Council of European National
Top-Level Domain Registries

# IETF 115

100-plus working group sessions, 2 technology deep dive sessions, a 2-day IETF hackathon and various side events

MARCO DAVIDS AND CASPAR SCHUTIJSER, SIDN LABS

# Table of contents

# Introduction

The 115th IETF meeting took place in London between 5 and 11 November 2022.

The mission of the Internet Engineering Taskforce (IETF) is to make the internet better. And everyone is welcome to get involved. Most of the IETF's work is done online, by means of mailing lists. However, the organisation also holds meetings three times a year. The 115th IETF meeting was held in London from 5 to 11 November.

With 1,630 participants, IETF 115 was a well-attended (hybrid) meeting. There were 854 people physically present (just over 52 per cent), up again from the previous meeting, where physical attendance accounted for 43 per cent of the total. The remaining participants followed the meeting online.

With 39 project entries, the IETF hackathon attracted 452 participants, 350 on site and 102 remote.

COVID safety measures were once again in force. Facemasks were mandatory in the meeting rooms, but merely recommended elsewhere (which most participants interpreted as licence to dispense with face coverings for a while). Four COVID cases were ultimately reported1, compared with 17 after IETF 114.

Every IETF meeting has a packed programme. The latest week-long gathering featured 100-plus working group sessions, a HotRFC, a plenary session and 2 early-morning technology deep dive sessions devoted to QUIC. There were also countless side meetings, where subjects such as encryption, internet censorship, human rights and privacy figured prominently.

# Informal activities

During the weekend prior to the main proceedings, there were various informal activities: a Hackathon, the IEPG and the HotRFC.

## Hackathon

The Saturday kicked off with the now traditional hackathon, at which the applicability and interoperability of new concepts are tested. After all, the IETF's motto is "rough consensus and running code". The hackathon also has a very important social function, because it enables people from various organisations to collaborate and get to know each other. Groups are formed spontaneously to work on a variety of experiments. This year's projects included early implementations of a draft version 5 of the NTP protocol, the detailed reporting of DNS errors, which led to a working prototype, and many others. The 452 enthusiastic participants engaged in two days of intensive discussion and programming. The hackathon concluded with presentations of the results.

[1] This number was corrected afterwards, see: https://www.ietf.org/blog/ietf-115-post-meeting-survey/

Source: https://www.ietf.org/blog/ietf115-catchup

## IEPG

The Sunday morning always begins with the IEPG, where operational and related topics are discussed, albeit with 'operational' interpreted loosely. The London meeting's programme included a presentation by Geoff Houston (APNIC Labs) on DoH versus DoT. His research team has looked at aspects such as uptake of the two protocols. Although uptake is difficult to measure, APNIC has some access to data from Cloudflare's 1.1.1.1 resolver, and is therefore able to see whether DNS queries are submitted using DNS over TLS (DoT), DNS over HTTPS (DoH), or classic DNS over port 53 (Do53). While Cloudflare's market share is modest compared with, for example, Google's Public DNS, the data is statistically significant. The APNIC team found that the largest slice of the traffic, roughly 77 per cent, easily still uses Do53, while DoT accounts for a mere 3 per cent or so. The percentages vary from country to country, with Laos as a striking outlier. At roughly 19 per cent, the Asian country's DoT use is much higher than the global norm. The reason is not entirely clear, but seems to be related to Mozilla's decision to enable DoH by default in its Firefox browser.

## HotRFC lightning talks

The Sunday ended with the HotRFC lightning talks, where speakers raise all sorts of matters or pitch ideas for feedback. In this context, 'RFC' does not stand for 'Request For Comments' (an important category of documents produced by the IETF), but for 'Request For Conversation'. The HotRFC session is a high-paced affair; no questions are allowed there and then, and any feedback is given later.

Each time slot is just 4 minutes, enabling countless ideas and subjects to be covered. For example, Philip Hallam-Baker used Elon Musk's acquisition of Twitter as a vehicle for giving his ‘Everything’ idea further exposure. Everything is an open document format, which can serve as the base technology for a wide range of social media applications with end-to-end secured communication and data storage.

Andrew Campling made a presentation entitled Encrypted Client Hello (ECH) Deployment Considerations. ECH is a new TLS extension, which resolves the remaining privacy problems associated with TLS. Although TLS connections are encrypted, some of the information that is shared is not, such as the potentially sensitive SNI and the ALPN list. Consequently, the process of setting up an encrypted TLS connection may result in information disclosure, which is undesirable in principle. While addressing those issues, ECH does have certain implications and impact. For example, some security measures do not work properly with ECH, because they rely on information available in the ‘client hello’, which is illegible with ECH.

