IETF Year in Review for 2020

ICANN Office of the Chief Technology Officer

Paul Hoffman
OCTO-022
21 January 2021

ICANN

TABLE OF CONTENTS

This document is part of ICANN's Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This document supports ICANN's strategic goal to support and grow active, informed, and effective stakeholder participation. It is part of ICANN's strategic objective to improve the effectiveness of ICANN's multistakeholder model of governance.

1 Introduction

This document is an informal overview of the activities in the Internet Engineering Task Force (IETF) during 2020 that are of most interest to ICANN. The primary audience is those in the greater ICANN community who are interested in the technical side of ICANN's remit but do not actively follow the IETF. Thus, the coverage of what the IETF has done is fairly narrow; a document like this prepared for a different organization such as a large company would have a very different focus.

Readers who want more background on the IETF should see "The Tao of the IETF" and the introductory material on the IETF website. Links in this document for working groups are in the IETF Datatracker; readers who want to browse IETF working groups, Internet-Drafts, RFCs, meetings, and so on should explore the Datatracker.

In keeping with the IETF working model, participation by ICANN staff at IETF meetings is on an individual basis, not necessarily representing the interests of the ICANN org or community. If there are questions or comments regarding this document, please send email to octo@icann.org.

2 IETF Meetings in 2020

Under normal circumstances, the IETF has physical meetings three times a year in various parts of the world. This year, all meetings were held virtually. All three meetings were held during business hours for the locations in which they had originally been scheduled. The meetings used Meetecho for all online participants, just as they had done for many years before the pandemic.

2.1 IETF 107, March 2020

The IETF 107 meeting was scheduled for Vancouver. There were 701 attendees. The lower-than-average attendance for IETF 107 was probably due to the last-minute change from being a face-to-face meeting, but also due to a limited agenda focused on new working groups and birds-of-a-feather (BoF) sessions. Many working groups held virtual interim meetings after IETF 107, and reviews of those virtual interims were mixed.

2.2 IETF 108, July 2020

The IETF 108 meeting was scheduled for Madrid. There were 1,120 attendees, which is a bit below the typical attendance of an IETF meeting in the summer in Europe. The agenda was fairly full, and the general consensus was that the online meeting went well with only minor technical issues.

2.3 IETF 109, November 2020

The IETF 109 meeting was scheduled for Bangkok. There were 1,285 attendees, which is about normal for an IETF meeting in Asia. Like IETF 108, the meeting went fairly well, and improvements in the Meetecho system, such as a better mechanism for raising hands, and better recovery from connection problems, made the working group sessions more like normal face-to-face meetings.

3 Primary Working Groups and BoFs

This section covers the primary IETF working groups of interest to ICANN. In this case, interest is measured by the active participation of ICANN org staff in specific working groups.

3.1 DNSOP

The DNS Operations (DNSOP) Working Group is responsible for most of the DNS-related work in the IETF. Although the name indicates that it is only about operations, most new DNS protocol work is done in the DNSOP Working Group as well.

During 2020, DNSOP was responsible for seven RFCs:

- RFC 8749, "Moving DNSSEC Lookaside Validation (DLV) to Historic Status," is a minor document that formally retires DLV, which was a feature of DNS that was developed before DNSSEC was fully deployed and helped establish a chain of trust for DNSSEC validation prior to the root being signed in July 2010. With the signing of the root, DLV no longer provided any significant benefit.
- RFC 8767, "Serving Stale Data to Improve DNS Resiliency," is a new standard that describes how resolvers can be made more resilient in the face of denial-of-service (DoS) attacks against authoritative servers. Resolvers that implement this method will be able to keep serving data that has been cached longer than the time to live (TTL) assigned to the data by the zone administrator when the zone can no longer be queried. Because zone data typically does not change frequently, this feature balances the value of giving answers that are likely to be correct during attacks against the chance of inadvertently giving answers that were correct earlier but had been updated by the zone administrator while the zone's distribution servers were unreachable.
- RFC 8806, "Running a Root Server Local to a Resolver," is a revised standard that describes how resolvers can act as local root servers in order to increase privacy and give faster responses for some queries. This is sometimes called "hyperlocal root service." RFC 8806 replaces RFC 7706 with clearer descriptions and up-to-date examples. It is co-authored by ICANN's Paul Hoffman.
- RFC 8901, "Multi-Signer DNSSEC Models," is an informational document that describes many of the issues that organizations face if they sign their zones with DNSSEC and also have multiple DNS hosting providers. A major impetus for this document is that it is difficult to get DNS providers to coordinate the records required for DNSSEC signing, and this leads to some organizations choosing not to sign their zones.
- RFC 8906, "A Common Operational Problem in DNS Servers: Failure to Communicate," is a new standard that describes how authoritative servers should respond to queries for which there is no data. This RFC was needed because some servers give confusing or misleading replies due to unclear requirements in earlier RFCs.
- RFC 8914, "Extended DNS Errors," is a new standard extension to DNS that allows authoritative servers to provide, and resolvers to get, extra information in responses about the cause of errors. This extra information is particularly useful for DNSSEC, where many errors currently use the same code, but is also valuable in many other

