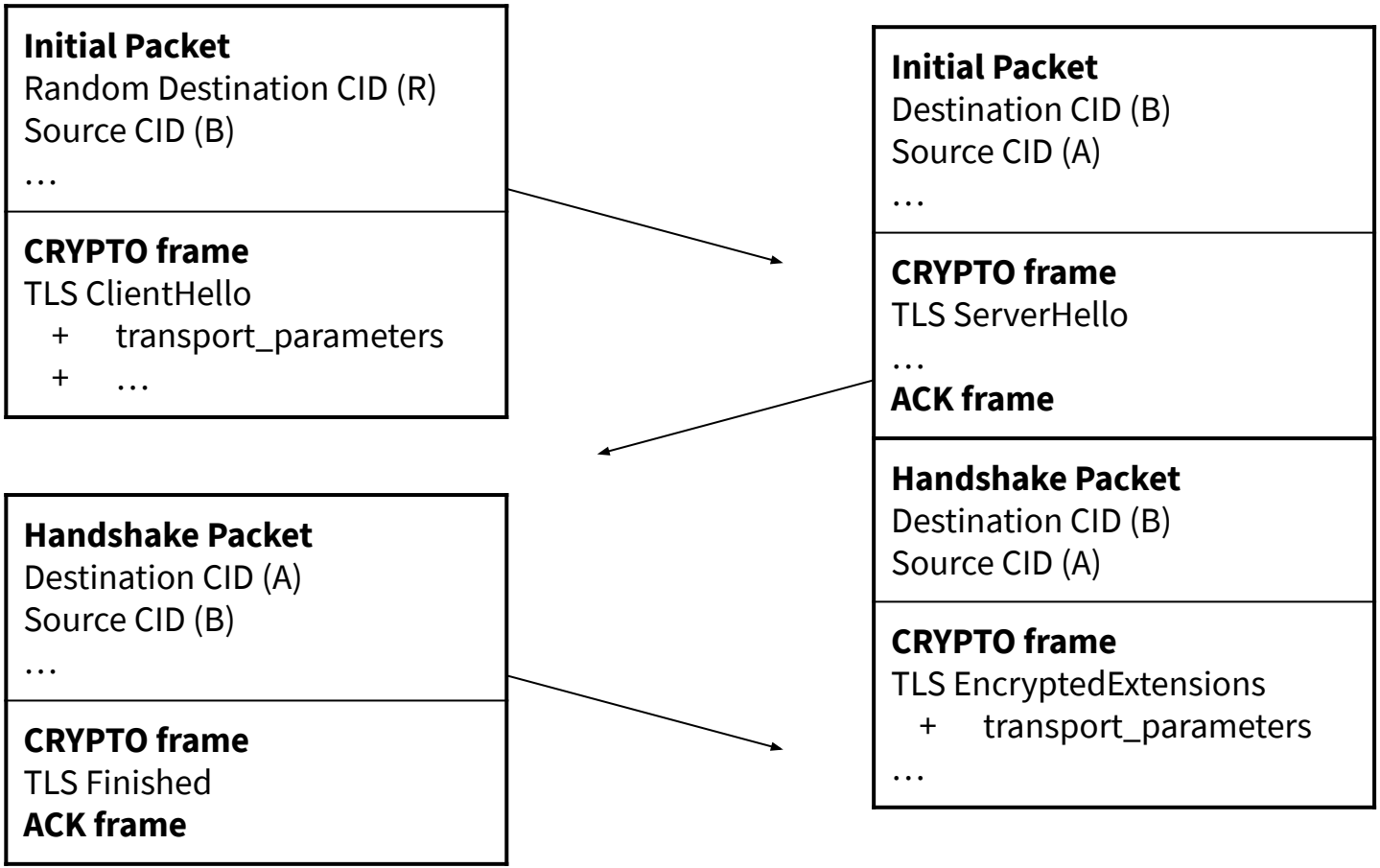
