IETF 95
Buenos Aires
3-8 de abril de 2016

LACTLD agradece a Hugo Salgado (nic.cl), por la revisión de la Edición en Español

Para acceder a la versión en inglés de este informe ira a Highlights de: **https://centr.org/**

Índice

Una visión general sobre el IETF

El IETF que se llevó a cabo en Buenos Aires contó con una cantidad récord de grupos de debate informales (BoF, por sus siglas en inglés) y, hasta cierto punto, implementó lo que el Director del IETF, Jari Arkko, propuso como los próximos trabajos del IETF. Además de las reuniones tradicionales de Grupos de Trabajo (WG, por sus siglas en inglés), el IETF en Buenos Aires parece haber dejado una vista preliminar de las posibles funciones nuevas del IETF como convocante de comunidades hacia temas que conciernen a todas sus áreas de interés. Algunas sesiones ejemplares en Buenos Aires fueron las de "Sistemas inteligentes de transporte" (ITS, por sus siglas en inglés), de redes móviles y cifrado (Accord), y del campo del Internet de las Cosas (IoT - Thing-to-Thing Research Group).

¿Puede el IETF actuar como convocante?

En el área del Internet de las Cosas (IoT, por sus siglas en inglés), la Junta de Arquitectura de Internet (IAB) se las arregló para reunir una serie de empresas, organizaciones y organismos de estandarización que nunca antes se habían acercado de esta manera, según informó Dave Thaler, de Microsoft, durante las sesiones plenarias en Buenos Aires. Junto con la petición de Arkko para que el IETF coopere de manera más activa con la comunidad de código abierto en el documento «Trends», estos avances podrían cambiar el enfoque del IETF hacia uno más abierto que también explore mecanismos de trabajo nuevos.

El impulso posiblemente se dio a partir de la preocupación de que el IETF se convierta en un viejo guardián de protocolos desactualizados que desempeñen un papel secundario en las labores actuales en relación con aplicaciones.

¿Importa el nombre? Sigue la controversia

Para la comunidad de los nombres de dominio, lo más interesante fue el manejo de nombres especiales, los avances en RDAP, y las conversaciones que se mantuvieron en las salas de reuniones sobre el desarrollo en la firma de la zona raíz (KSK, por sus siglas en inglés).

En primer lugar, un grupo de debate de ARCING llegó a un consenso generalizado acerca de la necesidad de contar con un documento nuevo que defina el concepto de «nombre de dominio». Como explicó Ed Lewis de ICANN, los nombres de dominio solo eran una subcategoría de los nombres de Internet y sistemas internivelados, y las correspondientes RFC estándares no contenían una definición clara de los nombres de dominio. Lewis tomó la delantera al ubicar a los «nombres de dominio» en las varias RFCs del IETF, y ahora elaborará un documento borrador para incluir la «definición».

Ted Hardie explicó la necesidad del contexto como indicador para determinar en qué sistema tiene que consultarse/resolverse un nombre de internet. Anunciar el contexto de resolución para un nombre determinado mediante una etiqueta o un prefijo —como en la resolución de nombres de dominio internacionalizados (IDN)— podría ayudar a distinguir entre nombres DNS y otros nombres de internet. El trabajo de ARCING es una continuación y una respuesta a las solicitudes de otros 11 dominios de nivel superior bajo los «nombres especiales» del procedimiento del IETF (RFC 6761).

Es interesante que, contrario a los intentos de evitar de alguna manera conflictos entre los procedimientos de gTLD (Dominios de nivel superior genéricos) de ICANN y la asignación de nombres especiales del IETF, hay al mismo tiempo solicitudes en Redes Domésticas para una asignación IETF adicional para los TLDs de uso especial como homenet y/o .hnsd. Mientras tanto, las solicitudes de dominios especiales que se presentaron en un principio de manera conjunta con la de asignación .onion (.gnu, .bit, .exit, etc.) por el momento no están siendo abordadas. El documento respectivo fue eliminado de la lista de documentos actuales y caducados del WG DNSOP.

El RDAP mediante el uso de OpenID para la autenticación federada y el acceso en capas

El WG RegEXT (antes llamado EPPEXT), además de haber llevado a cabo presentaciones cortas sobre extensiones adicionales requeridas por VeriSign, CNNIC y SIDR, se presentó con el trabajo de VeriSign sobre el uso de OpenID como método para la autenticación de usuarios para el acceso en capas al sistema sucesor de Whois. Hasta junio, los usuarios podrán experimentar la diferencia entre el acceso autenticado y el no autenticado a la información de VeriSign de Whois. Gmail, Hotmail, CZ.NIC y VeriSign Labs son los proveedores de servicios de autenticación para el experimento.

Implementación de las llaves de firma de raíz y zona

De acuerdo con la información brindada por participantes de la reunión del OARC (centro de operaciones, análisis e investigación) que precedió a la reunión del IETF, VeriSign anunció la firma de la clave de firma de zona (ZSK). Una persona cercana al proceso informó que es inminente el anuncio del cronograma para la transición de la llave de firma de la zona raíz (KSK, por sus siglas en inglés).

Versión 1.3 del protocolo de seguridad de la capa de transporte (TLS): casi lista

Al concluir la sesión, uno de los participantes informó que la versión 1.3 TLS hizo un gran avance al llegar a un consenso sobre el manejo de llaves. También se espera que la versión subsiguiente del MPTCP (Multipath Transmission Control Protocol) esté lista pronto.

El IETF por primera vez en América Latina y los debates acerca de la «selección de la sede»

La reunión del IETF que se celebró en Buenos Aires fue la primera en América Latina y, aunque tuvo una buena concurrencia, el número de participantes estuvo por debajo del que se había previsto. En la sesión plenaria se mantuvo un acalorado debate sobre los criterios de selección de la sede, en la que los participantes se concentraron en el problema de la criminalización de las relaciones homosexuales en Singapur, tras una queja de Ted Hardie (Google). Singapur es la sede que se eligió para la reunión del IETF100.

