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

E. Kinnear
T. Pauly
C. Wood
Apple Inc.

March 11, 2019

TLS Client Network Address Extension
draft-kinnear-tls-client-net-address-00

Abstract

This document describes a TLS 1.3 extension that can be by clients to request their public network address from a server. This information can be used for a variety of purposes, including: NAT detection, ASN identification, and privacy-driven transport protocol features.

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

Table of Contents

1. Introduction

This document describes a TLS 1.3 [RFC8446] extension that can be by clients to request their public network address from a server. This has several uses, including: NAT detection, ASN identification, and privacy-driven transport protocol features. Servers that support this extension can send the perceived client address to clients. The latter may then confirm whether or not this representation matches their known public address.

Unlike the related NAT detection extension for IKE [RFC3947], clients do not send their perceived IP address to servers, even in an obfuscated form. Doing so would introduce an unwanted privacy regression for clients.

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. Client Network Address Use Cases

Knowledge of a public client network address can serve several purposes. This extension allows clients to detect the presence of a NAT or other address-transforming proxy involved in a TLS connection. The following sections descibe several uses for this information.

2.1. Connection Lifetime Optimizations

Middleboxes such as NATs typically have short lifetimes for connection state. Detecting such middleboxes may help influence client connection management logic, such as the use of keep-alive messages.

Since NATs often apply to all traffic from an endhost, detection via a TLS connection may assist other non-TLS and non-TCP connections that can be more sensitive to NAT timeouts.

2.2. Privacy Stance Enhancements

Address-transforming proxies such as NATs may improve communication privacy by masking the public IP address of clients in a session. Modulo other cleartext signals such as session identifiers, the anonymity set of a connection passing through a NAT is proportional to the number of clients serviced by the NAT. Absent NAT detection, clients cannot determine if their connections are linkable via IP-layer information, such as stable source addresses. As a result, clients cannot determine if privacy-driven policies such as never resuming TLS connections improve privacy.

If clients can detect NATs, they can make informed decisions about connection reuse. As a motivating example, consider DNS-over-TLS [RFC7858][RFC8310]. Privacy-sensitive clients may wish to use fresh connections for individual queries so as to not allow recursive resolvers the ability of building client query histories. However, in the absence of a NAT, reusing a connection does not pose a significant privacy regression since such clients are generally identifiable by their IP address.

Client network awareness may also influence privacy-driven connection migration policies, such as those prescribed by QUIC [I-D.ietf-quic-transport]. For example, if clients know they are not behind a NAT, then connection ID rotation serves little value in preventing linkability.

2.3. Metric Collections

Clients may passively use their public address discovered via TLS to identify their corresponding ASN without the use of explicit probes.

3. Network Address Extension

Servers may send the perceived client IP address to its peer using the following "network_address" extension:

```
enum {
    network_address(TBD), (65535)
} ExtensionType;
```

When sent by a client, this extension MUST be empty. A server which receives a non-empty network_address extension MUST terminate the connection with an "Illegal Parameter" alert.

Supporting servers which receive this extension may respond with a "network_address" extension, shown below, inside the EncryptedExtensions.

```
struct {
    opaque address<32..255>;
} NetworkAddress;
```

address The client's perceived address.

In this case, NetworkAddress.address carries the raw network-order byte-wise representation of the client IP address. (Since the extension is encrypted, there is no need to obfuscate the address for transit.) Clients which receive a non-empty NetworkAddress extension may use it to record their public IP address. Clients MUST treat empty NetworkAddress.address extensions as an error and send an Illegal Parameter alert in response.

4. IANA Considerations

IANA is requested to Create an entry, network_address(TBD), in the existing registry for ExtensionType (defined in [RFC8446]), with "TLS 1.3" column values being set to "CH, EE", and "Recommended" column being set to "Yes".

5. Security Considerations

Since NetworkAddress extension contents are encrypted, this extension introduces no (known) additional security or privacy issues.

An earlier design let clients send their address to servers in an obfuscated form, e.g., by hashing the client's perceived IP address with ClientHello.random, so that servers could measure whether or not clients were also behind NATs. However, such obfuscation mechanisms are subject to dictionary attacks and therefore could be used by malicious on-path attackers to learn a client's true public address. Absent this information, there are no explicit signals from a single (non-resumed) TLS connection that such attackers can use to learn the client's public address.

In general, absent a mechanism to encrypt the client extensions, sending the client's perceived address in any form therefore constitutes a privacy regression.

6. 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>.

[RFC3947] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, DOI 10.17487/RFC3947, January 2005, <https://www.rfc-editor.org/info/rfc3947>.

[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, <https://www.rfc-editor.org/info/rfc7858>.

[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>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

Authors' Addresses

Eric Kinnear
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Email: ekinnear@apple.com

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