Council of European National Top-Level Domain Registries

IETF 114: DNS remains a hot topic

Onsite attendance doubled, but hybrid format retained for now.

MARCO DAVIDS, SIDN LABS

Table of contents

Introduction

IETF 114 was held in Philadelphia, between 23 July and 29 July.

The mission of the Internet Engineering Taskforce (IETF) is to make the internet better. And everyone is welcome to get involved. A large international community produces high-quality, technical documentation concerning the internet's design, use and governance.

Most of the IETF's work is done online, by means of mailing lists. Traditionally, the organisation has also held three meetings a year, plus occasional interim meetings for smaller groups. However, the COVID 19 pandemic had major implications for such gatherings. Between March 2020 (meeting 107) and November 2021 (meeting 112), all IETF meetings were completely virtual. All participation was online and involved very unsocial hours for some remote 'attendees'.

Since meeting 113 (March 2022, Vienna) the IETF has adopted a hybrid meeting format. Of the 1,428 participants in that meeting, 22 per cent attended in person and the remainder virtually. At the recent 114th meeting (July 2022, Philadelphia) personal attendance was twice what it had been in Vienna, with more than 43 per cent of the 1,427 registered participants physically present. The rise illustrates how personal interaction is valued and seen as conducive to useful and productive collaboration.

An IETF meeting involves a packed week featuring numerous working group sessions devoted to a wide variety of topics, from the Internet of Things to human rights, such as privacy. A lot of the proceedings are relevant to the CENTR community. Internet standards such as DNS(SEC), IPv6 and BGP form an integral and important element of our core business. It is therefore pertinent to summarise what was said about such matters at the recent 114th IETF meeting.

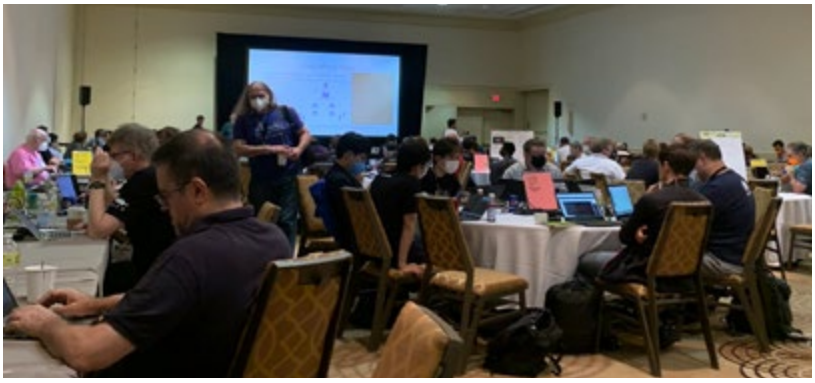
Informal activities

To get everyone in the mood, a Hackathon, the IEPG and the HotRFC were held during the weekend prior to the main proceedings.

Hackathon

The IETF week began on the Saturday with an informal hackathon. After all, the IETF's motto is "*rough consensus **and** running code*". It's good that theoretical concepts are tested in practical settings and that applicability and interoperability are verified. That is what the hackathon intends to achieve. However, it also has an important social dimension. Ad hoc groups are spontaneously formed and all sorts of experiments conducted. A good example from the IETF 114 hackathon is this L4S (Low Latency Networking) interoperability testing set-up.

Other participants tackled topics such as IPv6, IPsec / IKEv2, DNSSEC bootstrapping and the detailed reporting of DNS errors, to name just a few from a long list. Two days of intensive discussion and programming concluded with the presentation of the results.



IEPG

It has become traditional for the Sunday of an IETF week to start with the IEPG. This informal gathering is supposed to be for the consideration of operationally relevant matters, but the demarcation is fairly loose. The Philadelphia IEPG featured presentations on QUIC, IPv6 extension header testing, DANE and RPKI route origination validation (ROV) measurement. For the latter presentation, the researchers configured a valid aggregate route advertisement and an invalid more specific route advertisement within the context of RPKI, as described here: https://rov.koenvanhove.nl/. A series of measurements were then made. The conclusion of the study is that RPKI ROV does not guarantee that your traffic always reaches its intended destination. The technology nevertheless remains a recommended means of preventing route hijacking and, in particular, human failure.