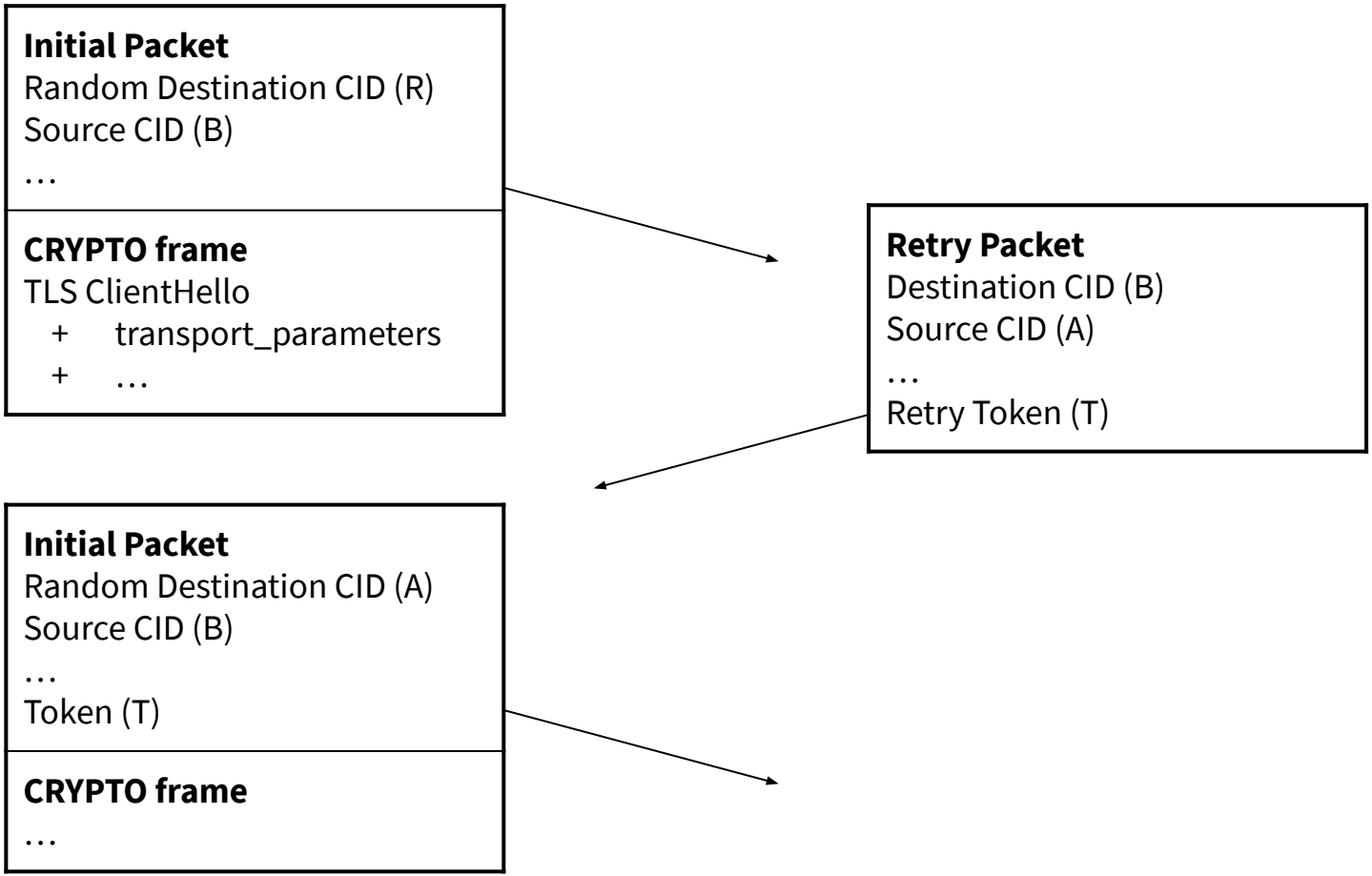
Securing the Next Version of HTTP

