HTTP
Internet-Draft
Intended status: Standards Track
Expires: 23 August 2025

B. M. Schwartz
Meta Platforms, Inc.
Y. Rosomakho
Zscaler

19 February 2025

Forward and Reverse HTTP/3 over WebTransport
draft-various-httpbis-h3-webtrans-00

Abstract

HTTP/3 was initially specified only for use with the QUIC version 1 transport protocol. This specification defines how to use HTTP/3 over a WebTransport session, which can be implemented using any WebTransport protocol. This enables operation of HTTP/3 when UDP based transport is not available, as well as server-initiated HTTP/3 requests.

About This Document

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

The latest revision of this draft can be found at https://bemasc.github.io/h3-webtrans/draft-various-httpbis-h3-webtrans.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-various-httpbis-h3-webtrans/.

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

Source for this draft and an issue tracker can be found at https://github.com/bemasc/h3-webtrans.

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/.

Copyright Notice

Table of Contents

1. Introduction

HTTP versions 2 [HTTP/2] and earlier were primarily specified to run over a reliable stream transport. Initially, this transport was normally TCP, but TLS over TCP [TLS13] is now often used instead. Other reliable stream transports are also used, especially for interprocess HTTP requests on a single host.

HTTP version 3 [HTTP/3] was specified only to run on QUIC version 1 [QUIC], but its specification anticipates support for other transports ([HTTP/3], Section 3.2):

> The use of other QUIC transport versions with HTTP/3 MAY be defined by future specifications.

In fact, nothing in HTTP/3 relies on the transport being a QUIC version at all, so long as it provides transport capabilities similar to QUICv1. These include:

* A session establishment procedure.
* Support for multiple streams within a session.
* Unidirectional and bidirectional streams, initiated by either party.
* Transmission of independent datagrams (for HTTP/3 Datagrams [HTTP-DGRAM]).

Another transport system that provides these capabilities is the WebTransport session interface [WEBTRANS], which we refer to here as "WebTransport". WebTransport can be implemented within an HTTP/2 [WEBTRANS-H2] or HTTP/3 [WEBTRANS-H3] connection, and implementations based on WebSocket and other protocols have been proposed. A WebTransport server endpoint can always be identified by a URI, which might or might not use the "https" URI scheme.

After a WebTransport session is established, the interface presented to the client and server are largely identical. Either party can open or accept new streams of either type, send datagrams, and eventually terminate the session. Thus, once we have defined HTTP/3 over WebTransport (H3-WT), it is straightforward to define Reverse H3-WT, in which the HTTP client and server roles are reversed.

H3-WT is a general-purpose specification that may be put to various uses. One motivating use case for Forward H3-WT is to enable HTTP/3 over a TCP-based WebTransport protocol, for cases where the client and server prefer HTTP/3 but a network element only permits TCP. Other creative uses are also possible.

For Reverse H3-WT, one motivating use case is to enable a hidden backend server to delegate TCP server functions to a proxy server. With this specification, the hidden backend can create a Reverse H3-WT session over which the proxy can issue multiple HTTP CONNECT requests.

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.

2.1. Roles

To distinguish actions on the WebTransport session from actions on the H3-WT connection that it carries, we define the following roles:

* Dialer - initiates the WebTransport session

* Listener - accepts the WebTransport session

* Client - sends requests on the H3-WT session

* Server - receives these HTTP requests

* Participant - A Client or Server.

In Forward H3-WT, the Dialer is the Client. In Reverse H3-WT, the Dialer is the Server.

3. Specification

3.1. Establishment

Establishment of an H3-WT session is not constrained by this specification. Any new WebTransport session MAY be used with this specification, subject to prior arrangement by the endpoints. This specification does not constrain any URLs or protocol IDs associated with the session establishment process.

A future specification could allocate TLS ALPN IDs that indicate the use of this specification with a particular WebTransport protocol.

3.2. Applicability

An H3-WT connection can carry HTTP requests with any method, scheme, authority, and path. These values are not constrained by any similar values that may have applied to the WebTransport session itself. For example, if the Listener's URI is "https://my-origin.example.com/wt", this does not limit the origins to which requests may be sent on the H3-WT connection.

Clients MUST determine the permissible set of origins for an H3-WT session by private arrangement (see Section 4). Servers SHOULD send an ORIGIN frame [ORIGIN] at the beginning of the connection to indicate which origins are actually available on the session, unless that set is unambiguous (i.e., fixed by private arrangement) or unbounded (e.g., in the case of a proxy service).

3.3. Streams

To create a stream, participants use WebTransport's "create a unidirectional stream" or "create a bidirectional stream" operation. If this operation fails, it MUST produce a connection error of type H3_STREAM_CREATION_ERROR.

