SAN JUAN – Sesión diaria de los becarios
Lunes, 12 de marzo de 2018 - 12:00 a 13:30 AST
ICANN61 | San Juan, Puerto Rico

SIRANUSH VARDANYAN: Nos quedan cuatro o cinco minutos. Por favor, siéntense, así vamos a empezar.

Por favor, ahí está el almuerzo. Les pido que tomen el almuerzo y vengan para aquí. Les pido a todos los becarios que se acerquen. No quiero verlos lejos. Quiero verles la cara a todos.

¿Tenemos algún micrófono móvil aquí? ¿Alguno volante? ¿Tenemos un micrófono volante o no? Sí. Muy bien. Gracias. Rachel, ahora lo traen.

Todavía no estamos grabando, ¿no es cierto? No estamos grabando, ¿no? ¿Es así?

Hoy tenemos la sesión diaria del programa de becarios. Hoy tenemos una sesión especial con los gurús técnicos. Ellos estarán a cargo de esta sesión. Estoy muy bien acompañada aquí. Quisiera darle la palabra a Rachel y luego voy a dejar que los demás se presenten para que sepan quién estarán a cargo de estas presentaciones. Por favor, asegúrense de tomar el almuerzo y venir y tomar asiento y prestar atención porque es

una sesión sumamente interesante. Seguramente la van a disfrutar. Rachel.

RACHEL REYES: Hola. Buenas tardes. Bienvenidos a esta sesión de los aspectos fundamentales del DNS para ver cómo funciona. Vamos a tener una sesión con 30 minutos luego para preguntas. Soy Rachel Reyes. Soy personal de apoyo técnico para ICANN org. John Crain está aquí conmigo, a la derecha, y me va a ayudar con la parte de preguntas y respuestas.

JOHN CRAIN: Soy John Crain. Soy funcionario a cargo de la ICANN para estabilidad, seguridad y resiliencia. También trabajo en los servicios de los servidores raíz desde hace más de 20 años. En el teléfono está Matt Larson, también conocido como Señor DNS, quien también está en la industria del DNS seguramente desde hace más tiempo que yo. Ahora le doy la palabra nuevamente a Rachel.

RACHEL REYES: Muy bien. Espero que todos me presten atención mientras disfrutan de su almuerzo. Las direcciones IP son fáciles de usar para las máquinas, lo cual es cierto. Es fácil para nosotros recordar nombres pero es muy difícil para nosotros recordar

números. Vamos a tomar por ejemplo el hecho de que algunos de nosotros, por lo menos yo, tengo dificultades para recordar los números telefónicos de mis familiares y amigos. Lo mismo nos pasa con los nombres y los números que hay que recordar en el sistema DNS.

En los primeros días de la Internet los nombres eran muy sencillos. No había nombres de dominio todavía. Eran nombres con una sola etiqueta, con 24 caracteres como máximo y eran lo que llamábamos nombres host. La resolución de los nombres tiene que ver con mapear los nombres con direcciones de IP. En los primeros días de Internet los archivos host eran archivos nominados host.txt y estaban mantenidos a nivel central por el Centro de Información de Redes, que llamábamos NIC, en el Instituto de Investigación de Stanford. Eran actualizados en forma manual a través de correos electrónicos. Esto se daba a conocer una vez por semana y se descargaba a través de FTP. Esto ocurría en los primeros días de la Internet.

El problema con este sistema es que todo se editaba en forma manual. Por lo tanto, era un sistema muy proclive a los errores y sumamente ineficiente porque había que enviar un correo electrónico antes de que se pudiera hacer la actualización. A su vez, eso requería un ancho de banda significativo cuando se trataba de cargar o descargar un archivo. Eso no duró mucho

tiempo. Por eso la gente empezó a conversar en los años 80 sobre cómo remplazar el sistema actual.

Llegaron a lo que ahora conocemos como el concepto del sistema de nombres de dominio donde se abordaban las cuestiones de escalabilidad de este sistema host.txt y se simplificaba el enrutamiento de las direcciones de email. Ustedes pueden encontrar más información en los RFC que están mencionados aquí, el 799 y el 819, que les van a contar más sobre la discusión de este concepto del sistema de nombres de dominio DNS.

