MONTREAL – Cómo funciona: operaciones de servidor raíz
Domingo, 3 de noviembre de 2019 – 15:15 a 16:45 EDT
ICANN66 | Montreal, Canadá

STEVE CONTE: Vamos a comenzar en unos minutos. Estamos en una sala excesivamente grande. Si se quieren acercar, nos podemos ver. La manera en que lo vamos a hacer. RSSAC va a hacer una presentación y después tenemos bloques de preguntas y vamos a pedirles preguntas. Ya he tomado los pasos correspondientes para hoy. Cuanto más se acerquen, mejor va a ser para mí. Tiene que ver conmigo. Empezamos en unos minutos.

ANDREW MCCONACHIE: Hola. Soy Andrew McConachie. Trabajo para ICANN como el apoyo del comité asesor del servidor raíz. Vamos a hablar del tutorial para el sistema del servidor raíz. No me voy a sentar. Disculpas a los remotos, si la cámara me tiene que andar siguiendo. Les prometo que la presentación es más interesante que una foto mía. Adelante.

Vamos a hacer esto en coordinación con un colega que va a hacer la segunda parte, Ozan Sahin. Se va a hablar del DNS, que es un poco de revisión para muchos de los que están aquí porque entiendo que ya han visto los primeros conceptos. Después vamos a hacer alguna explicación de Anycast y las diferencias con Unicast y por qué es importante para el sistema de servidor raíz. Un poco de antecedentes,

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 archivo, pero no debe ser considerada como registro autoritativo.

de historia. Después, Ozan va a hablar de RSSAC, del comité de RSSAC y el trabajo en desarrollo sobre la evolución del sistema de servidor raíz. ¿Por qué no empezamos?

Reseña del sistema de nombres de dominio. La mayoría de ustedes seguramente saben sobre identificadores en Internet y los distintos tipos de identificadores. Esta diapo habla de direcciones IP, su importancia para la Internet. Todos los que están conectados a Internet necesitan una dirección de IP. Es un identificador. Puede ser IPv4 o IPv6. Es fundamental.

¿Por qué DNS? ¿Cuál era el problema con utilizar directamente las direcciones IP? Las direcciones IP son difíciles de recordar. Cambian a menudo. Hay problemas modernos también que han surgido después de la interrupción de DNS porque las direcciones IP se pueden compartir. Los clientes pueden tener múltiples direcciones. Lo mismo los servidores, los hosts. ¿Cuál usamos? Puede usar el sistema de nombres para ayudar con esto.

Como probablemente habrán aprendido en los conceptos básicos de DNS, en las presentaciones correspondientes, el sistema de DNS era el que contiene una raíz en la parte superior y después, por debajo, los dominios de alto nivel .UK, .ORG, .EDU. Hay distintos niveles y podemos seguir. Pensándolo como un mapeo entre nombres y direcciones IP. Probablemente se puede llamar Quad A Mapping. Hay otros tipos de mapeo también. Los nombres también se mapean con los nombres de los servidores de correo, con las búsquedas inversas.

Tenemos dos diapos llenas de definiciones y es bueno que las veamos antes de ingresar a fondo. Estos son algunos términos no solamente en los documentos sino también en la presentación. El primero que ya utilicé es el sistema del servidor raíz. Este es el conjunto de servidores de raíz que colectivamente implementan el servicio raíz. Vamos a ir entrando en mayor detalle.

Después tenemos la zona raíz, que son los datos. Los datos, como les dije antes, la jerarquía de DNS, vamos a hablar de los datos que ayuda a distribuir el sistema de servidor raíz. En la zona raíz es donde se ayuda a distribuir. Contienen toda la información necesaria para ponerse en contacto con los dominios de alto nivel. Después, en las instancias de Anycast, hay otros operadores que están utilizando Anycast. Cuando hace la referencia a servidores individuales o a máquinas físicas en particular de lo que estamos hablando es de instancias Anycast.

Creo que los llamamos roles de la organización. El administrador de la zona raíz es la organización responsable del manejo de los datos dentro de la zona raíz. Esta es la función de IANA fundamentalmente. Involucra la asignación de los dominios de alto nivel a los operadores y mantener los detalles técnicos y administrativos. Las maneras en las cuales uno resuelve un dominio de alto nivel, que haya un servidor que responda consultas para ese dominio de alto nivel y la persona que lo administra, la actualización del servidor, tiene que hablar con el administrador de la zona raíz.

También tenemos la función de mantenimiento, que es Verisign. Es la organización responsable de aceptar los datos del administrador de la zona raíz dándole forma de archivo de zona criptográficamente firmado y luego distribuyéndolo a los operadores del servidor raíz. Los operadores del servidor raíz, que son 12, son las organizaciones responsables del manejo del servicio raíz sobre las direcciones IP especificadas en la zona raíz y el archivo de datos raíz. Estas son las organizaciones que se ocupan físicamente de esto.

Ya hablé un poquito de esto en realidad. Aquí estamos hablando de la diferencia entre datos y cómo uno los recibe. Hay servidores que sirven los datos en los datos per se y la zona raíz habla de esos datos. Es un archivo de zona y después el sistema de servidor raíz. Tenemos servidores que sirven esos datos. En esta diapositiva los compara. Respecto de la zona, es el punto de partida. Es la lista de TLD, sus servidores de nombres, para ver cómo se resuelve. Va al servidor de nombre y a los TLD para resolver los nombres que están por debajo de esos TLD. ICANN maneja la zona raíz según la política de la comunidad.

Como se dijo en la diapositiva anterior, tenemos la función de mantenimiento de las distintas RSO y es información que es servida por los servidores raíz. El sistema de servidor raíz es un sistema formado por servidores que responde con datos de la zona raíz a las consultas. Actualmente hay 26 direcciones IP que forman el sistema. 13 en IPv4 y 13 en IPv6. Hay más de 1.000 instancias físicas. La cantidad varía. Está subiendo con el tiempo lentamente. Ahora tenemos más de 1.000. En algún momento teníamos una cifra absoluta

pero como sigue creciendo decimos más de 1.000. Es un rol totalmente técnico, servir y ser responsable de los operadores del servidor raíz.

