2021 Topic Summary

Top Five Most Viewed Call Topics for 2021

1. [iCloud Private Relay](#)
2. [DNS-over-QUIC (DoQ)](#)
3. [Google's Private Prefetch Proxy](#)
4. [Issues Raised by the Mozilla TRR Public Consultation](#)
5. [Rule 53](#)

Full List of Topics for 2021

Date	Link	Summary
4th January	Network / Client Negotiation	A continuation of the discussion started on 21st December by Vinny Parla (see separate recording accessible here). As a reminder, Vinny covered topics including the multiplexing of DNS and content, the importance of end-to-end encryption and the implications for network operators that want to enforce policy controls.
11th January	DNS-over-QUIC (DoQ)	A briefing by Andrey Meshkov of AdGuard on the company's DNS-related developments, in particular focusing on its DNS-over-QUIC activities including its DoQ resolver.
18th January	NSA: Adopting Encrypted DNS in Enterprise Environments	A short presentation summarising recent advice from the US National Security Agency to enterprises about the use of encrypted DNS, followed by a discussion on the points arising.
25th January	Issues Raised by the Mozilla TRR Public Consultation	A discussion about some of the issues raised by the recent Mozilla TRR public consultation, with initial input by Paul Vixie of Farsight Security, Vittorio Bertola of Open-Xchange, Till Sommer of ISPA UK and Chris Box of BT
1st February	Encrypted DNS Malware, Botnets and more	A general discussion covering DoH-based malware and botnet protection, the IETF ADD interim working group session, the impact of misrouted traffic due to missing EDNS and the potential exchange of DoH trial data.
8th February	Safety Versus Privacy	A general discussion followed by reflections on the potential conflict between safety and privacy by Mike Tunks and Sarah Smith at the IWF.
15th February	Centralisation	A panel discussion on centralisation and the privacy trade-offs involved in DoH and ECH. The expert panel for the discussion comprised: • Carl Gahnberg, Internet Society • Amod Malviya, Udaan • Joey Salazar, Article 19 • Vittorio Bertola, Open-Xchange With the opening comments from the panelists followed by Q&A

419.Consulting

22nd February	The Impact of Post-Quantum Cryptography on DNSSEC	The main focus of the call was a discussion on the Impact of Post-Quantum Cryptography on DNSSEC with Moritz Muller of SIDN Labs and Jins de Jong of TNO. This was followed by a brief update on some of the recent DNS-related announcements from the European Commission and an update on the IETF ADD working group.
1st March	Raising the DoH	The main focus of the call was a discussion on progress with some of the recent DoH resolver deployments, with input from Charter Communications, Comcast, Deutsche Telekom and Quad9. There was also a brief review of plans for the ADD working group sessions at IETF 110.
12th March	IETF 110 Highlights	The following is a list of the key topics that I noted during the IETF 110 conference that took place from 8th to 12th March 2021. I've included the name of the session together with details of key topics followed by links to the meeting materials and session recording.
15th March	IETF 110 Review	The call focused on a review of some of the more interesting topics raised at the recent IETF 110 conference, with particular emphasis on those items related to various aspects of DNS, privacy and resilience
22nd March	DNS Privacy vs.	A presentation titled "Privacy vs." with Mallory Knodel, CTO of the Centre for Democracy and Technology, and Shivan Sahib, Senior Software Engineer at Salesforce. The presentation highlighted some of the potential tradeoffs to improve DNS privacy and was followed by a discussion focused on the issues raised.
29th March	Discovering Split Horizons	A presentation about the split-horizon discovery draft by Tiru Reddy and Dan Wing that was recently issued to the IETF ADD working group. The ensuing discussion considered a number of issues, including whether the proposal had applications that extended beyond enterprise environments to, for example, edge capabilities on ISP networks or even home routers.
12th April	European Resolution	A presentation about the recently announced European Resolver Policy (see also www.EuropeanResolverPolicy.Com) followed by Q&A
19th April	DoQ-umenting DNS Shotgun	Tomáš Křížek of CZ.NIC gave an update on some new features within DNS Shotgun, the DNS benchmarking tool, which supports encrypted DNS (DoT and DoH) – see also https://dns-shotgun.readthedocs.io, https://www.youtube.com/watch?v=YQI4Nke5NHw and https://blog.apnic.net/2021/04/06/introducing-dns-shotgun/. Tomáš also shared his views on the advantages of DoQ (DNS-over-QUIC) compared to DoH (DNS-over-HTTPS).
22nd April	Google's Private Prefetch Proxy	A discussion with Kenji Baheux, a Google Chrome product manager, about the company's proposed implementation of a private prefetch proxy with its Chrome browser.
26th April	Round Up	The discussion this week covered: • Google's Private Prefetch Proxy proposal • Encrypted Client Hello (ECH) the replacement for eSNI • The European Resolver Policy • Forthcoming industry events The ECH article referred to is accessible at https://blogs.infoblox.com/security/esni-ech-impact-on-

