WEBTRANS WG
IETF 122

Hybrid Meeting

Thursday, March 20, 2025

15:00 - 16:30 Bangkok Time

Session III, Boromphimarn 4

Mailing list: webtransport@ietf.org

MeetEcho: webtrans (ietf.org)

Notes: https://notes.ietf.org/notes-ietf-122-webtrans

This session is being recorded

IETF 122 Meeting Tips

In-person participants

- Make sure to sign into the session using Meetecho (usually the “Onsite tool” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

This session is being recorded

IETF 122 Remote Meeting Tips

- Enter the queue with  , leave with 
- When you are called on, you need to enable your audio to be heard.
- Audio is enabled by unmuting  and disabled by muting 
- Video can also be enabled, but it is separate from audio.
- Video is encouraged to help comprehension but not required.

Resources for IETF 122

- Information about IETF 122
  https://www.ietf.org/how/meetings/122
- Agenda
  https://datatracker.ietf.org/meeting/agenda
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Note well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

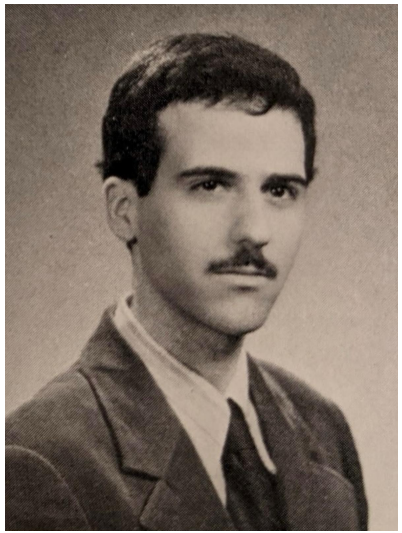
Note really well

- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need to confidentially raise concerns about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior -- in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

About this meeting

- Agenda: https://datatracker.ietf.org/doc/agenda-122-webtrans/
- Notes: https://notes.ietf.org/notes-ietf-122-webtrans
- WG Chairs: David Schinazi, Nidhi Jaju, Lucas Pardue
- Zulip Scribe:
- Note Takers: ?

In Memoriam: Bernard Aboba



Agenda

- Preliminaries, *Chairs* (15 minutes)
  - Note Well(s), Note Takers, Participation hints
  - Agenda Bash
- W3C WebTransport Update, *Will Law* (15 minutes)
- WebTransport over HTTP/2 and HTTP/3, *Victor Vasiliev, Eric Kinnear* (40 minutes)
  - https://datatracker.ietf.org/doc/html/draft-ietf-webtrans-http2
  - https://datatracker.ietf.org/doc/html/draft-ietf-webtrans-http3
- As Time Permits: Forward and Reverse HTTP/3 over WebTransport, *Ben Schwartz* (10 minutes)
  - https://datatracker.ietf.org/doc/html/draft-various-httpbis-h3-webtrans/
- Wrap up and Summary, *Chairs & ADs* (10 minutes)

W3C WebTransport Update (1 of 8)

W3C WebTransport WG progress since July 25 2024

- **Status:** Published a Working Draft - latest version 12 February 2025
- **Charter** current charter was extended to 31 December 2025.
- **Timetable** for year
  - May, 2025: Candidate for Recommendation - requires stability in API
  - July 2025: Proposed Recommendation - requires two independent implementations per our charter.
  - August 2025: Call for Review of a Proposed Recommendation
  - Sept 2025: Publication by W3C as a Recommendation after AC review
- **Milestone** status
  - Candidate Recommendation (86% complete, 9 open (6 ready-for-PR), 60 closed)
- **Annual TPAC meeting** will be held 10-14 Nov in Kobe.

W3C WebTransport Update (2 of 8)

Major decisions and updates since last IETF report (July 25 2024):

- **Redirection treated as a network error #612 -** any HTTP redirection response is treated as a network error and is indistinguishable from any 3XX,5XX error.