A more detailed account is available on the RIPE Labs website.

HotRFC

Sunday concluded with the so-called 'HotRFC', another informal event, at which candidates were encouraged to comment on a variety of topics during brief 'lightning talks'. Got an idea, problem or proposal you think IETF people should hear about? Do you feel there's something that the IETF should tackle, but think your ideas need more work, or want to gauge interest before proceeding? If so, the HotRFC session is your opportunity to start the ball rolling.

Once again, a wide selection of questions were raised, including what has the IETF so far done to promote a greener, more sustainable internet and energy conservation standards? Could the IETF do better? What challenges are involved? The challenges and opportunities associated with post-quantum cryptography were also discussed. Protocols including IPSEC, TLS, DNSSEC and others make use of cryptography. How secure will the related cryptographic algorithms be when quantum computers enter use? One of the organisations to have investigated the matter is NIST, who recommended a number of algorithms that are expected to remain secure. However, use of the algorithms places an additional computational load on servers. It is therefore important to look ahead and assess the impact of adopting quantum-secure algorithms.

Formal proceedings

The conference proper began on the Monday (25 July 2022).

Of the many topics discussed, the following warrant consideration here.

SAVNET

Along with deliberate or accidental advertising of incorrect address prefixes, which RPKI can protect against, source address spoofing is another common problem. UDP traffic is particularly easy to spoof without using any sophisticated methods. Consequently, UDP-based standards such as NTP, SNMP and DNS, under which simple queries of a few bytes generate much larger responses, are attractive vectors for amplification DDoS attacks.

Solutions to that problem, such as the well-known BCP38, were devised long ago. Yet the problem has persisted, leading to the recent publication of a supplementary document, RFC8704. The SAVNET Working Group (WG), formally established at the previous meeting, is also looking at this issue. It has started to explore several possible avenues, with the aim of having an RFC ready for publication and submission to the IESG process by March 2025.

Adaptive DNS Discovery (ADD) and DPRIVE

Naturally, IETF members have a strong interest in all things DNS-related, and the organisation devotes considerable attention to the DNS. The DNSOP, ADD and DPRIVE working groups remain very active, and numerous developments within the IETF are relevant to our sector, the CENTR community.

The DPRIVE Working Group and the ADD Working Group held a joint session, reflecting the overlap between their spheres of activity. DPRIVE is concerned with the development of standards aimed at improving the confidentiality, authenticity and privacy of the DNS, such as DNS over TLS (DoT) and now also DNS over QUIC (DoQ). Meanwhile, ADD is active in the field of the automatised discovery of such services. The two working groups are therefore mutually complementary.

It is worth noting that, while the above-mentioned standards originally worked exclusively between client and resolver, steps are now being taken to encrypt the path between recursive resolver and 'authoritative' server (and to use TLS for zone file updates between pairs of authoritative servers).

With a view to promoting the adoption of encryption (particularly DoT and DoQ) between client and authoritative server, a draft has been released defining a method that resolvers can use to probe whether an authoritative server is reachable using DoT or DoQ. That would be done on an opportunistic basis, with support for the use of a 'self-signed' certificate as the TLS certificate. If a server is found to be reachable using DoT or DoQ, the resolver could then switch protocols, e.g. from Do53 to DoT.

It appears that the Google Public DNS resolvers, at least, already perform such unilateral probing, perhaps suggesting that this approach will quickly gain traction.

Although there was briefly a separate working group for DNS over HTTPS (DoH), which is therefore not strictly a DPRIVE development, DoH is rightly often considered in conjunction with DoT and DoQ. Nowadays, therefore, the user can potentially choose from multiple resolver 'flavours' as well as traditional, unencrypted DNS (aka Do53).

As mentioned earlier, work is underway within the ADD WG to develop discovery mechanisms that would allow the user to select the most appropriate resolver automatically, in the background. So an available DoH resolver could be selected in preference to the designated classical Do53 resolver. However, that would require the client to know of the DoH resolver's existence and location. A proposal has therefore been made, that the discovery of a designated resolver should be enabled by means of special DNS records.