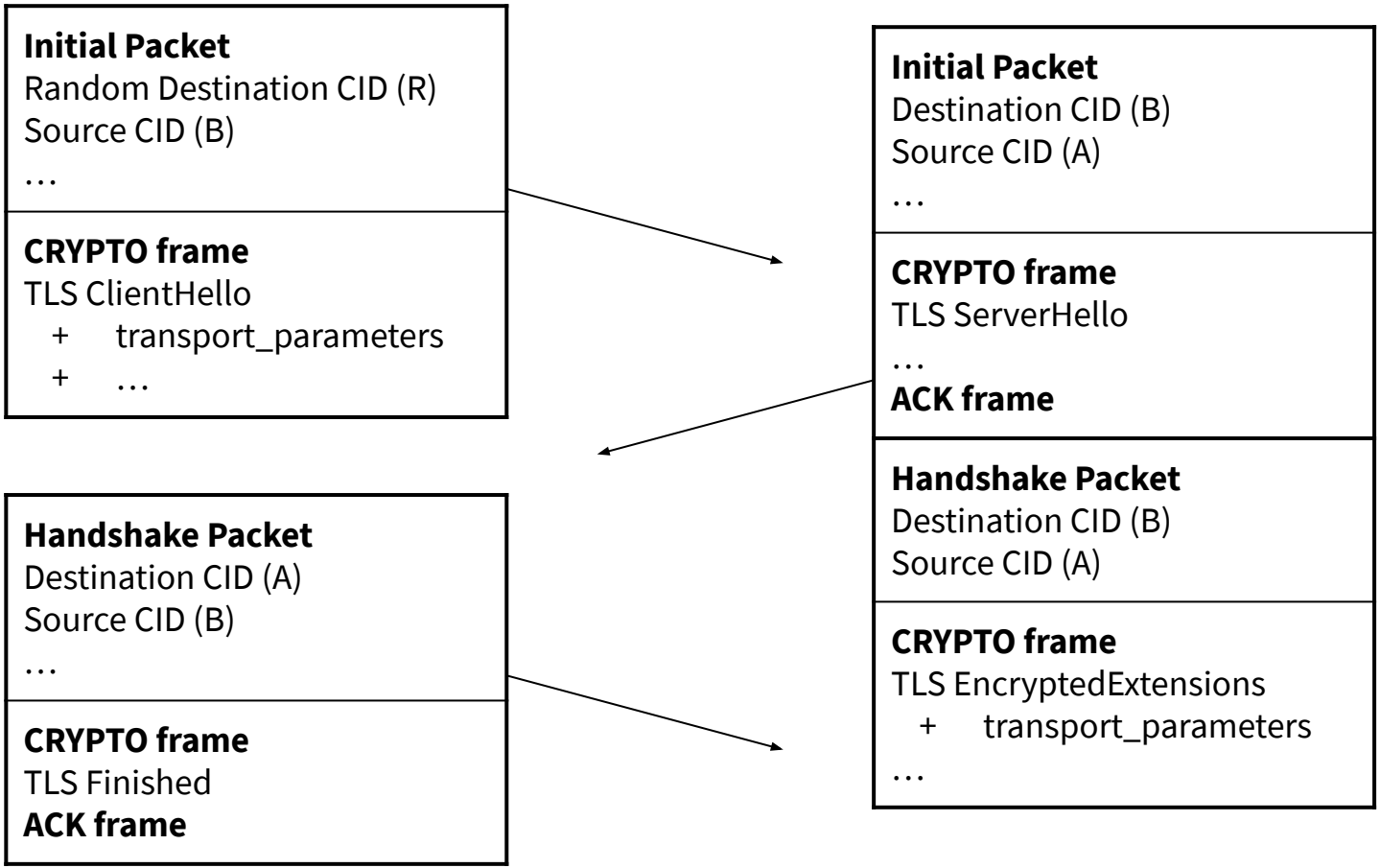
How QUIC and HTTP/3 Compare to HTTP/2


HTTP/2
HTTP semantics mapping
Stream multiplexing
Stream flow control
TLS
Crypto handshake
Record layer encryption
TCP
Congestion, flow control
Transport handshake
HTTP/3
HTTP semantics mapping
QUIC
Stream multiplexing, flow control
Connection congestion, flow control
Record layer encryption
Transport Handshake
TLS Crypto handshake
UDP
IP


HTTP/2
HTTP semantics mapping
Stream multiplexing
Stream flow control
TLS
Crypto handshake
Record layer encryption
TCP
Congestion, flow control
Transport handshake
HTTP/3
HTTP semantics mapping
QUIC
Stream multiplexing, flow control
Connection congestion, flow control
Record layer encryption
Transport Handshake
TLS Crypto handshake
UDP
IP


Initial Packet
Random Destination CID (R)
Source CID (B)
…
CRYPTO frame
TLS ClientHello
+ transport_parameters
+ …
Initial Packet
Destination CID (B)
Source CID (A)
…
CRYPTO frame
TLS ServerHello
…
ACK frame
Handshake Packet
Destination CID (B)
Source CID (A)
CRYPTO frame
TLS EncryptedExtensions
+ transport_parameters
…
Handshake Packet
Destination CID (A)
Source CID (B)
…
CRYPTO frame
TLS Finished
ACK frame


Initial Packet
Random Destination CID (R)
Source CID (B)
…
CRYPTO frame
TLS ClientHello
+ transport_parameters
+ …
Retry Packet
Destination CID (B)
Source CID (A)
…
Retry Token (T)
Initial Packet
Random Destination CID (A)
Source CID (B)
…
Token (T)
CRYPTO frame
…


Initial Packet
Random Destination CID (R)
Source CID (B)
…
CRYPTO frame
TLS ClientHello
+ transport_parameters
+ …
Initial Packet
Destination CID (B)
Source CID (A)
…
CRYPTO frame
TLS ServerHello
…
ACK frame
Handshake Packet
Destination CID (B)
Source CID (A)
CRYPTO frame
TLS EncryptedExtensions
+ transport_parameters
…
Handshake Packet
Destination CID (A)
Source CID (B)
…
CRYPTO frame
TLS Finished
ACK frame

Packet format invariants

```
Long Header Packet {
  Header Form (1) = 1,
  Version-Specific Bits (7),
  Version (32),
  Destination Connection ID Length (8),
  Destination Connection ID (0..2040),
  Source Connection ID Length (8),
  Source Connection ID (0..2040),
  Version-Specific Data (..),
}
```