- **Add stats.atSendCapacity #603** - A value of false indicates the estimatedSendRate might be application limited, meaning the application is sending significantly less data than the congestion controller allows. A value of true indicates the application is sending data at network capacity, and the estimatedSendRate reflects the network capacity available to the application. When atSendCapacity is `true`, the estimatedSendRate reflects a ceiling.

- **Add protocols constructor argument to WebTransport + protocol read arg #59** -

W3C WebTransport Update (3 of 8)

Major decisions and updates since last IETF report (July 25 2024):

- **Add protocols constructor argument to WebTransport + protocol read arg #598**

```
const wt = new WebTransport(url, {protocols: ["moqt", "mychat"]});
try {
  await wt.ready;
  console.log(wt.protocol); // "moqt", "mychat" or ""
} catch (e) {
  if (e.name != "WebTransportError") throw;
  // server rejected connection, possibly over unsuitable protocol
}
```

- **Adjust estimatedSendRate definition to exclude framing overhead #632**
  The estimatedSendRate statistic now specifies that it "*excludes any framing overhead and represents the rate at which an application payload might be sent.”*

W3C WebTransport Update (4 of 8)

Major decisions and updates since last IETF report (July 25 2024):

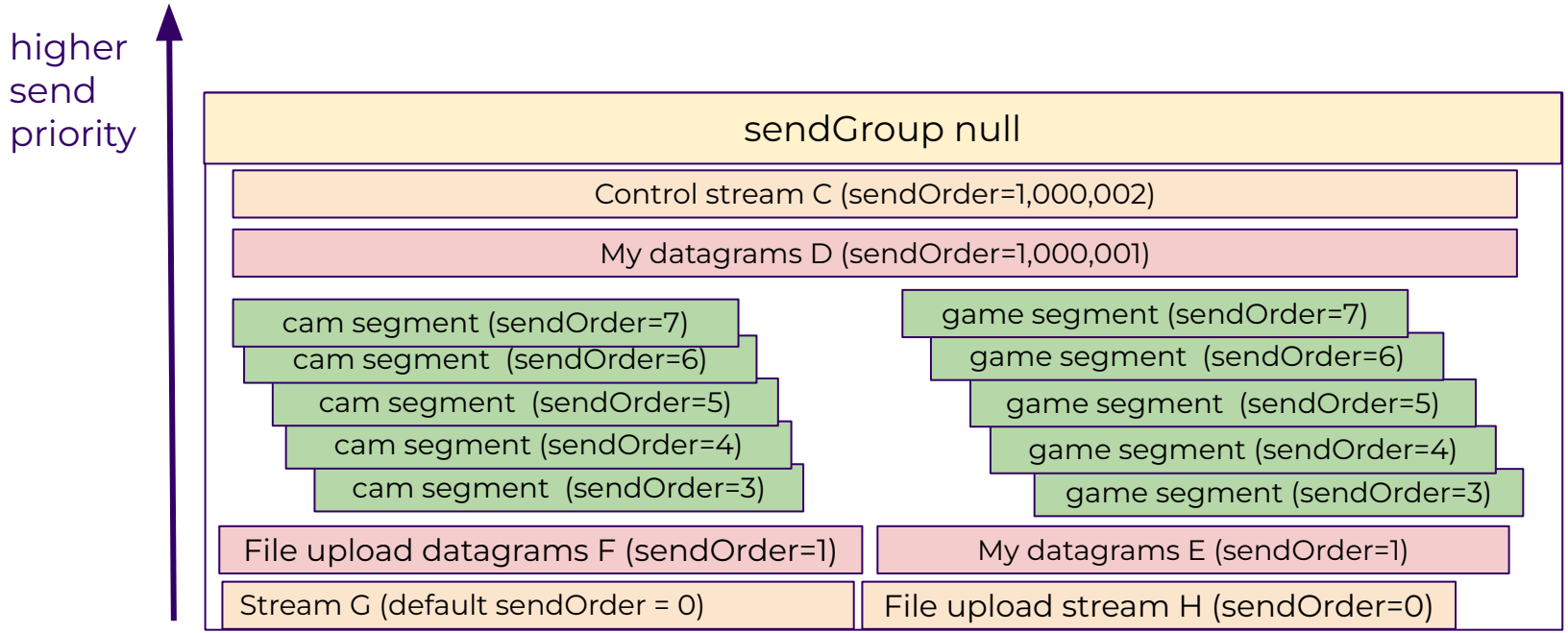
- **Add datagrams.createWritable({sendGroup, sendOrder}) #629**
  Consider removing wt.datagrams.writable #624 (decision: yes, ready for PR)

```
const wt = new WebTransport(url);
await wt.ready;
console.log(wt.datagrams.writable); // undefined
const audioDatagrams = wt.datagrams.createWritable();
const videoDatagrams = wt.datagrams.createWritable();

await Promise.all([
  audioDatagramsProducer.pipeTo(audioDatagrams);
  videoDatagramsProducer.pipeTo(videoDatagrams);
]);
```

