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 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)
Agenda

Welcome & Status Updates (10 min.)

Documents (5 min.)

Workshops (5 min.)

Programs (20 min.)

Open Mic (10 min.)
What's IABopen?

IAB organized session focusing on technical and architectural aspects

Goals

Increase visibility of the work the IAB is doing

Collect feedback and community input to on-going and new work
Mailing lists to use

architecture-discuss@iab.org for architectural discussions and IAB documents

iab@iab.org for comments and concerns directly to the IAB

Program mailing lists for direct comments on work of a specific program
IAB virtual retreat

In preparation: Internal IAB survey about challenges and opportunities for the IAB, as well as general trends

June 1-5: 3x 1h all-IAB meetings + break-out groups:

• Architectural guidance
• Mission of the IAB: strategic/long term issues of the Internet
• COVID-19: Impact on technical work
• COVID-19: Impact on the IETF working model
• Technical factors related to deployment of increased security
• Impact/disruptions by other parties
• Evaluate/review the success of the IETF

Social interactions based on 3 coffee breaks/happy hour slots on each Tuesday and Thursday (joint with IESG)

Documents

Active IAB Documents

- draft-iab-for-the-users (in RFC editor queue) - see next
- draft-iab-dedr-report (workshop report)

Recently published IAB Documents (2019/2020)

- RFC 8546: The Wire Image of a Network Protocol
- RFC 8558: Transport Protocol Path Signals
- RFC 8752: Report from the IAB Workshop on Exploring Synergy between Content Aggregation and the Publisher Ecosystem (ESCAPE)
The Internet is for End Users
draft-iab-for-the-users

“This document explains why the IAB believes that, when there is a conflict between the interests of end users of the Internet and other parties, IETF decisions should favour end users. It also explores how this can more effectively be achieved.”

- August 2015: Started as individual I-D
- August 2019: Adopted by IESG
- March 2020: Approved by the IAB

Community review helped shape the document:
- More clearly identify as suggestions from the IAB
- Expand suggestions for how to better represent user needs

Next steps?
Workshops

Recent Workshops

• IAB workshop on Design Expectations vs. Deployment Reality in Protocol Development (DEDR), June 2019

Proposed Workshops

• IAB workshop on COVID-19 Network Impacts, virtual, Nov 2020

“Report from the IAB workshop on Design Expectations vs. Deployment Reality in Protocol Development”
(draft-iab-dedr-report-00.txt)

Report authors: Jari Arkko & Ted Hardie
- highly influenced by notes from Jim Reid, Geoff Huston, etc

IETF 108 IABOPEN
Reason for this discussion

Ask for reviews before we publish it as an RFC

• Any feedback or missing pieces?
• In particular, if you were there, can you review?
• Workshops typically have public reports/conclusions (this draft) and the any position papers that were submitted (21 in this case, see https://www.iab.org/activities/workshops/dedr-workshop/)

More general thoughts about deployment expectations topic can be discussed too

• But maybe a better topic for the architecture-discuss list or the open discussion part of this meeting
Workshop Topic

Often, Internet technology development has presumed specific deployment models

But actual deployments often differ

• Impacted by economies of scale, DDoS resilience, market consolidation, etc.

• Resulting in an impact on interoperability, centralisation, etc.

• Generally, interesting interaction between economics, technology, and deployments

Workshop agenda
i. Experiences
ii. Principles
iii. Centralised deployment
iv. Security
v. Future
Some Conclusions

The non-surprising confirmation that technologies sometimes get deployed in surprising ways. Economics!

There are also technical issues that make things harder, e.g., lack of DDoS defence or micropayments solutions

Architecture work: Threat model? Continue discussion of centralization? Document principles (e.g., re-application of e2e principle)?

Technical work: Reputation systems? Tools to limit certificate scopes? E2e encryption for apps?
Thank you!

Questions, comments, feedback, interest?
COVID-19 Network Impacts Workshop

Organizing Committee:
Jari Arkko, Stephen Farrell, Cullen Jennings,
Colin Perkins, Ben Campbell, Mirja Kühlewind

IETF 108 IABOPEN
Background

The pandemic has had a tremendous impact on all of us, but also on networking.

Large numbers of people working from home or otherwise depending on the network for their daily lives, network traffic has surged.

- ISP, mobile operator, and IXP traffic growth
- Conversational multimedia traffic and #users growth

Internet has coped relatively well (but not perfectly) with this traffic growth. Many things changed, however.
Goals

Learn about traffic patterns and their changes

It is interesting to see how the technology, operators and service providers have responded to large changes in traffic patterns

This is an opportunity to share our understanding of what the impacts where, what type of actions were needed, what worked and what didn’t, etc.

