QUIC
Internet-Draft
Intended status: Standards Track
Expires: March 14, 2019

G. Montenegro
N. Banks
P. Balasubramanian
Microsoft Corporation

September 10, 2018

QUIC Negotiation for Packet Number Protection
draft-montenegro-quic-negotiate-pnp-01

Abstract

This document defines an extension to reduce the cost of QUIC deployment in environments like datacenters by allowing packet number protection to be optionally disabled.

Note to Readers

Discussion of this draft takes place on the QUIC working group mailing list (quic@ietf.org), which is archived at https://mailarchive.ietf.org/arch/search/?email_list=quic [1].

Working Group information can be found at https://github.com/quicwg [2]; source code and issues list for this draft can be found at https://github.com/quicwg/base-drafts/labels/-recovery [3].

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 March 14, 2019.

Table of Contents

1. Introduction

QUIC is a new transport for the internet. In its generality, there are features which are not well suited for some environments. In particular, QUIC uses Packet Number Protection (PNP) to prevent ossification and to provide unlinkability upon (voluntary) migration. However, there are environments where these are not a concern, in particular, connections within a datacenter.

This document defines a negotiation mechanism using transport parameters to disable PNP. Internet facing nodes SHOULD NOT disable PNP, so browsers, for example, should not implement this extension. On the other hand, configured nodes within a datacenter could turn off PNP in their exchanges to avoid the CPU cost that PNP implies.

2. Conventions and Definitions

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Transport Parameter to Disable Packet Number Protection

This document defines a new transport parameter for QUIC [QUIC-TRANSPORT]:

disable_packet_number_protection (0x000c ?, value TBD): The endpoint is disabling packet number protection as specified in [QUIC-TLS]. This parameter is a zero-length value. This parameter only affects short headers.

A successful negotiation of the "disable_packet_number_protection" parameter requires both peers to send this transport parameter as well as the "disable_migration" parameter.

An endpoint MUST treat receipt of "disable_packet_number_protection" without the "disable_migration" parameter as a connection error of type TRANSPORT_PARAMETER_ERROR.

Peers that have successfully negotiated the "disable_packet_number_protection" parameter MUST NOT use packet number protection on short header packets.

4. Security Considerations

Per section 6.11.5 of [QUIC-TLS], PNP is used as a partial mitigation against linkability, and to prevent ossification. The "disable_packet_number_protection" parameter should be negotiated in environments in which these are not a concern.

5. IANA Considerations

Per section 13.1 of [QUIC-TLS], this document requests IANA assign a value for the new transport parameter and record it in the registry for "QUIC Transport Parameters" under the "QUIC Protocol" heading. IANA is further requested to assign a value with the first byte in the range 0x00 to 0xfe (in hexadecimal) as follows:

Value	Parameter Name	Specification
0x000c	disable_packet_number_protection	This document

6. References

6.1. Normative References

[QUIC-TLS] Thomson, M., Ed. and S. Turner, Ed., "Using Transport Layer Security (TLS) to Secure QUIC", draft-ietf-quic-tls-latest (work in progress).

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

[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>.

6.2. URIs

[1] https://mailarchive.ietf.org/arch/search/?email_list=quic

[2] https://github.com/quicwg

[3] https://github.com/quicwg/base-drafts/labels/-recovery

Authors' Addresses

Gabriel Montenegro
Microsoft Corporation

Email: Gabriel.Montenegro@Microsoft.com

Nick Banks
Microsoft Corporation

Email: NiBanks@Microsoft.com

Praveen Balasubramanian
Microsoft Corporation

Email: PravB@Microsoft.com