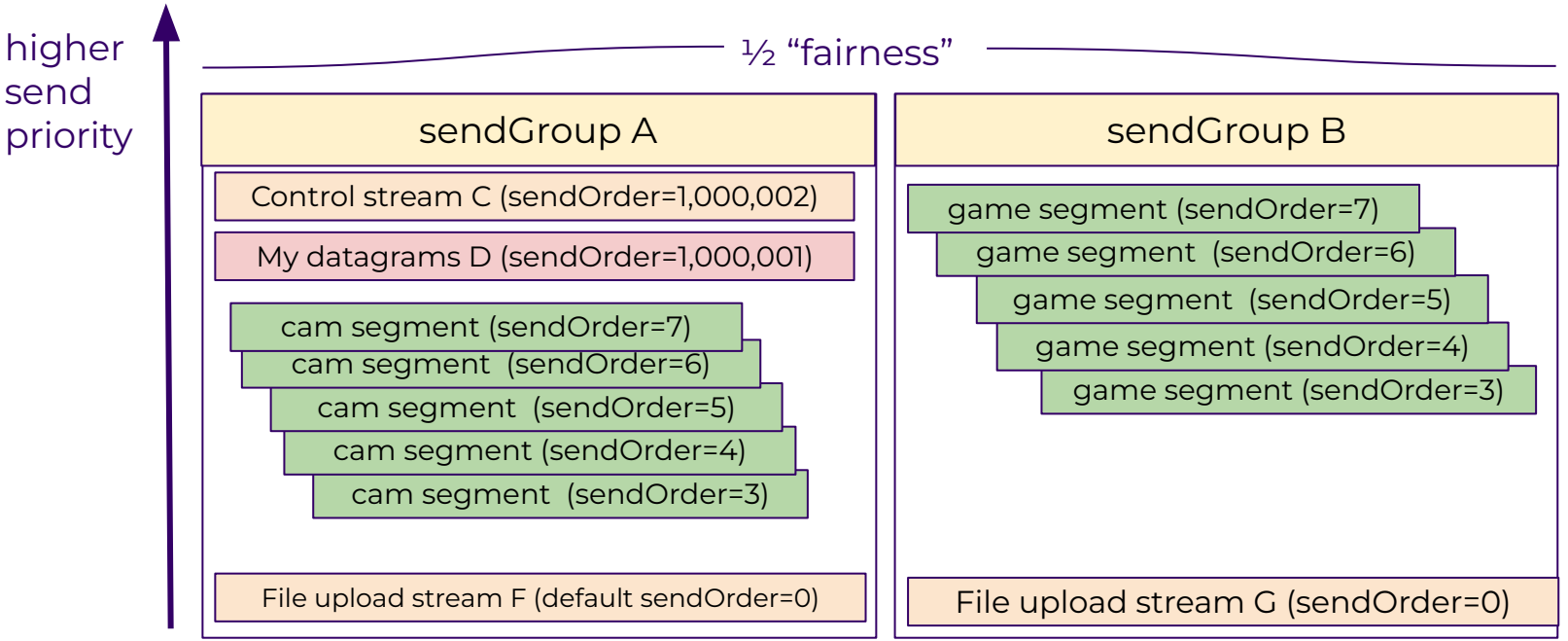
Prioritization example with default null sendGroup, resulting in strict priorities between all streams and datagrams

```
const C = wt.createUnidirectionalStream({sendOrder: 1,000,002});
const D = wt.createDatagramsWritable({sendOrder = 1,000,001});
const E = wt.createDatagramsWritable({sendOrder=1});
const F = wt.datagrams.createWritable({ sendOrder=1}); const G = wt.createUnidirectionalStream();
const H = wt.createUnidirectionalStream();
```



