

SAN JUAN – Cómo funciona: Operadores de servidores raíz

Lunes, 12 de marzo de 2018 – 10:30 a 12:00 AST

ICANN61 | San Juan, Puerto Rico

CATHY PETERSEN: Buenos días a todos. Bienvenidos a esta sesión “Cómo funciona”. Realmente después de esta maravillosa ceremonia de apertura estamos un poco demorados pero vamos a iniciar nuestra sesión en breve. Gracias.

ORADOR DESCONOCIDO: Vamos a dar inicio a la sesión en dos o tres minutos. Vamos a empezar 15 minutos más tarde porque se demoró la ceremonia de apertura. Les pido por favor que estén aquí todos dentro de dos o tres minutos para empezar.

CATHY PETERSEN: Buenos días a todos. Vamos a iniciar la sesión de “Cómo funciona”. En esta sesión vamos a hablar de los operadores de servicio raíz. Nuestro primer presentador es Andrew McConachie.

ANDREW MCCONACHIE: Hola. Mi nombre es Andrew McConachie. Trabajo para el apoyo del RSSAC de la ICANN. Vamos a hablar entonces del sistema de servidores raíz. Primero vamos a hablar de que tenemos cuatro

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archive, pero no debe ser considerada como registro autoritativo.

secciones. Una que es las generalidades del sistema de nombres de dominio, cómo está el sistema de servidores raíz hoy y sus características. Después le voy a pasar la palabra a Steve Sheng. Él va a hablar y va a dar una explicación de lo que es el Anycast. Vamos a hablar entonces de lo que es RSSAC y algunas actividades recientes del RSSAC. Después va a haber un lugar para preguntas y respuestas. También tenemos aquí operadores de servidor raíz que van a poder venir al estrado y contestar las preguntas. Pueden hacer cualquier tipo de pregunta.

Vamos a hablar ahora de las generalidades de lo que es el sistema de nombres de dominio y los servidores raíz. Vamos a ver qué son las direcciones IP y cuáles son los identificadores dentro de Internet. Las direcciones IP son los identificadores. Ustedes saben que tuvimos distintos protocolos IPv4, IPv6. También necesitan igual una dirección IP para poder operar. Esto se trata de una etiqueta numérica. Realmente no son amigables para los seres humanos porque son solo números.

Ustedes saben que no funciona del todo bien el clic. ¿Por qué necesitamos el DNS? El problema original, como se mencionó anteriormente, es que las direcciones de IP son difíciles de recordar y cambian mucho. El problema original con el DNS es tener algún nombre recordable por los humanos que nos pueda servir para no tener que recordar las direcciones IP. También hay algunos problemas modernos como por ejemplo que las

direcciones de IP pueden estar compartidas y que puede haber direcciones múltiples de IP que van a un único servicio. Podemos tener este problema de muchos a uno y uno a muchos, que se suma al problema original que tenía que ver con lo difíciles que eran de recordar las direcciones IP.

El sistema de nombres de dominio es jerárquico. Como pueden ver, en este diagrama tenemos una raíz. Por debajo tenemos lo que nosotros llamamos los TLD o dominios de alto nivel, donde tenemos .EDU, .MIL, .UK. Además de eso tenemos lo que se suele referir como segundo nivel y tercer nivel, etc. Este es un mapeo de lo que son las direcciones de IP pero hay otros mapeos también y otros mapas que se utilizan como pueden ser los servidores de correo electrónico, los reversos o lo que se llama PTR, la dirección vuelve a los nombres, por eso se llaman inversos.

Aquí es un poco complejo lo que muestra. Me voy a detener. En esta imagen tenemos el proceso de resolución del DNS. Cómo utilizamos entonces la experiencia del DNS cuando el usuario pasa por los distintos pasos. Este es el flujo de qué significa la interacción con el DNS para que el usuario pueda resolver un nombre de dominio o una dirección y, obviamente, un sitio web. Aquí a la derecha tenemos, si queremos ir a www.ejemplo.com, como servidor web, lo primero que hacen... Tenemos un navegador, tenemos un pedido al DNS y ese pedido al DNS pasa

al servidor recursivo de nombres. Este servidor recursivo, si no tiene nada en su caché, para los fines de esta demostración no tenemos nada en el caché. No conoce nada. Está vacía.

Lo que tenemos es una consulta para `www.ejemplo.com`. Tiene que hacer mucho trabajo antes de darle una respuesta al usuario. Lo primero que va a hacer es ir a la raíz. Le va a decir a la raíz: “Hey. Aquí tengo `www.ejemplo.com`. ¿Dónde está?” La raíz le va a decir: “No sé dónde está pero sí sé dónde está `.COM`”. Entonces vuelve al servidor de nombres recursivos donde la dirección de los `.COM` está incluida. Este servidor recursivo le va a decir al servidor de nombres: “¿Dónde está `www.ejemplo.com`?” Y le dice: “No sé dónde está todo esto pero sí sé dónde está `ejemplo.com`”. Este es el servidor que tiene eso. El servidor de nombres recursivos pasa a tener la dirección de `ejemplo.com` y va al servidor de nombres `ejemplo.com` y le dice: “¿Dónde está `www.ejemplo.com`?” Finalmente, le da la respuesta que está buscando y el servidor de nombres recursivos puede responder al usuario con la dirección `www.ejemplo.com`. Así entonces nuestro usuario atraviesa todo el proceso de resolver el nombre de dirección y llegar al sitio web.

Aquí hay cosas que no mencioné, que tienen que ver con la seguridad. La DNSSEC o lo que se llama el aspecto de seguridad del DNS que son que estas preguntas entre el servidor de nombres recursivos y cada uno de estos servidores autoritativos

de nombres, que es el servidor de nombres de raíz, el servidor de nombres .COM y el servidor de nombres ejemplo.com son los autoritativos. Este servidor de nombres recursivos puede validar que la respuesta es correcta a través de estas extensiones. Que no ha habido ninguna interferencia, que no fue el servidor de nombre autoritativo incorrecto. Todo esto se hace a través de las DNSSEC. Este es el proceso de resolución de nombres de dominio.