To accept a stream, participants use WebTransport's "receive a unidirectional stream" and "receive a bidirectional stream" operations. Participants MUST accept additional unidirectional streams whenever there are fewer than 3 active, and SHOULD accept additional bidirectional streams whenever there are fewer than 100.

If the Client receives a bidirectional stream, and no HTTP extension has been negotiated to permit this stream, it MUST produce a connection error of type H3_STREAM_CREATION_ERROR.

3.3.1. Stream IDs

WebTransport streams do not expose a Stream ID. To enable HTTP/3 functions that rely on Stream IDs, such as GOAWAY ([HTTP/3], Section 7.2.6) and Datagrams, the creator of each stream MUST write the H3-WT Stream ID at the beginning of each stream, and the H3-WT receiver must consume this Stream ID before passing the stream to HTTP/3.

The H3-WT Stream ID is encoded as a QUIC variable-length integer ([QUIC], Section 16) and follows the QUICv1 stream numbering convention ([QUIC], Section 2.1), so the Client's first stream has stream ID 0x00.

3.4. Datagrams

If SETTINGS_H3_DATAGRAM was negotiated on the H3-WT connection, participants send and receive each HTTP/3 Datagram using the WebTransport "send a datagram" and "receive a datagram" operations. HTTP/3 MUST derive the datagram's Quarter Stream ID from the corresponding stream's H3-WT Stream ID.

Note that datagrams in H3-WT may be unreliable even when H3-WT is running over a reliable protocol, as the HTTP request or the WebTransport session may be forwarded by an intermediary onto a connection that uses a different protocol.

3.5. Closure and Errors

When closing a stream successfully, participants use the WebTransport "send bytes" operation with a FIN indication. Receipt of a FIN indication in "receive bytes" indicates successful completion of the stream.

When closing a stream abruptly, the stream error code is passed to the WebTransport "abort send side" or "abort receive side" operation as appropriate, and retrieved by the other participant from the "send side aborted" or "receive side aborted" event.

An H3-WT connection is terminated using the WebTransport "terminate a session" operation. The connection error is passed to this operation and retrieved by the other participant from the "session terminated" event.

4. Security Considerations

HTTP clients generally rely on the transport (TCP, TLS, or QUIC) to ensure that they are connected to the intended server before sending a request. For "https" URIs, this involves TLS server authentication. In H3-WT, the implementor is responsible for employing suitable authentication of the WebTransport session. WebTransport guarantees TLS-equivalent authentication of the Listener to the Dialer, which may be sufficient for some Forward H3-WT deployments. Authentication of the Dialer to the Listener can be accomplished using TLS client authentication (if exposed by the WebTransport protocol), HTTP Authentication (when using WebTransport over HTTP), or Capability URLs [CAPABILITY] (when using WebTransport

with a URI scheme that supports a non-empty path).

If the WebTransport protocol exposes a TLS Exported Authenticator capability, participants MAY use it to enable Secondary Certificate Authentication [I-D.ietf-httpbis-secondary-server-certs] and/or HTTP Concealed Authentication [RFC9729] within the H3-WT session.

5. Examples

5.1. Hidden Origin Configuration

In some cases, it can be desirable for an HTTP origin server to operate through a public gateway without exposing a publicly reachable IP address. For example, the origin server might be subject to request flood attacks if its IP address were publicly reachable. Reverse H3-WT allows a hidden origin server to make itself available only to the gateway.

One potential implementation proceeds as follows:

1. The public gateway instructs the origin operator to use "https://gateway.example/reverse/$customer_id" as the URL for Reverse H3-WT, along with a specified secret Bearer token.

2. The origin operator selects a generic HTTP gateway implementation that supports Reverse H3-WT over HTTP with Bearer authentication, and configures it to forward requests to the origin server.

3. The origin operator configures this local gateway with the specified URL and Bearer token for Reverse H3-WT.

4. The local gateway opens a WebTransport session to the public gateway using an Extended CONNECT request to the specified URL.

