



# Hot Issues

## How we did this

We went through ALL the issues (yes, we did that)

We tagged, assigned, closed. What this means:

**quicv2**: this is not in-scope for v1; v2 will happen

**parked**: not blocking and will re-examine before v1

**needs-discussion**: this needs to be resolved soon

**closed**: not an issue, or we believe that it is resolved

As always, if you disagree, say so!



# Discuss on List

IETF101: QUexit

# Fixing HTTP Priority for QUIC: Request IDs

Today: HTTP mapping uses Stream IDs.

## Motivation:

HTTP/2 allows use of 'phantom' streams in PRIORITY, which QUIC doesn't have

## Proposed Mechanism:

Expand Push ID to Request ID, allowing use of phantom streams and replace references to stream IDs

Issue [#441](#)

# Connection ID Privacy

**Question:** Can we encrypt connection IDs?

**Answer:** Sure, but it will hurt. A lot.

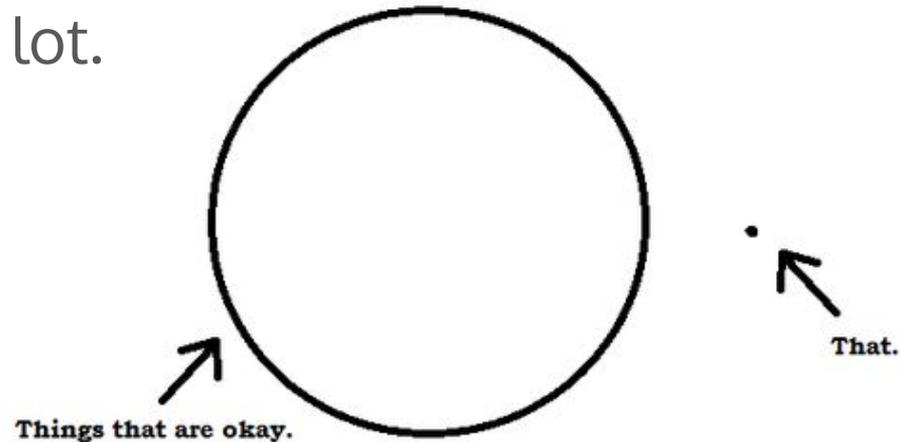
**Proposed Resolution:**

Close with no action

All of the solutions that we know of have horrible costs

If someone comes up with a good solution, we can reopen

Issue [#598](#)



# Prime client with connection ID for 0-RTT

**Today:** Server cannot specify connection ID for 0-RTT

## Motivation:

Makes it easier to limit replay and amplification attacks by routing 0-RTT to a smaller set of machines.

## Possible Mechanism:

- new NewSessionTicket Frame for session tickets
- include server-issued connection ID

Issue [#584](#)

# QPACK

How far do we want to diverge from HPACK?