The system would work as follows. Suppose that a client has obtained the IP address of a Do53 resolver in the traditional way. To establish whether a DoH server is also available, the client would send a traditional Do53 query for the qtype SCVB and the qname `_dns.resolver.arpa.` The associated DNS response might then read as follows:

```
_dns.resolver.arpa.  IN SVCB 1 doh.example.nl (

alpn=h2 dohpath=/dns-query{?dns} )
```

That tells the client that in this case, a DoH resolver is indeed available at https://doh.example.nl/dns-query?dns=[something]

As well as that SVCB record, the 'additional section' of the DNS response would include A and/or AAAA records for (in this case) 'doh.example.nl' in order to avoid the need for a number of further DNS queries.

According to the draft, DoT and DoQ (QUIC) resolvers could be discovered in a similar way.

Another draft is under development, which will put forward a mechanism for communicating similar information about DoT, DoH and DoQ resolvers to the client using the DHCP(v6) option.

DNSOP

A lot of DNS-related ideas and documents are continuing to come out of the DNSOP Working Group (and beyond)! No fewer than seventeen active drafts are being considered by DNSOP, and there are another six expired drafts that could be reactivated in the future. Clearly, that is too many to consider in detail here. We know of a further thirty-six DNS-related drafts[1] not currently under consideration by any existing WG. There may be more, since we have counted only drafts with 'DNS' in the title.

With a view to gaining a better understanding of how the plethora of proposals relate to the DNS, the re-establishment of a DNS Directorate made up of a small number of expert volunteers was proposed during this session. A more substantive proposal is expected in the period ahead.

Another noteworthy development is that, since the previous IETF meeting, 'draft-ietf-dnsop-nsec3-guidance' has become RFC9276. For any TLD registry/DNS operator that uses NSEC3, it is certainly worth reading this RFC and considering its recommendations.

In a nutshell, the authors advise configuring NSEC3PARAM with zero iterations and an empty 'salt', e.g.:

```
tld. IN NSEC3PARAM 1 0 0 -
```

The RFC explains the rationale for the advice, which a few TLDs (including .com and .uk) have since implemented.

1 Slide 13

In addition, two notable drafts -- 'draft-ietf-dnsop-rfc5933-bis' and 'draft-ietf-dnsop-avoid-fragmentation' -- have proceeded to the 'WG last call' stage. The latter is particularly worth reading, preferably followed immediately by 'draft-ietf-dnsop-glue-is-not-optional'. Anyone seeking a concise summary of DNSSEC-related RFCs is likely to find 'draft-ietf-dnsop-dnssec-bcp' very helpful. Our final reading tip is 'draft-ietf-dnsop-dnssec-validator-requirements'.

During the WG session itself, a number of new ideas were put forward, including 'draft-yorgos-dnsop-dry-run-dnssec'. This draft proposes a mechanism that would allow a new DNSSEC configuration to be given a 'dry run', without putting the operational set-up at risk. Such a mechanism is seen as desirable because slips are easily made, and DNSSEC tends to be unforgiving. The potentially serious consequences of minor mistakes are all too familiar to the likes of Slack! The mechanism proposed in the draft should considerably reduce the likelihood of such incidents. What it entails is defining a new digest type for inclusion in DS records, which would tell validating resolvers that testing is in progress, and that the response should not be deemed bogus in the event of a validation issue. It would nevertheless be possible to report such issues, e.g. using the extended DNS errors method.

The draft is currently still under development, but the concept is interesting and potentially attractive for future use in various circumstances, with a view to minimising the impact of DNSSEC errors.

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 WGs come under the umbrella of the Internet Research Task Force (IRTF) and they regularly cover 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). During the session, the results of an earlier workshop on the theme were presented. The workshop's central conclusion was that the problem is unlikely to resolve itself, and that intervention by the internet community will therefore be needed.

The Measurement and Analysis for Protocols (MAPRG) sessions are well-known for their high-quality content. At the Philadelphia meeting, current events in Ukraine figured prominently. Studies based on data from various sources have sought to determine what changes could be observed in the Ukrainian internet in the first weeks after the Russian invasion of 24 February 2022. For example, there were sudden surges in the use of Google Maps and in visits to characteristically Ukrainian websites by users in other countries. Such observations could be used to trace the flow of refugees, for example.

