HTTP/2 provides multiplexing of HTTP requests over a single underlying transport connection. HTTP/2 Transport defines a transport abstraction enabling delivery of byte stream and datagram data using streams of an HTTP/2 connection.
1. Introduction

HTTP/2 [RFC7540] provides a framing layer that describes the exchange of HTTP messages. This framing layer includes multiplexing of multiple streams on a single underlying transport connection, flow control, stream dependencies and priorities, and exchange of configuration information between endpoints.

Section 8.3 of [RFC7540] defines the HTTP CONNECT method for HTTP/2, which converts a HTTP/2 stream into a tunnel for arbitrary data. [RFC8441] describes the use of the extended CONNECT method to negotiate the use of the WebSocket Protocol [RFC6455] on an HTTP/2 stream.

This document defines protocol names for use in the extended CONNECT handshake that allow negotiation of HTTP/2 streams that transport arbitrary byte streams or datagrams. It also extends the CONNECT handshake to allow both endpoints of an HTTP/2 connection to establish streams that tunnel data. Being able to transport arbitrary data on individual HTTP/2 streams allows an underlying connection to be shared by multiple protocols and allows all protocols to benefit from the features provided by HTTP/2 framing.

1.1. Notational Conventions

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. The SETTINGS_ENABLE_BIDIRECTIONAL_CONNECT Parameter

As described in Section 5.5 of [RFC7540], SETTINGS parameters allow endpoints to negotiate use of protocol extensions that would otherwise generate protocol errors. Use of the CONNECT method extension defined in [RFC6455] requires the SETTINGS_ENABLE_CONNECT_PROTOCOL parameter to be received by a client prior to its use.

This document introduces another SETTINGS parameter, SETTINGS_ENABLE_BIDIRECTIONAL_CONNECT, which MUST have a value of 0 or 1.

Once a SETTINGS_ENABLE_BIDIRECTIONAL_CONNECT parameter has been sent with a value of 1, an endpoint MUST NOT send the parameter with a value of 0.

Upon receipt of SETTINGS_ENABLE_BIDIRECTIONAL_CONNECT with a value of 1, an endpoint MAY use the extended CONNECT defined in [RFC6455] with the protocol values defined in this document. An endpoint that supports receiving the extended CONNECT method SHOULD send this setting with a value of 1.

Note that [RFC6455] restricts SETTINGS_ENABLE_CONNECT_PROTOCOL to have no effect if received by a server. This document modifies that restriction and allows both SETTINGS_ENABLE_CONNECT_PROTOCOL and SETTINGS_ENABLE_BIDIRECTIONAL_CONNECT to take effect if received by either endpoint of an HTTP/2 connection.

3. Negotiating Byte Stream and Datagram Tunnels

[RFC6455] defines the psuedo-header field :protocol which can indicate the protocol intended to be used on the tunnel established by the CONNECT method. Values for the :protocol psuedo-header field are maintained in an Upgrade Token Registry established by [RFC7230] for protocol-name tokens.

After receiving both SETTINGS_ENABLE_CONNECT_PROTOCOL and SETTINGS_ENABLE_BIDIRECTIONAL_CONNECT, either endpoint of an HTTP/2 connection can send a request in HEADERS frames to establish a byte stream or datagram tunnel via the extended CONNECT method. Similarly, either endpoint may be required to respond to an incoming CONNECT request seeking to establish such a tunnel.
3.1. Initiating the Extended CONNECT Handshake

Endpoints using this mechanism to establish byte stream or datagram tunnels over HTTP/2 streams follow the CONNECT handshake procedure defined in [RFC6455]. However, instead of supplying "websocket" for the :protocol pseudo-header field to indicate a WebSocket connection, they specify "bytestream" or "datagram" to indicate a byte stream or datagram connection, respectively.

The :scheme and :path pseudo-headers are required by [RFC6455]. The scheme of the target URI MUST be set to "https" for both byte stream and datagram tunnels. The path is used in the same manner as for the WebSocket protocol, and MAY be set to "/" (an empty path component) if not desired for use.