Aquí vemos todos los detalles de una consulta y respuesta de DNS. Vamos a ir viendo lo que pasa con la computadora cuando quiere resolver un nombre y pasa por el servidor de nombres recurrentes. Empezamos a la derecha. Tenemos el usuario de Internet llamado cliente, que tiene una computadora y quiere llegar a esta dirección: www.example.com. Suponiendo que este servidor recursivo se acaba de encender, no tiene nada en el caché, es totalmente ignorante, solamente sabe cómo llegar a los servidores raíz. Lo que hace la computadora del usuario es contactarse con el servidor de nombres recursivos que está en el medio de la imagen. Manda la consulta al servidor de nombres recursivos preguntando la dirección IP de www.example.com.

Como acaban de encender el servidor y todavía no tiene nada en la caché se pone en contacto en primer lugar con el sistema de servidor raíz, un servidor de nombre raíz. Normalmente manda toda la consulta completa a este servidor diciendo: ¿Cuál es la dirección IP para www.example.com? El servidor le dice: No sé la dirección para este nombre pero sí sé cómo comunicarte con .COM. Aquí tenemos una firma para estos datos.

Se lo manda al servidor de nombres recursivos. El servidor de nombres recursivos dice: Bien. Sé cómo llegar a .COM y también tengo la firma. Lo comparo criptográficamente con la parte pública de la raíz KSK que está dentro del servidor de nombres recursivos determinando que la

respuesta del servidor de nombres raíz para la ubicación de .COM es correcto y ahora me voy a poner en contacto con .COM.

Se contacta con el servidor de nombres de .COM y dice: ¿Dónde queda www.example.com? Entonces, el servidor de nombre de .COM dice: No sé, pero sí sé dónde está example.com y hay una firma para los datos. El servidor de nombres recursivos hace lo mismo y dice: Muy bien. Tengo example.com. Puedo verificarlo con la firma criptográfica y voy al servidor de nombre example.com y llego a la respuesta para www.example.com. Junto con la firma vuelve al servidor de nombres recursivos que dice: Bien. Tengo la dirección IP para www.example.com y tengo la firma, hago la comparación criptográfica. Muy bien. Funciona. Solamente ahora el servidor de nombres recursivos le dice al usuario, a la computadora del usuario la dirección IP es tal. Lo que hemos ilustrado aquí es que a través de una consulta sencilla iniciada por el usuario hay una iteración, un proceso recursivo importante que se da en el servidor de nombres recursivos y hasta que termina no viene al usuario nuevamente.

Bien. Un poco más de detalle sobre lo que hablamos. Los servidores raíz solamente saben lo que hay que preguntar después. No saben cómo resolver todo el nombre. Solamente la lista de los servidores .COM, por ejemplo. Con los servidores recursivos recuerdan las respuestas y las ponen en caché. No hace falta ir a menudo a los servidores raíz. El TTL o tiempo de vida de esa información de caché es de dos días. Si el servidor recursivo le pregunta a la raíz dónde están los nombres de servicios de .COM, probablemente tiene información de dos días y no hace falta volver a preguntar hasta que haya un time

out, que se acabe el plazo. Hay algunos refinamientos modernos del DNS. Hablamos de firmas criptográficos en los datos del DNS. Se define todo dentro de DNSSEC. Las extensiones de seguridad del DNS que se utilizan como abreviatura para hablar de toda la inicialización y validación que hace falta crear para verificar criptográficamente que los servidores recursivos y los clientes reciban la información correcta del servidor.

Hay algunas mejoras de privacidad de DNS más recientes porque los tradicionales decían 53 UDP o TCP en texto plano. Las normas estaban en desarrollo para encriptar el transporte de DNS y también ahora el TLS para utilizar HTTPS. En este punto, los operadores que han implementado Anycast, y hay una sección sobre Anycast a posteriori, podemos hablarlo luego. Esto me lleva directamente a la explicación de Anycast. Al principio estaba solamente Unicast. Unicast quiere decir que los paquetes de las fuentes van todos al mismo destino. Hay un destino y los paquetes de todos lados van a ese destino. Básicamente, la IP se corresponde con un servidor, con un solo punto de destino. Esto está bien salvo que uno quiera escalar las cosas. Anycast nos permite la escalabilidad. La facilita. Eso es importante si queremos tener consultas más válidas, incrementar los servicios. También es lindo si la gente manda ataques distribuidos de denegación de servicio. Si uno quiere tener ese tráfico descargado a muchos servidores distintos, es mucho más fácil de manejar.

En Anycast, el mapeo entre una dirección IP y el destino cambia. Tenemos una dirección IP mapeada a múltiples destinos, a múltiples servidores. Hay distintas fuentes que llegan a distintos destinos pero

siguen mandando tráfico a la misma dirección IP llegando a distintos destinos físicos. Se hace más rápido. Hay menos saltos intermedios porque las fuentes pueden estar más cercanas a los destinos y el tráfico de ataque de DDoS se envía a la instancia más cercana sin perturbar a otras.

Este es un ejemplo muy sencillo de Unicast, cómo fluye el tráfico. Hay una ruta más corta hasta un destino más cercano. Un origen, un destino. Si agregan otro origen, va al mismo destino. Esto es Anycast. Tenemos múltiples destinos que están en azul, el símbolo en azul. Seguimos teniendo un solo origen pero imagínense otro origen cerca de otro destino que va a ese otro destino. Es mucho más fácil de distribuir el tráfico.

Este es uno de los beneficios de Anycast. Lo que pasa sobre los ataques distribuidos de denegación de servicio. Los orígenes que utilizan destinos que están lejanos del ataque DDoS no se ven afectados. Un ataque local geográfica o virtualmente cercano puede estar restringido un servidor y no afectar a todo el resto del mundo. Es uno de los grandes beneficios de Anycast. Ahora vamos a hablar un poco de los antecedentes del sistema de servidor raíz y lo que pasa hoy. De 1983 hasta el 86 había cuatro direcciones en el sistema de servidor raíz y hay un incremento hasta el 98. Hay 13 direcciones. Quizá la palabra no sea direcciones, la más correcta, pero fíjense que esto está creciendo con el tiempo. Hay cambios. Hoy por hoy, como se agregó IPv6, vemos que el sistema tiene 26 direcciones. 13 IPv4 y 13 IPv6. Por Anycast podemos decir que hay 26 direcciones IP de las cuales 13 IPv4 y 13 IPv6, son más de 1.000 instancias físicas.