Ustedes saben que tengo que intentar varias veces para que funcione el puntero. Como vimos anteriormente, el servidor de raíz no tiene el TLD como .COM, etc. Sin embargo, en general no se hace mucho. En el ejemplo previo nosotros tenemos esta situación hipotética con el servidor de nombres recursivos que estaba encendido y no tenía nada en la memoria caché. Esto es bastante raro en general porque los servidores de nombres recursivos tienen bastante en la memoria caché y en general esto se resuelve desde la memoria caché. Es decir, no hay muchas consultas que lleguen a la raíz. No tantas como se puede pensar originalmente.

Vamos a ver algunas de las cosas modernas que pasan. Nosotros a veces hablamos de seguridad DNSSEC, extensiones de seguridad DNSSEC o las DNSSEC. La idea es que tienen que firmar respuestas que van al servidor de nombres recursivos para que las pueda validar. Por validar estoy diciendo que este

servidor puede decir que es la respuesta correcta porque fue firmada criptográficamente por una clave. Tenemos la certeza de que es correcta.

También ha habido mejoras en la privacidad. Es algo en lo que se sigue trabajando, sobre todo a través del IETF. Hay cosas como la seguridad transportada por capas, que garantiza que se transmite toda la consulta y que no lo pueden ver ojos ajenos. Esto es lo que se está desarrollando.

Hay otro ajuste que es el Anycast. Anycast lo usan mucho los operadores de servidores raíz porque hay dos cosas importantes en el Anycast. Una es que hay servidores múltiples que pueden compartir una única dirección IP y además evita los ataques DDoS. Después Steve Sheng va a hablar mucho más de Anycast y de cómo funciona.

Zona raíz versus servidores raíz. La zona raíz son los datos a los que prestan servicio los servidores raíz. Es decir, la zona raíz es el punto de partida donde tenemos los TLD y es la parte superior del árbol de jerarquía. Esto lo genera la ICANN a través de la política de la comunidad. Lo tiene a su cargo la entidad de mantenimiento de la zona raíz. Además es el contenido de la base de datos de los servidores raíz. Es decir, son los datos que utilizan los servidores raíz.

Por otro lado, los servidores raíz son los que responden con datos de la zona raíz. En la actualidad hay 13 identidades y más de 900 instancias en distintos lugares de todo el mundo. Los servidores raíz tienen una función técnica. Prestan servicios a la zona raíz. Cada una de estas nubes Anycast que operan los operadores de servidores raíz tiene la responsabilidad de esta zona raíz.

Vamos a ver qué hacen los operadores de servidores raíz. Son 12 grupos de ingeniería profesional diferentes que se concentran en lo que es la estabilidad y confiabilidad del servicio, la accesibilidad para todos los usuarios de Internet. Son profesionales y cooperan unos con otros a la vez que actúan independientemente. Son diversas organizaciones, lo que significa que son técnica, organizativa y geográficamente diversas.

Sin embargo, los operadores no participan en la generación de las políticas. Tampoco en la modificación de los datos sino que prestan los datos que están precisamente en la zona raíz. Son los que prestan servicios a estos. Son los que implementan modificaciones técnicas, las evalúan también. Hablan de las normas a través del IETF y además garantizan que el servicio sigue siendo estable, pueda ser accedido por todos quienes quieran hacerlo y que además sea sólido.

Estas fueron las generalidades del DNS. Es bastante técnico. Espero que no haya sido tan técnico. Ahora vamos a pasar a lo que es el sistema de servidores raíz. Hoy en día, cuáles son algunas de sus funciones. En algún momento va a pasar la imagen. Ahí está.

Vamos a ver el crecimiento del sistema de servidores raíz. Aquí podemos ver un poco de historia con las cifras de los servidores raíz, las entidades durante los años de la década de los 80. Ustedes pueden ver cómo ha avanzado. Desde 1998 tenemos 13 identidades diferentes. Los cambios en general tuvieron que ver con las demandas técnicas así como temas de escalabilidad. Hoy en día ustedes saben que con Anycast no tenemos más problema de escalabilidad. Realmente ha sido una herramienta fantástica y ha solucionado todos los problemas de escalabilidad. Los servidores raíz hoy en día funcionan con IPv6 e IPv4. Hay 13 pares de direcciones IPv4 e IPv6, más de 900 instancias.

Estos son algunos de los principios fundamentales del sistema de servidores raíz. Son cinco. Es importante que el sistema de servidores raíz provea una plataforma flexible, confiable y estable para el sistema de nombres de dominio que opere para el bien común de todo Internet. La IANA es la fuente de los datos raíz de DNS. Los cambios de la arquitectura se realizan sobre la base de la evolución técnica y de la necesidad técnica

demostrada y la operación técnica. Las expectativas del DNS están definidas por el grupo de trabajo de ingeniería de Internet, o el IETF. Si están interesados en un poco de historia de este sistema de servidores raíz, pueden bajarse, si así lo desean, el RSSAC023 donde tienen toda la historia de todo el sistema de servidores raíz. Esto está en la página del RSSAC.

Estos son entonces los operadores de los servidores raíz hoy en día. Podemos ver que hay 13 identidades. Tenemos aquí a la izquierda el nombre del host. Después tenemos las direcciones IP que, como dije, son IPv4 e IPv6 para todos ellos. Algunas de estas direcciones IPv4 e IPv6, al menos todas las IPv4, funcionan en la nube de Anycast. Es decir, por detrás hay muchos servidores. Más de 900 pero esto crece permanente. La última vez que di esta presentación decía más de 800 instancias y ahora estoy diciendo que más de 900 instancias. Constantemente está creciendo.

Aquí para que vean dónde están los servidores raíz. Esto es de root-servers.org. Es una imagen general de dónde están los servidores raíz. No es exactamente precisa porque no les dice exactamente, por ejemplo, que existen siete instancias en Madagascar. Es un gráfico. Es interesante. Si quieren, pueden ir al sitio web que mencioné abajo y profundizar. Dice después cuáles son las ciudades en las que está cada una de las

instancias pero esta es una imagen general. Si van al sitio web, obviamente pueden profundizar en la información.

