Council of European National
Top-Level Domain Registries

IETF 114: DNS nog altijd ‘hot topic’

‘Onsite’ aanwezigheid verdubbeld, maar hybride formaat blijft voorlopig.

MARCO DAVIDS, SIDN LABS

Inhoud

INLEIDING 3

INFORMELE DEEL 3

Hackathon 3

IEPG 4

HotRFC 4

FORMELE GEDEELTE 5

SAVNET 5

Adaptive DNS Discovery (ADD) en DPRIVE 5

DNSOP 6

IRTF 7

EPILOOG 8

Inleiding

De 114e IETF werd gehouden van 23 juli tot 29 juli in Philadelphia

De missie van de Internet Engineering Taskforce (IETF) is om het internet beter te maken. En iedereen kan zich hierbij aansluiten. Een grote internationale gemeenschap produceert hoogwaardige, technische documenten die relevant zijn voor de manier waarop het internet ontworpen, gebruikt en beheerd wordt.

Het meeste werk gebeurt online, via mailinglijsten. Daarnaast zijn er drie keer per jaar conferenties (met soms, in kleiner verband, nog wat interim-bijeenkomsten). De COVID-19 pandemie bracht hierin grote veranderingen teweeg. Tussen maart 2020 (meeting 107) en november 2021 (meeting 112) waren noodgedwongen alle conferenties volledig online. Deelnemers moesten op afstand, soms op lastige tijdstippen, de conferenties volgen.

Sinds meeting nr. 113 (maart 2022, Wenen) is sprake van een hybride concept. Van de 1428 deelnemers was 22% ter plekke aanwezig en de overige deelnemers online. De onlangs gehouden 114e IETF meeting (juli 2022, Philadelphia) liet een verdubbeling zien in het aantal fysiek aanwezige deelnemers (ruim 43% van de in totaal 1427 inschreven deelnemers). Dit is een indicatie dat persoonlijke contacten worden gewaardeerd en bevorderlijk worden geacht voor een goede, productieve samenwerking.

IETF-conferenties bestaan uit een volgepropte week met tal van werkgroep-sessies over de meest uiteenlopende onderwerpen, variërend van het 'Internet der dingen' tot mensenrechten, zoals privacy. Veel van het werk is voor de CENTR-gemeenschap relevant. Internetstandaarden zoals DNS(SEC), IPv6 en BGP zijn een integraal en belangrijk onderdeel van onze corebusiness. Laten we daarom kijken wat hierover zoal besproken is tijdens de afgelopen 114e IETF-conferentie.

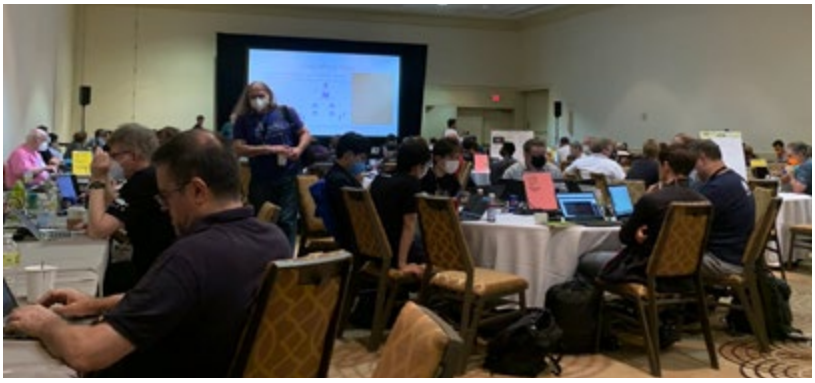
Informele deel

Om in de stemming te komen wordt er in het weekend afgetrapt met een Hackathon, de IEPG en de HotRFC

Hackathon

De IETF-week wordt al op zaterdag afgetrapt met een informele hackathon. Het credo van de IETF is immers niet voor niets: "*rough consensus **and** running code*". Het is goed dat theoretische concepten worden getoetst aan de praktijk en toepasbaarheid en interoperabiliteit worden geverifieerd. Dit is waar de hackathon om draait. Maar daarnaast wordt ook het sociale aspect niet uit het oog verloren. Ad hoc groepjes ontstaan spontaan en er word gewerkt aan diverse experimenten. Een voorbeeld hiervan tijdens IETF 114 was deze L4S (Low Latency Networking) interoperabiliteit test-setup.

