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

Abstract

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

Note to Readers

   Discussion of this draft takes place on the HTTP working group
   mailing list (ietf-http-wg@w3.org), which is archived at
   https://lists.w3.org/Archives/Public/ietf-http-wg/ .

   Working Group information can be found at http://httpwg.github.io/ ;
   source code and issues list for this draft can be found at
   https://github.com/httpwg/http-extensions/labels/origin-frame .

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 April 1, 2017.

Copyright Notice

Table of Contents

[1](#). Introduction

HTTP/2 [[RFC7540](#)] allows clients to coalesce different origins
[[RFC6454](#)] onto the same connection when certain conditions are met.
However, in certain cases, a connection is is not usable for a
coalesced origin, so the 421 (Misdirected Request) status code
([[RFC7540], Section 9.1.2](#)) 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
usable 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](#)].

[2](#). The ORIGIN HTTP/2 Frame

The ORIGIN HTTP/2 frame ([[RFC7540], Section 4](#)) allows a server to
indicate what origin(s) [[RFC6454](#)] the server would like the client to
consider as members of the Origin Set ([Section 2.1](#)) for the
connection it occurs within.

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

```
+-------------------------------+-------------------------------+
|         Origin-Len (16)       | Origin? (*)                ...
+-------------------------------+-------------------------------+
```

The ORIGIN frame's payload 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 or could be authoritative for.

The ORIGIN frame defines the following flags:

CLEAR (0x1): Indicates that the Origin Set MUST be reset to an empty
   set before processing the contents of the frame it occurs upon.

REMOVE (0x2): Indicates that the origin(s) carried in the payload
   must be removed from the Origin Set, if present; if not present,
   it/they have no effect.

2.1. The Origin Set

The set of origins (as per [RFC6454]) that a given connection might
be used for is known in this specification as the Origin Set.

When a connection is first established, its Origin Set is defined to
be those origins that the client would normally consider the
connection authoritative for; see [RFC7540], Section 10.1.

The ORIGIN frame allows the server to modify the Origin Set. In
particular:

1. A server can add to its members by sending an ORIGIN frame
    (without any flags set);

2. A server can prune one or more origins from it by sending an
    ORIGIN frame with the REMOVE flag set;

3. A server can remove all its members and then add zero or more
    members by sending an ORIGIN frame with the CLEAR flag set and a
    payload containing the new origins.

Adding to the Origin Set (cases 1 and 3 above) does not imply that
the connection is authoritative for the added origins (in the sense

of [RFC7540], Section 10.1) on its own; this MUST be established by
some other mechanism.

A client that implements this specification MUST NOT use a connection
for a given origin unless that origin appears in the Origin Set for
the connection, regardless of whether or not it believes that the
connection is authoritative for that origin.

2.2. Processing ORIGIN Frames

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

When received by a client, it can be used to inform HTTP/2 connection
coalescing (see Section 2.1), but does not relax the requirement
there that the server is authoritative.

The origin frame MUST be sent on stream 0; an ORIGIN frame on any
other stream is invalid and MUST be ignored.

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.

The following algorithm illustrates how a client can handle received
ORIGIN frames:

1. If the client is configured to use a proxy, ignore the frame and
    stop processing.

2. If the frame occurs upon any stream except stream 0, ignore the
    frame and stop processing.

3. If the CLEAR flag is set, remove all members from the Origin Set.

4. For each Origin field "origin_raw" in the frame payload:

    1. Parse "origin_raw" as an ASCII serialization of an origin
        ([RFC6454], Section 6.2) and let the result be
        "parsed_origin".

    2. If the REMOVE flag is set, remove any member of the Origin
        Set that is the same as "parsed_origin" (as per [RFC6454],
        Section 5), and continue to the next "parsed_origin".

    3. Otherwise, add "parsed_origin" to the Origin Set.

3. 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.

4. 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: https://www.mnot.net/

Erik Nygren
Akamai

Email: nygren@akamai.com