situations in which a client can use the error information to determine whether to send queries to additional servers or resolvers. It is co-authored by ICANN's Roy Arends.

- RFC 8945, "Secret Key Transaction Authentication for DNS (TSIG)," updates and clarifies the earlier definition of this protocol that is used for in-band authentication between primary and secondary authoritative servers and for dynamic DNS updates.

3.2 DPRIVE

The DNS PRIVate Exchange (DPRIVE) Working Group covers issues related to adding privacy to the DNS. It is the working group in which DNS over TLS (DoT) was developed. Recently, it has focused more on privacy in DNS operations.

During 2020, DPRIVE produced just one RFC:

- RFC 8932, "Recommendations for DNS Privacy Service Operators," is a standard that lists many considerations for resolver operators who offer DoT or DNS over HTTPS (DoH) to their clients. Although it focuses on privacy, it also covers various policy issues such as publishing a formal operator privacy statement and how to handle data stored in the resolver's logs and operational considerations, such as updating certificates and monitoring increased resource use.

3.3 REGEXT

The Registration Protocols Extensions (REGEXT) Working Group is the main place where extensions to the Extensible Provisioning Protocol (EPP) are developed. EPP is the standard way for registries and registrars to communicate, so EPP extensions are of particular interest to ICANN. The working group also covers the Registration Data Access Protocol (RDAP).

During 2020, three RFCs came out of REGEXT:

- RFC 8748, "Registry Fee Extension for EPP," is a new standard extension that describes various financial fees and credits that are associated with billable transactions between registries and registrars.
- RFC 8807, "Login Security Extension for EPP," is a new standard that gives better security in EPP logins from clients, such as allowing for longer passwords and specifying security events associated with each login.
- RFC 8909, "Registry Data Escrow Specification," is a new standard that describes how data escrow deposits from domain name registries are formatted and handled. It can also be applied to other types of registry data that is escrowed. It is authored by ICANN's Gustavo Lozano.

3.4 ADD

The Adaptive DNS Discovery (ADD) Working Group was chartered in February 2020, but the issues it covers have been talked about for a long time. The core of the ADD charter states, "This working group will focus on discovery and selection of DNS resolvers by DNS clients in a variety of networking environments, including public networks, private networks, and VPNs, supporting both encrypted and unencrypted resolvers."

So far, the working group has made limited progress. There have been many proposals for mechanisms for resolver discovery, but little agreement on the use cases. Currently, the working group is wrestling with concepts such as what it means for two resolvers to be "equivalent" and how network administrators provision users of their networks.

4 Leadership, Administration, and Other Activities

4.1 IESG and IAB

In the fall of each year, approximately half of the Internet Engineering Steering Group (IESG) and half of the Internet Architecture Board (IAB) are selected through a Nominating Committee (NomCom). The IETF NomCom is selected at random from volunteers who have attended at least three of five previous IETF face-to-face meetings, although this criterion is being adapted due to the current lack of face-to-face meetings. The IETF NomCom also selects members for other boards and committees that are related to the IETF's work.

Alissa Cooper, the IETF Chair since 2017, chose not to stand for nomination again. This brought out seven candidates from many parts of the IETF to replace her; Lars Eggert from NetApp was selected. Most of the area directors that were up for renewal indicated that they wanted to continue, and were renewed. A total of 16 people applied for the six open slots on the IAB; the three new members are David Schinazi from Google, Deborah Brungard from AT&T, and Russ White from Juniper.