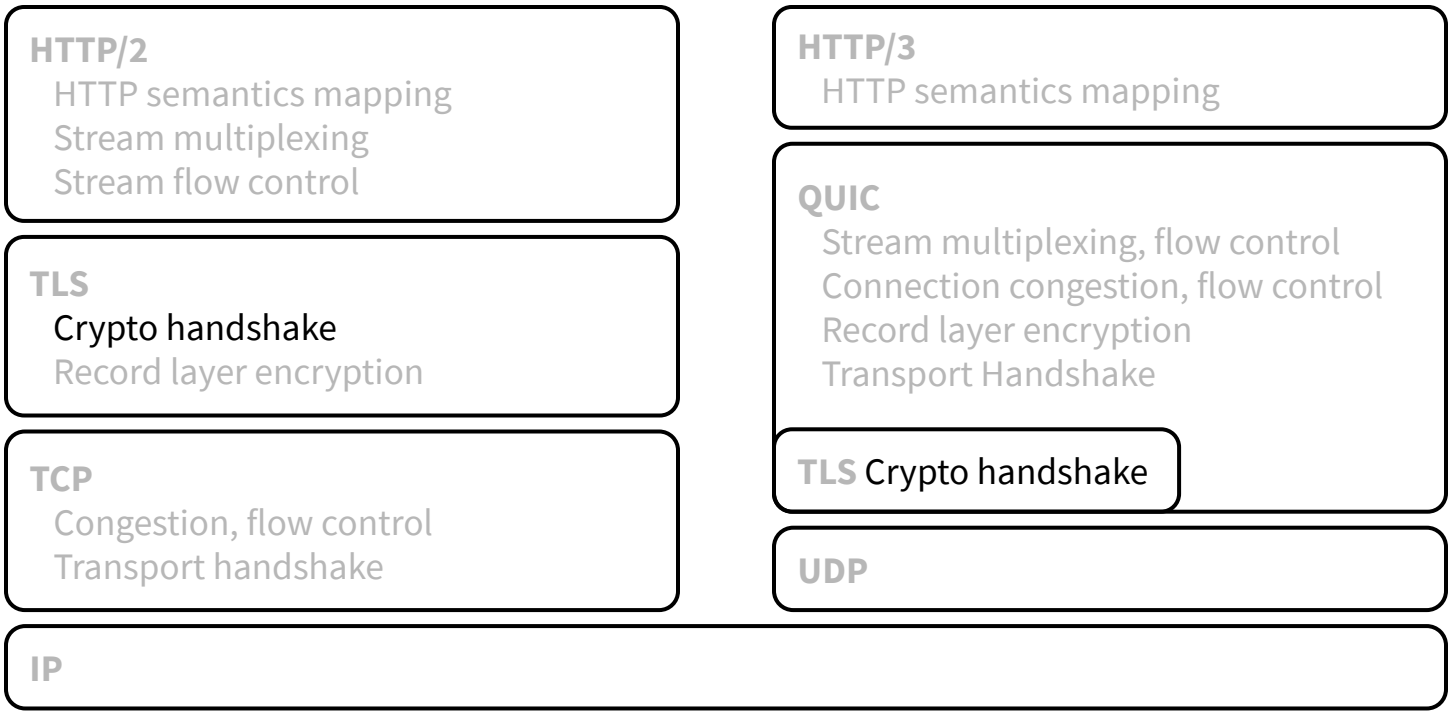
```
Short Header Packet {
  Header Form (1) = 0,
  Version-Specific Bits (7),
  Destination Connection ID (..),
  Version-Specific Data (..),
}
```