John Border used his presentation to advertise a side event devoted to EToSat (Encrypted Transport over Satellite). For his part, Rich Kulawiec pleaded for people to consider the impact of mass security scans. Such scans often trigger alarms, with significant financial and workload implications. He asked whether participants regarded that as a problem and, if so, whether it was seen as something that could and should be addressed.

Hans-Dieter Diep (LIACS/CWI) spoke about TMP (Time Modulation Protocol), an EU-funded research project involving a new way of using atomic clocks and other ultra-precise clocks to boost the end-to-end privacy of communication channels.

Finally, Dan Sexton, CTO of the Internet Watch Foundation, asked “Is Privacy Preserving Web Filtering Possible?” He argued that technical solutions such as homomorphic encryption could make it possible, and invited participants to a side event devoted to the topic.

Those are just a handful of the many presentations made at the HotRFC, at which encryption and privacy were amongst the prominent themes.

## Technology Deep Dive

The deep dives were organised by the IESG. The deep dive is an experimental format, which may yet undergo significant modification. The idea is to provide a framework within which technical topics can be examined in greater depth. The sessions are therefore educational and informative. IETF 115 featured 2 early morning sessions, at which the spotlight fell on QUIC, a promising new network protocol that is attracting a lot of interest.

# Formal proceedings

Of the many working group sessions, we would like to highlight two:

## ADD (shared session with DPRIVE)

Having considered ADD at some length in our report on IETF 114, we can now report that Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS is soon to be revised in the light of feedback from major public resolvers, such as Google Public DNS.

For the CENTR community, the most significant part of the document is Section 3, which says:

```
An authoritative server SHOULD implement and deploy DNS over TLS
(DoT) on TCP port 853.

An authoritative server SHOULD implement and deploy DNS over QUIC
(DoQ) on UDP port 853.
```

Although the document is currently only a draft, and therefore non-binding, it is attracting a lot of attention, implying that the situation could change quickly. Considering the possible implications of that passage therefore seems worthwhile.

## DNSOP Working Group

Various updates were delivered at IETF 115, but no important new developments were revealed.

## Side meetings

The side meetings, also known as BOFs, are gatherings that are not included in the formal programme. Their purpose is often to discuss the possibility of forming a new working group. A variety of side meetings took place on the fringes of IETF 115, including one devoted to post-quantum cryptography.

The meeting was concerned with data security based on algorithms capable of standing up to the huge computational power of future quantum computers. Although the arrival of quantum computers may seem a long way off, the associated security challenges are already pertinent. The reason being that, if confidential encrypted communications are intercepted, they can be retained for future decoding when quantum computers become available. It is therefore wise to plan ahead.

Against that background, the possibility of setting up a post-quantum cryptography working group (PQC WG) has been under discussion for some time.

Every IETF working group has a charter: a brief statement defining the issue that the working group has been set up to address and the results that the group wants to achieve. The purpose of the PQC side meeting at IETF 115 was to discuss the contents of the proposed new working group's charter. It was suggested that the charter should state that the PQC WG would provide a forum for the discussion of problems relating to the transition to post-quantum cryptography and experiences relevant to IETF activities in this field. However, it is explicitly not the intention that the working group should itself develop new cryptographic protocols.

## IAB open meeting

The IAB open meeting provides an opportunity for direct interaction between the community and the IAB. In addition to the usual updates, the session featured a presentation by Mahsa Alimardani of the Oxford Internet Institute and ARTICLE 19, explaining how internet technology can support Iranian demonstrators. Simone Basso also presented the findings of monitoring of Iranian state censorship by the Open Observatory of Network Interference (OONI).

## IRTF open meeting

The centrepiece of the IRTF Open Meeting was the presentation of Applied Networking Research Prizes (ANRP). The winners also presented their research results to the audience. The latest roster included Gautam Akiwate talking about his research into the risk of domain name hijacks, and Daniel Wagner appealing for increased and improved collaboration in the fight against DDoS attacks.

## IRTF

Most IETF working groups are concerned with the production of internet standards. However, a number of them are engaged in more general research. Such working groups come under the umbrella of the Internet Research Task Force (IRTF), which is regularly invited to consider some interesting topics.

For example, one of the subjects being looked at by the Decentralized Internet Research Group (DINRG) is increasing internet centralisation (and how to counter it). The DINRG is currently working on an interesting document entitled A Taxonomy of Internet Consolidation, which intends to streamline discussions by flagging issues and providing clear definitions (e.g. of the term 'consolidation'). A related document entitled Protocol and Engineering Effects of Consolidation is also under development.

