

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2019

T. Pauly
C. Wood
E. Kinnear
Apple Inc.
March 11, 2019

QUIC Address Extension
draft-pauly-quic-address-extension-00

Abstract

This document defines an extension to the QUIC transport protocol that adds support for requesting and receiving the public network address of an endpoint from its peer.

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 <https://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 September 12, 2019.

Copyright Notice

Copyright (c) 2019 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 (<https://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

1.	Introduction	2
1.1.	Requirements Language	2
2.	Motivation	2
2.1.	Connection Lifetime Optimizations	3
2.2.	Privacy Stance Enhancements	3
3.	Transport Parameter	3
4.	Address Request and Response Frame Types	3
5.	Address Frame Usage	4
6.	Security Considerations	4
7.	IANA Considerations	5
8.	Normative References	5
	Authors' Addresses	6

[1.](#) Introduction

The QUIC Transport Protocol [[I-D.ietf-quic-transport](#)] provides a secure, multiplexed connection for transmitting reliable streams of application data. Connections are associated with unique Connection Identifiers (CIDs) that facilitate migration for clients that are mobile or have multiple network associations. CIDs also help connections survive Network Address Translator (NAT) port re-bindings, provided that the client behind the NAT sends a new packet with a known CID before the server drops the connection.

There is currently no explicit signal an endpoint can use to detect the presence of NATs. This problematic as it can encourage endpoints to aggressively send packets to keep NAT bindings alive.

This document describes an extension to QUIC that enables peers to request their public address and port from peers. This can be used to detect NATs and to help guide CID rotation policies.

[1.1.](#) Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

[2.](#) Motivation

There are several cases in which an endpoint might wish to know its public network address.

[2.1.](#) Connection Lifetime Optimizations

Knowing whether or not an endpoint is behind a NAT can help guide connection keepalive mechanisms. For example, peers that are not behind NATs might not need to send frequent keepalive packets (such as packets containing PING frames) to prevent NAT bindings expiration. This is particularly useful for UDP-based protocols such as QUIC, since UDP often has low idle timeouts configured on NATs or other middleboxes.

Note that there may still be stateful firewalls present in the network that have short timeouts, so NAT detection cannot be used as the only heuristic for a QUIC client's keepalive algorithm.

[2.2.](#) Privacy Stance Enhancements

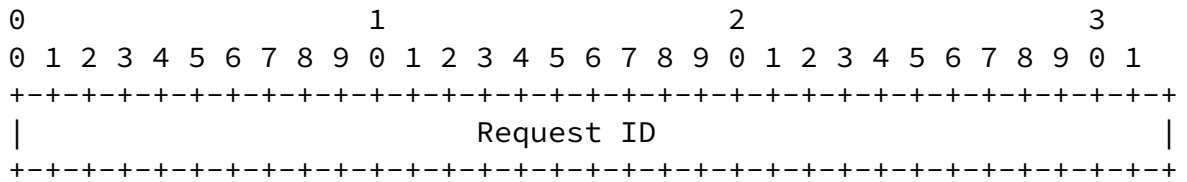
A QUIC endpoint might choose to rotate CIDs and UDP ports even over the same network interface to decrease the linkability of its traffic. However, the effectiveness of this approach can be limited if the endpoint is communicating using a fixed public IP address. Detecting a NAT increases the likelihood that rotating CIDs and UDP ports will be an effective strategy to obscure client traffic patterns.

[3.](#) Transport Parameter

Support for sending and receiving PUBLIC_ADDRESS_REQUEST and PUBLIC_ADDRESS_RESPONSE frames is advertised by means of a QUIC Transport Parameter (name=supports_address_request, value=0x000f). An endpoint that includes this parameter supports both requests and responses. Endpoints MUST NOT send requests or responses unless both parties signal support for these frames. An endpoint that receives a PUBLIC_ADDRESS_REQUEST or PUBLIC_ADDRESS_RESPONSE frame when it without sending the supports_address_request parameter MUST terminate the connection with error `PROTOCOL_VIOLATION`.