En resumen, vamos a explicar qué es el DNS. Esta es la terminología que utilizamos en el sistema DNS. Tenemos DNS, datos del DNS, los resolutores, servidores de nombres, el guardado en la memoria caché y la replicación. Voy a entrar en los detalles utilizando este gráfico que ustedes ven aquí.

Tenemos el resolutor de pestaña, que es lo que vamos a mencionar, y tenemos el servidor de nombres recursivos, que es el que envía consultas a nuestros servidores de nombres. Estos son los servidores que están a mi izquierda y a su derecha. Estos servidores de nombres son aquellos que les dan una respuesta definitiva a la consulta que mandan los servidores recursivos. Tenemos aquí una pequeña burbuja que habla de caché. La memoria caché se utiliza en el sistema DNS para que sea más

eficiente y escalable. Luego vamos a profundizar en este tema más adelante en la presentación.

El espacio de los nombres. El espacio de los nombres es la estructura de la base de datos del DNS que tiene la forma de un árbol invertido. Podemos mirarlo de arriba hacia abajo pero normalmente en nuestro trabajo diario lo vemos de abajo hacia arriba. Vamos a tomar este esquema. No leemos .com.ejemplo.www sino que decimos www.ejemplo.com, que es lo que nosotros denominamos un nombre de dominio totalmente calificado.

En el espacio de los nombres, en primer lugar, tenemos la raíz. Ese es el nodo raíz. Luego, lo que llamamos los nodos de primer nivel seguidos por los nodos de segundo nivel y luego los nodos de tercer nivel. Cada uno de estos nodos tiene una etiqueta. Las etiquetas constan de los caracteres legales que se pueden utilizar para las etiquetas que son lo que llamamos en inglés LDH que corresponde a las letras, los dígitos y los guiones. Tenemos una longitud máxima de 63 caracteres. Aquí podemos escribir .com todo en minúscula o podemos poner una letra en mayúscula y las otras en minúscula. En realidad no importa si utilizan mayúsculas o minúsculas porque no es sensible a eso.

Cada nodo tiene un nombre de dominio. En nuestro ejemplo, vamos a utilizar aquí este árbol que señalo aquí. La etiqueta

resaltada o el nombre de dominio resaltado es www.example.com. Estos términos están todos separados por puntos. Como mencioné antes, los nombres de dominio totalmente calificados o FQDN terminan con un punto. La mayoría de las veces cuando nosotros estamos haciendo una búsqueda de un nombre de dominio, en realidad no utilizamos ese punto al final. Simplemente tipeamos www.example.com y nada más.

Un dominio es un nodo y todo lo que está por debajo de este. En nuestro ejemplo, .COM es el nodo superior de nuestro dominio y todo lo que está por debajo de esto corresponde al territorio de .COM o al dominio de .COM.

Las zonas. Las zonas son regiones administrativas y cada zona se basa en los límites de una autoridad que se delega a una entidad. Una zona de DNS puede tener un dominio o muchos dominios o subdominios. La delegación crea zonas. Una zona delegada es la principal y las otras zonas creadas son las secundarias. Podemos tener aquí este ejemplo que es delegado a esta zona secundaria que es esta línea azul que ven en este ejemplo.

Los servidores de nombres, como mencioné antes, son los que responden las consultas que son entregadas por los servidores recursivos. Los servidores de nombres autoritativos para una

zona tienen un conocimiento completo de esa zona. Cuando ustedes envían una consulta a un servidor recursivo vacío va a ir a una zona porque esa zona tiene que poder darle una respuesta a esa consulta. Las zonas tienen múltiples servidores autoritativos. Eso es por cuestiones de redundancia y de eficiencia.

¿Cómo se mantienen los datos de una zona sincronizados con distintos servidores autoritativos? Tenemos un protocolo de DNS que está incorporado en el servidor que hace la replicación de la zona. Esto utiliza un servidor primario y uno secundario. El servidor primario tiene los datos de la zona definitivos. Si ustedes quieren hacerle un cambio a esa zona, esto tiene que hacerse en el servidor primario.

