TODO Working Group
Internet-Draft
Intended status: Informational
Expires: 13 December 2021

E. Nygren
Akamai

11 June 2021

Alt-Svc Fixes and Feature Candidates
draft-nygren-altsvc-fixes-00

Abstract

HTTP Alternative Services has become the primary mechanism for HTTP/3 upgrade, but overlaps with and disagrees with other developing standards, such as the HTTPS resource record in DNS. This document explores a set of potential fixes and/or additional features for Alt-Svc. It is used to record and share thoughts, and is not expected to progress on its own.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the mailing list (httpbis@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/httpbis/.

Source for this draft and an issue tracker can be found at https://github.com/MikeBishop/alt-svc-bis.

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 13 December 2021.

Copyright Notice

Copyright (c) 2021 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 (https://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. Overview

Alt-Svc [AltSvc] was published in April of 2016. Since then, it has become the primary mechanism to upgrade connections to HTTP/3, at least until HTTPS RRs [SVCB] are standardized and widely supported.

This brainstorms a set of potential fixes and feature candidates for an Alt-Svc BIS. In the spirit of brainstorming, some of the things

in this list may be bad ideas. One of the points of this document is to judge interest in each of these items to determine what potential authors may be interested in including in a draft.

A number of these items were deferred out of the SVCB/HTTPS draft. Others are based on regrets from implementation experience with AltSvc. A few are potentially valuable features.

It is not yet defined whether this should be a new header or can be done via extensions to Alt-Svc as it exists today.

A number of major clients have yet to implement Alt-Svc to other hostnames fully, and some of this is due to concerns that they have with the current specification.

It may make sense to split this list into batches, but another option would be to try and get all of these done at once even if as separate but cooperating drafts.

2. Potential Scope Items

2.1. Incorporating errata and Editorial improvements

(Hopefully this is non-controversial.)

Includes:

* Incorporate errata
* Reference RFC 8336 "ORIGIN Frames" (regarding disabling connection coalescing)
* Incorporate [I-D.pardue-httpbis-dont-be-clear]
* ...

2.2. Fix ALPN handling

The ALPN semantics in [AltSvc] are ambiguous, and problematic in some interpretations. We should update [AltSvc] to give it well-defined

semantics that match the HTTPS RRs. For example, specify that the ALPN [ALPN] negotiated via the TLS handshake does not need to be the same as the ALPN indicated in the AltSvc.

(From HTTPS RR #246 (https://github.com/MikeBishop/dns-alt-svc/issues/246) and other discussion threads during HTTPS RR. David Benjamin also has strong opinions on this topic.)

One option would be to pull in the text we landed on for the HTTPS/SVCB draft, see Section 6.1 of [SVCB]. See also [I-D.thomson-tls-snip].

2.3. Address concerns about Alt-Svc lifetime bounding

Some people have expressed concerns that Alt-Svc allows a compromised Origin to hold onto clients forever by continuing to offer updated Alt-Svc entries. There may be ways to reduce the vulnerability exposure here, such as by periodic reconfirmation with the "real" origin or something it controls. This is of particular concern when an Alt-Svc record has a much longer lifetime than an HTTPS RR.

For example, if the Alt-Svc records were signed with a key published in DNS. Records remain valid so long as the key that signed them is still claimed by the domain. An unsigned record has a very short lifetime bound.

2.4. Support ECH

The HTTPS RR [SVCB] is currently the only way to retrieve keys for Encrypted Client Hello [ECH]. To maintain security, it puts Alt-Svc out-of-scope, since Alt-Svc cannot deliver ECH keys.

Two options (and there may be more) include:

* Add an ech= parameter to Alt-Svc

* Defining some better integration between Alt-Svc and HTTPS RRs. For example, allow an AltSvc server name to be treated as an "AliasMode" reference to an HTTPS record.

2.5. Better Interactions with HTTPS Record

This was deferred out of the HTTPS RR draft. There are a number of design options here, but requirements and pros/cons will want to be discussed in-detail before proposing designs. Supporting ECH and Alt-Svc together is a primary goal.