Andere deelnemers hielden zich bezig met onderwerpen zoals IPv6, IPsec / IKEv2, 'DNSSEC bootstrapping' en het uitgebreid rapporteren van DNS-fouten. En dit zijn slechts enkele onderwerpen uit de lange lijst. Er wordt twee dagen lang druk overlegd en geprogrammeerd, waarna later de resultaten worden gepresenteerd.



IEPG

De zondagochtend begint traditioneel met de IEPG. Beoogde onderwerpen van deze informele bijeenkomst hebben in principe een operationele component, hoewel men hier flexibel in is. Dit keer waren er presentaties over QUIC, IPv6 Extension Header testing, DANE en RPKI Route Origination Validation (ROV) metingen. Voor dat laatste hebben de onderzoekers een geldige 'aggregate route advertisement' en een ongeldige 'more specific route advertisement' geconfigureerd binnen de context van RPKI, zoals hier beschreven: https://rov.koenvanhove.nl/. Vervolgens zijn hiermee metingen gedaan. De conclusie van dit onderzoek is dat RPKI ROV op zichzelf geen garantie geeft dat je verkeer altijd op de juiste plek uitkomt. Maar desondanks is het nog steeds een aanbevolen techniek tegen 'route hijacking' en -met name- menselijk falen.

Het uitgebreidere verhaal vind je op de site van RIPE Labs.

HotRFC

De zondag werd afgesloten met de zogenaamde HotRFC, eveneens een informeel gebeuren waarbij kandidaten via compacte 'lightning talks' op prikkelende wijze allerlei onderwerpen kunnen aanstippen. Heb je een idee, probleem of voorstel waar IETFers over zouden moeten horen? Wil je IETF-werk voorstellen, maar weet je niet zeker of je idee klaar is of wie er geïnteresseerd is? Dan kun je een balletje opgooien tijdens de HotRFC-sessie.

Dit keer ook weer uiteenlopende onderwerpen, zoals: wat heeft de IETF tot nu toe gedaan aan een groener, duurzamer internet en energiebesparende standaarden? Kan dit beter? Welke uitdagingen horen daarbij? Maar ook de uitdagingen en kansen van 'post-kwantum' cryptografie kwamen aan bod. Protocollen zoals IPSEC, TLS, maar ook DNSSEC e.d. maken van cryptografie gebruik. Hoe veilig zijn de daarvoor gebruikte algoritmes straks nog, wanneer kwantumcomputers in zwang gaan komen? O.a. NIST heeft hier onderzoek naar gedaan en zij kwamen recent met een aantal aanbevelingen voor algoritmes die ook post-kwantum nog voldoende veilig zouden zijn. Maar deze algoritmes stellen andere eisen aan de rekenkracht van servers en het is belangrijk om te weten welke impact dat zal hebben, dus het is belangrijk hier nu al op te kunnen anticiperen.

Formele gedeelte

Op maandag begint daadwerkelijk de conferentie.

Hieronder enkele van de vele onderwerpen die we graag in dit verslag willen uitlichten.

SAVNET

Naast het onjuist adverteren van adresprefixen (al dan niet opzettelijk), waar RPKI bescherming tegen kan bieden, is 'source address spoofing' een ander nog regelmatig voorkomend probleem. Met name UDP-verkeer laat zich zonder specifieke maatregelen vrij gemakkelijk 'spoofen'. En UDP-gebaseerde standaarden die op basis van een eenvoudige vraag van enkele bytes groot een veel groter antwoord terugsturen, zoals NTP, SNMP of DNS, vormen daardoor een gewilde aanvalsvector voor het uitvoeren van zogenaamde amplificatie DDoS-aanvallen.