Aspectos destacados

6761: comienza la pelea

La disputa sobre la designación de .onion como dominio de nivel superior de uso especial (SUTLD, por sus siglas en inglés) tuvo como consecuencia debates casi "religiosos" sobre el futuro del registro de nombres especiales, RFC 6761. Tras la preparación del primer planteamiento del problema preparado por un equipo de diseñadores conformado por Alain Durand (ICANN), Peter Koch (DENIC), Joe Abley (Dyn), junto con la participación de Warren Kumari (Google); Ted Lemon (Nominum) presentó otra alternativa.

En esencia, los dos borradores abordan los problemas con el mecanismo de designación de la 6761 que se experimentaron durante la decisión sobre .onion: la falta de claridad sobre qué organismo tiene la capacidad de tomar las decisiones, las condiciones para la asignación, etc. Ambos mencionaron también la obsolescencia/suspensión de la 6761 como una de las posibles opciones de mitigación.

Sin embargo, la propuesta anterior realizada por el equipo de diseñadores es más escéptica de la 6761 y de la forma en que trascendió. La contrapropuesta de Lemon ahora cuestiona los argumentos de "pureza" y ansía encontrar una manera de avanzar con respecto a la 6761, por lo menos quizás permitir un .homenet TLD especial en el WG de redes domésticas en un futuro próximo.

Mientras tanto, otro borrador corto elaborado por George Michaelson (APNIC) solicita básicamente cerrar la 6761.

Dos borradores en competencia en el problema de los nombres especiales

Lemon critica duramente a Durand, Koch, Abley y Kumari por «mezclar distintos problemas» en el planteamiento del problema. Opina que, por ahora, los siguientes tipos de SUTLDs están perfectamente en consonancia con el consenso del IETF:

nombres que deberían resolverse usando el protocolo DNS sin tratamiento especial
nombres que deberían resolverse usando el protocolo DNS, pero que requieren un tratamiento especial en el resolutor.
Los TLDs como «.local» que actúan como señal para indicar que el resolutor stub local debería usar un protocolo no DNS para la resolución del nombre.

En el contexto de los comentarios técnicos de la IAB sobre la raíz única del DNS, la misma RFC 6761 y muchos otros documentos (documentos .onion, nombres locales, el estudio de colisión de nombres de la Autoridad para la Asignación de Números de Internet —IANA, por sus siglas en inglés— y algunos más), Lemon hace referencia a tres tipos de «purezas arquitectónicas», varios «problemas de ocupación/problemas legales» y posibles cuestiones de seguridad.

Con respecto a la pureza, la equiparación de dominios con nombres DNS está implícitamente rechazada (Lemon indica que si el DNS fuera el único protocolo por seguir para resolver nombres de dominio, entonces .local, .onion, y los hosts tendrían que depreciarse). Si la unicidad universal (el hecho de que cada dominio signifique lo mismo en todas partes) fuera a establecerse como una condición, el mDNS quedaría obsoleto. Lemon estima que el cambio de protocolo puede ser un futuro mecanismo solicitado por los resolutores (para evitar filtraciones y problemas de privacidad). La posible competencia o los problemas legales que derivan del periodo landrush/ocupación y del riesgo de demanda por enrutar por fuera de ICANN se pueden enfrentar mediante aclaraciones de casos de uso para las SUTLD del IETF y el proceso de aplicación con la posible colaboración de ICANN en el intento de contar con ayuda para examinar los nombres de manera individual y coherente. Permitir el uso experimental de SUTLDs bajo una extensión .alt podría dar paso a designaciones por tiempo limitado. Esto podría prevenir la designación indefinida de cadenas de caracteres a proyectos que puedan fracasar en el futuro.

La versión de Lemon incluye, en el planteamiento del problema, el trabajo que está realizando en relación con la arquitectura de los nombres en redes domésticas, el cual investiga una posible disociación adicional de los dominios especiales (¿.homenet, .hndb?).

«No se puede pretender que todas las TLDs de uso especial sean nombres no DNS; por ejemplo, es posible que el Grupo de Trabajo de Redes Domésticas proponga el uso de una TLD de uso especial para una red doméstica en los casos en que esta no tenga un nombre único asignado globalmente. De todas maneras, esto podría resolverse de la misma manera en que lo hace la consulta inversa RFC1918, mediante el envío de una consulta a un resolutor local usando el protocolo DNS».

La Base de Datos de Nombres de Redes Domésticas (HNDB, por sus siglas en inglés) de Lemon tiene como objetivo permitir la publicación de servicios de redes domésticas dentro de la red local y también más allá —mientras se evita la colisión de nombres y se provee la asignación y la gestión de los nombres de redes domésticas de una manera automatizada para los usuarios comunes (véase WG de redes domésticas más abajo).

El 24 de abril la RFC 7788, adoptada recientemente, estableció que .home sea la extensión por defecto para todas las consultas de redes domésticas. Pero, curiosamente, no se mencionó una asignación de la IANA en la última RFC. Esto hace que el estado de .home sea incierto —no está asignada ni solicitada en la 6761. Al mismo tiempo, podrían existir quejas de quienes solicitaron la extensión .home en el nuevo proceso gTLD de ICANN (los solicitantes incluyen a Google, TLD Holdings, Uniregistry y otros).

El planteamiento del problema elaborado por Durand, Koch, Abley y Kumari parte de la misma noción de «falta de claridad» de la 6761 y los problemas que esto trae aparejados, e investiga algunos de los problemas más detalladamente.

Aborda problemas arquitectónicos, técnicos y organizacionales. En cuanto a lo arquitectónico, la pregunta de base era: « ¿Nos referimos a un mismo espacio de nombres con diferentes protocolos de resolución o a espacios de nombres independientes?». Esto podría indicar cambios a otros espacios de nombres como en .onion, un cambio a otro protocolo como mDNS o Tor, o la necesidad del uso local de un nombre como en .local o .home. Los autores afirman que ninguno de los cambios se documentó debidamente.