419.Consulting

		content-filtering. More information on ICANN's KINDNS initiative can be found at https://community.icann.org/display/KINDNS.
3rd May	Truffle Hunting	A presentation followed by Q&A with Audrey Randall of UCSD. The presentation covered the reverse engineering of public resolver cache strategies, the Tufflehunter tool and three case studies: stalkerware, contract cheating and typo-squatting.
10th May	Access Denied	Dan Wing of Citrix and Neil Cook of Open-Xchange presented their Internet-Draft titled "DNS Access Denied Error Page" (see https://datatracker.ietf.org/doc/html/draft-reddy-dnsop-error-page-07), which addresses the problems caused when a DNS server filters queries without offering any explanation to users. The ensuing discussion clarified a number of points and identified additional areas to be addressed by the paper.
13th May	European Resolver Policy Endorsed	Details of the first organisations to endorse and adopt the European Resolver Policy.
17th May	A Peek into the DNS Cookie Jar	Casey Deccio of Brigham Young University gave a presentation titled "A Peek Into the DNS Cookie Jar: An Analysis of DNS Cookie Use". The presentation covered the first study measuring the deployment of DNS Cookies in nearly all aspects of the DNS architecture as well as an analysis of the current benefits of DNS Cookies and the next steps for stricter deployment.
24th May	Be Kind	Adiel Akplogan, VP Technical Engagement at ICANN, outlines the organisation's KINDNS programme, followed by Q&A. The discussion then moves on to cover the ICANN DNS Symposium, IGF 2021 and the Wikipedia entry for public recursive name servers.
7th June	Discovery	A discussion led by Barbara Stark of AT&T focusing on how well the current DNS discovery solutions address the requirement of supporting a home router with a private IP address and DNS forwarding. The document that Barbara and others have been working on to capture their thoughts is accessible at https://bhstark2.github.io/dns-forwarder-analysis/draft-stark-add-dns-forwarder-analysis.html.
14th June	DNSSEC	The focus of the discussion was whether DNSSEC is ready for prime time, whether it must be used for resolvers. Ulrich Wisser of Internetstiftelsen, Vittorio Bertola of Open-Xchange, Bill Woodcock of PCH and John Todd of Quad9 addressed questions posed by Peter Lowe of DNSFilter, with input from various other participants on the call.
21st June	Clouding the Issue	Apple's iCloud Private Relay service was the main focus of the call, with the discussion primarily intended to help identify potential issues in advance of a follow-up call with the Apple team. The explanatory Apple video about the service is accessible at https://developer.apple.com/videos/play/wwdc2021/10096.
28th June	Public Responses	A discussion about Mozilla's Trusted Recursive Resolver public consultation of earlier this year with the authors of some of the consultation responses.
5th July	More Public Responses	The second part of a discussion about Mozilla's Trusted Recursive Resolver public consultation of earlier this year with the authors of some of the consultation responses. This time, Steve Hill, Technical Director of Opendium, talked about some of the points in his response, highlighting challenges faced by