Lang geleden zijn hiervoor al oplossingen bedacht, zoals het welbekende BCP38. Maar toch blijkt er sprake van een hardnekkig probleem, wat recent nog tot de publicatie van een aanvullend document (RFC8704) heeft geleid. De SAVNET werkgroep, die sinds de vorige meeting officieel bestaat, houdt zich ook met dit onderwerp bezig en verkent inmiddels meerdere oplossingsrichtingen, die in maart 2025 moeten leiden tot een uitgewerkte RFC die rijp is voor publicatie en het IESG-proces.

Adaptive DNS Discovery (ADD) en DPRIVE

Uiteraard is er veel aandacht (en belangstelling) voor alles wat met DNS te maken heeft bij de IETF. De DNSOP-, ADD- en DPRIVE-werkgroepen zijn nog altijd heel actief en er zijn behoorlijk wat ontwikkelingen die ook voor onze sector, de CENTR-community, relevant zijn.

De sessie van de DPRIVE-werkgroep was gecombineerd met die van de ADD-werkgroep. Dat is begrijpelijk, want tussen beide werkgroepen is een zekere overlap. DPRIVE houdt zich bezig met de ontwikkeling van DNS-standaarden die vertrouwelijkheid, authenticiteit en de privacy van DNS verbeteren. Denk aan DNS-over-TLS (DoT) en tegenwoordig ook DNS-over-QUIC (DoQ). En ADD gaat over het geautomatiseerd kunnen ontdekken van dergelijke services. Samen versterken ze elkaar dus.

Bovengenoemde standaarden werkten overigens oorspronkelijk alleen tussen client en resolver. Maar er zijn ontwikkelingen gaande om ook op het pad tussen recursieve resolver en 'authoritative' server te versleutelen (en om zonefile updates over TLS tussen twee authoritative servers te doen).

Om de adoptie van versleuteling (met name DoT en DoQ) tussen client en authoritative server te bevorderen is er een draft die beschrijft hoe resolvers eventueel kunnen 'proben' of een authoritative server ook via DoT of DoQ bereikbaar is. Dit gebeurt dan opportunistisch, waarbij het TLS-certificaat bijvoorbeeld ook een 'self signed' certificaat kan zijn. En indien zo'n server wordt gevonden, dan kan de resolver bijvoorbeeld overschakelen van Do53 naar DoT.

Het schijnt dat in elk geval de Google Public DNS resolvers deze 'unilateral probing' al doen, wat misschien wel een aanwijzing is dat deze ontwikkelingen in een stroomversnelling zullen gaan komen.

Hoewel voor DNS-over-HTTPS (DoH) korte tijd een separate werkgroep bestond en het dus formeel niet uit de DPRIVE-koker komt, wordt het -terecht- toch dikwijls in één adem genoemd met DoT en DoQ . De gebruiker heeft dus tegenwoordig potentieel de keuze uit meer resolver-smaken dan enkel het onversleutelde, traditionele DNS (aka Do53).

Binnen de ADD-wg wordt, zoals reeds opgemerkt, gewerkt aan ‘discovery-mechanismes’ die het mogelijk moeten maken voor de gebruiker om (geautomatiseerd en op de achtergrond) de beste keuze te kunnen maken voor een resolver. Bijvoorbeeld een beschikbare DoH-resolver gaan gebruiken i.p.v. de standaard toegewezen klassieke Do53-resolver. Dan moet de client echter wel weten dat deze er is (en waar). Er is een voorstel om de betreffende ‘discovery’ van zo’n ‘designated resolver’ via speciale DNS-records mogelijk te maken.