Esta es una lista de los nombres de host, las direcciones IPv4 e IPv6 y el administrador, el operador del servidor raíz para el sistema actual de servidor raíz. Los distintos operadores, todos los nombres de host tienen tanto dirección IPv4 e IPv6 asociadas con ellos. Podemos ver que tienen las letras de la A a la M.

Esto es un mapa que se tomó de root-servers.org. Lo que podemos hacer es ir a root-servers.org. Pueden levantarlo, está en la página de inicio. Pueden hacer un seguimiento de ciudades específicas. Pueden buscar el continente, el país, la ciudad y ver qué operadores están operando servidores o instancias dentro de esas ciudades. Esto es al mayor nivel. Pueden ir ingresando y acercándose. El mapeo agrupa cosa. Esencialmente, esto muestra que hay instancias en todo el mundo, en todos los continentes… No debería decirlo porque no sé, no sé si hay una en la Antártida. Quizá alguien pueda corregirme pero al menos, salvo Antártida, todos los continentes lo tienen. Si están interesados en entrar más en detalle, entren a root-servers.org y fíjense en el mapa. Miren cuáles son las instancias que están cerca de ustedes y cómo se pueden operar, etc.

Aquí vemos el proceso de los cambios a la zona raíz. Cómo se ingresa a los verdaderos servidores raíz y cómo los resolutores los buscan. A la izquierda encontramos los operadores de TLD. Esos operadores digamos que tienen que hacer una solicitud de cambio, contactan a IANA y le dicen: “Nuestro TLD, nuestros servidores de nombres, utilizan esta dirección IP y queremos utilizar esta otra”. IANA tiene varios procedimientos de verificación para asegurarse de que es el operador del TLD, que es una buena cadena que no va a romper nada. Cuando

IANA le dice al mantenedor de la zona raíz que este es un archivo de zona raíz, actualiza la información a la próxima zona. El mantenedor luego compila la zona raíz, la firma criptográficamente y la distribuye a los operadores. Luego aparecen todas las burbujitas con RS que se supone que representan todas las instancias. Hay muchas para cada operador. Hay muchas instancias.

A la derecha vemos los resolutores recursivos que envían consultas a las respuestas. Este es entonces el flujo sobre cómo un muy alto nivel de información o un muy alto flujo de información va generando cambios. Vamos a ver un poco más de información. Como dije, hay 12 operadores de servidores raíz. Se ocupan de la confiabilidad, la estabilidad y la accesibilidad para todos los usuarios de Internet. Cooperan entre sí a través de RSSAC y otras instancias. Se focalizan en el profesionalismo también y tienen distintos tipos de organizaciones. No siempre son sin fines de lucro. Tampoco son siempre organizaciones. Es decir, hay una diversidad geográfica, organizativa, hay modelos de financiación, etc.

Esta es una de las maneras en las que ellos coordinan. Ya mencioné varias de las reuniones de la industria, organismos como ICANN, RSSAC, el IETF, las reuniones de los RIR, los operadores de red, DNS o ARC, etc. Hay otras herramientas también que comparten datos entre ellas. Hay ejercicios como tabletop, por ejemplo, donde se planifican las respuestas ante la emergencia.

Los servidores de raíz también se ocupan de la evolución y operación de los servicios. Evalúan las modificaciones técnicas, quizá a un

protocolo de DNS. También participan en el IETF para poder hacer eso y se aseguran de que la estabilidad y la robustez se mantengan. Los operadores no están involucrados en la formulación de políticas y ciertamente tampoco en la modificación de datos. Ellos publican los datos. No están involucrados en qué son o qué contienen esos datos.

Vamos a continuar sobre lo anterior. Esta diapositiva muestra alguno de los mitos que el RSSAC fue encontrando con los años y la realidad también. El primer mito es que los servidores de raíz controlan adónde va el tráfico de Internet. La verdad es que los paquetes de los ruteadores controlan ese tráfico. Los servidores de raíz responden consultas de los servidores recursivos.

Otro mito es que la mayoría de las consultas de DNS son manejadas por los servidores de raíz pero la verdad es que la mayoría de las consultas no son manejadas por los servidores de raíz porque no tienen que hacer la misma pregunta cada vez. Otro mito es que la administración de la zona raíz y la provisión de servicios son lo mismo. De nuevo, esto se retrotrae a la diferencia entre los datos y el servicio de los datos. La administración de los datos es bastante diferente de responder consultas sobre los datos.

Otro mito es que alguno de los servidores tiene una identidad con un significado especial. La verdad es que ninguno de ellos tiene una identidad especial. Otro mito es que solo hay 13 servidores de raíz. La realidad es que no. Por Anycast hay más de 1.000 pero solamente hay 13 identidades técnicas. Los operadores de servidor de raíz no operan independientemente sino que tienen que colaborar y coordinar con

otros. El último mito es que los operadores de servidor raíz solamente reciben la porción de TLD de una consulta.

Cuando yo explico cómo funciona la resolución de DNS, tengo un string de DNS que llega hasta el servidor raíz. Tradicionalmente, así es como funcionan las cosas el 90% de las veces. Por eso hay una nueva tecnología que se llama QNAME Minimization, que es una nueva tecnología de privacidad que proviene del IETF. No está muy implementada, la verdad. Tiene cada vez más implementación pero la realidad es que los operadores de servidor raíz normalmente reciben la totalidad de la consulta. Si ustedes están operando una red, alguna de las cosas para pensar con respecto al DNS y la interacción con los servidores de raíz, seguramente van a necesitar tres o cuatro instancias cercanas. Cercanas quiere decir topológicas y cercanas a la red. No necesariamente geográficamente cercanas. Quizá podemos aumentar la cantidad de pares si estamos experimentando cierta latencia. Hay muchas cosas que podemos hacer.