Relative prioritization of streams and datagrams using sendOrder and sendGroups

Multiple sendGroups allow for parallel flows of data, with bandwidth fairly shared between them. Within the sendGroups strict priorities can still be applied between streams and datagrams



W3C WebTransport Update (5 of 8)

Browser support as of March 2025

WebTransport - WD

Usage % of all users ?

Global 78.28%

Limited availability across major browsers

Protocol framework to send and receive data from servers using HTTP3. Similar to WebSockets but with support for multiple streams, unidirectional streams, out-of-order delivery, and reliable as well as unreliable transport.

Current aligned | Usage relative | Date relative | Filtered | All

Chrome	Edge *	Safari	Firefox	Opera	IE	Chrome for Android	Safari on iOS *	Samsung Internet	Opera Mini *	Opera Mobile *	UC Browser for Android	Android Browser *	Firefox for Android	QQ Browser	Baidu Browser	KaiOS Browser
4-90																
91-94																
95-96	12-97		2-113	10-82				4-17.0								
97-132	98-132	3.1-18.2	114-134	83-113	6-10		3.2-18.2	18.0-26		12-12.1		2.1-4.4.4				2.5
133	133	18.3	135	114	11	133	18.3	27	all	80	15.5	133	135	14.9	13.52	3.1
134-136		18.4-TP	136-138				18.4									

Notes | Test on a real browser | Known issues (2) | Resources (6) | Feedback

All major browser engines are working on implementing this spec.

W3C WebTransport Update (6 of 8)

Here are the remaining core issues to be resolved

1. Is CORS preflight necessary for WebTransport if we add header support? #637

   Our understanding is that the one original reason for CORS was to protect legacy servers in the case of plain HTTP. Can a request be recognized as a regular HTTPS request? No for WebTransport, yes for WebSocket.

   Today, neither Chrome nor Firefox implement CORS Preflight with WebTransport or WebSockets. Both include a Protocols Header that is sent at connection time.

   If we allow ad-hoc application headers to be sent, does the requirement change?

W3C WebTransport Update (7 of 8)

Here are the remaining core issues to be resolved

2. Consider removing serverCertificateHashes#623 - are they safe?

Arguments for removal of `serverCertificateHashes`

1. **Security risk / parallels to Web Push**
   A repeat of the “shared private key” problem, where people distribute the same private key widely (e.g. across many devices) as a quick hack. That undermines real security, because anyone who gets that key can intercept or impersonate the endpoint.
2. **Local dev alone does not justify a new API**
   The original motivation—local testing or development—might not meet a high bar for web platform features.
3. **Need a broader, not per-API, solution**
   Since the real problem is local HTTPS or ephemeral cert usage, solving it for just WebTransport may be short-sighted. They suggest the web platform should address local HTTPS in a more unified way.
4. **No buy-in from some UA engines**
   WebKit says it will not implement it, while Chrome and Mozilla are in favor of retaining serverCertificateHashes and have implemented support.