5. The public gateway verifies that the Extended CONNECT request carries the correct Bearer token for this customer ID.

6. The local gateway uses the ORIGIN frame to enumerate the origins that are available on this session.

7. The public gateway validates that this customer is permitted to serve the indicated origins.

8. The public gateway starts forwarding incoming HTTP requests for those origins over this session.

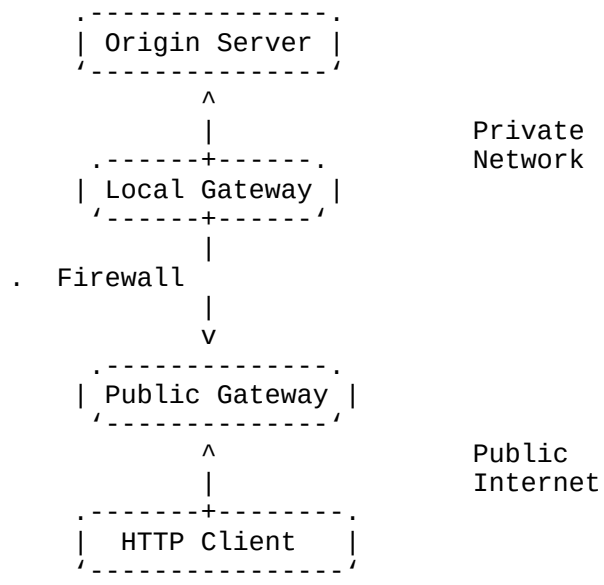

Figure 1: Hidden Origin Configuration

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[HTTP-DGRAM] Schinazi, D. and L. Pardue, "HTTP Datagrams and the Capsule Protocol", RFC 9297, DOI 10.17487/RFC9297, August 2022, <https://www.rfc-editor.org/rfc/rfc9297>.

[HTTP/3] Bishop, M., Ed., "HTTP/3", RFC 9114, DOI 10.17487/RFC9114, June 2022, <https://www.rfc-editor.org/rfc/rfc9114>.

[ORIGIN] Bishop, M., "The ORIGIN Extension in HTTP/3", RFC 9412, DOI 10.17487/RFC9412, June 2023, <https://www.rfc-editor.org/rfc/rfc9412>.

[QUIC] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[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/rfc/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/rfc/rfc8174>.

[WEBTRANS] Vasiliev, V., "The WebTransport Protocol Framework", Work in Progress, Internet-Draft, draft-ietf-webtrans-overview-08, 25 August 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-webtrans-overview-08>.

[WEBTRANS-H2] Frindell, A., Kinnear, E., Pauly, T., Thomson, M., Vasiliev, V., and G. Xie, "WebTransport over HTTP/2", Work in Progress, Internet-Draft, draft-ietf-webtrans-http2-10, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-webtrans-http2-10>.

[WEBTRANS-H3] Frindell, A., Kinnear, E., and V. Vasiliev, "WebTransport over HTTP/3", Work in Progress, Internet-Draft, draft-ietf-webtrans-http3-11, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-webtrans-http3-11>.

7.2. Informative References

[CAPABILITY] "Good Practices for Capability URLs", February 2014, <https://www.w3.org/TR/capability-urls/>.

[HTTP/2] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113, DOI 10.17487/RFC9113, June 2022, <https://www.rfc-editor.org/rfc/rfc9113>.

[I-D.benfield-http2-p2p] Benfield, C., "Peer-to-peer Extension to HTTP/2", Work in Progress, Internet-Draft, draft-benfield-http2-p2p-02, 9 October 2015, <https://datatracker.ietf.org/doc/html/draft-benfield-http2-p2p-02>.

[I-D.draft-bt-httpbis-reverse-http] Schwartz, B. M., Reddy.K, T., Boucadair, M., and P. S. Tiesel, "Reverse HTTP Transport", Work in Progress,

Internet-Draft, draft-bt-httpbis-reverse-http-01, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-bt-httpbis-reverse-http-01>.

[I-D.ietf-httpbis-secondary-server-certs]
Gorbaty, E. and M. Bishop, "Secondary Certificate Authentication of HTTP Servers", Work in Progress, Internet-Draft, draft-ietf-httpbis-secondary-server-certs-01, 12 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-secondary-server-certs-01>.

[I-D.kazuho-httpbis-reverse-tunnel]
Oku, K., "Reverse Tunnel over HTTP", Work in Progress, Internet-Draft, draft-kazuho-httpbis-reverse-tunnel-00, 19 February 2024, <https://datatracker.ietf.org/doc/html/draft-kazuho-httpbis-reverse-tunnel-00>.

[I-D.lentczner-rhttp]
Lentczner, M. and D. Preston, "Reverse HTTP", Work in Progress, Internet-Draft, draft-lentczner-rhttp-00, 4 March 2009, <https://datatracker.ietf.org/doc/html/draft-lentczner-rhttp-00>.

[RFC9729] Schinazi, D., Oliver, D., and J. Hoyland, "The Concealed HTTP Authentication Scheme", RFC 9729, DOI 10.17487/RFC9729, February 2025, <https://www.rfc-editor.org/rfc/rfc9729>.

[TLS13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

Acknowledgments

This specification is inspired by earlier proposals related to reversing connection establishment over HTTP, including:

* [I-D.lentczner-rhttp]

* [I-D.benfield-http2-p2p]

* [I-D.draft-bt-httpbis-reverse-http]

* [I-D.kazuho-httpbis-reverse-tunnel]

Authors' Addresses

Benjamin M. Schwartz
Meta Platforms, Inc.
Email: ietf@bemasc.net

Yaroslav Rosomakho
Zscaler
Email: yrosomakho@zscaler.com