Otra cosa que se puede hacer es encender los resolutores de validación de DNSSEC, que los datos estén firmados en la zona raíz, que tengamos los datos correctos, que estén sin modificar entre el servidor recursivo y el servidor de raíz y otros servidores autorizados y que nadie esté modificando los datos que están en tránsito. La validación de DNS para datos firmados y la validación de los datos en el resolutor local simplemente ayudan. Si ustedes están interesados, también pueden participar y contribuir al grupo de RSSAC. Vamos a hablar un poco más en mi reunión sobre de qué se trata ese grupo.

Si son operadores de red y están interesados en operar una instancia Anycast pueden hablar con un miembro de RSSAC después de la presentación. Hay un periodo de preguntas y respuestas o también pueden enviar un email a esta dirección que está aquí ask-rssac@icann.org. Ahora le voy a pasar la presentación a mi colega, que va a hablar de la parte más organizativa.

OZAN SAHIN: Gracias, Andrew. Mi nombre es Ozan. Soy miembro de la organización de la ICANN y apoyo el trabajo del comité asesor sobre el servidor raíz o RSSAC. Vamos a iniciar con el rol del RSSAC que es bastante estricto, bastante restringido. El rol del comité asesor del sistema de servidores raíz es asesorar a la comunidad de la ICANN y a la junta de la ICANN sobre asuntos que están vinculados a la operación, administración, seguridad e integridad del sistema del servidor raíz de Internet.

Hay dos asuntos que RSSAC hace y dos que no. El RSSAC es un comité que produce asesoramiento primeramente para la junta directiva de la ICANN pero también para otros organismos de la ICANN y otras organizaciones que están involucradas en los asuntos del DNS general. Los operadores de servidor raíz están representados dentro del RSSAC pero el RSSAC no se involucra en sí mismo en los asuntos operativos.

Si miramos la organización del RSSAC vamos a ver que está compuesto de representantes designados de los operadores de servidores raíz. También hay suplentes a estos representantes. Hay enlaces también. También está este otro organismo que es el grupo de RSSAC. Es un grupo de voluntarios que son expertos en los asuntos específicos. Los

miembros de este grupo son confirmados por el RSSAC sobre la base de una declaración de interés. Es decir, si ustedes quieren convertirse en miembros del grupo de RSSAC deben presentar una solicitud como acaba de mencionar mi colega. Esa es una declaración de interés donde uno expresa que quiere ser miembro del RSSAC.

Tenemos dos copresidentes. Están aquí en esta sala. Brad Verd y Fred Baker. Quiero decir también que el RSSAC está pasando una transición a un modelo de presidente y vicepresidente. Al final del año habrá elecciones para el vicepresidente y el RSSAC tendrá un liderazgo que estará compuesto de un presidente y un vicepresidente.

Como acabo de decir, hay enlaces en RSSAC. Cuatro de ellos son enlaces ingresantes y hay otros cuatro que son salientes. Es decir, que hay un enlace del operador de funciones de la IANA, otro del mantenedor de la zona raíz, otro de la junta de la arquitectura de Internet, o IAB y también otro del comité asesor de estabilidad y seguridad, que es otro comité asesor dentro del sistema de la ICANN. Hay también cuatro enlaces salientes, una del Comité de Nominaciones, uno de la junta directiva, otro del Comité Permanente de Clientes y otro del comité de revisión de evolución de la zona raíz.

El grupo del RSSAC tiene más de 100 expertos técnicos que son miembros. Como dije también, cualquier persona interesada puede ser miembro del grupo de RSSAC presentando su declaración de interés. Reciben un crédito público por su contribución a las publicaciones del RSSAC. El grupo efectivamente, en cuanto a la transparencia del RSSAC, indica que uno puede participar en el trabajo del RSSAC y ser

parte de ese grupo. Como dije, estos son expertos en DNS que traen su experiencia para las publicaciones.

Actualmente existen dos grupos de trabajo dentro de RSSAC. Uno es el estudio de las conductas modernas de resolutor. Allí se estudia la conducta de resolutores recursivos de software implementados existentes, ambos a través de bases de código y conjuntos de datos disponibles. Lo otro es el de las expectativas del sistema de servidor raíz y las métricas vinculadas. Tiene que ver con una definición a lo largo del sistema y de métricas verificables que demuestren que el RSS como un todo está online y que sirve a las respuestas correctas y adecuadas para los usuarios. Hay algunos mecanismos y herramientas que contribuyen a la transparencia del RSSAC y de los operadores de servidor raíz. Vamos a mencionar algunos.

Tenemos rssac.icann.org. En esa página web podemos encontrar los nombres de los miembros del RSSAC, los del grupo. Se puede acceder a las publicaciones. También podemos encontrar las actas de las teleconferencias del RSSAC. El RSSAC tiene reuniones públicas. Por lo tanto, si ustedes están interesados pueden participar de esas reuniones. El RSSAC tiene también algunas reuniones con otros grupos dentro de ICANN durante las reuniones públicas. Por ejemplo, en esta reunión los copresidentes del RSSAC tuvieron una reunión con el comité asesor gubernamental. También la junta directiva se va a reunir con el RSSAC y el RSSAC va a tener una reunión cerrada con el comité asesor de seguridad y estabilidad. Efectivamente, hay una conversación con otros grupos. El RSSAC tiene publicaciones. Es la

publicación 000, que define sus procedimientos operativos y su transparencia.

Las RSO también tienen algunas herramientas. El sitio web es root-servers.org. El mapa que mi colega Andrew les mostró muestra qué puede ocurrir en el resto del mundo. Los operadores RSO también tienen sus páginas individuales y publican informes colaborativos sobre los grandes eventos así como también lo que mencionó Andrew. Si tienen preguntas pueden presentarlas y las mandan por email a ask-RSSAC@icann.org. Allí van a recibir sus respuestas.