4.2 IETF Hackathon

At face-to-face meetings, the IETF Hackathon attracts hundreds of developers who are working on a variety of IETF standards to come together to code, design, and test existing or emerging Internet standards, helping ensure that IETF standards are implementable. In the past few years, the DNS community has been well-represented at the hackathons. A common theme has been to be sure that protocols that are near completion actually work as described, and to find edge cases that need to be documented before the protocols are standardized. ICANN has helped sponsor these events in the past.

In 2020, the virtual IETF Hackathons have attracted much less interest, probably due to the joy of being in a big room with other like-minded folks who one can chat with while working. The DNS community still shows a strong interest, particularly for writing code for protocols under development.

5 Expected Activities of Interest During 2021

It is difficult to make long-term predictions about the IETF and its activities because of shifting trends in Internet traffic, unexpected security threats, changes in the ways that billions of Internet users access their favorite content, and now, the pandemics. Thus, this section focuses only on short-term, one-year predictions that relate to IETF work that is of most interest to ICANN.

5.1 Plans for Future IETF Meetings

Like other standards development organizations, the IETF has become quite reliant on face-to-face meetings for making progress on its work. Although the latter two virtual meetings of the year were more productive than the first, many working groups are making slower progress than in previous years, and many attribute this to the lack of face-to-face meeting, particularly the lack of hallway discussions. However, some working groups are reporting faster progress because they are feeling less constrained by the timing of face-to-face meetings. The IETF follows RFC 8719, “High-Level Guidance for the Meeting Policy of the IETF,” in its scheduling of all meetings, including the virtual ones.

The IETF leadership is spending a lot of effort to determine how to deal with virtual meetings in the future. Surveys taken after the meetings show widely divergent views about having fewer face-to-face meetings even after the pandemic is over, the value of interim meetings, and so forth. Different working groups have adopted very different work styles, which heavily influences their desires for face-to-face meetings, virtual meetings that might be at difficult times, and more work on the mailing lists. After IETF 109, the IETF published an interesting retrospective about the evolving technical aspects of holding remote IETF meetings.

At the time this document is published, IETF 110 will be online in March 2021. It was scheduled for Prague, one of the most popular venues for IETF meetings, with the meetings being held from 1200 to 1800 UTC every day. IETF 111 is still scheduled for San Francisco in July 2021, and IETF 112 is still scheduled for Madrid in November 2021.

5.2 Working Group Activities

The DNSOP Working Group has over a dozen documents for which it has agreed to work on, and has a handful more waiting to be adopted. There is no overall theme for the work: it includes operational issues such as zone transfers, privacy enhancements, private use names, new DNSSEC algorithms, and many others. ICANN org staff are active in the working group as both document authors and reviewers.

The REGEXT Working Group is working on numerous documents about RDAP and further extensions to EPP, some of which should be finished in early 2021. There are many other documents ready for working group adoption as well. ICANN org staff are particularly active in the working group as authors of extensions used in current contracts, and participate in the development of new extensions that may be required in future gTLD contracts.

The DPRIVE Working Group has forthcoming RFCs on adding privacy to zone transfers, and on general privacy issues for DNS. The working group is discussing possibly extending privacy between resolvers and authoritative servers using DoT, although the working group’s progress is quite slow in all areas. ICANN org staff are active in promoting this future work in order to reduce the amount of user-identifiable data leaked in the normal use of the DNS.

The ADD Working Group is still trying to find where there is consensus about the use cases for discovering resolvers. If the working group succeeds at that, it will likely be documented in an

RFC that could come out in 2021. The working group would then have to narrow down discussion of protocols that meet those use cases, and probably discuss about the value and cost of having multiple protocols.

5.3 Other Protocols

The much-discussed QUIC protocol is tangentially related to ICANN's core work, but will probably be used by DNS-related protocols after it is standardized this year. Finalizing QUIC brings up the question of whether we should expect DNS-over-QUIC to be finished in the DPRIVE Working Group, or if there is interest in "DNS-over-HTTP-over-QUIC". It is too early to tell whether there is much interest from applications and operating system vendors to go with one or both of these variants, or whether the vendors want to stay with DoT and DoH until they know more about the operational effects of encrypted DNS.