Instructions

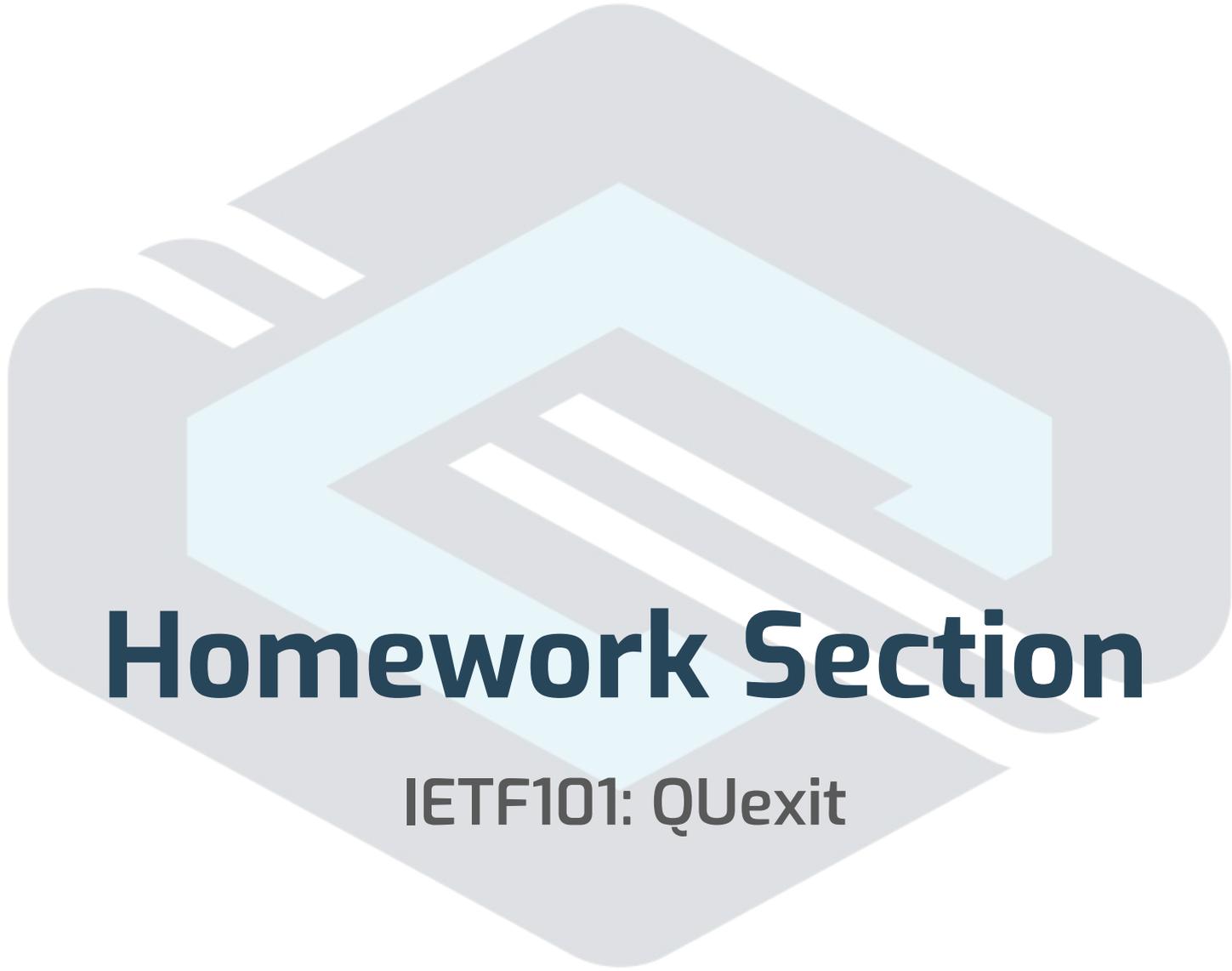
Add some

Compress the instruction space

String encoding

Integer encoding - Huffman

New static table



# Homework Section

IETF101: QUexit

# Handshake Corner Cases

Several issues with ACKs and the handshake.

Several relate to the client's second flight:

Marten Seeman's pathological loss recovery case [#1190](#)

How to acknowledge it [#829](#)

Authentication of that flight [#1018](#)

Packet number shadowing attacks (also [#1018](#))

**Homework:** Give us some ideas



# Discuss Now

IETF101: QUexit

# PADDING and PING

**Today:** Both PADDING and PING instigate ACK frames and count towards bytes in flight

## Problems:

- PADDING and PING are redundant
- Cannot add PADDING to all ACK-only packets

**Principle:** Instigates Ack **iff** Packet is added to bytes in flight

- Need an ACK to remove a packet from bytes in flight

Issues [#837](#), [#838](#)

# PADDING and PING

**Option 1:** Remove PING, because it's redundant

- Still could not add PADDING to all ACK-only packets

**Option 2:** PADDING does not instigate an ACK

- PADDING-only and ACK+PADDING packets do not count towards bytes in flight
- ACK congestion control is hard, PADDING could make it important

Issues [#837](#), [#838](#)