En la segunda fase de la presentación les voy a hablar un poco sobre el trabajo que está en marcha sobre la evolución del sistema de servidor raíz. Vamos a comenzar mirando esta línea de tiempo. Hace más de un año, el RSSAC 037 y 038 se publicaron. Básicamente se propone un nuevo modelo en la gobernanza del sistema de servidor raíz. Luego, la junta directiva de la ICANN indicó a ICANN org que analice estos documentos y trabaje. Eso fue en abril de 2019 cuando ICANN org finalmente publicó lo que se denomina un documento de concepto. En agosto de 2019, el periodo de comentario público para ese documento de concepto cerró y la consulta de los distintos grupos fue recibida. Al considerar todos estos comentarios, los próximos pasos son que para enero del año 2020 habrá un grupo de trabajo de gobernanza que ya estará formado y que va a trabajar sobre el desarrollo del modelo para los años 2020-2021. Para el año 2022 se espera que el nuevo modelo ya esté implementado.

Vamos a mirar ahora de qué se trató la RSSAC 037. Definió 11 principios para la operación y evolución del sistema de servidores raíz. Básicamente propuso un modelo de gobernanza inicial para el sistema de servidor raíz y sus operadores. También demuestra de qué manera la RSSAC 037 funciona a través de un conjunto de escenarios sobre la designación y remoción de los operadores de raíz.

En esta diapositiva vemos tres recomendaciones que complementan esta RSSAC037. La primera es iniciar el proceso para producir una versión final del modelo sobre la base de la 037. La segunda estima los costos del sistema de servidor de raíz y el desarrollo del modelo. Los esfuerzos iniciales también se deben focalizar en desarrollar una línea de tiempo y de implementar la versión final del modelo sobre la base de principios de rendición de cuentas, transparencia, sustentabilidad e integridad del servicio.

Aquí, en esta diapositiva, vemos un gráfico que muestra cuáles fueron las propuestas. Vemos entonces tres áreas distintas. Gobernanza, operaciones del DNS, la incorporación de los operadores. En el aparte de gobernanza vemos tres partes interesadas de la comunidad de la ICANN. El IETF y la junta de arquitectura de Internet. También los operadores de servidor de raíz. También vemos las cinco funciones propuestas por el modelo. Ellos incluyen la función de desempeño y de monitoreo, la de remoción. También hay una financiera, una de política de arquitectura y otra de secretaría. Estas cinco funciones fueron todas propuestas por el modelo.

En la parte de abajo de la diapositiva ven que hay algunas métricas de desempeño que se utilizan en la incorporación y desincorporación de los operadores de servidores raíz. Hablamos de la incorporación y de la remoción.

Hablábamos recién de las funciones y volviendo al modelo de concepto prevé las distintas estructuras en base al modelo 037 que corresponde a las cinco funciones. Una es la junta de gobernanza del sistema de servidor raíz. Es el comité, el panel de revisión del operador de servidor raíz y las últimas funciones son las de finanzas y de secretaría de ICANN org.

El trabajo sobre concepto indica el proceso impulsado por la comunidad para terminar el modelo de cooperación y gobernanza para RSS basado en la recomendación uno de RSSAC 038. En la fase uno, ICANN org revisa y evalúa el RSSAC 037 en la dirección de la junta de ICANN. En la segunda fase, el trabajo de concepto y los documentos del grupo de trabajo de gobernanza están disponibles para comentario público. La fase tres tiene que ver con el desarrollo de un modelo nuevo de cooperación y gobernanza para RSS con dos caminos. Uno es el estructural, donde el grupo de trabajo de gobernanza desarrolla el modelo, y después está el camino administrativo para planificar la implementación del modelo GWG liderado por ICANN org.

¿Qué es el grupo de trabajo de gobernanza? Está compuesto de representantes de RSSAC, la organización de apoyo de nombres de ccTLD, la junta de arquitectura de Internet, el grupo de partes

interesadas de registro y el comité de asesoramiento de seguridad y estabilidad. También hay vínculos con la junta de ICANN, la IANA, y la estructura de mantenimiento de la zona raíz. Tiene que desarrollar los detalles del modelo y el trabajo de concepto también delinea alguna de las guías para el grupo de trabajo de gobernanza que tiene que ver con un compromiso con un plazo con hitos claros que trabaje de manera transparente y abierta, que busque aportes informados cuando sea necesario. También que siga los principios desarrollados en RSSAC 037, básicamente haciendo referencia al trabajo de concepto y el feedback del comentario público recibido sobre el mismo. Estamos en la parte de preguntas y respuestas. Tenemos representantes de los operadores de RSSAC, de los miembros de RSSAC. Permítanme sugerir, si pueden acercarse a la mesa para las preguntas. Va a haber micrófonos volantes. Si levantan la mano, les vamos a pasar los micrófonos para que hagan las preguntas.

STEVE CONTE: Vamos a llevar el micrófono. A ver si podemos ver a la persona que está preguntando. La primera pregunta está por aquí.

ORADOR DESCONOCIDO: No soy técnico. ¿Cómo determinan cuándo y dónde necesitan otra instancia del servidor raíz? ¿Cómo es que es diferente con el servidor de nombres? ¿Cuál es la diferencia entre el servidor recursivo y el servidor de nombres regular, común?

FRED BAKER: Vemos dónde aterrizan las cosas. Eso es todo. Tenemos el proceso por el que pasamos, que comienza con la necesidad. ¿Por qué necesitamos un servidor raíz? ¿Por qué un nuevo RSO? En caso de que haya una necesidad válida hay una serie de principios por los cuales identificamos a una empresa o a una organización que pueda hacerlo. Francamente, sugiero que lea el material específico sobre el tema porque hay mucho trabajo hecho sobre eso.

WES HARDAKER: No habló de operador sino de instancia, me parece.

FRED BAKER: Vienen a uno de nosotros, a uno de los operadores de servidor raíz. Por ejemplo, a mi empresa, ISC. Si uno va a isc.org van a encontrar algo que dice: "Seleccione aquí en la instancia del servidor raíz". Me imagino que esto es válido para todos nosotros. Después hablamos de sus requisitos. Tenemos algunas expectativas para ir a conectividad IPv4 o IPv6 con el sistema. Tiene que haber un ancho de banda adecuado, electricidad, ese tipo de cosas. Finalmente, intercambiamos un memorándum de entendimiento para comenzar a operar. Nosotros operamos el servidor en su rack. Lo operamos de manera remota. Básicamente, si lo desean, nos piden y comenzamos con el diálogo.