Un punto importante dentro de los problemas técnicos tiene que ver con cómo se manejan las expectativas de los nuevos gestores de TLDs especiales. Se advierte en el borrador que reservar un dominio TLD especial mediante el IETF, por ejemplo, no asegura que las consultas DNS no sean enviadas a través de Internet. La filtración de datos privados se consideró, entonces, como uno de los problemas por tratar.

Con respecto a las cuestiones organizacionales, la causa del problema fue el descuido del proceso: el primer candidato exitoso de la 6761, RFC 6762 (.local), había sido aprobado como una presentación individual sin discusión documentada. Por otro lado, se debatió sobre la extensión .onion (RFC7686) en las DNSOP (DNS Operations) y en el IESG antes de su aprobación —y ahora resultó en el extenso debate sobre las SUTLDs. Los autores también señalan que la adopción de la RFC 6761 fue en primer lugar una presentación RFC individual. Los críticos opinan que el IETF o el IESG deberían haber examinado mejor las especificaciones base de las SUTLD o bien culpan a ICANN por no exigir más debate al respecto.

Finalmente, los autores del primer planteamiento del problema hacen referencia al proceso de aplicación e investigación de ICANN, el que creen sería difícil de imitar para el IETF.

La inclusión de .home en la RFC 7788 sin siquiera considerar un proceso de aplicación de la 6761 podría contribuir al argumento de Abley-Durand-Koch sobre que el IETF no se comporta de manera coherente.

Debate y pasos por seguir

Dos líneas argumentales principales derivan del controvertido debate que se está llevando a cabo en las DNSOP. Una considera que la apertura del proceso de aplicación de las SUTLDs es una oportunidad para mantener al IETF abierto frente a la creciente cantidad de desarrolladores de aplicaciones que crean nuevos sistemas de nombres alternativos, permitiéndoles interactuar con el DNS, lo cual podría pasar a un «segundo plano», según Andrew Sullivan, presidente de la IAB. El grupo central de red doméstica/local (Nominum, Apple, e.a.) incluso advirtió que «no había ninguna ley para que usaran el DNS» (Stewart Cheshire), implicando que los grandes proveedores de aplicaciones estaban al volante. «Un comportamiento coherente por parte del IETF» y la evasión de conflictos con ICANN (MoU RFC2860) son el principal argumento desde el bando «purista». David Conrad señaló que la ICANN no tomaba una posición oficial con respecto a esta controversia (pese a que Durand es autor del planteamiento del problema más crítico). Con la ICANN rehusándose a mostrar su interpretación de la RFC2860, la comunidad del IETF tiene que resolver esta cuestión a los puños.

Mientras muchos participantes celebraban el borrador de Lemon por ser más fácil de leer y más claro, los codirectores de las DNSOP, Suzanne Woolf y Tim Wiczinski, cerraron el Grupo de Diseño después de la reunión y pidieron comentarios acerca de los dos borradores de planteamientos de problemas con la intención de escoger uno antes de la reunión en Berlín.

Stephane Bortzmeyer (AFNIC) posteó un borrador más para ayudar con el «cambio». El borrador sugiere registros DNAME para permitir respuestas NXDomain desde las SUTLDs.

Coexistencia de resoluciones de nombres: un mágico cambio de contexto demasiado difícil de conseguir

La controversia en torno a la designación de nombres especiales en el Domain Name System por el IETF (conforme a la RFC 6761) impulsó un debate más amplio sobre «Alternative Routing Contexts for Internet Naming» (Contextos de enrutamiento alternativos para los Nombres en Internet) con una primera BoF en Buenos Aires. Todavía no queda claro si habrá otro Grupo de Trabajo creando BoF en la próxima reunión del IETF o si los borradores que emanan del ARCING se entregarán a otros Grupos de Trabajo (por ejemplo, al de las DNSOP).

Ser o no ser inclusivos en el DNS – y ¿quién toma la delantera?

En la primera BoF sobre ARCING en Buenos Aires, Suzanne Woolf (codirectora de DNSOP y ARCING) trazó una línea entre el debate sobre ARCING y los pasos siguientes para las 10 aplicaciones extra para los nombres especiales que estaban fuera de alcance.

Para ese momento, los borradores sobre las extensiones .bit, .gnu, .i2p, etc. habían sido eliminados de la lista de documentos del Grupo de Trabajo de DNSOP. Woolf informó a la reportera de CENTR que no podía en ese momento hablar sobre los pasos por seguir en relación con los cosolicitantes de .onion.

En vez de debatir sobre cómo proseguir con las aplicaciones 6761, lo cual Woolf consideró «fuera de alcance», el ARCING pretende abordar el problema mayor, sobre sistemas identificadores alternativos en la red.
El presidente de la IAB, Andrew Sullivan, señaló que, como objetivo general, el IETF debía ocuparse de la interoperabilidad, ya que se están diseñando nuevos sistemas de nombres más rápidamente de lo que puede el IETF reaccionar. El mismo IETF ha desarrollado o al menos aceptado varios sistemas de nombres que ya incluyen el multicast DNS, el sistema Handle o el enrutamiento onion. Según Sullivan, el deseo de crear nuevos sistemas identificadores nunca se esfumaría, sino que seguiría creciendo, por lo que «necesitaremos contar con una manera de hacer que estos identificadores sean útiles».

Steward Cheshire (Apple), autor de la RFC 6761 y de una propuesta para asignar la extensión .home como otra TLD especial en el Grupo de Trabajo de redes domésticas, hizo énfasis en que el IETF no tuvo la opción de no hacer un seguimiento de las iniciativas de la industria. Ciertamente, es interesante comparar las extensiones .home y .bit, .gnu, .exit y el statu quo de la aplicación .home, que son buenos ejemplos de cómo las grandes compañías tienen mejores oportunidades para influir sobre los debates arquitectónicos.