Aquí tenemos la estructura de la gestión de la zona raíz. Aquí tenemos la zona raíz, cómo llegan los datos. El operador de TLD necesita hacer un cambio en la zona raíz. Quizá tiene que ver con los registros. Tienen que cambiar algo de la información que tiene que ver con alguno de los registros para el TLD. Lo que hacen es ir a la IANA, hacer ese cambio. Ese cambio entonces va a aparecer en la entidad encargada del mantenimiento de la zona raíz, que va a ser Verisign y creo que dos veces por día hacen la distribución de ese cambio. Lo distribuyen a toda la zona raíz, a todos los operadores de la zona raíz. Los operadores de la zona raíz son los responsables para que esto vaya a la nube Anycast y que respondan a todas las consultas que pueden llegar de los resolutores.

Vamos a ver algunas de las funciones de los operadores del servidor raíz. Existe una diversidad de estructura organizativa, de historia operativa, porque a veces es diferente. También utilizan distintos hardware y distinto software, distintas plataformas de hardware, distintas plataformas de software. Esto ayuda en la seguridad porque entonces hay una correlación entre una mayor diversidad y una mejor seguridad. También tienen distintos modelos de financiamiento porque son distintos tipos de organizaciones y por eso obtienen sus fondos de distintos

medios. Comparten las mejores prácticas en lo que es la seguridad física. También el sobreaprovisionamiento de capacidad que puede tener que ver con algún ataque DDoS y también tienen personal confiable y profesional.

Cooperan a través de distintas reuniones de la industria en la comunidad. La ICANN es una de ellas pero también tenemos el grupo de trabajo de ingeniería de Internet, NANOG, DNS-OARC, que es un grupo de operaciones e investigación. También utilizan herramientas de colaboración basadas en Internet. Son transparentes en sus operaciones. También hacen coordinación para prepararse para posibles emergencias, para proteger la infraestructura en caso de catástrofes u otro tipo de emergencias. También hay actividades periódicas para precisamente ayudar a esta respuesta en caso de emergencias y no puedo leer la última viñeta porque me desapareció de la pantalla.

Las respuestas a una Internet en evolución. Internet evoluciona. Se necesitan nuevos requisitos en el sistema del DNS. Con el tiempo ustedes saben que los operadores de la zona raíz implementaron el IPv6, DNSSEC, los IDN, como mencionamos aquí, porque hay muchos en la zona raíz y también Anycast. Lo importante es mejorar lo que es la solidez, la capacidad de respuesta y la flexibilidad. Como dije, hay más de 900 instancias Anycast en el mundo que están implementadas hoy en día.

Esos son algunos de los mitos. Los mitos que puede tener la gente o falsos entendimientos o malentendidos de lo que es. Por ejemplo, los servidores raíz controlan dónde va el tráfico. Esto no es así. No puedo decir que es mentira en absoluto pero no es verdad porque son los routers o los enrutadores los que controlan el tráfico. Quizá este mito surgió porque los mapas de DNS mapean los nombres a las direcciones IP pero en definitiva son los enrutadores lo que, basados en la dirección de IP, controlan dónde van los paquetes. La mayor parte de las consultas de DNS son manejadas por los servidores raíz. Como vimos en el ejemplo, es verdad si el caché está vacío pero esto no pasa en la realidad. En general, las consultas de DNS no son manejadas por el servidor raíz sino en la memoria caché del servidor de nombres recursivos.

La administración de la zona raíz y la provisión de servicios son lo mismo. Este es otro mito. Esto no es así. En el diagrama quizá tendría que haber mostrado la división de responsabilidad sobre cómo cambia porque esto hace que atravesase la zona raíz pero hay diferentes partes involucradas.

Por otro lado, las identidades de servidores raíz tienen un significado especial. No es así. Existen solo 13 servidores raíz. En realidad hay más de 900. Otro mito es que los operadores de servidor raíz realizan las operaciones en forma independiente. Si bien sí lo hacen, son organizaciones independientes, hay mucha

coordinación y hay mucha cooperación entre ellos para garantizar que existe un servicio estable en todo el sistema de servidores raíz.

El último mito es que los operadores de servidores raíz solo reciben la porción TLD de una consulta cuando esto no es así. Reciben toda la consulta. Así funciona el DNS. Sí hay un trabajo en el grupo de trabajo de ingeniería de Internet para cambiar esto, si a alguien le interesa. En realidad pueden ir a lo que se llama QNAME minimization. Ahí pueden ver la porción superior de lo que es la consulta o query. Ahora le voy a ceder la palabra a Steve Sheng, mi colega. Él les va a hablar de Anycast.

STEVE SHENG:

Muchas gracias, Andrew. Me llamo Steve Sheng. También soy personal de apoyo de RSSAC en el área de políticas. Les voy a dar una explicación de Anycast y también de RSSAC y sus actividades. Anycast es un término de dirección y de ruteo. Hay dos términos aquí: Unicast y Anycast. Hay diferencias importantes entre ambos. En Unicast los paquetes o los datagramas de las distintas fuentes van todas al mismo destino en una única instancia que sirve a todas las fuentes. En caso de que haya un ataque de denegación de servicio distribuido todo el tráfico va a ir a esa instancia única. Eso es Unicast. Mientras que en Anycast hay múltiples instancias que sirven a los mismos

datos para llevarlos a todas las fuentes. Todos tienen la misma dirección IP, estas distintas instancias, y hay políticas de enrutamiento intermedias que determinan el destino basándose en las fuentes. Es decir, que la fuente llega al destino más cercano más rápido y el tráfico de ataque de DDoS es enviado a la instancia más cercana.