Perhaps also an opportunity to learn for future
Topics in Scope

Measurements about traffic, user experience, performance, and other relevant aspects

Discussion about the behind-the-scenes network management and expansion activities

Experiences in general connectivity, conferencing, media/entertainment, and Internet infrastructure

Lessons learned for preparedness and operations

Lessons learned for Internet tech and architecture
Tentative logistics

This is an over-the-Internet virtual workshop

• Several sessions will be scheduled for the different topics on the week of November 9, 2020 (one week before IETF-109)

Participation is by invitation, based on position paper submissions

• Submissions Due: 9 October 2020

• Invitations Issued by: 15 October 2020
Thank you!

Questions, comments, feedback, interest?
IAB technical programs

Active:

• Internet Threat Model (model-t) Program

Recently concluded (2019):

• Privacy and Security (privsec) Program
• IP Stack Evolution (stackEvo) Program

Currently under discussion:

• Proposed Program on Evolvability, Deployability, and Maintainability (EDM)
Internet Threat Model (model-t) Program

Jari/Stephen “helping”
• Sadly, this time around, nothing much happened;-(
• Had a good call April 20th but lack of follow up (mea culpa mostly)

Planning to do a virtual meeting soon – will start to schedule on the list this week
Anyone about this Thursday 30th at 1610 UTC – let’s meet for an informal chat?
• Details of both the above will be on list

Goal: consider evolution of threat model and possibly offer updates to BCP72 for IETF consideration


List: https://www.iab.org/mailman/listinfo/model-t

Despite my utter inactivity as a helper, a bunch of people have written/revised/split drafts...
Drafts being discussed

draft-thomson-tmi

draft-mcfadden-smart-endpoint-taxonomy-for-cless

draft-mcfadden-smart-threat-changes

draft-lazanski-protocol-sec-design-model-t

draft-lazanski-users-threat-model-t

draft-arkko-farrell-arch-model-t

draft-arkko-farrell-arch-model-t-7258-additions

draft-arkko-farrell-arch-model-t-3552-additions
Evolvability, Deployability, & Maintainability

Proposed IAB Program
Evolvability

Design for greasing
draft-iab-use-it-or-lose-it,draft-iab-protocol-maintenance
QUIC greasing, HTTP greasing

Explain extension points
e.g., RFC 5507 Design Choices When Expanding the DNS

Which are preferred
Which are stable or ossified

Encourage practices for codepoint allocations that make extension easy
Deployability

Allow working groups to track running code

Catalog implementations and versions

Interoperability results

Active experiments
### TLS 1.3 Implementations

<table>
<thead>
<tr>
<th>name</th>
<th>language</th>
<th>role(s)</th>
<th>version</th>
<th>features/limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fizz</td>
<td>C++</td>
<td>C/S</td>
<td>RFC 8446</td>
<td>Based on libsodium, includes secure design abstractions. Zero-copy for advanced performance.</td>
</tr>
<tr>
<td>NSS</td>
<td>C</td>
<td>C/S</td>
<td>RFC 8446</td>
<td>Almost everything, except some crypto primitives</td>
</tr>
<tr>
<td>Mint</td>
<td>Go</td>
<td>C/S</td>
<td>-18</td>
<td>PSK resumption, 0-RTT, HRR</td>
</tr>
<tr>
<td>nqsb</td>
<td>OCaml</td>
<td>C/S</td>
<td>-11</td>
<td>PSK/DHE-PSK, no EC*, no client auth, no ORTT -- live server at tls13test.nqsb.io port 4433, records traces, ping @hannesm, contains a static PSK/DHE_PSK token: id: 0x0000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶ secret:</td>
</tr>
<tr>
<td>ProtoTLS</td>
<td>JavaScript</td>
<td>C/S</td>
<td>-13</td>
<td>EC/DHE/PSK, no HelloRetryRequest</td>
</tr>
<tr>
<td>mTLS</td>
<td>F*</td>
<td>C/S</td>
<td>RFC 8446</td>
<td>EC/DHE/PSK/0-RTT, no RSA-PSS, no post-HS-auth, no ESNI</td>
</tr>
<tr>
<td>Tris</td>
<td>Go</td>
<td>C/S</td>
<td>RFC 8446</td>
<td>ECDHE/PSK/0-RTT, no HelloRetryRequest</td>
</tr>
<tr>
<td>BoringSSL</td>
<td>C</td>
<td>C/S</td>
<td>-23, -28, RFC 8446</td>
<td>P-256, X25519, HelloRetryRequest, resumption, 0-RTT, KeyUpdate</td>
</tr>
<tr>
<td>Wireshark</td>
<td>C</td>
<td>other</td>
<td>-18 to -28, RFC 8446</td>
<td>Full decryption and dissection support for drafts 19-21 since 2.4.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(keylog format). Supports 18-21 since 2.4.2, -22 since 2.4.3, -23 since 2.4.5, -24 to -28 (+0RTT trial decryption) since 2.6.0. Tracking bug.</td>
</tr>
<tr>
<td>picots</td>
<td>C</td>
<td>C/S</td>
<td>-18,-21,-23,-26</td>
<td>P-256, X25519, HelloRetryRequest, resumption, 0-RTT</td>
</tr>
<tr>
<td>rustls</td>
<td>Rust</td>
<td>C/S</td>
<td>-28 (final on branch)</td>
<td>P-256/P-384/curve25519, HRR, resumption, 0-RTT client</td>
</tr>
<tr>
<td>Haskell tls</td>
<td>Haskell</td>
<td>C/S</td>
<td>-28</td>
<td>ECDHE w/ P* and X*, full, HRR, PSK, ORTT</td>
</tr>
</tbody>
</table>
Implementations
Alessandro Ghedini edited this page on Jun 23 - 415 revisions