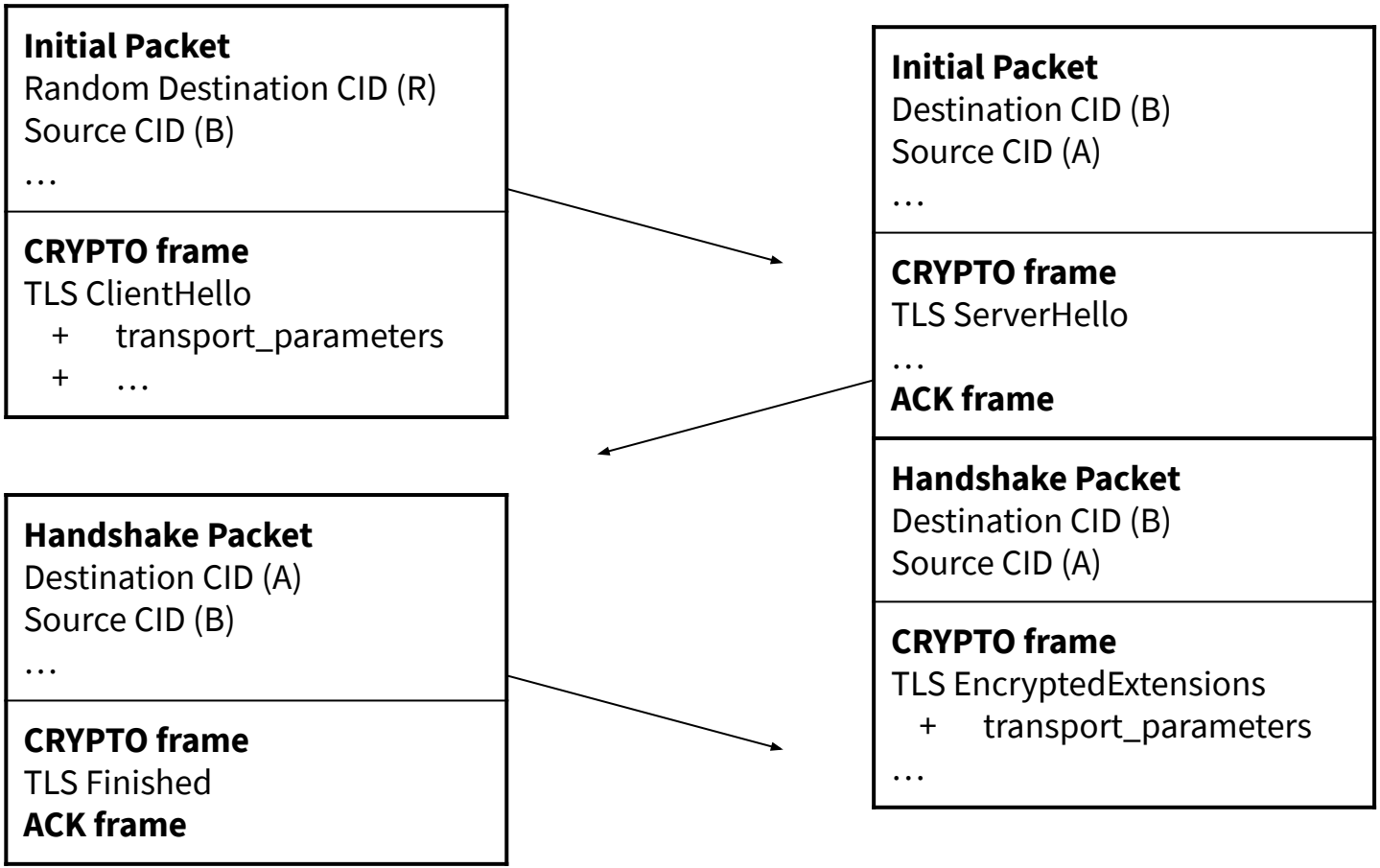
QUIC Connection IDs

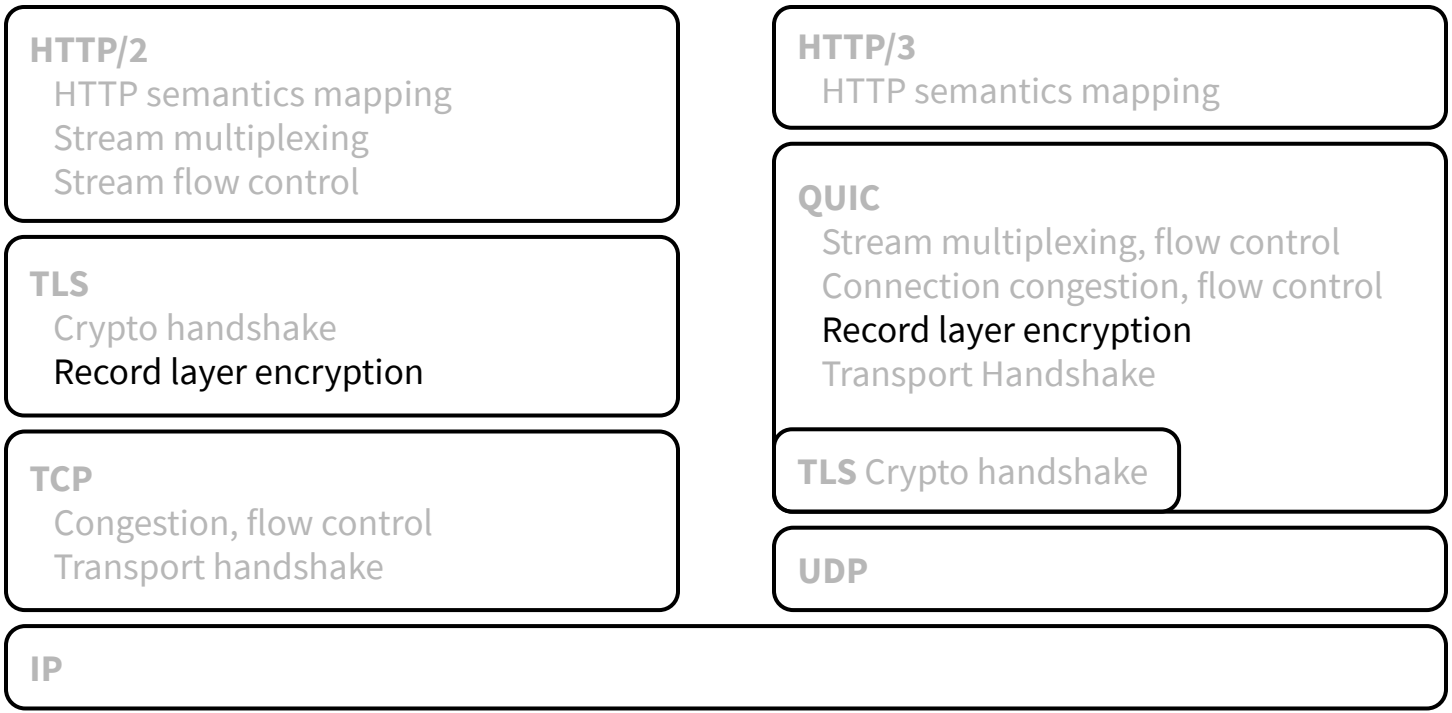
Used in place of 5-tuple to identify a QUIC connection