WES HARDAKER: Tenemos requerimientos de distintos lugares. Algunos externos de personas que están comenzando un punto de intercambio nuevo. Viene un cliente nuevo y nos dice: "Vamos a ser nuevos. No tenemos

nada instalado. ¿Nos quieren ayudar?" Somos los primeros que llegamos con la solución pero tenemos requisitos internos sobre el análisis de cómo se viene sirviendo al mundo. Estoy en el proceso de dispersión geográfica para tener la mejor cobertura geográfica que podamos. Hay una matriz interna y otra externa y damos la bienvenida a los aportes de las personas que nos quieran contar que no tienen un servicio adecuado en su área.

BRAD VERD: Hay distintos enfoques porque cada uno de los operadores trabaja de su manera más apropiada. Tiene que ver con la necesidad de tráfico o la necesidad geopolítica. Hay una serie de necesidades diversas que justificarían una instancia. La segunda parte de la pregunta. Hay una diferencia en un resolutor autoritativo y recursivo. El nuestro es autoritativo para la raíz. El resolutor recursivo está dentro del ISP. Este es el intermediario entre los autoritativos. .COM es autoritativo. .US y demás. Uno no habla directamente con nosotros sino con el servidor recursivo que a su vez se comunica con nosotros cuando el momento es adecuado y si la respuesta no está todavía preparada.

OZAN SAHIN: ¿Alguna otra pregunta?

ORADOR DESCONOCIDO: Esto es para el panel. No sé si estoy en la sala equivocada. Tiene que ver con HTTPS. Entiendo que Firefox y Chrome en meses o semanas, el 95% del tráfico de DNS podría estar encriptado. No sé. Sé que están

moviendo la cabeza. A lo que voy es que no sé sobre cómo va a afectar a toda la presentación a principio de la reunión, cómo va a cambiar el trabajo de DNS o si va a seguir igual pero oculto. No he visto paneles sobre ese tema en todo el programa de ICANN. Pareciera que es algo importante sin embargo. Si puedo encontrar este tema aquí o si no, mejor dicho, cuéntenme donde puedo ir a averiguarlo.

WES HARDAKER: Yo estoy en el panel de arquitectura de Internet. Yo estoy trabajando en ese tema respecto del proceso de estandarización. Sé algunos hechos sobre la implementación de Firefox y Chrome. Lo están haciendo de manera muy distinta. No nos equivoquemos sobre cómo va a pasar. La otra cosa que están haciendo es que está entre el buscador y el resolutor.

En el caso de Firefox toman el resolutor por omisión y tienen un menú desplegable. Toman el resolutor que quieren utilizar y lo activan por omisión en Estados Unidos este mes. El resto del mundo está buscando otros socios para hacerlo. El resolutor no hace DNS encriptado con el resto del sistema, incluido la raíz y el TLD como .COM, los ccTLD y ejemplos de este tipo.

Chrome está haciendo algo un poco distinto. Están tratando de ver si el resultado de los ISP locales lo permiten. Si está la lista aprobada, se comunican con DoH a través del ISP. No hacen como Firefox, que lo manda a un solo lugar. La implementación es totalmente distinta y lamentablemente hay mucha confusión porque esa información está cambiando con mucha rapidez. Firefox solamente decía usar

Cloudflare en Estados Unidos. Es una resolución muy reciente y en dos semanas habrá mucha más charla en IETF, que se va a realizar en Singapur. Se está desarrollando el debate técnico pero en un par de meses va a haber alguna diferencia sumamente clara.

BRAD VERD: Quisiera reiterar que eso está entre el cliente y el resolutor, sobre dónde está el encriptamiento, no como es ahora. Se está hablando de un tema muy interesante de Marrakech. Voy a hablar sobre el tema, sobre el programa específico. No sé qué día me tocaba pero hay una presentación importante de SSAC. Creo que era ccNSO. Hay un todo un documento que habla sobre este tema y sé que se sigue hablando de SSAC. Están hablando sobre este tema y hay trabajo en desarrollo. Hay mucho para ver.

FRED BAKER: Pregunto sobre DNSSEC. Los buscadores dependen de otro que lo haga. No pueden implementar DNSSEC. Cuando el buscador va a DoH, ¿se verifica el DNS?

WES HARDAKER: Qué buena pregunta para una reunión. Hay dos aspectos de la seguridad en general que la mayoría de la gente considera. El encriptamiento, se protegen los datos y después está el tema de si los datos son auténticos, si son los datos correctos. Pueden estar encriptados pero estar mal. Pueden tener un archivo malo encriptado. En DNSSEC se protege desde el origen, desde el lugar donde se crean

los datos, en este caso IANA, y por el mantenimiento de la zona raíz con firma de los datos y el resto, la mayoría de los TLD y todo lo que viene por debajo no importa. Uno puede mejor dármelo en mano, en un papel. Yo lo leo, lo escaneo y puedo verificar la firma contra lo que se creó originalmente en IANA y bajando por todo el árbol.

La pregunta de Fred es que DoH también hace integridad pero entre dos puntos. Si esa entidad por encima, el resolutor no lo trabajó con seguridad, no llegaría a usted de una manera no verificada. Algunos resolutores van a hacer validación de DNSSEC. Estar hablando con un resolutor sobre un canal protegido de integridad de asegurada probablemente esté asegurado de extremo a extremo. Hay algunos que están haciendo validación. No sé el resto.

BRAD VERD: Vale la pena verificarlo.

STEVE CONTE: ¿Va a hacer un seguimiento rapidito?

ORADOR DESCONOCIDO: Los datos no son visibles para los ISP en el entorno HTTPS. No pueden ver ya los errores y todo lo que va por la red pero ustedes siguen viéndolo. Quién va a poder ver todavía o quién tiene visibilidad en la solicitud de DNS y quién no la tiene en el mundo de DNS y HTTPS.