Dit werkt als volgt: stel, dat een client op traditionele wijze de beschikking heeft gekregen over een IP-adres die hij kan gebruiken als Do53-resolver. Als hij wil weten of er een DoH-server beschikbaar is, dan kan hij een traditionele Do53-query doen voor het qtype SCVB en de qname `_dns.resolver.arpa.` Het betreffende DNS-antwoord zou er zo uit kunnen zien:

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

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

Dus; er is in dit voorbeeld inderdaad een DoH-resolver beschikbaar en wel op: https://doh.example.nl/dns-query?dns=[something]

Naast dit SVCB-record, zitten in de ‘additional section’ van het DNS-antwoord tevens A- en/of AAAA-records van (in dit geval) ‘doh.example.nl’ om zodoende enkele DNS-vragen uit te kunnen sparen.

Op soortgelijke wijze kunnen volgens deze draft ook DoT en DoQ (QUIC) resolvers worden gevonden.

Er is daarnaast ook nog een draft in ontwikkeling die het mogelijk maakt om via DHCP(v6) optie soortgelijke informatie over DoT-, DoH- en DoQ-resolvers over te kunnen brengen naar de client.

DNSOP

Nog altijd ontstaan er veel DNS-gerelateerde ideeën en documenten binnen deze WG (en daarbuiten)! Binnen deze WG zijn er maar liefst 17 actieve drafts en 6 verlopen drafts die mogelijk nog een keer actief worden. Teveel om allemaal in detail te benoemen. Daarnaast telden we nog 36 drafts[1] die niet ondergebracht zijn in een bestaande WG, maar die wel DNS-gerelateerd zijn. Waarschijnlijk zelfs meer, maar dit is uitgaande van drafts met het woord ‘dns’ in de titel.

Om binnen deze brei van voorstellen de samenhang met DNS beter in kaart te brengen, werd tijdens deze sessie de (her-)oprichting van een ‘DNS directorate’ voorgesteld, bestaande uit een kleine groep deskundige vrijwilligers. Hierover zal de komende tijd meer bekend worden.

Vermeldenswaardig is verder dat ‘draft-ietf-dnsop-nsec3-guidance’ sinds de vorige IETF-bijeenkomst overgegaan is in RFC9276. Als registry/DNS-operator van een TLD die NSEC3 doet, is het zeker de moeite waard om deze RFC te lezen en de aanbevelingen die daarin worden gedaan te overwegen.

Dat komt neer op de NSEC3PARAM configureren met 0 ‘iterations’ en lege ‘salt’, bijvoorbeeld:

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

RFC legt uit waarom dit de aanbevolen instelling is en enkele TLD’s (zoals bijvoorbeeld .com en .uk) hebben deze aanbevelingen inmiddels overgenomen.

Verder zijn er twee drafts in ‘WG last call’ gegaan, te weten: ‘draft-ietf-dnsop-rfc5933-bis’ en ‘draft-ietf-dnsop-avoid-fragmentation’. Met name die laatste is het lezen waard. En lees dan meteen

1 Slide 13

ook ‘draft-ietf-dnsop-glue-is-not-optional’. En voor wie behoefte heeft aan een compact overzicht van DNSSEC-gerelateerde RFC’s, is deze handige ‘draft-ietf-dnsop-dnssec-bcp’ waarin ze overzichtelijk staan opgesomd wellicht interessant. En als laatste lees-tip noemen we tenslotte graag nog ‘draft-ietf-dnsop-dnssec-validator-requirements’.