Variable length, issued by endpoint

Should appear to be random

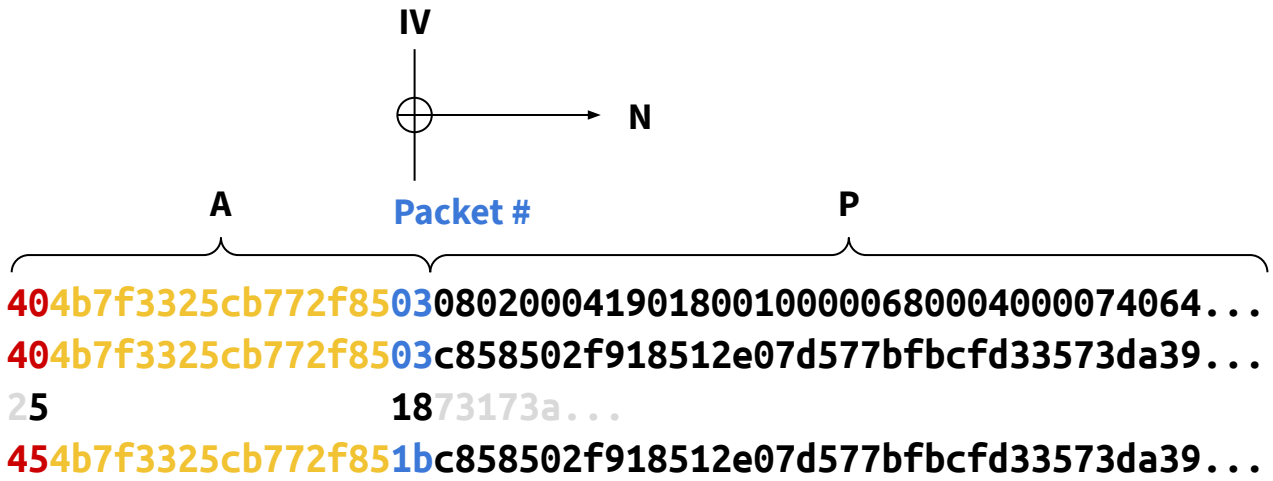

HTTP/2
HTTP semantics mapping
Stream multiplexing
Stream flow control
TLS
Crypto handshake
Record layer encryption
TCP
Congestion, flow control
Transport handshake
HTTP/3
HTTP semantics mapping
QUIC
Stream multiplexing, flow control
Connection congestion, flow control
Record layer encryption
Transport Handshake
TLS Crypto handshake
UDP
IP