Por otra parte, tenemos un servidor esclavo o secundario. Allí es donde se recuperan los datos de zona de otro servidor autoritativo. El proceso a través del cual se hace esto se llama transferencia de zonas. La transferencia de zona en realidad es la comunicación entre un servidor de DNS y otro servidor autoritativo.

Otro servidor que tenemos que mencionar aquí es el servidor maestro, a partir del cual se origina el archivo de zonas. Hay que recordar que un servidor maestro no tiene que ser

necesariamente servidor primario. El servidor secundario puede funcionar como servidor primario o maestro también.

La transferencia de zonas es iniciada por el servidor secundario. Pueden encontrar en este RFC, por ejemplo el 1996, que tiene la descripción de un mecanismo cómo se realiza esta transferencia de zonas y cómo se hacen cambios al archivo de zona.

Ahora podemos ver los registros de recursos de DNS. Los registros de recursos de DNS es lo que nosotros llamamos RR. Si ustedes recuerdan que yo mencioné antes, cada nodo tiene un nombre de dominio. El nombre de dominio tiene distintos tipos de datos vinculados. Estos datos en el nombre de dominio se guardan en los RR. Tenemos distintos tipos de registros de recursos pero solamente vamos a discutir algunos de ellos nada más.

Pasemos a ver el formato de estos registros de recursos. Los registros de recursos cuentan con cinco campos. El dueño, TTL, clase, tipo y luego RDATA. El dueño es el nombre de dominio con el cual se asocia ese registro de recurso. El tiempo durante el cual dura es el tiempo en segundos en que se puede guardar en la memoria caché ese registro en el servidor. La clase es un mecanismo para la extensibilidad que muchas veces no es utilizado. El tipo es el tipo de datos que guarda ese registro. RDATA son los datos que lleva ese registro.

Si ustedes miran esto tal vez les resulte más conocido. Se lo puedo mostrar. Esta información es lo que llamamos los registros de recursos. Si ustedes están familiarizados con el trabajo en red van a estar al tanto de lo que les estaba explicando antes. Volvamos.

Aquí tenemos el tipo y RDATA, que siempre aparecen porque esto es necesario. Estos son los tipos de registros de recursos más comúnmente utilizados: A corresponde a una dirección IPv4. Si tenemos AAAA significa la dirección IPv6. NS es el servidor de nombres autoritativos, SOA. Es el inicio de autoridad que siempre aparece en el vértice de la zona. En nuestro ejemplo podemos encontrar la información SOA en el .COM. CNAME es el nombre de un alias para otro nombre de dominio. MX significa servidor de intercambio de correos y PTR es un puntero que utilizamos para el mapeo.

Hay muchos otros registros de recursos disponibles. Desde diciembre del 2017 hay 84 tipos. Pueden ingresar a este sitio web que está aquí en pantalla para encontrar más de estos tipos de registros de recursos. Si ingresan a esa página, esto es lo que van a ver.

Vamos a ver ahora A y los registros AAAA. Como les dije, este es el formato que tiene el registro A. Les va a dar la dirección de IPv4 y AAAA les va a dar la dirección de IPv6.

El servidor de nombres, NS, especifica el servidor de nombre autoritativo para una zona. Aparece en dos lugares, en la zona principal y secundaria. En este ejemplo a la izquierda tenemos el nombre de la zona y a la derecha tenemos el nombre del servidor de nombres, no la dirección IP. Así se hacen las delegaciones de los registros, del principal al secundario o del padre al hijo. En .COM tenemos 13 servidores de nombres. Básicamente, estas son las 13 zonas raíz que tenemos. Los registros NS aparecen aquí, desde la raíz hasta el nivel de .COM.

Durante la delegación también incluimos un registro de pegado. ¿Qué es este registro de pegado? Es un registro de recursos de IPv4 e IPv6. Está incluid en el registro principal como parte de la delegación. ¿Por qué tenemos que tener este registro de pegado? Porque si están haciendo una consulta para la dirección IP de www.example.com tienen que entrar por la zona raíz y les va a dar la dirección IP de un servidor de nombre y van a decir cuál es la dirección IP de www.example.com. Va a ir hasta la raíz y no va a encontrar la respuesta porque no tiene la dirección de IP todavía. Ese es el motivo por el cual tenemos que tener un registro de pegado.