La definición para nombres de dominio y un mecanismo para cambio de resolución

En la BoF se debatieron tres documentos, incluido el de una definición de nombres de dominio, el cual recibió gran apoyo. El autor Ed Lewis (ICANN) observó la falta de una definición «formal y escrita» y explicó que el desarrollo histórico del concepto derivó del sistema de nombre de host, influenciado fuertemente por el SMTP (Protocolo Simple de Transferencia de Correo). En su borrador, Lewis presenta definiciones de Diestel y Lyman Chapin, las cuales, puede esperarse, se debatirán ya sea en un nuevo Grupo de Trabajo o en las DNSOP.

El borrador de Ted Hardie se concentra en el tópico de la sensibilidad del contexto y la idea general de que sería de utilidad conocer dónde tiene que ser resuelto un nombre dado. Las ideas sobre cómo permitir la presentación de un nombre junto con un indicio de dónde debería resolverse se mencionaron brevemente en una solución de subárbol DNS o un delimitador de cadenas de caracteres como en la resolución de contexto de IDN (RFC5891). Hardie señaló que, mientras algunos pidieron como solución rápida para las aplicaciones pendientes para .gnu, etc., el subárbol .alt durante la sesión, otros consideran que eso sería enviarlas a un «gueto». El delimitador de cadenas de caracteres podría «ser utilizado para construir esquemas URI multifacéticos, de los cuales uno de sus aspectos contenga el indicador de protocolo habitual y otro el contexto de resolución».

Las otras dos opciones, simplemente continuar como con la aplicación de nombres especiales de la 6761 o arreglar ya sea el número de gTLDs o el número de contextos de resolución futuros, no eran viables a los ojos de Hardie. En su borrador, Hardie concluye que:

«Claramente, hay compensaciones entre las alternativas disponibles, ya que cada una tiene sus desventajas como indicador de contexto de resolución. Sin embargo, dado que la existencia de múltiples señales podría generar incluso más problemas de interoperabilidad y preocupaciones operacionales, no es deseable la creación de múltiples señales. Cualquier sistema que permita que nombres de Internet de contextos de resolución alternativos sean usados en sistemas de protocolo comunes puede funcionar, siempre y cuando sus desventajas se justifiquen y se mitiguen debidamente».

En Buenos Aires se hizo referencia a otros dos sistemas para el cambio de contexto: el Name System Switch desarrollado para sistemas unix (nsswitch.conf) y clases de DNS. Para el último, sin embargo, el presidente de la IAB, Andrew Sullivan, propone dejar de lado la respectiva RFC.

El tercer borrador explora las propiedades de un servicio de nombre ideal. El autor, Brian Trammell (ETH Zurich, miembro de la IAB), enumeró las siguientes propiedades:

federación, unidad, transparencia y revocabilidad de nombres y su unicidad,
la autenticidad de la delegación y la respuesta (incluida la de respuestas negativas),
coherencia dinámica y respaldo para las incoherencias explícitas, y
apoyo explícito para las compensaciones entre latencia, eficiencia, rastreabilidad, coherencia.

Trammell notó que un sistema ideal se parecería realmente al DNS. De todas maneras, podían hacerse mejoras con respecto a la autenticidad mediante la solicitud de que las firmas sean obligatorias. Según Trammell, esto dejaría obsoletas a las lentamente utilizadas Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC, por sus siglas en inglés).

Stephane Bortzmeyer ha preparado un registro DNAME para las TLDs de uso especial, para resolver el problema de la «incoherencia explícita».

Rotación de Llaves

Aunque no es uno de los temas en la agenda oficial del IETF, hubo algunas novedades con respecto a la rotación tanto de la llave de zona como la llave de la raíz.

Según una fuente cercana al proceso, se anunciará a la brevedad el calendario para la rotación de la llave de firma de raíz. El grupo de diseñadores envió a ICANN las propuestas definitivas hace poco. La fuente informó que, después de un período de observaciones públicas, la ICANN decidió seguir adelante y prepararse para la implementación hacia finales de este año. Se dijo que el anuncio se daría durante estos

días. Queda por ver cómo la ICANN se preparará con respecto a la comunicación que se necesita.

Mientras tanto, durante la reunión OARC que precedió al IETF, Geoff Huston dio otra presentación sobre los problemas por enfrentar en la implementación. Específicamente, el problema de que algunos resolutores de validación podrían ser desconectados de la resolución de dominios firmados. Uno de los problemas principales es que no hay forma de medir el nivel de fracaso en la red DNS de manera global.

Durante otra presentación, VeriSign dio a conocer sus planes para rotar la ZSK a finales del mes. En su rol actual de mantenimiento de la zona raíz en virtud de un contrato con el gobierno de los Estados Unidos, VeriSign había aclarado los pasos con la NTIA (Administración Nacional de Telecomunicaciones e Información) y la ICANN, según informó una fuente. Expertos opinan que «esconder» la ZSK detrás de la firma KSK no arrojará luz en la rotación de la KSK. Otra pregunta sin responder tiene que ver con la intención de VeriSign de considerar la pronta rotación de las llaves .com y .net. Ninguna ha sido implementada anteriormente.

Muchos expertos piensan que fue negativo evitar la rotación por tanto tiempo —o no establecer un calendario para la rotación en las especificaciones del IETF antes de que se firmara la raíz. Se espera que el día de la transición haya altos y visibles tasas de error.

Grupos de trabajo, grupos de debate informal y partes de sesiones plenarias

REGEXT

El grupo de trabajo REGEXT sigue destacándose en dos aspectos: no se desempeña de la misma forma que el típico grupo de trabajo del IETF, sino que aprueba las extensiones en los Protocolos de Registro (el EPP y el RDAP son el paso por seguir). No solo estos temas entre Registrador y Registro son altamente específicos, sino que a veces no queda claro qué viene primero: si la política ante ICANN entre registro y registrador, o las especificaciones técnicas que pueden volver a la ICANN como «estándares del IETF». En Buenos Aires, el WG decidió esperar, por el momento, el desarrollo de políticas en la ICANN con respecto a una propuesta del RDAP presentada por personal de ICANN.