An important item here is which takes precedence, providing safe and time-bounded ways to allow Alt-Svc to take precedence over HTTPS records. Alt-Svc has the ability to be delivered in a user-specific manner -- useful operationally, but potentially problematic for privacy. HTTPS records can be easily revalidated, which is more difficult with an Alt-Svc record.

Providing a way for Alt-Svc to act as AliasMode references to HTTPS SvcMode records seems like one clean way for interaction in that it avoids needing to duplicate SVCB in Alt-Svc. We would still need to address time-bounding and trust considerations.

2.6. HTTP/3 Frame Definition

The ALTSVC frame has not been defined for HTTP/3. Perhaps it should be [I-D.bishop-httpbis-altsvc-quic]. Alternatively, if the frame has not been widely adopted, should it be deprecated from HTTP/2 instead?

2.7. Accept-Alt-Svc Request Header

There is significant variation in client support for the Alt-Svc specification, including some clients which only implement a subset of the specification. Having an Accept-Alt-Svc request header that lists a set of supported Alt-Svc features allows for extension of Alt-Svc but also allows for deprecation.

If we don't deprecate the frames, we'd also need a SETTINGS equivalent.

There are potential client fingerprinting concerns here, so we'll want to not go too far with this.

2.8. Improve/Replace Alt-Used Header

There is limited implementation support for Alt-Used out of privacy concerns. It also only sends a subset of the Alt-Svc record being used, and there are unclear interactions between Alt-Used and HTTPS RRs.

Daniel Stenberg points out:

> Alt-Used (RFC 7838 section 5) is a request header that only sends host name + port number, with no hint if that port number is TCP or UDP (or ALPN name), which makes at least one large HTTP/3 deployment trigger its Alt-Svc loop detection when only switching protocols to h3.

It is proposed that we replace or redefine Alt-Used and also define how it interacts with SVCB. Note that hostile origins have many knobs for getting this information (e.g., encoding in hostnames, ports, or IPv6 addresses) so a goal would be to allow non-hostile origins to get information on which Alt-Svc or SVCB record is being used in a way that doesn't make things worse from a privacy perspective.

Some options include:

* Just send the whole Alt-Svc or SVCB binding used in the header

* Have a param encoding an N-bit or N-character value for the record-id. This value would be sent as Alt-Used. How many bits to use is an open question.

  - Allowing for a dynamic length where the client chooses how many bits or characters to include based on privacy budget is one attractive but complicated option. Server implementers would put the most important info into earlier bits/characters.

The goal here is to allow for virtual hosting of alternative services, allowing the server to know which alternative service was used (eg, for load feedback, diagnostics/debugging, loop detection, and other operational purposes), but without hacks like separate ports or IP addresses that leak information to passive network observers.

The usefulness of Alt-Used is currently limited by the fact that most servers simply send ":443" and some clients won't consider any other alternative offered.

See some discussion and other options here (https://github.com/MikeBishop/dns-alt-svc/issues/107).

2.9. Path-Scoped Alt-Svc

The largest-scope, most disruptive, and perhaps most controversial item would be to allow Alt-Svc to be scoped to URL paths with a way to indicate that transitions to use the Alt-Svc should be done synchronously.

This is desired for use-cases of large content libraries where an Origin would like to have clients use different endpoints for different objects while sharing a single Origin. This would also likely need negotiation.

This use-case is similar to that served by [I-D.reschke-http-oob-encoding], which is one possible solution. In that model, the origin retains control of the entire namespace while delegating delivery of particular objects to other endpoints.

Extending Alt-Svc is another approach which might allow more flexibility. For example:

* Client indicates via a request header (eg, Accept-*) or a SETTING that it supports this feature

* Server's Alt-Svc indicates that the path="/movies/MurderOnTheExampleExpress/" should be accessed by a particular alternative service

* Server returns a new 3xx response header response header indicating that the Alt-Svc should be used synchronously to fetch the response

2.10. Persist and Caching Concerns

[AltSvc] defines the "persist" parameter.