419.Consulting

		content filtering companies - the response is accessible here. Mark Gaudet, General Manager at Cira, followed Mark by discussing the TRR program from the perspective of a resolver operator, in his case Canadian Shield - more details about the service are accessible here. We also touched briefly on the court case in Germany involving Sony and Quad9. Quad9's blog post on the case can be found here.
12th July	iCloud Private Relay	A discussion with Apple's Tommy Pauly about the recently-announced iCloud Private Relay service, addressing questions raised by a range of stakeholders. The site that Tommy mentions, containing advice on preparing networks for the service, is accessible here.
20th July	IETF 111	The discussion mainly focused on the agenda of the forthcoming IETF 111 conference at the end of July, identifying those sessions of greatest interest to the participants of the call. In addition to talking about the agenda of IETF 111, RFC 9065 was mentioned. This informational paper discusses some implications of transport header encryption for network operators and researchers that have previously observed transport headers, and it highlights some issues to consider for transport protocol designers.
26th July	Mozilla TRR Public Consultation and IETF 111	The main focus of the discussion was the recent TRR public consultation by Mozilla, with input from Juliana Guerra, Advocacy Officer of Derechos Digitales on the organisation's consultation response. This was followed by a presentation by Andrew Campling analysing all 57 consultation responses, building on his post which featured on the APNIC and Ripe NCC blogs. After this, there was a brief review and discussion about sessions of interest at the IETF 111 conference, which started later the same day.
2nd August	Highlights from IETF 111	The discussion this week focused on the IETF 111 Conference, identifying some of the highlights from the week that warrant viewing as well as some of the related talking points from the key sessions.
9th August	Network Policy and Content Filtering	Two topics were the main focus of the discussion: 1. Method(s) for a network to securely signal policy to clients; 2. Follow-up to the presentation and discussion about the "Structured Data for DNS Access Denied Error Page" paper at the DNSOP session during IETF 111. This was followed by a couple of brief points under any other business. The protective DNS document referenced during the discussion is accessible here and Quad9's blog post on its current court case with Sony Music is accessible here.
23rd August	The Education & Finance Sectors and Encrypted Client Hello	The focus of the discussion was on the potential impact of the Encrypted Client Hello (ECH) standard, a proposed extension to the TLS protocol, on the education and finance sectors. A recent roundtable considered the potential impact of ECH on the education and finance sectors, after which a report was

419.Consulting

		published with recommendations to mitigate those effects - both the narrative of the roundtable and subsequent analysis can be found [here]().

6th September	General Catch Up	A general discussion covering a number of recent news events as well as some conferences that are coming up in the next few months.
		
		The following topics were touched on during the discussion:
		
		1. SIDN Labs, New Machine Learning applications that boost Internet security
		- https://blog.apnic.net/2021/09/03/machine-learning-boost-internet-security/
		2. ETSI releases the first Group Report on Encrypted Traffic Integration, protecting end users from malicious attacks
		- https://www.etsi.org/newsroom/press-releases/1961-etsi-releases-the-first-group-report-on-encrypted-traffic-integration-protecting-end-users-from-malicious-attacks
		3. Secure64 DNS Proxy Puts Service Providers Back In Control Of HTTPS DNS Traffic
		- https://aithority.com/technology/customer-experience/secure64-dns-proxy-puts-service-providers-back-in-control-of-https-dns-traffic/
		4. APNIC 52 Schedule – 13-16th September
		   • Tuesday 14th: Tech Keynotes, Tech Session 2 – Threat Hunting using DNS
		   • Wednesday 15th: Tech Session 3 – Oblivious DNS and DNSSEC Key Lifecycles

13th September	Connection Management	The focus of the call was on a proposal to develop an open standard for content filtering. Or, more accurately, an open standard for "connection management" as the intent is primarily to determine which connections will be allowed based on the destination rather than the content of a specific interaction. A presentation by the team at Charter Communications outlined both the need for such a standard as well as the shape of a potential solution. This then led to a discussion amongst participants on the call to begin to develop the idea further, identify likely supporters and explore next steps.
20th September	Private Relay Revisited	The call covered two topics: 1 - the advisability of approaching IANA for a Special Use Domain Name (SUDN) for use by local access providers 2 - analysis of the implications of Apple's new Private Relay Service for Network Operators and Internet Service Providers.
28th September	Dreaming of Privacy	The call covered two topics today: 1. Differentiating DoH packets from encrypted web packets with Levi Csikor and Dinil Divakaran of

