MASQUE CONNECT-UDP

draft-ietf-masque-connect-udp

IETF Interim – Virtual – 2021-01

David Schinazi – dschinazi@google.com

The 5-second summary

CONNECT-UDP is like CONNECT, but for UDP!

When used in HTTP/3, it uses QUIC DATAGRAM frames to avoid retransmissions

KIDS
ROBOT PLANET

Mea Culpa

Some issues were closed without individual details explaining what text fixes the issue, I was rushing to get this done in time for this interim

This should be better going forward

Issue #16: Cardinality of Flow IDs

This topic is now part of H3-DGRAM since Datagram-Flow-Id was moved there

Format of Datagram-Flow-ID allows one-to-one, one-to-many, and many-to-one mappings from request to flow ID

One-to-one: one CONNECT-UDP request maps to one flow ID

  This is how CONNECT-UDP works when no extensions are in use

One-to-many: one CONNECT-UDP request can use multiple flow IDs

  Example: encode 2 ECN bits in flow ID instead of in every payload

Many-to-one: many CONNECT-UDP requests share a flow ID

  Example: QUIC proxy extension maps connection ID lifetimes to requests
    but share a flow ID because they have the same semantics

Issues #8 and #23 – We need a request target URI

The scheme does not convey any useful information here,
and it is not needed for the protocol to work

But, according to HTTP Semantics, all new methods MUST have a target URI

There was an exception for CONNECT but it doesn't help with a new method

Proposal: let's just use "https"

Issues #15, #24, #28 – Stream Format

Like CONNECT, CONNECT-UDP has no request/response bodies, instead takes over the entire stream

Uses Connect-UDP Stream Chunks

- Sequence of TLVs
- Type of 0 conveys UDP payloads
- Other types for extensibility (creates IANA registry)
- Skip over unknown Chunks

In HTTP/3, CONNECT-UDP Stream Chunks are sent in HTTP/3 DATA frames

Issues #1 and #3 – Intermediaries

Datagram-Flow-Ids are negotiated per-hop

Datagram-Flow-Id can only be sent on connections that exchanged a SETTING

Intermediaries that send the SETTING will perform negotiation on each connection

New "Performance Considerations" Section

Addresses several issues:

#10 UDP Pacing and Bursting Limits

#12 Nested Congestion Control

#13 Nested Loss Recovery

Issue #11 – Limit packets before server response

CONNECT inherits this protection from TCP: it won't send anything to the target other than the SYN until it receives a SYN-ACK

UDP doesn't provide the same property

In practice, DoS attacks target open TCP ports so this protection isn't particularly useful

Resolution: added a note about this in Security Considerations

Questions?

MASQUE CONNECT-UDP

draft-ietf-masque-connect-udp

IETF 109 – Virtual – 2020-11

David Schinazi – dschinazi@google.com