El WG EPPEXT, el cual fue reorganizado con una nueva denominación (WG REGEXT), tiene una extensa lista de documentos considerados hitos en su nueva acta constitutiva. No es necesario que las extensiones de registro enumeradas sean sometidas a prueba para determinar si «aprueban como documento WG o no», sino se convirtieron automáticamente en documentos WG. El calendario se extiende desde febrero de 2016 hasta junio de 2017 (véase abajo), y termina con el tema del acceso de proveedores terceros a las bases de datos del registro/registrador. Sobre esto último, Olafur Gudmundsson (Cloudflare) propuso un documento específico (Operador externo de DNS para el protocolo de registros y registradores), el cual todavía no está entre los hitos.

Grandes usuarios del proceso por el momento siguen siendo VeriSign y CNNIC. La ICANN también es presentadora frecuente. Otros registros con una o dos propuestas en la lista actual de hitos son ICANN, CIRA y CentralNIC.

El borrador de CentraINic sobre «extensiones de tarifa» examinó tres opciones con respecto a los objetos incluidos —ya sea mantener la sintaxis existente y que no haya relación entre los objetos enumerados en la parte principal (A), incluir solo un elemento, la información de tarifa que se calcula para cada objeto en la parte principal (B) o permitir elementos varios y la información de tarifa que se calcula para cada combinación objeto y extensión (C). Haciendo referencia a posibles problemas relacionados con DDOS (ataque de denegación de servicios) a la información sobre tarifas de extensión, Alexander Mayrhofer (nic.at) pidió una opción C limitada que permita a los registradores revisar, crear y renovar los precios en un solo comando, un elemento «periodo» por «comando».

Otros borradores que se debatieron brevemente en Buenos Aires fueron tres elaborados por el CNNIC, uno de la lista de hitos sobre la extensión del revendedor (draft-zhou-eppext-reseller-mapping) y dos nuevos, sobre la verificación de contacto del EPP y sobre el mapeo de los nombres de dominios. La ICANN presentó otros dos borradores nuevos, ambos relacionados con el RDAP (draft-lozano-rdap-nameservers-sharing-name, draft-lozano-ietf-eppext-registrar-expiration-date). No obstante tanto los participantes como los Directores decidieron que sería prematuro adoptar el borrador sobre la fecha de expiración, ya que la ICANN todavía deber tomar decisiones con respecto a las políticas correspondientes.

Autenticación federada para el acceso en capas al RDAP

El RDAP ya es un tema incluido en varios borradores. En una presentación sumamente interesante, Scott Hollenbeck de VeriSign describió un proyecto piloto que se está llevando a cabo para utilizar OpenID para la autenticación federada para permitir el acceso en capas a la futura base de datos del RDAP, planificado por la ICANN (¿VeriSign y otros?) para ser usado como el protocolo sucesor de Whois. Por ahora, usar credenciales de Yahoo, Google, CZNic y VeriSign permite obtener un conjunto de datos del RDAP más amplio. Al mismo tiempo, Hollenbeck destacó que VeriSign no estaba interesado en convertirse en proveedor de credenciales/IDs.

Jun 2017	Enviar para su publicación una RFC informativa con los requisitos para un protocolo de registros para proveedores externos de DNS
Feb 2017	Enviar para su publicación «CIRA IDN EPP Extension» draft-wilcox-cira-idn-eppext
Feb 2017	Enviar para su publicación «EPP IDN Table Mapping» draft-gould-idn-table
Feb 2017	Enviar para su publicación: draft-ietf-eppext-idnmap
Oct 2016	Enviar para su publicación «Allocation Token Extension for EPP» draft-gould-allocation-token

Oct 2016	Enviar para su publicación «Change Poll Extension for EPP» draft-gould-change-poll
Jun 2016	Enviar para su publicación «EPP Domain Name Mapping Extension for Bundling Registration» draft-kong-eppext-bundling-registration
Jun 2016	Enviar para su publicación «EPP China Name Verification Mapping» draft-xie-eppext-nv-mapping
Jun 2016	Enviar para su publicación «Verification Code Extension for EPP» draft-gould-eppext-verificationcode
Abr 2016	Enviar para su publicación «EPP Reseller Mapping» draft-zhou-eppext-reseller-mapping
Abr 2016	Enviar para su publicación «Reseller Extension for EPP» draft-zhou-eppext-reseller
Abr 2016	Enviar para su publicación «Registry Fee Extension for EPP» draft-brown-epp-fees
Abr 2016	Enviar para su publicación «EPP and RDAP Status Mapping» draft-gould-epp-rdap-status-mapping
Mar 2016	Enviar para su publicación «TMCH functional specifications» draft-ietf-eppext-tmch-func-spec
Mar 2016	Enviar para su publicación «Launch Phase Mapping for EPP» draft-ietf-eppext-launchphase

Grupo de trabajo sobre DNSOP: Clases del DNS en discusión — Chequeos en delegación de dominios e intentos para robustecer el sistema

Además de los temas más importantes: el conflicto sobre los TLDs de uso especial y el futuro del enfoque del IETF en cuanto a los nombres (vea los aspectos destacados arriba), se incluyó en dos sesiones de grupos de trabajo en Buenos Aires la revisión de una extensa lista de borradores en vigor y algunas propuestas nuevas. Una propuesta controvertida que se debatió tenía que ver con la idea de evitar que las "clases" se usen en el DNS en un futuro y, como consecuencia, que se cierre el registro de la IANA correspondiente. Muchos de los borradores que se debatieron en Buenos Aires intentan combatir los ataques de denegación de servicio (DDoS, por sus siglas en inglés) y ataques de amplificación de una u otra manera, por ejemplo el cacheo negativo agresivo de NSEC/NSEC3, la clarificación de las respuestas NXDomain y la limitación o incluso la denegación de responder solicitudes *any.*

Tres anteproyectos preparados por Cloudflare (y socios) ya están en la última llamada del WG o cerca de estarlo: los problemas para la utilización de la extensión DNSSEC que derivan de una infraestructura que no cumple con las normas (Roadblock Avoidance), la limitación de respuesta «*any*» desde los resolutores (o la completa denegación de respuestas *any*, como lo propone un segundo documento) con el objeto de evitar el abuso de respuestas largas para la amplificación, y la implementación de una opción para

«eliminar el registro DS» y una para «habilitar la validación de DNSSEC» para CDS y CDSKey. Esta última habilitará el aviso del cese o el comienzo de una validación DNSSEC desde el usuario a su proveedor DS.