El inicio de la autoridad, SOA. Esto está ubicado en el vértice, en el ápice de la zona. Aquí tenemos un ejemplo de cómo se ve este SOA. Tenemos el dominio, el servidor de nombres, hostmaster.example.com es el administrador de la zona. Luego

el número de serie que es la versión actual del archivo. Refresh significa la cantidad de segundos que el servidor secundario tiene que esperar antes de buscar una actualización. El reintento o retry es la cantidad de segundos que un servidor secundario tiene que esperar hasta intentar hacer una transferencia de zona que ha fallado. Expire es la cantidad de segundos que un servidor secundario puede utilizar los datos antes de que tenga que hacer una actualización o darse por vencido. El mínimo es el TTL.

El CNAME crea un alias de un nombre de dominio a otro. A la derecha, y supongo que a la izquierda de ustedes, está el CNAME y a la derecha es el nombre canónico. Del otro lado tenemos el alias. Aquí se genera un alias que llamamos nombre canónico, pero no lo sobreutilicen. No generen cadenas o bucles porque no se ve bien en los datos.

El tipo de registro de intercambio de correo. MX significa un servidor de correo electrónico y una preferencia para un destino de correo. Por ejemplo, en nuestro ejemplo que dice example.com MX 10 mail.example.com. Estos 10 y 20, el número de correspondencia, tiene que ver con la priorización. Cuanto más bajo es el número mejor es porque esa es la forma en que nosotros preferimos que se enrute el correo.

Un mapeo inverso. La mayor parte de las veces estamos buscando la dirección de IP de un nombre de dominio pero a veces tenemos que buscar un nombre de espacio y no una dirección. Ahí es donde tenemos el registro de PTR que nos resulta muy eficiente. No lo usamos permanentemente pero sí está dentro de los datos siempre. Así se ve. Voy a preguntarle a John Crain por qué tenemos in-addr.arpa.

JOHN CRAIN: De esa forma nosotros hacemos referencia a la inversión. Algunos protocolos verifican esto para ver que el nombre esté de acuerdo con la dirección.

RACHEL REYES: Aquí tenemos otros tipos de recursos que tenemos, otros registros de recursos que tenemos pero excepto el CDS y el CDNSKEY, que es parte del DNS. Este es un ejemplo de un archivo de zona, por ejemplo, para example.com. Tenemos el SOA, el nombre del servidor, el IPv4, IPv6, también lo que es el registro MX y el CNAME. Finalmente tenemos el registro de pegado. Dice entonces cuál es la dirección de IP que yo dije porque si no, esto entra en un bucle.

Vamos ahora al proceso de resolución. Como mencioné anteriormente, tenemos estos resolutores terminales. Tenemos

los servidores de nombres recursivos y estos son los que buscan los datos del DNS en el espacio de nombres. Estos resolutores pueden estar en la laptop, en el teléfono y los servidores de nombres recursivos son los que envían las consultas al servidor de nombre autoritativo y los de nombres son los que envían la respuesta a esa consulta.

Una consulta de DNS siempre tiene tres parámetros: el nombre de dominio, la clase y el tipo, que es lo que tenemos aquí en nuestro ejemplo. Hay dos tipos de consultas. Tenemos los resolutores terminales, que envían consultas recursivas y entonces los servidores de nombres recursivos envían lo que son consultas iterativas o no recursivas, lo que llamamos de derivación. Después vamos a hablar de esto.

Voy a saltear estas transparencias. De esta tengo que hablar. Ustedes empiezan un proceso de resolución donde el servidor recursivo está vacío o en territorio desconocido. Entonces van directamente a los servidores de zona raíz porque el archivo de zona raíz está ahí. ¿Cómo funciona, cómo encuentran a estos servidores raíz? Esto tiene que estar configurado desde el servidor de nombres y lo hace el operador de servidores.