Implementations should note that the Origin, Sec-WebSocket-Version, Sec-WebSocket-Protocol, and Sec-WebSocket-Extensions header fields are not included in the CONNECT request and response header fields, since this handshake mechanism is not being used to negotiate a WebSocket connection.

If the response to the extended CONNECT request indicates success of the handshake, then all further data sent or received on the new HTTP/2 stream is considered byte stream or datagram data.

3.2. Responding to the Extended CONNECT Handshake

A recipient of the extended CONNECT method follows the same procedure outlined by [RFC8441].

If the recipient encounters a :protocol pseudo-header with an unknown value or a value corresponding to a protocol they do not support, or if the recipient encounters violations of the extended CONNECT handshake protocol, they MUST return an HTTP response with an appropriate error code, such as 400 Bad Request. Otherwise, unknown header fields are ignored.

Once the handshake has been validated and is considered successful, the responder sends a HTTP response with status 200. After that response, all further data sent or received on the new HTTP/2 stream is considered byte stream or datagram data.

4. Using Tunnels Established via the Extended CONNECT Handshake

DATA frames are used as usual on the stream established by the CONNECT handshake to transmit data.
If the application negotiated the "bytestream" protocol, then individual DATA frames represent segments of an in-order bytestream and are delivered to the application as a stream of bytes. Implementations can deliver data to the application as soon as it becomes available, since there are no message boundaries to preserve.

If the application negotiated the "datagram" protocol, individual DATA frames are considered complete messages on the stream. Implementations SHOULD preserve these message boundaries when delivering data to the application. This prevents applications from needing to insert another level of framing to delineate message boundaries while transmitting datagram messages over HTTP/2 streams. Additionally, if an application is forwarding messages received over a "datagram" stream, the contents of each DATA frame should be sent in individual datagrams where possible.

The same considerations around intermediaries as defined in Section 7 of [RFC6455] apply to the extended CONNECT method, a client that connects via HTTP/2 to an HTTP proxy should use a traditional CONNECT request to tunnel through that proxy to the destination server. It should then

Streams created via the extended CONNECT method participate in flow control, stream prioritization, and other HTTP/2 features in the same manner as request and response streams defined in [RFC7540]. Stream closure continues to be interpreted as defined in Section 5 of [RFC8441].

Note that the frame type restrictions defined in Section 8.3 of [RFC7540] remain in effect: only DATA, RST_STREAM, WINDOW_UPDATE, and PRIORITY frames are allowed on the connected streams and any other frame types MUST be treated as a stream error (Section 5.4.2 of [RFC7540]) if received.

4.1. Example

An example of negotiating a "bytestream" stream on an HTTP/2 connection follows. This example is intended to closely follow the example in Section 5.1 of [RFC8441] to help illustrate the minor differences defined in this document.
HEADERS + END_HEADERS
:method = CONNECT
:protocol = bytestream
:scheme = https
:path = /
:authority = server.example.com

HEADERS + END_HEADERS
:status = 200

DATA
Byte Stream Data

DATA + END_STREAM
Byte Stream Data

5. IANA Considerations

This specification registers two entries in the "HTTP Upgrade Tokens" registry that was established by [RFC7230].

A new token, "bytestream", for byte stream data.

- Value: bytestream
- Description: Arbitrary bidirectional byte stream data
- Expected Version Tokens:
- References: [[RFC Editor: Please fill in this value with the RFC number for this document.]]

A new token, "datagram" for datagram data.

- Value: datagram
6. Security Considerations

The tunnels established by the CONNECT handshake are expected to be protected with a TLS connection. They inherit the security properties of this cryptographic context.

The security considerations of [RFC8441] Section 8 and [RFC7540] Section 10, and Section 10.5.2 especially, still apply to this use of the CONNECT method.

7. Acknowledgments

Thanks to Anthony Chivetta, Joshua Otto, and Valentin Pistol for their contributions in the design and implementation of this work.

8. Normative References


Authors' Addresses

Eric Kinnear
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Email: ekinnear@apple.com

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Email: tpauly@apple.com