QUIC Negotiation for Header Protection
draft-montenegro-quic-negotiate-pnp-03

Abstract

This document defines an extension to reduce the cost of QUIC deployment in environments like datacenters by allowing header 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 August 1, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
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 Header Protection 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 header protection. Internet facing nodes SHOULD NOT disable header protection, so browsers, for example, should not implement this extension. On the other hand, configured nodes within a datacenter could turn off header protection in their exchanges to avoid the CPU cost that header protection 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 Header Protection

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

disable_header_protection (0x000c ?, value TBD): The endpoint is disabling header 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_header_protection" parameter requires both peers to send this transport parameter as well as the "disable_migration" parameter.

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

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

4. Security Considerations

Header protection was added as a partial mitigation against linkability, and to prevent ossification. The "disable_header_protection" parameter should be negotiated in environments in which these are not a concern.

5. IANA Considerations

Per section 10 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:

<table>
<thead>
<tr>
<th>Value</th>
<th>Parameter Name</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x000c</td>
<td>disable_header_protection</td>
<td>This document</td>
</tr>
</tbody>
</table>

6. References
6.1. Normative References

[QUIC-TLS]

[QUIC-TRANSPORT]


6.2. URIs

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


Acknowledgments

Thanks to the following individuals for useful discussions: Christian Huitema, Martin Thomson, Mikkel Fahnoe Joergensen, Ian Swett, Martin Duke, Lucas Pardue.

Authors’ Addresses

Gabriel Montenegro
Microsoft Corporation

Email: Gabriel.Montenegro@Microsoft.com

Nick Banks
Microsoft Corporation

Email: NiBanks@Microsoft.com