Lo que sigue a continuación para la última llamada del WG, según Tim Wicinski, copresidente de DNSOP, es una clarificación de las respuestas NXDOMAIN que pondrá como regla que un resolutor de caché DNS debe dejar de buscar en su caché al momento en que se encuentre una respuesta NXDOMAIN almacenada.

Otro intento para detener los ataques DDoS sobre los servidores DNS es el llamado cacheo negativo agresivo NSEC/NSEC3. Hacen que la condición de coincidencias exactas para cacheos negativos sea más flexible (a.example.com, b.example.com). Conforme al anteproyecto de K. Fujiwara (JPRS) y A. Kato (Keio/WIDE), «cuando una consulta por nombre tiene un registro de recurso coincidente NSEC o NSEC3 en el caché, y no existen comodines (wildcards) en la zona a la que pertenece la consulta del nombre, un resolutor completo tiene permitido responder con un error NXDOMAIN de inmediato». Y ese procedimiento de coincidencia se puede aplicar a todos los nombres de dominio ancestros de los nombres de consulta. Una cuestión a tener en cuenta es que quizás los nombres de dominio asignados recientemente en una zona tengan que esperar para que sea efectiva la información negativa de expiración. Otro enfoque alternativo ("cheese-shop") no seguirá siendo revisado por el WG.

Sobre la base del desarrollo de una nueva herramienta para controlar las delegaciones de zonas, el Zonemaster, preparado por expertos en IIS y AFNIC, Patrik Wallström (IIS) y Jakob Schlyter (Kirei), presentó como propuesta un documento que enumera los requisitos de delegación DNS. El documento describe todos los requisitos de una «delegación correcta de nombres de dominio DNS», y al mismo tiempo puede usarse como base para un conjunto de pruebas de delegación. Algunos debates en el WG sobre qué alcance debería tener el documento fueron bienvenidos —solo como un documento informativo, de mejores prácticas o normativo. Para el caso en el que fuera normativo, algunos participantes solicitaron una revisión exhaustiva sobre la coherencia en relación con el comportamiento normativo para la asignación DNS esparcida en varias RFCs. También existió un debate sobre el alcance con respecto a qué conjunto de requisitos serían aceptables ampliamente —solo un conjunto mínimo o uno que intente ser exhaustivo.

Otro de los problemas que se discutió en Buenos Aires fue el posible cierre del registro de Clase DNS en la IANA. Andrew Sullivan (Dyn/Director de IAB) propone interrumpir el registro debido a su mal funcionamiento. Las opiniones fueron diversas, muchos expertos estuvieron de acuerdo, pero una cantidad similar de miembros se opuso a esa terminación, ya que el problema no eran las clases de DNS: «el problema es el software mal escrito», (Wes Hardacker, Parsons). Hardacker y otros como Mark Andrews recomendaron considerar escribir «directrices operacionales en las que diferentes clases sean asignadas en paralelo». Algunos problemas podrían solucionarse usando clases.

En Buenos Aires también se discutió la «opción Key Tag EDNS» y una actualización del algoritmo DNSSEC. La opción Key Tag EDNS tiene el fin de permitir a los «resolutores

validadores finales que señalen a un servidor qué claves se referencian en su cadena de confianza» (vea el borrador). Las extensiones permitirán a los administradores de zona monitorear el progreso de las transiciones en una zona DNSSEC firmada.

El WG sobre DNSOP mantuvo de nuevo dos sesiones en Buenos Aires y cuenta con una lista importante de nuevas RFCs recientemente publicadas o en vías de ser publicadas. Entre el IETF94 y el 95 fueron publicadas 5 RFCs, lo que representó un número récord:
• draft-ietf-dnsop-root-loopback RFC7706
• draft-ietf-dnsop-dns-terminology RFC7719
• draft-ietf-dnsop-5966bis RFC7766
• draft-ietf-dnsop-qname-minimisation RFC7816
• draft-ietf-dnsop-edns-tcp-keepalive RFC7828

Quedan tres borradores en cola para el editor de las RFCs:
• draft-ietf-dnsop-rfc6598-rfc6303
• draft-ietf-dnsop-edns-chain-query
• draft-ietf-dnsop-edns-client-subnet

DPRIVE: más allá de la privacidad oportunística

Con la especificación base DPRIVE «DNS sobre TLS» realizada y el acercamiento de DNS sobre DTLS adicional, la última llamada del WG se concentra en los próximos pasos, especialmente en la autenticación de servidores recursivos y en perfiles de uso (estrictos, oportunísticos y sin opciones de privacidad).

El WG decidió que el tópico de la autenticación se tratará en un documento específico extra que el grupo está revisando actualmente. Está destinado a contribuir al perfil de privacidad oportunística y al perfil más estricto de privacidad fuera de banda vinculada a una llave descrito en la especificación base original DNS-sobre-TLS. La autenticación de la configuración directa del servidor del servidor recursivo y DHCP se considera con la verificación obligatoria ya sea mediante X.509 o DANE.

El debate en Buenos Aires se enfocó principalmente en cómo manejarían los usuarios varios perfiles y mecanismos de seguridad y cómo se vulneró mucha de la privacidad oportunista. Por otra parte, Christian Huitema (Microsoft) sostuvo que existía la necesidad de permitir a los usuarios un fácil cambio de escenarios de uso (por ejemplo, en las consultas de servidor DNS desde una red de oficina o un cibercafé).