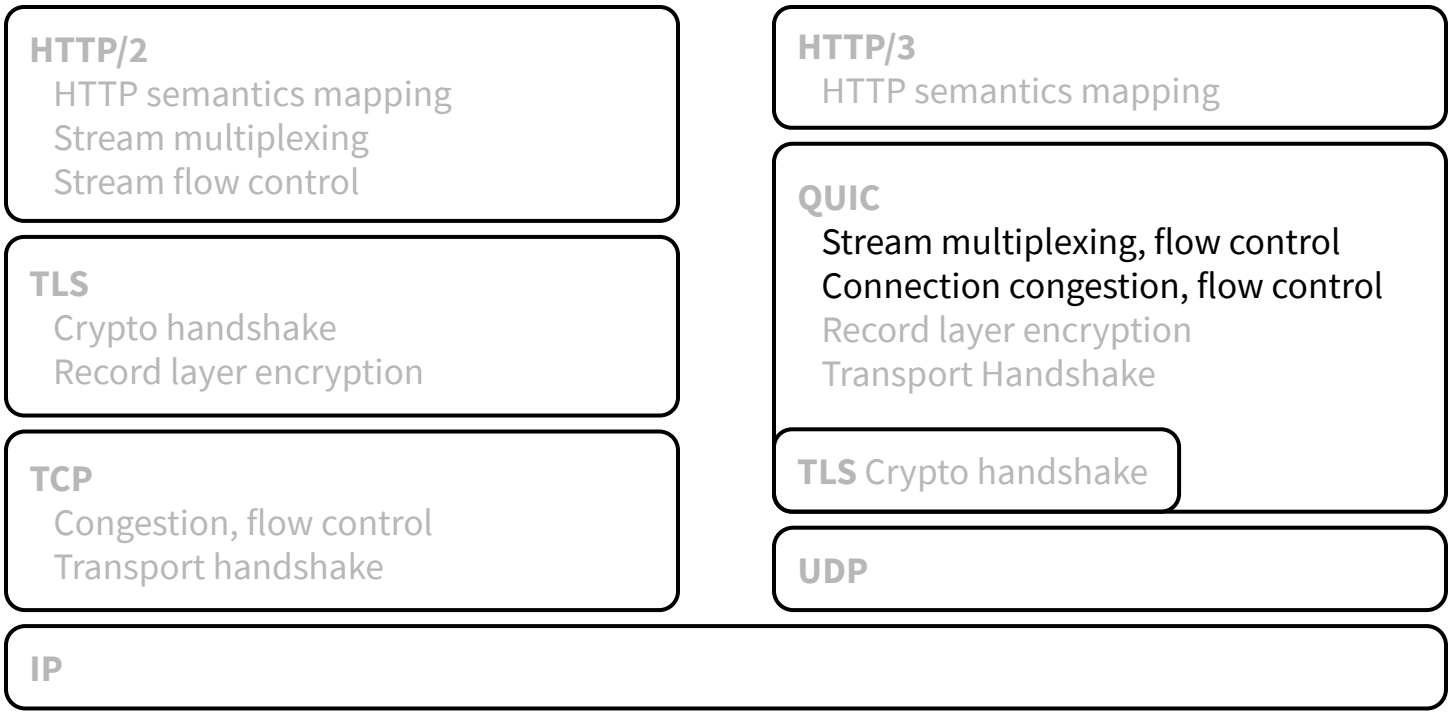

Initial Packet
Random Destination CID (R)
Source CID (B)
…
CRYPTO frame
TLS ClientHello
+ transport_parameters
+ …
Initial Packet
Destination CID (B)
Source CID (A)
…
CRYPTO frame
TLS ServerHello
…
ACK frame
Handshake Packet
Destination CID (B)
Source CID (A)
CRYPTO frame
TLS EncryptedExtensions
+ transport_parameters
…
Handshake Packet
Destination CID (A)
Source CID (B)
…
CRYPTO frame
TLS Finished
ACK frame


HTTP/2
HTTP semantics mapping
Stream multiplexing
Stream flow control
TLS
Crypto handshake
Record layer encryption
TCP
Congestion, flow control
Transport handshake
HTTP/3
HTTP semantics mapping
QUIC
Stream multiplexing, flow control
Connection congestion, flow control
Record layer encryption
Transport Handshake
TLS Crypto handshake
UDP
IP

QUICv1 Record Protection

AEAD(K, N, P, A) = C




HTTP/2
HTTP semantics mapping
Stream multiplexing
Stream flow control
TLS
Crypto handshake
Record layer encryption
TCP
Congestion, flow control
Transport handshake
HTTP/3
HTTP semantics mapping
QUIC
Stream multiplexing, flow control
Connection congestion, flow control
Record layer encryption
Transport Handshake
TLS Crypto handshake
UDP
IP

Streams, flow control, and other frames

STREAM frames carry application data

Flow control updates sent in MAX_DATA (per connection), MAX_STREAM_DATA (per stream), and MAX_STREAMS frames