The Measurement and Analysis for Protocols (MAPRG) sessions are well-known for their high-quality content. A variety of interesting presentations were once again made at IETF 115.

At the previous IETF meeting, the focus had been on the results of research into DoH resolvers. At the London meeting, attention turned to the impact of the new DNS over QUIC (DoQ) protocol. The tentative conclusion is that DoQ reduces the loading time of a simple web page by 10 per cent, compared with DoH.

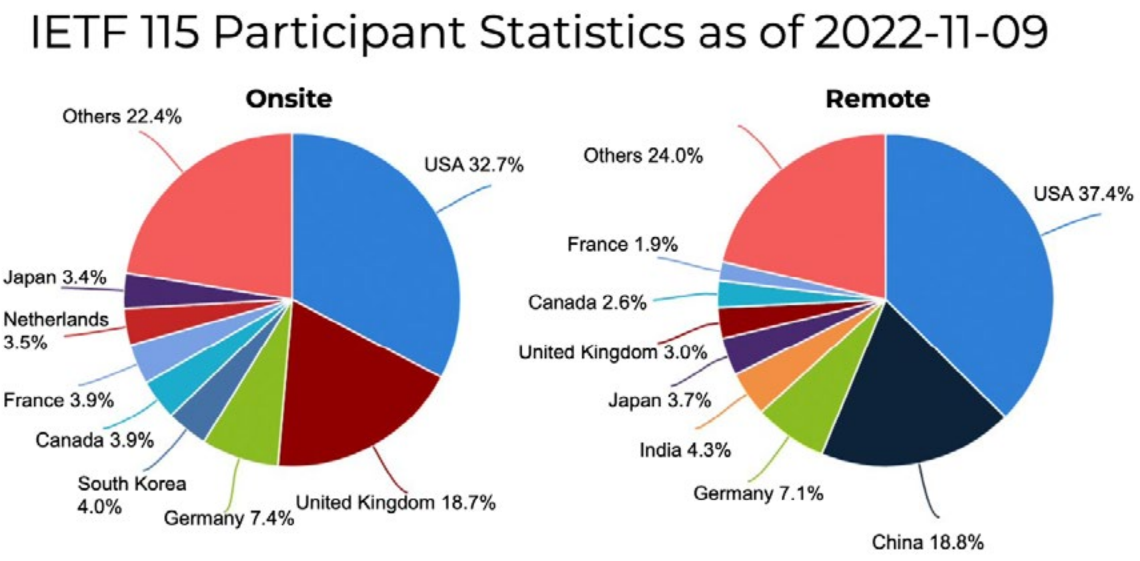
One of the other presentations was about research into the performance of Starlink, the SpaceX satellite network for broadband internet access. In terms of bandwidth, Starlink's performance is apparently similar to a 100 Mbit/s landline connection. However, losses are more frequent, even when load levels are light.

The implications of Russia's invasion of Ukraine were again a topic of discussion. A survey has been conducted to look for measurable shifts in the .ru and .рф top-level domains since the start of the conflict on 24 February 2022. The study looked at things such as website hosting, authoritative name server use and TLS certification. The conclusion is that, long before the conflict broke out, Russia was well aware that the internet could be used to apply pressure. While various significant shifts were also observed, they had caused Russia no existential problems.

For the last six months, work has been in progress within IETF circles, with a view to standardising the future-oriented SCION internet architecture. The discussions are currently taking place mainly within the Path Aware Networking Research Group (PANRG). Important steps taken so far include the brief definition of SCION and the subsequent division of SCION into separate components whose standardisation can then be discussed individually. A document about the SCION control-plane PKI has now been made available as well. A status update was given at IETF 115.

# Epilogue

IETF 115 was another hybrid conference, with the number of people attending in person again well up on the previous meeting. The intention is that IETF meetings should continue to use a hybrid format for the time being, with active remote participation enabled by Meetecho. Although the system is not yet perfect, it is improving all the time.



Source: https://datatracker.ietf.org/meeting/115/materials/slides-115-ietf-sessa-ietf-chair-iesg-report-00

The next IETF meeting is scheduled for 25 to 31 March 2023 in Yokohama.

Council of European National
Top-Level Domain Registries

# About CENTR

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 52 full and 8 associate members – together, they are responsible for over 80% of all registered domain names worldwide.

**The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.**

Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

## CONTACT

**CENTR VZW/ASBL**
Belliardstraat 20
1040 Brussels, Belgium
0885.419.166 | RPR Brussels

☎ +32 2 627 5550

✉ **secretariat@centr.org**

**www.centr.org**

## FOLLOW US

To keep up-to-date with CENTR activities and reports, follow us on Twitter or LinkedIn