> Alternative services that are intended to be longer lived (such as those that are not specific to the client access network) can carry the "persist" parameter with a value "1" as a hint that the service is potentially useful beyond a network configuration change.
>
> When alternative services are used to send a client to the most optimal server, a change in network configuration can result in cached values becoming suboptimal. Therefore, clients SHOULD remove from cache all alternative services that lack the "persist" flag with the value "1" when they detect such a change, when information about network state is available.

For some clients (e.g. cURL), detecting network changes is very tricky. Certain clients default to behaving like persist=1 for all alternatives.

The RFC text today seems to imply that servers factor in client network properties when deciding what to advertise. That is not true for all deployments. The recommendation that a client invalidate Alt-Svc cache entries based on their own network state changes can seem mistaken today. The situation can potentially get worse with protocol evolution (connection migration, multipath, etc).

This feature was designed to address the "mistaken mapping" scenario, where either DNS mapping or anycast landed you at one POP but the server knows another one is closer to you: You're in Seattle, your VPN endpoint and DNS server is in Sacramento, and so DNS resolution gives you a CDN node in California. The California endpoint gives you the unicast IP of the Seattle endpoint as a friendly shove.

Similarly, it's one of the best work-around options for off-net DNS (via DoH, ODoH, etc.) if there is a CDN endpoint very close to the user's network, but doesn't work so well if the Alt-Svc record keeps being used after a network change.

When you're no longer in the same network environment, we can trust

mapping again. What is the signal this redirect is no longer useful if clients can't reliably detect network changes?

2.11. Radical Simplification

If we are able to reach wide deployment and use of the HTTPS record, it may supersede many use cases for Alt-Svc. We should reassess the needs from the new baseline to see whether Alt-Svc can be radically simplified. (Chrome never fully implemented Alt-Svc redirection anyway.)

3. Security Considerations

TODO Security

4. IANA Considerations

This document has no IANA actions.

5. Informative References

[ALPN] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/rfc/rfc7301>.

[AltSvc] Nottingham, M., McManus, P., and J. Reschke, "HTTP Alternative Services", RFC 7838, DOI 10.17487/RFC7838, April 2016, <https://www.rfc-editor.org/rfc/rfc7838>.

[ECH] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-10, 8 March 2021, <https://tools.ietf.org/html/draft-ietf-tls-esni-10>.

[I-D.bishop-httpbis-altsvc-quic] Bishop, M., "ALTSVC Frame in HTTP/QUIC", Work in Progress, Internet-Draft, draft-bishop-httpbis-altsvc-quic-01, 15 May 2020, <https://tools.ietf.org/html/draft-bishop-httpbis-altsvc-quic-01>.

[I-D.pardue-httpbis-dont-be-clear] Pardue, L. and A. Ramine, "Reserving the clear ALPN Protocol ID", Work in Progress, Internet-Draft, draft-pardue-httpbis-dont-be-clear-00, 15 March 2021, <https://tools.ietf.org/html/draft-pardue-httpbis-dont-be-clear-00>.

[I-D.reschke-http-oob-encoding]
Reschke, J. F. and S. Loreto, "'Out-Of-Band' Content Coding for HTTP", Work in Progress, Internet-Draft, draft-reschke-http-oob-encoding-12, 24 June 2017, <https://tools.ietf.org/html/draft-reschke-http-oob-encoding-12>.

[I-D.thomson-tls-snip]
Thomson, M., "Secure Negotiation of Incompatible Protocols in TLS", Work in Progress, Internet-Draft, draft-thomson-tls-snip-01, 3 January 2021, <https://tools.ietf.org/html/draft-thomson-tls-snip-01>.

[SVCB] Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-05, 21 April 2021, <https://tools.ietf.org/html/draft-ietf-dnsop-svcb-https-05>.

Acknowledgments

Martin Thomson, Lucas Pardue, and Mike Bishop reviewed and commented on an early version of this draft (https://docs.google.com/document/d/1QNaXduqohACK93qLPpxkPJ2rHQMgWqUPL-DkZS11htQ/edit?ts=60a5dc92#).

Author's Address

Erik Nygren
Akamai

Email: erik+ietf@nygren.org