Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 3, 2016

M. Nottingham
E. Nygren
Akamai

January 31, 2016

The ORIGIN HTTP/2 Frame
draft-nottingham-httpbis-origin-frame-01

Abstract

This document specifies the ORIGIN frame for HTTP/2, to indicate what origins are available on a given connection.

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 August 3, 2016.

Copyright Notice

Copyright (c) 2016 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

1. Introduction 2
1.1. Notational Conventions 2
1.2. The ORIGIN HTTP/2 Frame 2
2. Security Considerations 3
3. Normative References 3
Authors' Addresses 4

1. Introduction

HTTP/2 [RFC7540] allows clients to coalesce different origins [RFC6454] onto the same connection when certain conditions are met. In some cases, the server is not authoritative for a coalesced origin, so the 421 (Misdirected Request) status code was defined.

Using a status code in this manner allows clients to recover from misdirected requests, but at the penalty of adding latency. To address that, this specification defines a new HTTP/2 frame type, "ORIGIN", to allow servers to indicate what origins a connection is authoritative for.

1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. The ORIGIN HTTP/2 Frame

The ORIGIN HTTP/2 frame ([RFC7540], Section 4) indicates what origin(s) [RFC6454] the sender considers this connection authoritative for (in the sense of [RFC7540], Section 10.1).

The ORIGIN frame is a non-critical extension to HTTP/2. Endpoints that do not support this frame can safely ignore it.

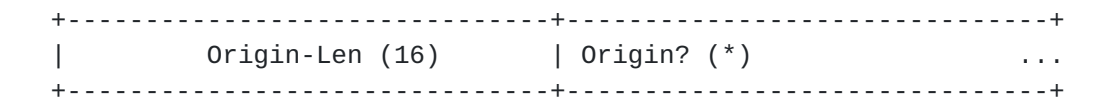
It MUST occur on stream 0; an ORIGIN frame on any other stream is invalid and MUST be ignored.

When received by a client, it can be used to inform HTTP/2 connection coalescing (see [RFC7540], Section 9.1.1), but does not relax the requirement there that the server is authoritative.

If multiple ORIGIN frames are received on the same connection, only the most recent is to be considered current.

Once an ORIGIN frame has been received and processed, clients that implement this specification SHOULD NOT use that connection for a given origin if it did not appear within the current ORIGIN frame.

The ORIGIN frame type is 0xb (decimal 11).



The ORIGIN frame contains the following fields, sets of which may be repeated within the frame to indicate multiple origins:

Origin-Len: An unsigned, 16-bit integer indicating the length, in octets, of the Origin field. Origin: An optional sequence of characters containing the ASCII serialization of an origin ([RFC6454], Section 6.2) that the sender believes this connection is authoritative for.

The ORIGIN frame does not define any flags. It can contain one or more Origin-Len/Origin pairs.

The ORIGIN frame is processed hop-by-hop. An intermediary must not forward ORIGIN frames.

Clients configured to use a proxy MUST ignore any ORIGIN frames received from it.

2. Security Considerations

Clients that blindly trust the ORIGIN frame's contents will be vulnerable to a large number of attacks; hence the reinforcement that this specification does not relax the requirement for server authority in [RFC7540], Section 10.1.

3. Normative References

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

[RFC6454] Barth, A., "The Web Origin Concept", RFC 6454, DOI 10.17487/RFC6454, December 2011, <http://www.rfc-editor.org/info/rfc6454>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <http://www.rfc-editor.org/info/rfc7540>.

Authors' Addresses

Mark Nottingham
Akamai

Email: mnot@mnot.net
URI: http://www.mnot.net/

Erik Nygren
Akamai

Email: nygren@akamai.com