MASQUE

Multiplexed Application Substrate over QUIC Encryption

David Schinazi – Google
dschinazi@google.com

draft-schinazi-masque — IETF 104 — Prague — 2019-03

Feature: UDP proxying

Client can request that the server proxy UDP datagrams to a given IP and port

Uses QUIC DATAGRAMs with a DATAGRAM IDENTIFIER per (IP, port)

(When falling back to HTTP/2, uses a dedicated HTTP/2 stream)

Allows proxying QUIC, WebRTC, DTLS, etc. over MASQUE

Feature: IP proxying / VPN

Client sends full IP datagrams that the server can forward

Server can optionally NAT datagrams to obfuscate clients to end servers

Traffic Analysis

Currently considered out of scope

QUIC allows grouping multiple STREAM, DATAGRAM and PADDING frames in one encrypted UDP packet

Allows endpoints to obfuscate traffic patterns

Are there good obfuscation techniques that could be relevant here?

Path MTU Discovery

When proxying IP or UDP, MASQUE adds overhead and reduces MTU

Client needs to ensure it does send packets exceeding that MTU and communicate it to the end server

Transport Considerations

Running QUIC over MASQUE implies stacking two congestion controllers

QUIC design principle was to encrypt congestion control information

Are there good solutions here?

Next Steps

Is this work interesting?

Does anyone want to collaborate on code?

Does anyone want to collaborate on standardization?

Should we find an existing or new home for this work?