Les voy a dar un ejemplo para que entiendan esto. Voy a mostrarles un diagrama. Aquí tenemos un ejemplo de Unicast. Aquí vemos una fuente, un punto de origen, y un destino. Este es el destino identificado como una instancia única. El tráfico llega a ese destino único a través de la ruta más corta. Aquí, en Anycast, podemos ver que hay tres puntos de destino en azul. Estos destinos están publicados con la misma dirección de IP. La política de enrutamiento determina cuál es el destino más cercano a esa fuente. Esto significa que la ruta desde una fuente hasta un destino se acorta y los datos se entregan de manera más rápida.

¿Cómo ayuda esto a lidiar con los ataques de DDoS? En este tipo de ataques el atacante ataca el destino pero como tenemos este enrutamiento por Anycast el tráfico solamente va al enlace más cercano. Por lo tanto, uno de los destinos puede estar sobrecargado pero los otros todavía pueden atender ese tráfico.

Una de las preguntas que nosotros recibimos muchas veces en estas sesiones tutoriales tiene que ver con el sistema de servidores raíz y sus redes. Algunos de ustedes son operadores de redes, otros operan otro tipo de instancias. Si son operadores de redes van a querer tener tres o cuatro instancias cercanas. Esto obtiene la instancia que está más cercana a ustedes y reduce el tiempo de viaje de ida y vuelta del tráfico.

A su vez, ustedes quieren aumentar las conexiones con los pares y todos esos ordenamientos. A veces pueden tener una instancia más cerca de ustedes pero el tráfico igualmente va por todo el mundo para llegarles a ustedes. Eso es por las conexiones de pares que tienen. Esto también es un factor importante que tener en cuenta.

Si ustedes son operadores de resolutores recursivos para aumentar el guardado en la memoria caché pueden considerar implementar la tecnología RFC7706. Esto da una copia de la zona raíz en una dirección en loop, en bucle. Esto significa que muchas veces se reduce el riesgo de privacidad de un resolutor recursivo al servidor raíz a partir de ese punto de origen. Es importante activar la validación de DNSSEC en los resolutores para asegurarse de tener datos no modificados en todo ese tráfico, como mencionó Andrew, a través de los datos correctos.

Por último, y creo que porque estamos en ICANN, nosotros invitamos a los expertos técnicos y a otros profesionales a sumarse y a partir y a aportar al consejo del RSSAC. Aquí es donde tenemos todo el asesoramiento técnico del RSSAC, donde se genera todo ese asesoramiento. Les voy a dar un resumen general de las actividades de RSSAC.

RSSAC significa que es el comité asesor del sistema de servidores raíz, que tiene el mandato de brindar asesoramiento a la comunidad de la ICANN y a la junta directiva sobre cuestiones relacionadas con la operación, la administración, la seguridad y la integridad del sistema de servidores raíz de Internet. Tengan en cuenta que aquí suman datos. Su ámbito de operación es muy acotado dentro de la comunidad de la ICANN. Hay que hacer una distinción que es importante, que muchas veces entra en conflicto con otras partes en la ICANN. El RSSAC es un comité que genera asesoramiento, principalmente para la junta directiva, pero también para otros órganos de la ICANN y otras organizaciones que participan en el negocio del DNS en general.

Los operadores de los servidores raíz están representados dentro del RSSAC. Es importante destacar que en sí mismo el RSSAC no se involucra con cuestiones operativas. Creo que esta es una distinción muy importante para hacer porque no queremos confundir estas dos entidades.

Dentro del organigrama de gobernanza de la ICANN es uno de los tres comités asesores... No, en realidad son cuatro. Son cuatro comités asesores. Asiste al ecosistema de la ICANN desde este punto, aquí en el organigrama. Dentro de su organización el RSSAC está compuesto por representantes designados de los operadores de servidores raíz y cada uno de estos a su vez puede designar a un remplazo o a un suplente en el RSSAC. También hay coordinadores de enlace con las organizaciones técnicas clave y con los socios en los servidores raíz. El consejo de RSSAC que mencioné antes es un órgano conformado por expertos voluntarios en temas específicos. Los miembros son confirmados por el RSSAC basándose en sus expresiones de interés. Los copresidentes del RSSAC son Brad, de Verisign y Tripti de la Universidad de Maryland. ¿Tripti y Brad están en la sala? Allí está Brad. No veo a Tripti pero tal vez haya salido momentáneamente de la sala.

Dentro del RSSAC hay distintos coordinadores de enlace. Uno corresponde al operador de las funciones de la IANA, la entidad de mantenimiento de la zona raíz. Andrew les mostró ese diagrama donde teníamos todo el flujo del mantenimiento de la zona raíz. Estas son dos entidades muy importantes. También tenemos coordinadores de enlace de la junta de arquitectura de Internet, la IAB, que nos da orientación en términos de

arquitectura a ISOC y el IETF en temas vinculados con la arquitectura de Internet.

Dentro de la ICANN, el RSSAC tiene un coordinador de enlace con el comité asesor sobre seguridad y estabilidad, la junta directiva de la ICANN, el Comité de Nominaciones de la ICANN, el Comité Permanente de Clientes que fue establecido para que analizara el desempeño de las funciones de la IANA realizadas por la PTI en este momento.

Por último, un comité de revisión de la evolución de la zona raíz. Este es un comité que fue conformado como parte del proceso de la transición de la custodia de las funciones de la IANA para analizar las cuestiones de arquitectura desde el punto de vista de la evolución de la zona raíz.

El consejo del RSSAC tiene 88 expertos técnicos en este momento. Sus expresiones de interés se han dado a conocer públicamente y para los miembros del consejo que contribuyen al trabajo hay un reconocimiento al final de cada informe. Se asigna un crédito en forma pública por el trabajo que hacen a nivel individual. El propósito es que los expertos en el DNS aporten su conocimiento especializado a las publicaciones, que haya transparencia con respecto a quién hace el trabajo que está en los archivos y que también haya un contexto para realizar las tareas. Si les interesa sumarse al consejo del RSSAC, esta es la

dirección de correo electrónico a la que tienen que enviar la información: rssac-membership@icann.org.