419.Consulting

		Trustwave and the National University of Singapore - see also this paper. 2. An update by Vinny Parla on Cisco's announcement last Friday of support within Umbrella for Discovery of Designated Resolvers (DDR) Both presentations were followed by Q&A sessions with a good range of points raised by participants.
5th October	Boosting Internet and DNS Security with Machine Learning	The main focus of the call was on a presentation by Thymen Wabeke of SIDN Labs outlining research planned to increase Internet security using machine learning, expanding on his APNIC blog post here. He also covered techniques used to identify fake online shopping sites and potentially fake "government" sites. The slides from the presentation are accessible here. After a Q&A session with Thymen, the discussion moved on briefly to touch on aspects of Apple's new Private Relay service, building on an article in the UK's Sunday Telegraph on 3rd October.
11th October	DoH, Android 13 and IETF Positions	The call covered a number of topics this week including: 1. Questions for Google about DoH support in Android - email me directly with any questions to include in the discussion; 2. Nominations for vacant IETF positions - see here for the nomination proforma; 3. IETF 112 - draft agenda and the ADD working group; 4. DNS Abuse taxonomy - see here and here for the incident mapping spreadsheet and feedback form. Together with a general discussion about some of the issues relating to the recent Facebook outage.
19th October	Good Home	The primary focus of the call this week was on two Internet-Drafts recently put forward for adoption by the IETF's Adaptive DNS Discovery (ADD) working group: • Discovery of Encrypted DNS Resolvers: Deployment Considerations • Split-Horizon DNS Configuration One of the co-authors of both documents, Tiru Reddy, gave an overview of the main points in each of the documents and took questions. Comments in support of the adoption of the two documents should be made on the ADD working group's mailing list.
25th October	IETF 112	The call this week concentrated on the agenda for the forthcoming IETF 112 meeting, discussing sessions most likely to be of interest. There was also mention of content to look out for during ICANN 72 which is running this week.
1st November	Microsoft DDR	The primary focus of the call was an update from Tommy Jensen of Microsoft covering the company's recent announcement of support for DDR in cooperation with Cisco Umbrella & Quad9. After Q&A, the call moved on to discuss ley sessions in the forthcoming IETF 2021 meeting.

8th November	IETF 112 Week	The IETF 112 meeting takes place from Monday 8th to Friday 12th November, with a total of 114 sessions running throughout the week. The list below includes details of some of the more interesting sessions, with the bracketed text indicating particularly notable content.
15th November	DNS4EU	This week the call covered: 1. The European Commission's DNS4EU project; 2. Other points arising from the Commission's High-Level group for Internet Governance (HLIG) meeting on 10th November; 3. Highlights from IETF 112. Along with brief mentions of several other items.
22nd November	IGF 2021 Preview	The call this week started with a discussion about the key workshops on the agenda for the forthcoming IGF 2021 conference, before touching on some interesting events coming up through to mid-December as well as a number of other items.
30th November	Rule 53	Peter Lowe of DNSFilter presented "Rule 53: If you can think of it, someone's done it in the DNS" covering the many and varied uses to which the DNS infrastructure has been put beyond its intended function. We also touched on forthcoming events of interest through to mid-December as well as topics to be covered on future calls.
6th December	Come As You Are	On our call today, Kevin Bock of the University of Maryland discussed "Server-Side Evasion of Filtering", expanding on a recent paper on the topic. Kevin's presentation covered the key concepts behind the tool developed to exploit the theories in the paper as well as an update on how the tool performed and adapted in action. The ensuing discussion reviewed a number of aspects of the implications of the concepts, both positive and negative.
9th December	The State of DNS Privacy Technologies	We had a very interesting panel discussion organised by ICANN about DNS privacy during IGF 2021. I gave my views on some of the most recent tech developments, after which Carlos Martinez focused more on the ISP perspective and then Roxana Radu looked more at the open resolvers. The ensuing discussion was moderated by Paul Hoffman of ICANN, with additional points coming from both online and in-room participants.
14th December	The Log4j Exploit	The call started with an overview of the recently discovered Log4j exploit by Vinny Parla of Cisco, covering details both of the exploit and potential mitigations. The discussion then moved on to cover highlights from the IGF 2021 conference, including the content of the DNS privacy technologies workshop. AoB included details of forthcoming events as well as an update on developments in the IETF's ADD working group, in particular the "split-horizons" proposal and "deployment considerations" draft.

419.Consulting