Además se planteó brevemente la cuestión de si el WG debería esperar más implementación antes de seguir adelante. También hay preparado un borrador sobre la medición del despliegue DNS sobre TLS.

Algunas posibles dificultades con respecto a la seguridad de las negociaciones de cero RTT (zero RTT handshake), que se espera estén incluidas en la nueva especificación TLS 1.3, son:
• que los datos no sean enviados de manera secreta

• que no se ofrezcan garantías para los reintentos entre conexiones
• en el caso de un servidor comprometido, un atacante podría manipular los datos 0-RTT sin ser detectado

Homenet (“Red doméstica”)

El WG de red doméstica está haciendo avances en varios aspectos; ha decidido que Babel será el protocolo de enrutamiento y está avanzando con respecto a la arquitectura de nombres. Durante las sesiones en Buenos Aires, se le dedicó un periodo de tiempo considerable al sistema de nombres.

La arquitectura de nombres de redes domésticas abordará todas las cuestiones relacionadas con el sistema de nombres:

Proveer un espacio de nombre en el cual se puedan publicar los nombres y anunciar servicios
Asociar un nombre dentro de ese espacio de nombre al conjunto de direcciones IP en las que el host sea localizable
Publicar servicios disponibles en la red local y asociar tales servicios con los nombres publicados en el espacio de nombre
Distribuir los nombres publicados en ese espacio de nombre a los servidores que puedan ser consultados para resolver nombres.
Corregir la publicación de los servidores de nombres que pueden ser consultados para resolver nombres
Eliminar en su debido momento los nombres publicados que ya no estén en uso

Estas consideraciones son clave para la arquitectura de nombres de la red doméstica, concretamente el suministro de una especie de sistema híbrido: la publicación de algunos servicios de redes domésticas debería solamente estar dirigida a usuarios de redes domésticas, mientras que otros podrían publicarse de manera más amplia, a usuarios fuera de las redes domésticas. Se espera que los servicios se publiquen fuera de red para algunos enlaces y no para otros.

La automatización debería ayudar a evitar errores, según lo que propone Lemon. *«Todas las operaciones que se mencionan aquí deben funcionar de manera fiable y automática, sin que sea necesaria la intervención del usuario o los análisis de errores. Incluso al punto tal en que los usuarios puedan hacer aportes en relación con la política, como por ejemplo, si un servicio debería o no publicarse fuera del hogar. El usuario debe ser capaz de brindar de manera segura tales opiniones sin contar con un modelo mental correcto de cómo funciona el sistema de nombres y el servicio de detección, y sin ser capaz de hacer razonamientos detallados relativos a la seguridad».*

Los conflictos con respecto a los nombres también deberían resolverse de manera automática. También se apoyará el multihoming «y por lo tanto, se necesita el apoyo a los dominios de suministro múltiple para lidiar con las situaciones en las que el DNS pueda arrojar distintas respuestas dependiendo de si se consultan los resolutores de cache en

un ISP o en otro».

Es interesante señalar que, solo días después de la reunión IETF95, se anunció la RFC 7788, que acordó establecer .home como la cadena de caracteres para los nombres en .homenet, sin considerar las posibles colisiones o el proceso completo de la asignación de nombres especiales del IETF (ni hablar de una aplicación de la ICANN para .home).

Caducando IPv4: ¿una locura o una buena señal?

Se desarrolló un intenso debate en el WG “Sunsetting IPv4” sobre la necesidad de que el IETF anuncie efectivamente el fin del ciclo vital del IPv4. Lee Howard (Time Warner) propuso el borrador que declara que «el IPv4 es histórico». Mientras algunos alertaron que esto es «una verdadera locura», después de un poco de debate, hubo algunos expertos que afirmaron que sería bienvenida una fuerte señal por parte del IETF, para seguir adelante con IPv6.

Según la RFC 2026, una especificación para la cual hay una nueva versión, se convierte en «histórica». Con el IPv6 disponible y en crecimiento, Howard dijo a esta reportera que en EE. UU. era bastante probable esperar que el 80% de las direcciones IP sean IPv6 dentro de los próximos 5 años. Afirmó que el IETF debería dejar de desperdiciar trabajo en tecnologías de transición para lo que el WG Sunsetting IPv4 se creó originalmente, después de que llegaran muchas propuestas a v6Ops. Las consecuencias de declarar histórico al IPv4 no solo se traducirían en suspender las actualizaciones para IPv4 —sino de hecho, ni siquiera se corregirían los errores.

Geoff Huston (APNIC) alertó que producir porquerías no es el trabajo de un organismo de normalización serio: puede que otros organismos de normalización quieran asumir las funciones del IETF. Frenar los desarrollos de doble pila v4/v6 sería como una invitación para ellos. Huston vociferó que sería incluso peor si «nos pusiéramos creativos de nuevo». También mencionó las consecuencias de que el IETF rechace el desarrollo de los estándares para la traducción de direcciones de red. Indicó que, por el momento, entre 50 y 60 millones de dispositivos serían empujados dentro del sistema de doble pila.

Los ingenieros de Facebook, Apple y Microsoft, interviniendo a título individual, fueron más acogedores. Al continuar resolviendo problemas del IPv4, el IETF creó la expectativa de que el IPv4 estaría en funcionamiento durante mucho tiempo. Se celebraron con entusiasmo los anuncios como el de Apple, que decidió que el sistema iOS9 usaría únicamente IPv6.

Ruediger Volk (Deutsche Telekom) y Fred Baker (Cisco) ofrecieron una alternativa para dar una fuerte señal: en vez de declarar histórico el IPv4, el IETF podría anunciar un estado de «fin de ingeniería» o «fin del ciclo de vida». El fin de la ingeniería se equipara a que todavía esté disponible, pero no se podría esperar que haya nuevas características. Hasta ahora, casi siempre se copiaron las características interesantes nuevas del IPv6 en el IPv4, lo que hizo que el nuevo protocolo no pudiera destacarse.

