

**Running DNS in Existing QUIC Connections**  
**draft-hoffman-dns-in-existing-quic-00**

Abstract

Intermediaries such as governments and ISPs spoof DNS responses, and block DNS requests to particular recursive resolvers, for a variety of reasons. They spoof by capturing traffic on port 53, or by redirecting port 853 traffic in the hopes that the client is using opportunistic encryption. They block if they know the address of a resolver that they don't like, such as public resolvers that give honest answers.

This document describes how to run DNS service over existing QUIC connections, such as those being used for HTTP for basic web service. This design prevents intermediaries from spoofing DNS responses, and makes it impossible for intermediaries to block the use of those recursive resolvers without blocking the desired HTTP connections. It also prevents intermediaries or passive observers from seeing the DNS traffic. This design is meant for communication between a DNS stub resolver and a DNS recursive resolver.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 12, 2017.

## Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	DNS in Existing QUIC Connections . . . . .	<a href="#">3</a>
<a href="#">2.1.</a>	QUIC DNS Frame Definition . . . . .	<a href="#">3</a>
<a href="#">2.2.</a>	Service Discovery . . . . .	<a href="#">4</a>
<a href="#">3.</a>	IANA Considerations . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">5</a>
<a href="#">5.</a>	References . . . . .	<a href="#">5</a>
<a href="#">5.1.</a>	Normative References . . . . .	<a href="#">5</a>
<a href="#">5.2.</a>	Informative References . . . . .	<a href="#">5</a>
	Author's Address . . . . .	<a href="#">6</a>

## [1.](#) Introduction

It is expected that, in the not-distant future, Internet users will be running QUIC [[I-D.ietf-quic-transport](#)] for basic web service to many web sites. Large web sites who care about good DNS resolution service (that is, DNS resolution that is not subject to getting wrong answers from intermediaries) might want to offer DNS resolution on the same servers as those running HTTP over QUIC. Running DNS over existing QUIC connection prevents intermediaries from spoofing DNS responses, and makes it impossible for intermediaries to block the use of those recursive resolvers without blocking the desired HTTP connections.

This document covers only the use case of getting DNS service once a QUIC connection is already set up. That means that the user already has some DNS service before getting to the DNS resolver that is running in the existing QUIC connection. That original DNS service might be standard DNS running on port 53 ([[RFC1035](#)]), or DNS-in-TLS running on port 853 ([[RFC7858](#)]), or even DNS in its own QUIC connection that could be defined in the future. Regardless, this



document is describing a second DNS service for the user, one that was bootstrapped by running DNS in a way that might have been spoofed by an intermediary.

A beneficial effect of using DNS over existing QUIC connections after using DNS over port 53 is that the DNS messages are then encrypted.

A parallel document, [[draft-hoffman-dns-in-existing-http2](#)], covers approximately the same use cases as this one, but describes how to carry DNS in HTTP/2 over TLS. A different parallel document, [[draft-huitema-quic-dnsquic](#)], covers a very different use case, namely starting new individual QUIC connections in order to pass DNS traffic.

## 2. DNS in Existing QUIC Connections

\*\*\*\* This section, which is the meat of the protocol, is completely tentative. The choice of using a new frame is an early guess for a protocol that meets the design objectives given above; the QUIC WG might have (much) better alternatives. For example, reserved streams might be a better idea than a new type of frame. As [[I-D.ietf-quic-transport](#)] matures, this section will become more definitive. \*\*\*\*

This document defines a new type of QUIC frame, "DNS".

DNS in QUIC is run as a stream of DNS frames. The DNS stub resolver opens a QUIC stream if it is not already open. The stub resolver then sends DNS wire-format requests ([[RFC1035](#)]), and the recursive resolver sends wire-format requests in the same stream. The wire format used is that for DNS over UDP (not with the extra two-octet header defined in [[RFC1035](#)] for TCP). Either side can close the QUIC stream for DNS whenever they wish.

### 2.1. QUIC DNS Frame Definition

DNS frames (type=0xTBD) convey variable-length sequences of octets associated with a DNS message. One or more DNS frames are used, for instance, to carry a DNS request or response payload.

DNS frames MAY also contain padding. Padding can be added to DNS frames to obscure the size of messages. Padding is a security feature; see [Section 4](#).

The format of the DNS frame is:





Figure 1: DNS frame format

The DNS frame contains the following fields:

**Pad Length:** An 8-bit field containing the length of the frame padding in units of octets. This field is conditional (as signified by a "?" in the diagram) and is only present if the PADDED flag is set for the frame.

**DNS message:** The wire-format of the message. The wire format used is that for DNS over UDP (not with the extra two-octet header defined in [\[RFC1035\]](#) for TCP).

**Padding:** Padding octets that contain no application semantic value. This is handled identically to padding in the STREAM frame in [\[I-D.ietf-quic-transport\]](#).

The DNS frame uses the RST\_STREAM and PADDED frame flags, identically to the STREAM frame in [\[I-D.ietf-quic-transport\]](#).

DNS frames MUST be associated with a stream. If a DNS frame is received whose stream identifier field is 0x0, the recipient MUST respond with a connection error of type `PROTOCOL_ERROR`.

DNS frames are subject to flow control identical to the STREAM frame in [\[I-D.ietf-quic-transport\]](#).

## 2.2. Service Discovery

The DNS stub resolver discovers whether the QUIC server with the existing connection supports DNS resolution by attempting to open a DNS stream in the QUIC connection. Because opening a QUIC stream requires sending protocol data, the stub resolver needs to pick a DNS request to use as a probe for DNS resolution service. The stub resolver might send a request for data it actually wants, or it could send a request that it does not care about, such as the A record for `example.com`.



### **3. IANA Considerations**

As this document gets closer to completion, this section will mostly likely be filled in with an assignment from one or more QUIC-related registries.

### **4. Security Considerations**

Running DNS over existing QUIC connections relies on the security of the QUIC connections themselves.

A beneficial effect of using DNS over existing QUIC connections after using DNS over port 53 is that the DNS messages are then encrypted.

\*\*\* Copy some text about the uses (and abuses) of padding from [Section 10.7 of RFC 7540](#) here. \*\*\*

### **5. References**

#### **5.1. Normative References**

[I-D.ietf-quic-transport]

Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport", [draft-ietf-quic-transport-02](#) (work in progress), March 2017.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<http://www.rfc-editor.org/info/rfc1035>>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", [RFC 7858](#), DOI 10.17487/RFC7858, May 2016, <<http://www.rfc-editor.org/info/rfc7858>>.

#### **5.2. Informative References**

[[draft-hoffman-dns-in-existing-http2](#)]

Hoffman, P., "Running DNS in Existing HTTP/2 Connections", 2017, <<https://tools.ietf.org/id/draft-hoffman-dns-in-existing-http2>>.

[[draft-huitema-quic-dnsquic](#)]

Huitema, C. and et. al, "Specification of DNS over QUIC", 2017, <<https://tools.ietf.org/id/draft-huitema-quic-dnsquic>>.





Author's Address

Paul Hoffman  
ICANN

Email: [paul.hoffman@icann.org](mailto:paul.hoffman@icann.org)