Tijdens de WG-sessie zelf kwamen een aantal nieuwe voorstellen ter tafel, waaronder ‘draft-yorgos-dnsop-dry-run-dnssec’. Deze draft moet het mogelijk maken om een ‘dry run’ te doen van een nieuwe DNSSEC-configuratie, zonder het risico te lopen dat er dingen stuk gaan. Want zoals bekend is DNSSEC nogal onvergefelijk en een fout is zo gemaakt. Dat dit nadelige consequenties kan hebben, weten ze bijvoorbeeld bij Slack nog maar al tegoed! Met de techniek die wordt voorgesteld in deze draft zou de kans op dergelijke incidenten kleiner moeten worden. Het idee is om validerende resolvers via een nieuw te definiëren ‘digest type’ in het DS record te laten weten dat sprake is van een test en dat eventuele validatieproblemen niet mogen leiden tot een bogus antwoord. Maar ze kunnen wel worden gerapporteerd, bijvoorbeeld via de ‘extended DNS errors’-methode.

De draft is nog in ontwikkeling, maar het betreft een interessant concept dat voor verschillende use cases een interessante optie kan zijn in de toekomst, om de gevolgen van DNSSEC-fouten te verkleinen.

IRTF

Werkgroepen richten zich gewoonlijk op het produceren van internetstandaarden, maar daarnaast zijn er een aantal groepen die zich richten op breder onderzoek. Deze vallen onder de Internet Research Task Force (IRTF). Daar komen regelmatig interessante onderwerpen voorbij.

Zo is de toenemende centralisatie van het internet (en het tegengaan daarvan) een onderwerp binnen de Decentralized Internet Research Group (DINRG). Tijdens de sessie werden de resultaten van een eerder gehouden workshop over dit thema gepresenteerd. Conclusie: dit probleem zal zich vermoedelijk niet vanzelf oplossen en de internetgemeenschap zal hiervoor in actie moeten komen.

De Measurement and Analysis for Protocols (MAPRG) sessies staat bekend om hun kwalitatief goede inhoud. Deze keer nam de actualiteit in Oekraïne een belangrijke plaats in. Onderzoeken bekeken aan de hand van diverse databronnen welke veranderingen konden worden waargenomen aan het Oekraïense internet gedurende enige weken vanaf de Russische invasie op 24 februari 2022. Zo bleek er een plotselinge toename te zijn van het gebruik van Google Maps en een plotselinge stijging van het bezoek aan typisch Oekraïense websites vanuit het buitenland. Op basis daarvan konden o.a. vluchtelingenstromen in kaart worden gebracht.

Daarnaast een presentatie met de resultaten van een onderzoek naar het gebruik DNS-encryptie (DoT/DoH) en hun impact op internet filtering. Daaruit blijkt dat deze technieken kunnen helpen tegen ‘internet censors’, maar dat sommige hardnekkige internet censors de meest bekende DoT/DoH-services desondanks hebben geblokkeerd of zelfs botweg alle ESNI (of ECH) connecties blokkeren. In het ideale geval zou dit niet meer zomaar moeten kunnen zonder heel veel ‘collateral damage’ te veroorzaken, stellen de onderzoekers. Bijvoorbeeld door de adoptie van ESNI of ECH gemeengoed te maken.