Aquí tenemos alguna de las publicaciones más recientes del RSSAC. RSSAC tiene una serie de publicaciones. Utiliza esta numeración. Actualmente tenemos el 31. Las últimas tres publicaciones son el RSSAC029, que describe los resultados de un taller que se hizo en octubre de 2017; el documento 030, que es una declaración sobre las entradas en las fuentes de raíz del DNS y 031 es una respuesta al grupo de trabajo sobre el proceso de desarrollo de políticas de la GNSO que se ocupa de los procedimientos posteriores a la introducción de los nuevos gTLD. La respuesta de RSSAC a ese grupo de trabajo tiene que ver con la escalabilidad de la raíz. Hay una sesión pública que va a realizar el RSSAC esta semana. Por favor, asistan para tener más detalles sobre estas publicaciones.

El trabajo actual que está realizando el RSSAC corresponde a dos áreas: la armonización de los procedimientos de anonimato para la recolección de datos y los tamaños de paquetes y el DNS. El 002 corresponde al RSSAC y los operadores de la zona raíz implementan eso para recolectar estadísticas sobre los servidores raíz en el sistema de servidores raíz. Hay un esfuerzo continuo por ver los procedimientos de anonimato para algunos de esos datos. Luego tenemos el otro grupo de trabajo que se ocupa de los tamaños de paquetes y el DNS.

Desde que se produjo la reestructuración del RSSAC en el 2013, se le ha dado mucha importancia a la meta de ser transparentes. Se ha logrado mucho avance en este sentido al establecer un consejo, al publicar todas las actas y los informes de los talleres de modo que la comunidad de la ICANN pueda entender cuál es el estado actual del trabajo y los informes de los talleres.

Hay un calendario público del RSSAC y del consejo donde se enumeran todas las reuniones de cada grupo de trabajo y hay sesiones públicas siempre en cada una de las reuniones de la ICANN. Tenemos también los tutoriales y las relaciones con los coordinadores de enlace para asegurarnos de que la información fluya hacia las organizaciones principales.

Por último, el RSSAC ha calificado los procedimientos operacionales que determinan cómo opera el RSSAC. Eso también está en el sitio web. Creo que ahora estamos pasando por la tercera revisión de estos procedimientos. Los operadores de los servidores raíz también toman medidas para mejorar la transparencia. Las agendas de los operadores de los servidores raíz son publicadas para las reuniones del IETF. Todos los operadores publican estadísticas de RSSAC002. Participan en RSSAC. Hay una página web pública, una única página web y a partir de allí ustedes pueden ingresar a las páginas web de cada uno de los operadores.

Hay colaboración en los informes sobre acontecimientos importantes. Por ejemplo, los eventos de ataque de DDoS del año pasado. El RSSAC actúa como una puerta de entrada para canalizar todas estas preguntas técnicas a los operadores de los servidores raíz, quienes van a responder estas preguntas. Si necesitan más información, aquí tienen el enlace para la página web principal del RSSAC. Si tienen alguna pregunta de índole general, la pueden enviar a esta dirección de correo electrónico. El enlace para la página web del consejo aparece aquí para solicitar ser miembros.

Quiero que presten atención al hecho de que el RSSAC recientemente publicó en su sitio web una sección de preguntas frecuentes. Creo que hay 25 preguntas que normalmente surgen. Algunas de ellas son generadas a partir de este tipo de sesiones y son muy útiles para entender el funcionamiento del RSSAC. Habiendo dicho esto, creo que hemos llegado al final de la presentación. Tenemos algunos miembros del RSSAC aquí. Quisiera invitarlos a que se sumen a la mesa principal, que se presenten y yo voy a actuar de moderador en caso de que haya preguntas. Con esto invito a los colegas del RSSAC a que se acerquen aquí a la mesa principal. Si tienen alguna pregunta, por favor, levanten la mano y nos dicen quiénes son. Vamos a hacer eso. Les voy a pedir primero a los miembros del RSSAC que se presenten.

FRED BAKER: Fred Baker.

JOHN CRAIN: John Crain, de ICANN.

KAVEH RANJBAR: Kaveh Ranjbar, de RIPE NCC.

BRAD VERD: Brad Verd, Verisign.

LARS-JOHAN LIMAN: Lars-Johan Liman, Netnod.

STEVE SHENG: Vamos a comenzar con una pregunta en línea.

CATHY PETERSEN: Tenemos una pregunta de José de la Cruz. La pregunta dice:
“¿Hay planes para ampliar las entidades a más de 13?”

STEVE SHENG: “¿Hay planes para expandir las entidades a más de 13?” ¿Quién quiere responder esta pregunta?

KAVEH RANJBAR: Yo puedo comenzar. Técnicamente debería ser posible expandirlas. Esa es la primera respuesta pero creo que la pregunta real es por qué deberíamos expandir la cantidad de identificadores. Esas letras básicamente son identificadores pero desde el punto de vista de la tecnología, si ustedes se fijan en la situación actual, agregar nodos o letras no va a tener una diferencia técnica significativa. ¿Cuál es el problema que están tratando de solucionar para agregar nuevos identificadores? Esa es mi respuesta.

BRAD VERD: Yo quisiera agregar que esta es una pregunta que es recurrente. Nos la hacen a menudo y la respuesta es que RSSAC está considerando no solamente agregar sino también quitar algún identificador. Tal vez 13 no sea el número correcto. Tal vez sean más o menos. No tenemos una respuesta definitiva. Es una de las cuestiones que tenemos en nuestra lista de trabajo para tratar pero, como dijo Kaveh, el objetivo sería resolver una cuestión técnica con esa respuesta.

STEVE SHENG: Gracias, Kaveh y Brad. Ahora tomamos preguntas. El señor que está aquí delante.

CATHY PETERSEN: Por favor, díganos quién es y a qué organización pertenece.

ABDULKARIM OLOYEDE: Muchas gracias. Soy Abdulkarim, de Nigeria. Soy becario por primera vez en la ICANN. Mi pregunta tiene que ver con los servidores raíz. Cada uno de los 13 servidores raíz están replicados en todas partes del mundo con la misma dirección de IP. Si hay un problema con una de las duplicaciones, ¿cómo pueden diferenciar si tienen la misma dirección de IP? ¿Cómo lo pueden resolver? Gracias.