Packets acknowledged via ACK frames

PATH_CHALLENGE and PATH_RESPONSE used to validate new paths

Implementation considerations

Flow control

Path validation

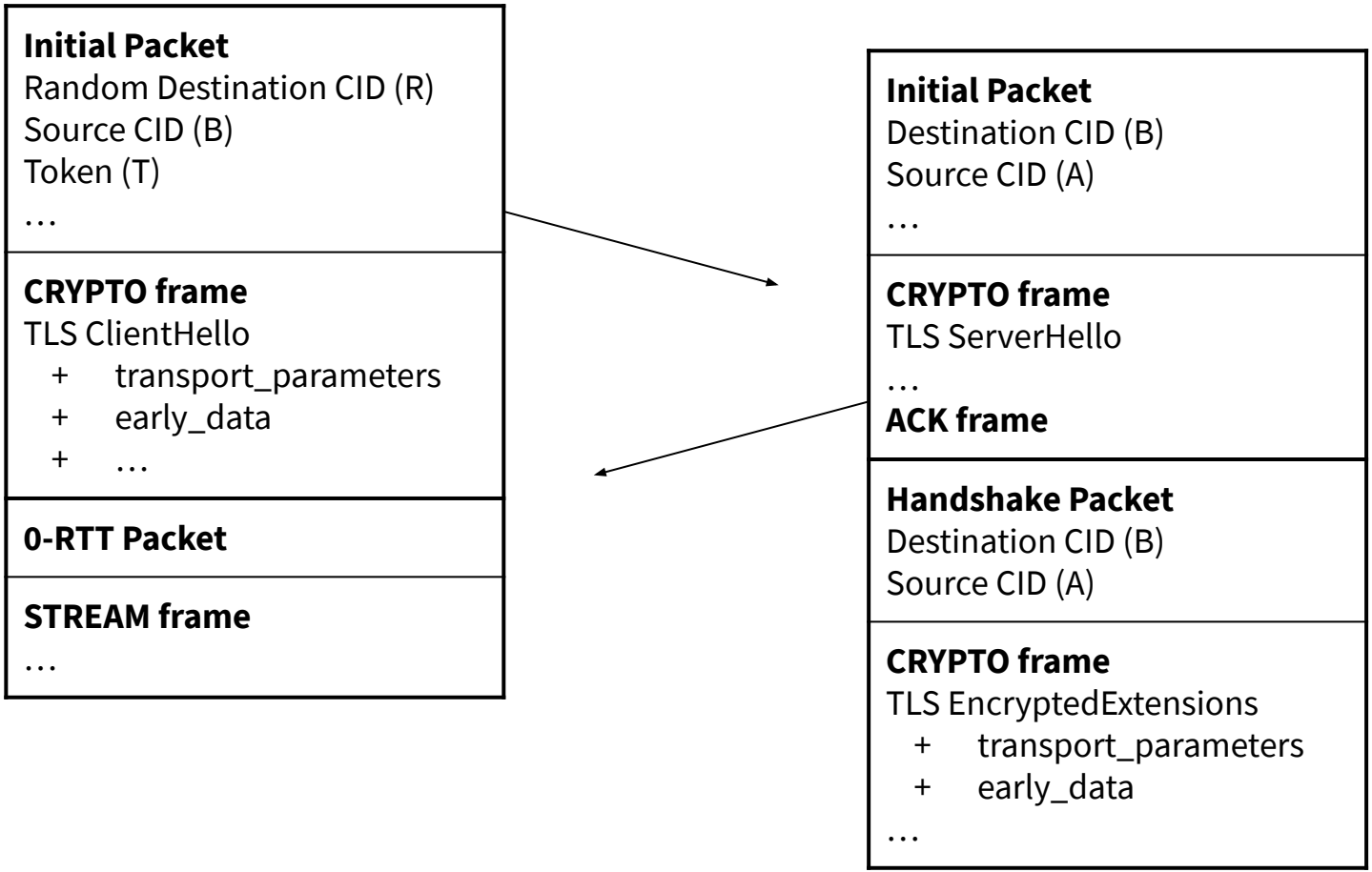
CVE-2019-9517 “Internal Data Buffering”

0-RTT Connection Resumption

Combines TLS 1.3 0-RTT resumption handshake with address validation token from QUIC transport

Server sends address validation token in NEW_TOKEN frame on previous connection

Server sends 0-RTT capable NewSessionTicket in TLS handshake on previous connection


Initial Packet
Random Destination CID (R)
Source CID (B)
Token (T)
…
CRYPTO frame
TLS ClientHello
+ transport_parameters
+ early_data
+ …
0-RTT Packet
STREAM frame
…
Initial Packet
Destination CID (B)
Source CID (A)
…
CRYPTO frame
TLS ServerHello
…
ACK frame
Handshake Packet
Destination CID (B)
Source CID (A)
CRYPTO frame
TLS EncryptedExtensions
+ transport_parameters
+ early_data
…

Summary

The HTTP/3 protocol stack has equivalent security as HTTP/2

HTTP/3’s use of QUIC improves performance

QUIC improves privacy