WES HARDAKER: Qué difícil de responder. El mes que viene va a ser distinto probablemente. Como les decíamos, esto es válido para la gente que utiliza Firefox, que se comunica con un proveedor DoH en otro lado. Cloudflare sí lo podría ver. A partir de ahí se distribuye. A veces hay que hacer una pregunta. Hay que ir y preguntar a alguien: "Te tengo que preguntar algo". Esa persona a la que le tienes que preguntar dónde está ese sitio siempre va a poder verlo. Siempre alguien sabe la respuesta a tu pregunta.

Para Chrome, por otro lado, como va a ser DoH, no va a cambiar la visibilidad del ISP. Depende en gran medida de la situación de implementación. Chrome y Firefox están trabajando de manera distinta. El lector de correo electrónico, si va dentro de un buscador, sí sería. De lo contrario no. No es una pregunta de sí o no. ¿Se entiende?

FRED BAKER: Entonces hablemos de la minimización del QNAME. Ese es un proyecto IETF. Va a aparecer en algún momento. La idea es dar la menor información posible y sin embargo responder la pregunta. Si estoy buscando www.example.com, por ejemplo, quizá pregunte al servidor recursivo y este diga: "No sé dónde está .COM. No lo descubrí todavía". En lugar de mandar todo el nombre completo al servidor raíz, que es lo que hace hoy, mandaría COM al servidor raíz, que le iría a preguntar a .COM y le devolvería el nombre y preguntaría example.com. Solamente el resolutor recursivo tendría acceso a esa información. Hay que mirar a la minimización del QNAME.

ORADOR DESCONOCIDO: La otra parte de esto es que hay miles de personas que van al mismo resolutor recursivo que sabe que existe la consulta pero hay miles de consultas del mismo recursivo que quizá no se atribuye al mismo origen. Quizá es mucha gente que utiliza ese mismo recursivo.

ORADOR DESCONOCIDO: Quisiera saber si los DSO retienen los logs o si hay normas de privacidad. Me interesa ver cuál es la financiación de los DSO para las operaciones de los servicios de dominio.

BRAD VERD: ¿RSO? Nos habla de DSO.

ORADOR DESCONOCIDO: Sí, correcto. Disculpas.

BRAD VERD: No escuché la primera parte de la pregunta pero la última parte de la pregunta es la financiación. Es un mandato sin financiación. Es todo voluntario. Como Internet, que orgánicamente aparecieron voluntarios para manejar los servidores raíz y se fueron agregando con el tiempo básicamente entre el 82 y el 98. Desde el 98 no ha habido un servidor raíz nuevo. Creo en 2001 apareció Anycast. Lo empezaron a usar los servidores raíz y pasamos de 13 identificadores, servidores, ahora hay mil de las mismas tres identidades con Anycast. Pudimos ampliarlo considerablemente y todo eso se hace con financiación

propia de cada una de las organizaciones. ¿Cuál era la otra parte de la pregunta? ¿Podría repetirla, por favor?

ORADOR DESCONOCIDO: Me interesa saber si hay algunas reglas de privacidad en las solicitudes de los logs.

BRAD VERD: Lo único que puedo referir es que cada año hay lo que se denomina una colección, que es un día en la vida, que se llama Diddle. Es una colección de un periodo de 48 horas que permite a los investigadores tener una gran cantidad de datos para ver qué hace Internet en un día específico. Todos los operadores de servidor raíz pueden contribuir junto con muchos otros TLD y ccTLD y otras organizaciones más grandes, operadores de DNS. Es un esfuerzo comunitario y esos datos se almacenan. Para acceder a la base de datos hay que poder ser miembro, firmar cuestiones de confidencialidad, etc.

WES HARDAKER: Un punto adicional. Muchos operadores anonimizan los datos. Eso significa que anonimizan la dirección IP y en general esa dirección IP es un resolutor. No está vinculado a la máquina de un usuario único. Entonces, con los más recientes, especialmente con el GDPR, hay que hablar con cada uno de ellos. No recuerdo el estatus único de quién es el que anonimiza cada una de las instancias.

OZAN SAHIN: Tenemos otra pregunta.

ORADOR DESCONOCIDO: Sí. Primero me disculpo porque creo que esta pregunta es un poco difícil de responder. Antes en las diapositivas, vimos que la mayor parte de las organizaciones que tienen las direcciones IP para los servidores de raíz son organizaciones estadounidenses. Me pregunto en un mundo en el que el gobierno de Estados Unidos realmente no se va a comprometer a la neutralidad, ¿qué puede asegurar? ¿Existe algún mecanismo que pueda asegurar que nuestros servidores raíz sigan siendo neutrales?

FRED BAKER: Muy bien. Seguramente hay más de una respuesta. Una de las cosas en las que trabaja el RSSAC ahora es cómo se mide el sistema. Una de las mediciones que nos preocupa es si el RSO que está siendo medido y estamos midiendo todos pero habla de uno de ellos en un momento específico en el tiempo, está específicamente sirviendo al sistema que provino de IANA. Si la zona raíz que estamos recibiendo de un servidor en particular es diferente, entonces eso es una violación a algunas cuestiones que nosotros consideramos importantes. Esto también sería considerado algo malo. Lo que nosotros hacemos es que literalmente descargamos la información por unos minutos de IANA. Le damos servicio durante un tiempo y luego descargamos un poco más. Siempre estamos pasando lo que IANA nos da. ¿Qué nos dio IANA? Nos dio los TLD y los ccTLD, los gTLD, convertidos en el formato de IANA. Tenemos estos nombres y estos registros asociados con la

IANA que son la parte neutral. Luego nosotros la gestionamos. Esto depende en realidad en términos de la neutralidad de la red. Es la ética en todo caso de IANA o de los ccTLD que lo hacen como empresa y de las RSO. ¿Esto responde a su pregunta?