FRED BAKER: Esto tiene que ver con el trabajo de Anycast. En las presentaciones anteriores se hizo referencia a este tema. Lo importante aquí tiene que ver con el enrutamiento. Cada uno de los servidores no solamente presta el servicio de responder a una solicitud y tiene una traducción sino que también se vincula con los ISP o con los IXP con los que está asociado. Allí anuncian la dirección. Entonces, cuando una solicitud pasa de alguien a esa dirección, el enrutamiento lo va a dirigir a la instancia del servidor que está lógicamente más cerca. Ahora, si uno de los servidores tiene un problema, si se pierde el enrutamiento, si ocurre un problema de alguna manera, esa dirección de ese

lugar ya no va a tener un enrutamiento de BGP sino que va a haber otras instancias que van a ofrecerle ese enrutamiento a esa misma dirección. El enrutamiento lo va a llevar a otro lugar. Así es como funciona el enrutamiento.

En el peor de los casos, y yo no sé por qué esto ocurriría, pero supongamos que se produce el caso de que la dirección ya no está disponible y el enrutamiento no existe. Uno de los motivos por los que tenemos 13 de estos servidores es para que la aplicación que hace esa solicitud, el resolutor en la computadora de alguien pueda utilizar otra dirección y hacer el pedido a otro lugar. Es como que hay un backup allí. Hay una reserva allí.

STEVE SHENG: Gracias. ¿Liman?

LARS-JOHAN LIMAN: Quisiera decir que cuando utilizan Anycast, cada servidor tiene dos direcciones IP. Una de ellas es la misma para todas las computadoras. Eso es lo que se usa para el tráfico de DNS. Además, cada servidor tiene una dirección única separada que utilizan los operadores para poder llegar desde atrás, digamos. Para hacer toda la parte de administración del servicio.

JOHN CRAIN: Sí. Creo que lo que está diciendo tiene que ver con una consulta de texto donde cada instancia tiene un nombre que se puede hacer la consulta dentro de los datos. Después se lo puedo mostrar personalmente en la computadora.

STEVE SHENG: Gracias. La persona que está en el fondo.

ORADOR DESCONOCIDO: Gracias. Soy de India. Parte de la seguridad del DNS tiene que ver con DNSSEC. ¿Nos podría decir en qué país fue completamente implementado el DNSSEC y cuáles fueron los problemas con la implementación?

STEVE SHENG: ¿Alguien puede responder a esto?

LARS-JOHAN LIMAN: Me parece que el miércoles hay un taller de DNSSEC. Al inicio van a mostrar la implementación que ha tenido en todo el mundo. Creo que ahí va a encontrar la información que está buscando.

BRAD VERD: De hecho, está un poco fuera del alcance del RSSAC. Para reformular la pregunta, quizá si hablamos de los atributos podamos entonces responder a lo que acaba de preguntar.

KAVEH RANJBAR: Como operadores, nosotros tenemos un archivo cada servidor raíz. Todo pasa después de que se haya recibido ese archivo de la zona raíz. Desde nuestro punto de vista, nosotros verificamos el archivo de la zona raíz y entonces ver la integridad de ese archivo. Nosotros preservamos esa integridad para mantenerlo cuando hay un archivo distribuido o cuando hay un contenido distribuido.

STEVE SHENG: Muchísimas gracias por eso. ¿Alguna otra pregunta? Caballero.

TARAU BAUIA: Yo soy Tarau, de Kiribati. Tengo una pregunta. Cuando implementamos las DNSSEC, ¿habría problemas con los subdominios por debajo de .COM o cuando cambiemos para el DNSSEC con las claves? ¿Sería un problema eso?

STEVE SHENG: Me parece que esto también es una pregunta de DNSSEC. Creo que sería mejor formularla en el taller de DNSSEC. Lo invito a que

vaya a ese taller, por favor. Cualquier cosa, yo le voy a dar los detalles de dónde se realiza ese taller. Gracias. Ahora vamos a pasar... Un segundito. Tenemos una pregunta en línea y después sigue usted.

CATHY PETERSEN: Tengo otra pregunta de José de la Cruz. Es: “¿Quién puede participar en el RSSAC?”

BRAD VERD: Este es un grupo de expertos. Tenemos más de 80 miembros expertos en temas específicos. Todos nuestros grupos de trabajo vienen de este grupo de expertos o consejo. Creo que está aquí en pantalla la membresía. Si están interesados pueden enviar entonces un correo electrónico al comité, que es el que revisa esa solicitud y tienen que manifestar dar una SOI, que es lo que llamamos declaración de interés para ser parte de este grupo de expertos y ser parte de la solución.

STEVE SHENG: Gracias, Brad. Gracias, José, por esa pregunta.

KAVEH RANJBAR: Perdón. Quiero agregar algo. La mayor del trabajo técnico del RSSAC lo hace este grupo de expertos. Básicamente el trabajo se

da ahí. El RSSAC, como dice aquí, son las 12 organizaciones donde ya mencionamos que hay 13 operadores. Hacen la mayor parte del trabajo administrativo. Cuando recibimos una pregunta o cuando se necesita un asesoramiento, nosotros generamos un grupo de trabajo dentro del grupo de expertos y entonces son todos los miembros del comité los que son también parte de este grupo de expertos. Si quieren ser parte de la solución, entonces también pueden ser parte de un grupo de trabajo. Cada pregunta que nosotros recibimos como comité asesor genera un grupo de trabajo. El trabajo se genera dentro de este grupo de expertos.

BRAD VERD:

Además, si bien se le da al grupo de expertos el trabajo, si uno es alguien de los que contribuye, también va a recibir parte de ese trabajo y puede ser parte de los grupos de trabajo.

STEVE SHENG:

Gracias.

ABDULKARIM OLOYEDE:

Soy Abdulkarim. Quiero saber cada cuánto se reúne el RSSAC y cada cuánto se reúne el grupo de expertos.