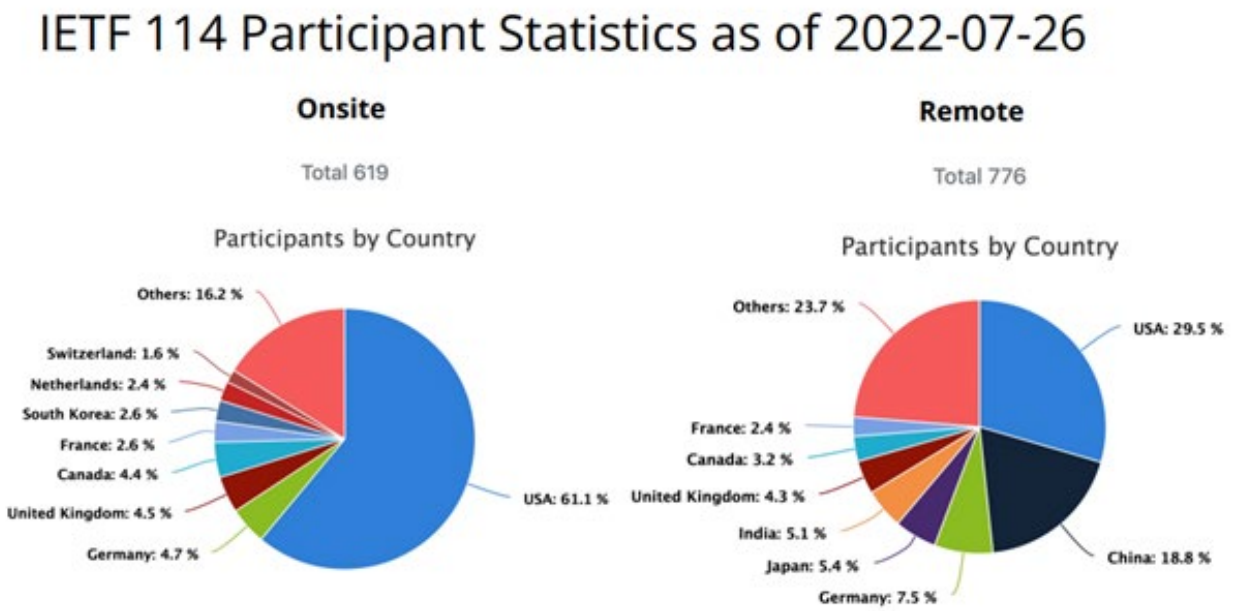
Verder nog de resultaten van een onderzoek naar de beschikbaarheid en responsetijden van bekende en minder bekende publieke DoH-resolvers (en hun verschillen). Bekende resolvers zijn bijvoorbeeld die van Cloudflare, Google, Quad9, NextDNS, CleanBrowsing en OpenDNS. Niet geheel onverwachts hebben deze bekende resolvers een snellere responsetijd, temeer daar deze vaak op basis van anycast bereikbaar zijn.

Epiloog

Dit was een beknopt overzicht van de vele onderwerpen die tijdens de 114e IETF-conferentie aan bod kwamen, de tweede conferentie met ‘onsight’ deelnemers sinds de COVID-19 crisis.

Ten opzichte van de 113e IETF was de ‘onsite’ aanwezigheid fors toegenomen. De organisatie had vooraf strikte maatregelen aangekondigd, zoals het verplicht dragen van mondmaskers tijdens de sessies (en social event). Uiteindelijk werden 16 besmettingsgevallen gemeld (wat neerkomt op 2,6% tegenover 2,9% na de vorige meeting).

Het ligt in de bedoeling om de IETF-conferenties voorlopig nog in hybride vorm te blijven organiseren. Dat betekent dat ‘remote’ deelnemers ook actief kunnen deelnemen via Meetecho, daar waar men remote voorheen alleen maar passief kon kijken en luisteren. Hoewel dit nog niet altijd soepel verloopt, gaat het wel steeds beter.



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

De volgende IETF-conferentie is van 5 tot 11 november in Londen.

Photo: Marco Davids

Council of European National
Top-Level Domain Registries

Over CENTR

CENTR is de vereniging van Europese landcode-top-level domein (ccTLD)-registers, zoals .de voor Duitsland of .si voor Slovenië. CENTR telt momenteel 52 volwaardige en 9 geassocieerde leden - samen zijn ze verantwoordelijk voor meer dan 80% van alle geregistreerde domeinnamen wereldwijd.

De doelstellingen van CENTR zijn het bevorderen van en deelnemen aan de ontwikkeling van hoge normen en 'best practices' onder ccTLD-registers.

Volledig lidmaatschap staat open voor organisaties, rechtspersonen of individuen die een landcode-topniveaudomeinregister beheren.

CONTACT

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussel, België
0885.419.166 | RPR Brussels

+32 2 627 5550

secretariat@centr.org

www.centr.org

VOLG ONS

Volg ons op Twitter of LinkedIn om op de hoogte te blijven van de activiteiten en rapporten van CENTR