Howard admitió que su propuesta de declararlo «histórico» podría ser algo prematura, pero argumentó que puede haber reguladores que podrían intervenir cuando algún proveedor ya no ofrezca IPv4. O bien podría ser una cuestión de competencia: algunos competidores nuevos tendrán que invertir mucho en la transición mientras que otros están cómodos sobre un colchón de ricas y antiguas reservas de direcciones.

UTA y los correos electrónicos seguros: en competencia con el protocolo DANE

La «Seguridad de transporte estricta» es un intento de los proveedores de servicio de correo electrónico (Google, Yahoo, Comcast, Microsoft, LinkedIn y 1&1) para obligar el matrimonio entre TLS (seguridad de la capa de transporte) con SMTP (el protocolo para la transferencia de correo simple), de manera que sea menos «oportunista». Para prevenir los ataques de "disminución de versión", los servidores de correo publicarán políticas que permitan al distribuidor de servicios de correo verificar si los servidores de correo receptores ofrecen TLS. En Buenos Aires, Mark Risher, de Google, afirmó que algunos proveedores hasta estarían satisfechos con la mera opción de informar. Las políticas podrían almacenarse como un registro de recurso nuevo o como un archivo de texto en el DNS.
Según Risher, el enfoque que se debatió intensamente en Buenos Aires en el WG UTA está en competencia con DANE y pretende estarlo de la manera en que se aborde la falta de utilización de DNSSEC. Indicó que, en vez de esperar la utilización de DNSSEC, se propuso el STS del SMTP. Sin embargo, el respaldo de los controles de políticas vía DNS (¿Y podríamos hacer que sea seguro, por favor?) pone una vez más en tela de juicio el no esperar a DANE. Como alternativa, se debatió la autenticación via WebPKI para dar lugar a un control de políticas de correo seguro. Con el debate en curso, parece que esto es algo que se desarrollará rápidamente en el borrador.

Otro enfoque en discusión considera el Mail User Agent Strict Transparency, que permitirá que los usuarios tomen decisiones fundadas con respecto al nivel de seguridad que están dispuestos a aceptar. El MUA STS, como se lo nombrará en vez del anterior «deep», brindará una variante más segura (TLS entre cliente de MUA y el servidor de correo) como la opción por defecto. El color indicará si una conexión determinada no se mantiene a la par del nivel de seguridad. El usuario deberá seleccionar el predeterminado para bajar el nivel de seguridad. Un simple «enviar de todas formas» desde el predeterminado seguro no estaría aceptado, conforme con el estandar propuesto. Solo un «trabajar sin conexión» o «intente nuevamente más tarde» serían las opciones, según comentó el autor, Chris Newman.

En vez de StartTLS, MUA STS usará TLS implícito, lo que permite negociar el TLS para la primera conexión (haciendo una señal sobre un puerto especial).

Polémica sobre la selección de las sedes

¿Debería el IETF considerar más criterios de selección desde la perspectiva de los derechos humanos o debería la comunidad del IETF, ante todo, tener más voz y voto en la elección de la sede? Las autoridades del IETF se enfrentaron con respecto a este asunto.

La selección de la sede para las reuniones IETF se convirtió en un importante tema de discusión en Buenos Aires, después de que Ted Hardie, ingeniero de Google y colaborador del IETF desde hace mucho tiempo, tomó el micróno para oponerse férreamente contra la sede elegida para el IETF100. Manifestó que Singapur todavía condena las relaciones homosexuales, lo que haría imposible traer familias a las reuniones del IETF para los participantes del colectivo LGBT.

Refiriéndose a los miembros del comité IAOC (quienes usualmente sí vienen con sus familias), Hardie pidió que «tengan la decencia de no llevar a sus familias a la reunión IETF100». Muchos miembros de la comunidad apoyaron a Hardie en el debate en sesión plenaria que le siguió. Varios de los miembros se enfurecieron cuando Tobias Gondrom, Director del Fondo de Inversiones del IETF y miembro de IAOC, intentó explicar que había demasiados criterios diferentes para poner en la balanza.

Aún antes de la plenaria, ya había existido un descontento importante con respecto al proceso de selección por varios motivos. Un BoF dedicado a la selección de la sede brindó explicaciones extensas sobre los criterios abordados actualmente en el proceso de selección de IAOC. Los criterios, además de las necesidades reales de espacio (las últimas reuniones del IETF contaban con hasta 1.300 asistentes) y la preferencia por la regla de que se efectúe «bajo el mismo techo» (es decir, al menos un tercio de los participantes puede encontrar una habitación de hotel en la sede del evento) incluyen cuestiones de patrocinio y otros aspectos. Hasta hay que tomar en cuenta si hay supermercados cerca, para tener opciones más baratas en cuanto al servicio de comidas. Aquí podrá encontrar un borrador RFC informativo.

Desde la perspectiva política, mantener una actitud abierta (para las reuniones y las relaciones) es uno de los principios fundamentales. Los problemas con la concesión de visas hicieron que haya un claro rechazo a elegir sedes estadounidenses en los últimos años, hecho que de vez en cuando critican algunos participantes estadounidenses (que son todavía mayoría).

Se informó que la reunión de Buenos Aires, impulsada por el director del IETF, Jari Arkko, fue una reunión muy costosa (que dejó un déficit presupuestario), a pesar de poner en práctica los planes de diversidad del IETF.

Los próximos pasos en relación con la elección de la sede incluyen la decisión de IAOC sobre la renegociación de la sede del IETF100, más debate sobre el mecanismo de selección, y discusiones sobre los criterios de selección.

Con el fin de lograr transparencia en lo que respecta a la selección de sedes, el IAOC pidió que la comunidad haga comentarios sobre los posibles problemas que pueden

aparecer con respecto a estas ciudades en consideración: París, Montreal y Copenhague.

Próxima reunión IETF: Berlín, del 17 al 22 de julio de 2016.