This wiki tracks known implementations of QUIC. See also our Tools listing. Current interop status; make sure you are looking at or editing the correct tab.

Please add your implementation below. Keep sorted alphabetically. There are three sections, one for "IETF QUIC Transport", one for "IETF HTTP over QUIC", and one for "QPACK". Entries may appear in multiple sections e.g. where a stack provides both IETF QUIC Transport and IETF HTTP over QUIC.

Note
If you are working on a QUIC implementation, please consider joining the QUIC Developers Slack Channel. Also, if possible, please set up a public server and publish its details below, so others can try and interoperate with your code.

IETF QUIC Transport
The following stacks implement the IETF versions of QUIC Transport. They may include an application layer mapping other than IETF HTTP over QUIC e.g. HTTP/0.9

aioquic
QUIC implementation using Python and asyncio.

- **Language:** Python
- **Version:** draft-29
- **Roles:** client, server, library
- **Handshake:** TLS 1.3
- **Protocol IDs:** 0xff00001d, 0xff00001c

  - **Public server:**
    - quic.aiortc.org:443
    - quic.aiortc.org:4434 (Stateless Retry)

AppleQUIC
AppleQUIC is a client and server implementation.
The following are known prototype implementations of draft-ietf-dnsop-svcb-https

Note some prototypes started off using TYPE65479 and other private types but are now switching over to the production types now that the wire format is stable.

Please feel free to submit PRs to update this page.

**Production / shipped implementations**

(TBD)

**Work-in-progress and prototype implementations**

**BIND9**

*Work-in-progress implementation for BIND9*

- Author: Mark Andrews <marka@isc.org>
- Tracker: BIND9 GL 1132
- Version: Implement draft-ietf-dnsop-svcb-https-01 (work-in-progress) **Previous versions implemented draft-nygren-httpbis-httpssvc-02 (and -01) and draft-nygren-dnsop-svcb-httpssvc-00 **Previous versions used TYPENN of HTTPS/65482 and SVBC/65481

**Unbound**

- Prototype of draft-nygren-httpbis-httpssvc-02 during IETF 105 hackathon

**dnspython**

*Work-in-progress implementation for dnspython.*

**Others**
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>h2o/quick</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>quant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>ngtcp2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>mvfst</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>picoQUIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>msquic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>f5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>f5_test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>ATS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>quiche</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>lquic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>nginx-cloudflare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>AppleQUIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>quic-go</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Quinn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>AkamaiQUIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>aioQUIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>--gQUIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Kwik&amp;Flupke</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Maintainability

Support a community of implementers

Current deployment practices

  Non-RFC content: wikis and FAQs

  Discussion venues

What happens when a working group closes?
TLS Testing Resources

This page lists correctness and safety testing resources for TLS implementations and related software dependencies. It excludes implementation-specific tests.

Note that there is no official conformance test suite.

- **badssl** - Insecure and uncommon server configurations
- **BoGo** - Test harness for (D)TLS, supported by BoringSSL and NSS. See [PORTING.md](#) for information about supporting other implementations.
- **TLS Attacker** - TLS-Attacker is a Java-based framework for analyzing TLS libraries.
- **tlsfuzzer** - Fuzzer and test suite for TLS (SSLv2, SSLv3, v1.0, v1.1, v1.2, v1.3) implementations.
- **Frankencerts** - Specially crafted certificates for testing certificate validation code in TLS implementations.

The following tools lists may help identify features or properties of different TLS implementations:

- **SSL Labs Browser and Server Tester** - Browser-based tool for checking features of TLS servers and browser implementations.
Tasks

Get representatives from IESG, Tools Team, broader community

Review successful models in working groups

Review cases where protocols struggle
Output

Write documents
Hold workshops
Build new IETF tools
Provide guidance for WGs and IETF reviews
Open Mic

How did you like the IABopen session? Should we do it again? Is it useful?

What would you expect from future IABopen meeting?

Other technical comments or feedback on the IAB work or Internet architecture in general?