BRAD VERD:

El RSSAC se reúne una vez por mes. Tenemos llamadas una vez por mes donde hay actas también y hablamos de distintos temas. Estas llamadas son públicas... ¿No? Perdón, las actas son públicas. Las actas. El RSSAC se reúne aquí, en las reuniones de la ICANN y también en los últimos años hemos tenido dos talleres por año y hemos estado trabajando con cierto trabajo de evolución. Si asisten a la reunión pública del RSSAC van a escuchar hablar de ellos.

En lo que hace al grupo de expertos, ellos trabajan en línea junto con los grupos de trabajo. Esos trabajan permanentemente, depende de cada grupo de trabajo y puede ser o una llamada por semana o cada dos semanas. Eso depende de la carga de trabajo. El grupo de expertos se reúne aquí, en la AGM y esto lo determina este grupo específico. Ellos son los que dicen cuándo necesitan reunirse. La última vez se decidió que nos reuniríamos en la asamblea general de la ICANN y en cualquier otra reunión del IETF, que es justamente donde coinciden las reuniones con el grupo de expertos.

STEVE SHENG:

La próxima reunión es el IETF 102 en Montreal. ¿Alguna otra pregunta? El caballero de la izquierda.

BONNIE MTENGWA: Gracias. Mi nombre es Bonnie Mtengwa. Vengo de Zimbabue, del regulador telefónico. Nosotros tenemos un servidor raíz pero querría saber cómo nos pueden ayudar como estado para tener un servidor raíz o si tenemos que negociar con el operador o cómo, porque es quizá la respuesta que nos dio ICANN. No sé si hay algún otro requisito que tenemos que cumplir.

STEVE SHENG: Gracias por manifestar el interés de tener el servidor raíz.

LARS-JOHAN LIMAN: La mayor parte de los operadores de servidores raíz tienen nubes Anycast. Realmente pueden participar en negociaciones. No sé si es con el país y el servidor raíz sino con quien ofrece ese servicio de host porque eso tiene que ver con algún ISP grande o algo por el estilo. Obviamente, como dijo, hay algunos requisitos que son financieros y técnicos. Estamos trabajando nosotros en recopilar distintos puntos de contacto pero le diría que podría hablar con cualquier operador de servidor raíz y nosotros vamos a tratar de explicar de qué forma vemos la relación o cuáles son nuestros requisitos desde nuestro lugar. Lo mismo cada uno desde su lugar. Obviamente, puede haber un servidor raíz en su entorno si se cumplen los requisitos. Tiene que funcionar, por eso existen requisitos.

STEVE SHENG: Gracias, Liman. ¿Alguna otra pregunta? Aquí, el caballero de frente.

ABDULKARIM OLOYEDE: Soy Abdulkarim otra vez más. Estuve pensando que el DNS, el servidor raíz, es una parte importante de la Internet. Lo que tiene que ver con el RSSAC y cómo funcionan los operadores parece muy abierto. ¿Qué pasa con los que atacan los servidores raíz? Cualquiera puede unirse, cualquiera puede ser parte de las reuniones. Cualquiera puede contribuir. ¿No hay peligro en eso? ¿Cómo lo manejan?

STEVE SHENG: Sí, siempre hay gente mala.

KAVEH RANJBAR: Es una buena pregunta. Hay distintas facetas. Una de las cosas que yo creo, y estoy hablando de RIPE NCC, es que no podemos garantizar la seguridad en forma total. Somos abiertos pero no solo la forma en la que trabajamos sino que el diseño del DNS también es abierto. Ustedes pueden ver cuáles son las instancias, los hosts, etc. Es público. Es fácil ver dónde está todo esto en el DNS. Es un sistema muy abierto. La capacidad que

nosotros tenemos desde el punto de vista tecnológico trata de garantizar responder a todas las consultas. Sí, es verdad que nosotros también recibimos lo que pueden ser consultas ilegítimas, por ningún motivo o para hacer un ataque, pero en general tenemos capacidad como para ver de qué se trata y poder prestar servicios a las consultas adecuadas.

JOHN CRAIN:

Estas son redes manejadas por profesionales. Todos los operadores tienen las habilidades y tienen además a los ingenieros y la gente profesional porque nosotros consideramos la integridad de nuestros sistemas desde un punto de vista muy serio. Si tenemos un host y hay requisitos, y los requisitos también son quién puede tener acceso a la máquina, etc. La seguridad es algo que nosotros consideramos con muchísima seriedad y, como dijo Kaveh, la idea es que el DNS por definición y por forma de estar estructurado es muy abierto. Esta es la naturaleza del protocolo, por llamarlo de alguna manera.

STEVE SHENG:

Brad.

BRAD VERD:

Específicamente, yendo a su pregunta, creo que en el RSSAC el grupo de expertos es abierto. Cualquiera puede unirse. ¿Cómo

evitar que alguien haga algo malicioso? Eso es lo que usted pregunta, si algún miembro puede unirse con estos fines. Ese es un riesgo, sí. Existe. Queremos ser abiertos, queremos ser transparentes y queremos tener multiplicidad de puntos de vista para llegar a la mejor solución, para algún problema técnico que se nos presente. Yo, como copresidente, creo que hay suficientes pesos y contrapesos de gente con buenas intenciones como para identificar gente que tiene otro tipo de intenciones, para ver qué es lo que está sucediendo. Al momento, me parece que nunca pasó nada de eso. Pero sí, es un riesgo.

STEVE SHENG: El caballero del fondo.

ORADOR DESCONOCIDO: Hola. Mi nombre es [inaudible]. Vengo de India. Quiero volver a lo que se señaló anteriormente en la presentación sobre el tráfico que no lo determina el servidor raíz sino el enrutador. Querría preguntarles sobre todo en lo que tiene que ver con lo que señalaron en los requisitos del RSSAC002, que tenía que ver con los operadores del servidor raíz, que debían publicar las estadísticas del servidor raíz. Si yo quiero determinar entonces cuál es el tráfico total de Internet o de un lugar en particular o de un país en particular, ¿cómo puede extrapolar todo eso de parte

de las estadísticas que ya existen en línea y que son de fuente abierta?