Arguments in favor of keeping `serverCertificateHashes`

1. **Needed for local network / ephemeral scenarios**
   See a strong use case for locally hosted devices that cannot easily get publicly valid certificates (e.g. local network cameras, ephemeral cloud VMs). Certificate pinning by hash works around the usual DNS + CA approach.
2. **No worse than typical cert usage**
   In practice, PKI certificates often reuse private keys, and short-lived certs can mitigate abuse. They argue that “shared private keys” is already possible with publicly trusted certs, so removing hash-based pinning doesn’t eliminate that risk.
3. **WebRTC parity**
   WebRTC (which is peer-to-peer) also uses a certificate-based identity. In principle, it is not so different to let WebTransport connect to a non-publicly trusted endpoint—just a client–server version of that.
4. **Developer experience**
   People want to avoid forcing developers to jump to WebRTC or unencrypted local HTTP. They say that by removing `serverCertificateHashes`, you might drive developers to worse security (plain HTTP or complicated setup).

- There is talk of limiting `serverCertificateHashes` to local networks only, or gating it behind a CSP directive, or removing it from version 1 of the spec. No conclusion has been reached.
- The group is currently waiting on more security-focused feedback and additional vendor input before deciding.

W3C WebTransport Update (8 of 8)

3. Exposing headers of the CONNECT response #264

   Do we want to allow web developers to add headers of the CONNECT request? #263

```
const wt = new WebTransport(url, {headers: {foo: 'bar'}});
const response = await wt.ready;
for (const [name, value] of response.headers.entries()) {
  ...
}
```

Do you want this capability for your applications?

WebTransport Open Issues

Victor Vasiliev, Eric Kinnear

https://datatracker.ietf.org/doc/draft-ietf-webtrans-http3/

https://datatracker.ietf.org/doc/draft-ietf-webtrans-http2/

https://datatracker.ietf.org/doc/draft-ietf-webtrans-overview/

#172 Subprotocol Negotiation

- In QUIC, we made ALPN mandatory to avoid protocol confusion attacks
- Should the new mechanism we're introducing for WebTransport be mandatory as well?

#172 Subprotocol Negotiation

- In QUIC, we made ALPN mandatory to avoid protocol confusion attacks
- Should the new mechanism we're introducing for WebTransport be mandatory as well?
- Victor: Already shipped some code
- Victor: HTTP resources are identified by URIs, which are different from QUIC endpoints (that only have host and port)

#150 Negotiation of flow control

- Pooling is necessary to make good decisions around prioritization
- Flow control provides the backpressure to enforce those decisions
- Flow control is as optional as pooling
- Additional mechanism for negotiation?

#150 Negotiation of flow control

- One option
  - Have the client send MAX_SESSIONS (again)
  - If either end is >1, flow control is happening
  - If either side is just 1, no flow control
  - If 0, no WebTransport

#150 Negotiation of flow control

- One option
  - Have the client send MAX_SESSIONS (again)
  - If either end is >1, flow control is happening
  - If either side is just 1, no flow control
  - If 0, no WebTransport
- Do we need this?

#179 Requirements on final size

- Section 4.5 of QUIC provides text about knowing how much data a stream consumed when its closed
- All sides need to agree

#179 Requirements on final size

- We say

```
Implementing WT_MAX_DATA requires that the QUIC
stack provide the WebTransport implementation with
information about the final size of streams
```

- Are all implementations comfortable with the requirement?
- Does it have W3C implications?

Open HTTP/2 Issues

This slide intentionally left blank.

Wrap-up, and Summary

David Schinazi
Nidhi Jaju
Lucas Pardue

Next steps

- Merge some PRs
- Write some Code
- Editorialize some Drafts
- WGLC all the Things
- Profit

Thank you

Special thanks to:

The Secretariat, WG Participants & ADs

Thank you