WES HARDAKER: Voy a agregar algo más. Les quiero recomendar leer la RSSAC 023, que contiene la historia de cómo se estableció el sistema de zona raíz como hasta hoy. Allí se explica cómo llegamos a las organizaciones que actualmente lo sirven y tiene que ver con la historia. No cambió en 20 años. Una de las metas del RSSAC 037 que es la arquitectura de cómo hacer cambios en el futuro, ya que la última persona que hizo cambios falleció hace 20 años, está sobre la mesa. Lo más importante es que las conversaciones que mencionamos antes sobre DNSSEC, si uno está haciendo una validación de DNSSEC sin importar cuál sea el dominio que esté siendo validado de arriba hacia abajo, vamos a saber que no hubo modificaciones y no importa por qué países pasó. Es políticamente independiente porque técnicamente sería imposible pensar lo que pasaría con esos datos. Lo que puedo decirte es que utilices DNSSEC que valide un resolutor.

BRAD VERD: Voy a agregar un poco más. RSSAC 037, que fue publicada y que todos la pueden leer, establece los principios rectores tal como los definieron los operadores de servidor raíz. Uno de esos principios es seguir siendo neutral. Es una visión apolítica. No hay política involucrada en la zona raíz. Es lo que nosotros recibimos de IANA. En cuanto a que esté

basado en Estados Unidos, esto es puramente un resultado del crecimiento orgánico. Internet empezó en Estados Unidos, creció en Estados Unidos. Hubo necesidad de operadores de servidores raíz y así es como ocurrió. No hay ninguna otra razón más que la cuestión orgánica.

FRED BAKER: Por supuesto que nosotros tenemos operadores de servidor raíz que están por fuera de Estados Unidos. Uno en Suecia, uno en Holanda y otro en Japón.

STEVE CONTE: Vamos a tomar la próxima pregunta aquí, que está un poco en la sombra.

ORADOR DESCONOCIDO: Sé que la denegación del servicio y los ataques de denegación de servicio distribuido, como muchas otras cosas de la seguridad, son como el gato y el ratón. ¿Qué es lo que se está haciendo exactamente para que los servidores de raíz puedan ser protegidos continuamente? ¿RSSAC se reúne con SSAC y hay reuniones para poder mantener protegidos a los servidores de raíz o cómo funciona eso?

BRAD VERD: Lo primero que te puedo enviar es que los operadores de servidores raíz acaban de publicar un documento que de algún modo trata la pregunta que usted hace directamente. Es decir, las amenazas al

sistema de servidores raíz y lo que se ha hecho para tratar de mitigar esas amenazas amplias. En cuanto a RSSAC, está en continuas conversaciones con la junta, con SSAC, sobre cualquier tipo de amenaza al sistema. Por eso hay una pregunta sobre DoH y DoA y las aplicaciones a la infraestructura una vez que algo como esto sucede. Estas conversaciones entonces están sucediendo todo el tiempo. No son operativas. Las preguntas operativas suceden dentro de las RSO y entre las RSO. En el caso de un DDoS o algún otro tipo de información que se comparte, allí ocurre entonces la mitigación.

WES HARDAKER: Ese documento no es un documento RSSAC. Está ubicado en el sitio web del servidor raíz, que es root.servers.org. Creo que está en la parte de arriba de la página.

ORADOR DESCONOCIDO: Quisiera hacer una última pregunta. Sé que con DNSSEC, cuando los servidores están mal configurados hay un potencial de lanzar un ataque de amplificación y también sé que hay mucho impulso para implementar DNSSEC. Quisiera saber si hay alguna manera en que también se aplique el DNSSEC en servidores configurados. Por ejemplo, limitando otros métodos. Hay una gran discusión que ocurrió en el año 2013 en representación de la ICANN y la seguridad del DNS.

WES HARDAKER: ¿Puede explicar un poco más su pregunta sobre cómo se malconfiguraron esos servidores? Está hablando de algo muy específico.

ORADOR DESCONOCIDO: Sí. Si hay alguien que configura un DNSSEC que apoya a los servidores y que está mal configurado y se lanza un ataque UDP con una dirección de IP, que básicamente se pueda tener una lista de servidores DNSSEC mal configurados y que esto permita que el ataque de amplificación sea más grande que una amplificación normal.

WES HARDAKER: Muy bien. Está hablando de un ataque de reflexión. DNSSEC tiene muchos datos. Las claves son muy grandes. Los datos son muy grandes y especialmente en el pasado DNSSEC se usaba por un ataque de reflexión porque se envía un pequeño paquete desde una dirección y allí iba una gran cantidad de tráfico. La mayoría de los servidores hoy, no estoy hablando solamente de los servidores raíz, la mayoría de los servidores tienen una tecnología que utilizan algo que se denomina limitación de la tasa de respuesta. Es decir, que un servidor no permite que se hagan muchas preguntas. Dice: “No te hablo más”. Puede seguir hablando conmigo pero tienes que hacerlo a través de TSP, que es mucho más difícil de spoofear.

Cuáles son las configuraciones para cada uno de ellos es algo muy distinto y puedo decir que antes, la mayoría de la gente lo encendía y había subidas y bajadas de tráfico constantes. En los años siguientes,

la mayor parte del tráfico era bastante plano porque la gente se dio cuenta de que ya no había formas viables de hacerlo. Ya casi no vemos ataques reflectivos en DNSSEC.

STEVE CONTE: Muchas gracias. ¿Hay alguna otra pregunta en la sala o alguna pregunta online? Esta es la última posibilidad de hacer preguntas.

WES HARDAKER: Todas estas son preguntas técnicas excelentes. Quiero agradecer a Andrew por la presentación. También a nuestros servidores de operador raíz. Sé que nuestro día casi terminó pero tenemos una nueva sesión que empieza a las 5:00 en la sala 512G. Tenemos a ARIN, que va a hablar sobre los registros regionales de Internet. Nos va a contar qué es lo que hacen. Quiero pedirles que nos acompañen en una sesión más, cinco en punto, 512G, sobre los registros regionales. Gracias a todos por darnos su tiempo.

WES HARDAKER: Quiero decir algo más. Hay un conflicto. También hay una charla de DNSSEC para principiantes que empieza a las cinco en punto.

STEVE CONTE: Muchas gracias a todos.

[FIN DE LA TRANSCRIPCIÓN]