The results of research into the use of DNS encryption (DoT/DoH) and the impact on internet filtering were also presented. One of the findings was that encryption techniques could be used to frustrate internet censors, but that some stubborn internet censors have nevertheless blocked the best-known DoT/DoH services or even imposed a blanket ban on ESNI (or ECH) connections. Ideally, that should not be possible without causing very considerable collateral damage, the researchers suggest. The general adoption of ESNI or ECH would be advantageous in that regard.

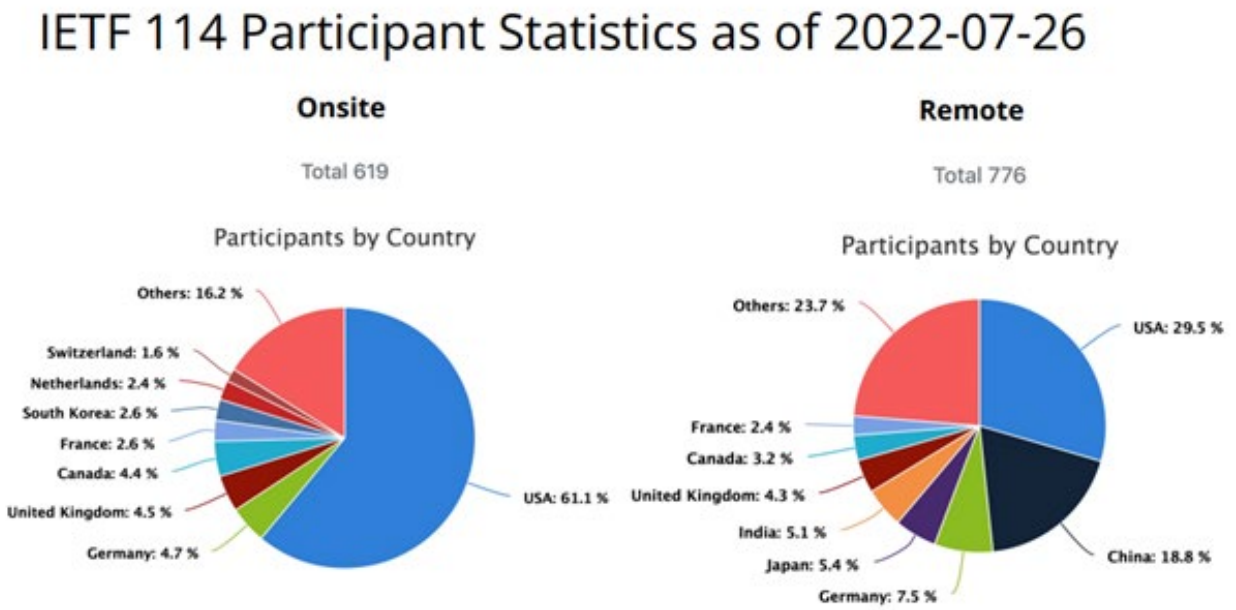
Also presented were the results of research into the availability and response times of various well-known and less well-known public DoH resolvers (and the differences between them). The well-known resolvers included those operated by Cloudflare, Google, Quad9, NextDNS, CleanBrowsing and OpenDNS. Not unexpectedly, those resolvers were found to have shorter response times, aided by, amongst other things, the use of anycast.

Epilogue

This document provides a brief summary of the many topics covered at the 114th IETF meeting. It was the second such meeting to have 'onsite' participants since the COVID-19 crisis.

At IETF 114, the number of people attending in person was far higher than at the 113th meeting. Strict infection control measures were in place, such as the mandatory use of facemasks during the sessions and the social event. 16 cases of infection were subsequently reported, representing 2.6 per cent of in-person attendees, compared with 2.9 per cent at the previous meeting.

The intention is that IETF meetings should continue to use a hybrid format for the time being. That implies remote participants being able to participate actively in the sessions by means of Meetecho, having previously been limited to following proceedings passively. Although the system is not yet perfect, it is improving all the time.



Source: https://datatracker.ietf.org/meeting/114/materials/slides-114-ietf-sessa-ietf-chair-and-iesg-plenary-report-00

The next IETF meeting is scheduled for 5 to 11 November in London.

Photo by Marco Davids

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 9 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