BRAD VERD: Yo creo que la respuesta más corta es que no se puede. El tráfico de raíz del DNS no se tiene que considerar como medida del tráfico total de Internet.

ORADOR DESCONOCIDO: No, pero yo pregunto cómo puedo hacer una estimación o aproximación, lo más aproximadamente posible. ¿Utilizando el tráfico del DNS?

KAVEH RANJBAR: Básicamente, incluso para tener una estimación útil no hay que utilizar el DNS porque no es la plataforma pero sí hay otras técnicas de medición. Por ejemplo, Google MLAP. Ellos tienen el tráfico que ven y tratan de estimar el resto del tráfico del país pero no el DNS porque no es la plataforma correcta. En primer lugar, el contenido no pasa por el DNS. En segundo lugar, lo que se obtiene del DNS en cualquier nivel, sobre todo en la raíz, tiene que ver con los resolutores de caché. Eso no nos resulta visible a nosotros. Básicamente es imposible incluso tener estimaciones útiles para el tráfico del DNS.

FRED BAKER: Cuando vamos al sistema de raíz, las estadísticas del RSSAC002 dicen: “Tengo estos pedidos de IPv6, etc.” y son pedidos a la raíz. Es gente que está tratando de encontrar los .COM, los .NET o lo que sea en el mundo. No particularmente están analizando una locación en particular, incluso una compañía en particular sino que están buscando registros. No son los datos correctos.

STEVE SHENG: Gracias. ¿Alguna otra pregunta? ¿Tenemos alguna pregunta en línea?

CATHY PETERSEN: No, ninguna.

STEVE SHENG: Hay una.

ABDULKARIM OLOYEDE: Una vez más. En lo que tiene que ver con el RSSAC y organizar la generación de capacidades, ¿hacen algo al respecto? Digo generación de capacidades para los países en desarrollo y quienes estén interesados, porque muchas veces, si por ejemplo tengo interés y nunca vi nada de esto, ¿cómo puedo estar interesado en algo que ustedes hacen? A veces hablan en un

lenguaje demasiado técnico porque no lo veo en mi vida diaria pero sí querría aprender más.

KAVEH RANJBAR:

No sé si entendí adecuadamente la pregunta. En primer lugar, quiero agradecerle porque es la primera vez que viene, es uno de los becarios, así que esto ha sido muy interactivo y le agradezco mucho toda su participación. En lo que hace a generación de capacidades, cada operador de zona raíz individual tiene su plan. Nosotros en RIPE NCC tenemos tareas específicas pero no solo en nuestra región sino que también hablamos de la región de Asia-Pacífico y África. Nosotros nos reunimos con otros RIR, por ejemplo, y tenemos un MOU con África o con APNIC para el caso de Asia-Pacífico. Voy a utilizar el ejemplo de África. Lo que nosotros hacemos en África es que AfriNIC formó una alianza con ISOC África y hay un financiamiento y hablan con los operadores, con las partes interesadas. De hecho, nosotros también tenemos algunas actividades que tienen que ver con esa actividad, con ese financiamiento. Esa es la metodología que nosotros estamos utilizando en RIPE y otros tienen otros métodos y otras formas de llegar a la población en las distintas regiones.

Quiero mencionar algo también porque hubo una pregunta sobre cómo conseguir instancias de raíz. Además de los servidores, tienen una lista de operadores. Además, tienen el

sitio web de esos operadores para el servidor raíz. También para Verisign, etc. Pueden encontrar esos datos. Por ejemplo, nuestros acuerdos con los RIR están también en esa lista.

BRAD VERD:

Si puedo agregar algo, muchas de estas preguntas son operativas por naturaleza y tenemos aquí algunos operadores de servidores raíz pero hago referencia al mandato del RSSAC. Nosotros damos asesoramiento sobre el sistema de servidores raíz a la junta directiva y a la comunidad. Muchas de estas preguntas no están dirigidas al RSSAC como tal. Queremos ser transparentes, queremos ser abiertos pero existe un límite entre lo que son los operadores de la raíz y el RSSAC. Quiero que esto quede claro.

STEVE SHENG:

Muchas gracias. ¿Alguna pregunta más? A la una... Liman.

LARS-JOHAN LIMAN:

Un último comentario. Si después de esta sesión se les ocurre alguna pregunta, por favor, acérquense a hablar conmigo o con cualquiera de mis compañeros. Queremos hablar con ustedes. Con gusto vamos a darles todas las respuestas que podamos.

BRAD VERD: Nuevamente, quiero resaltar el hecho de que en la página web del RSSAC hemos agregado toda la sección de preguntas frecuentes. A veces no podemos capturar todas las preguntas que nos hacen pero sí tenemos las más recurrentes. En estas presentaciones han surgido preguntas y en otros ámbitos nos han hecho estas preguntas, así que tenemos una lista de preguntas frecuentes que van evolucionando. Si ven que tienen una pregunta y no aparece en esa lista, acérquense a nosotros. Nosotros la vamos a agregar a nuestra lista de preguntas frecuentes. Así la alimentamos.

STEVE SHENG: Habiendo dicho esto, les quiero mostrar aquí en la pantalla, en nuestra página web del RSSAC que tenemos reuniones el grupo de expertos, las publicaciones y las preguntas frecuentes. Cuando hacen clic en el enlace van a encontrar mucha más información sobre las actas de las reuniones, los miembros del grupo de expertos, las publicaciones del RSSAC y las preguntas frecuentes. El sitio web: root-servers.org que se mencionó contiene la puerta de entrada a los sitios web de cada uno de los operadores en forma individual. Aquí es donde ustedes pueden ver, en la presentación, que nosotros les mostramos el mapa con todas las instancias Anycast. Pueden ahondar, pueden acercarse aquí y llegar a más información en ese sitio web.

Si no hay más preguntas, les agradezco por su participación y a los miembros del RSSAC por sus respuestas a las preguntas. Muchas gracias. Damos por concluida esta sesión.

CATHY PETERSEN: Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]