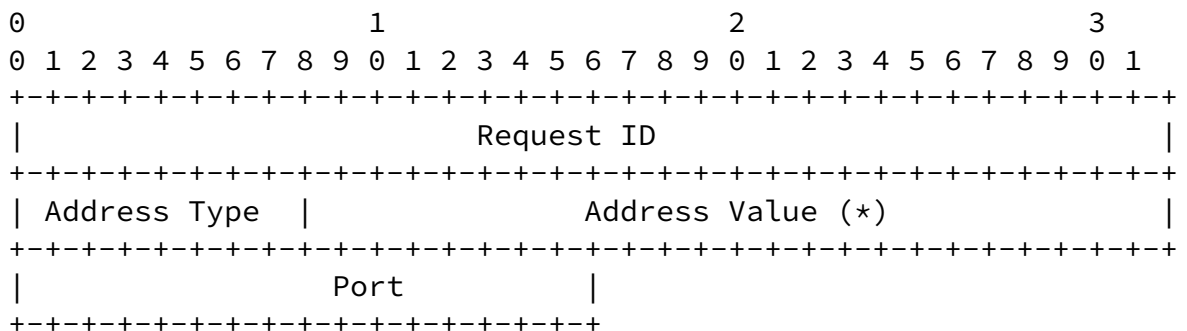
4. Address Request and Response Frame Types

A PUBLIC_ADDRESS_REQUEST frame has the following structure.



Request ID is a randomly generated 32-bit identifier for the request.

A PUBLIC_ADDRESS_RESPONSE frame has the following structure.



The fields of a PUBLIC_ADDRESS_RESPONSE frame are as follows:

Request ID: A 32-bit value indicating the ID of the corresponding request.

Address Type: A single octet equal to 0x00 or 0x01, indicating that the body carries an IPv4 or IPv6 address, respectively.

Address Value: A 32- or 128-bit value encoding an IPv4 or IPv6 address, respectively, depending on the value of Address Type.

Port: A 16-bit integer representing the peer's corresponding port.

5. Address Frame Usage

An endpoint MAY send a request or response frame at any point after connection establishment. Endpoints SHOULD send address request

frames following connection migration to learn if there is a change in its public address on the new path.

6. Security Considerations

PUBLIC_ADDRESS_REQUEST and PUBLIC_ADDRESS_RESPONSE frames are sent in encrypted QUIC packets and are therefore not visible to passive observers. Moreover, since endpoints can only request their public address, peers cannot accidentally transmit their (possibly private) address to a peer.

Endpoints that receive their perceived address from their peer cannot assume that the address is correct or trusted. The peer is able to send a fabricated address, so the result MUST NOT be used for any security-related decisions.

7. IANA Considerations

This document registers a new value in the QUIC Transport Parameter Registry:

Value: 0x000f (if this document is approved)

Parameter Name: supports_address_request

Specification: Indicates that the connection should enable support for PUBLIC_ADDRESS_REQUEST and PUBLIC_ADDRESS_RESPONSE. An endpoint that advertises this transport parameter can support both sending and receiving these frames.

This document also registers two new values in the QUIC Frame Type Registry:

Value: 0x1e (if this document is approved)

Frame Name: PUBLIC_ADDRESS_REQUEST

Specification: Requests that the peer sends back the public address

of sender

Value: 0x1f (if this document is approved)

Frame Name: PUBLIC_ADDRESS_RESPONSE

Specification: A response to a PUBLIC_ADDRESS_REQUEST containing the requester's public address

8. Normative References

[I-D.ietf-quic-transport]

Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport", [draft-ietf-quic-transport-18](#) (work in progress), January 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

Pauly, et al.

Expires September 12, 2019

[Page 5]

Internet-Draft

QUIC Address Extension

March 2019

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Email: tpauly@apple.com

Christopher A. Wood
Apple Inc.
One Apple Park Way
Cupertino, California 95014

United States of America

Email: cawood@apple.com

Eric Kinnear

Apple Inc.

One Apple Park Way

Cupertino, California 95014

United States of America

Email: ekinnear@apple.com