Aquí tenemos la lista de los servidores de nombres raíz y de los archivos para encontrar la raíz. NS es el nombre del servidor. A

tiene que ver con la dirección IPv4. AAAA, con las direcciones IPv6.

La administración de la zona raíz, esto es muy complicado. No vamos a hablar de esto sino que vamos a mantener todo lo fácil. Si quieren saber más sobre este tema, supongo que tienen que hablar con Matt Larson. Realmente si le dan algunos M&M, él va a poder conversar más con ustedes.

Hay dos organizaciones que son las que archivan el contenido de la zona. La ICANN y Verisign. Hay 12 organizaciones que son las que operan los servidores de nombres autoritativos. Quizá ustedes se preguntan por qué tenemos 12 si tenemos 13 servidores raíz. Esto se debe a que Verisign tiene dos: el servidor A y el servidor J. ¿Por qué tienen dos? Una vez más, John Crain y Matt Larson les van a poder responder. No creo que lo hablen aquí sino que lo van a hacer fuera, después de esta sesión, a menos que John tenga tiempo para contar toda la historia.

JOHN CRAIN: No. Tiene que ver con la historia. La última vez que los servidores de nombres se distribuyeron en la década de los 90 es cuando se agregaron los nuevos servidores de nombre. No todos estaban ubicados en organizaciones nuevas. Dos no tenían donde ubicarse. Uno de ellos fue a la costa este, a Verisign, donde tenía una buena relación con Jon Postel e ISA. El otro, el de la L, quedó

en ese lugar pero después, cuando la ICANN se formó, se transformó en algo administrado por la ICANN. Eso tiene que ver con la historia de distribución. Por eso el J fue a Verisign.

RACHEL REYES: Si quieren saber dónde están los servidores raíz en cada país, pueden ir a este lugar: root-servers.org. Yo se lo puedo mostrar aquí en pantalla. Digamos que queremos ver cuáles son los servidores raíz disponibles en Puerto Rico. Tenemos el L y el J que están disponibles en Puerto Rico en este momento. Pueden ir a este sitio web si es que están interesados en esta información.

También tenemos los Anycast, que están utilizando instancias de servidores raíz, instancias que nos ayudan a buscar los servidores raíz o DNS más cerca de la ubicación en la que están. También cuando están haciendo una búsqueda, porque es una forma más eficiente. Si tienen instancias dentro del regular geográfico en el que están, es más fácil encontrarlas con Anycast.

El proceso de cambio de la zona raíz. Como fue mencionado, esta es una versión simplificada porque hay muchos más procesos, en realidad, que los que se mencionan aquí. No los vamos a ver en profundidad. Es para que tengan una idea de cómo se modifica un archivo de la zona raíz. Se empieza con un

administrador de TLD que le pide a la IANA que haga un cambio. La IANA va a implementar esta solicitud de cambio. Va a actualizar la base de datos de la zona raíz y lo va a publicar. Va a publicar la zona raíz para todos los servidores de zona raíz.

Ahora vamos a lo que es el proceso de resolución. Esto es lo que sucede si están haciendo una consulta en el teléfono. No tiene que ser solamente en el teléfono. También puede ser la laptop o cualquier otro tipo de cliente. Tenemos un cliente que tiene este resolutor usuario terminal. Entonces se va a hacer una pregunta de cuál es la dirección IP de example.com. Esa pregunta va a ir entonces al servidor recursivo con una dirección de 4.2.2.2 y va a decir: "¿Cuál es la dirección IP de www.example.com?" El servidor de nombres recursivo va a responder: "No sé, pero probablemente el servidor raíz tiene esa información".

¿Por qué el servidor de nombres recursivo no tiene esa información aún? Es porque es nuevo. Es un servidor totalmente nuevo. Como yo dije anteriormente, está vacío o es totalmente nuevo. No tiene todo en la memoria caché, por eso va a ir directamente al servidor raíz para ubicar la dirección IP porque el servidor raíz obviamente tiene el archivo de zona raíz. El servidor raíz va a dar una derivación. Va a decir: "No sé la dirección pero sí sé la dirección .COM", entonces el servidor de nombres recursivo va a recurrir a este servidor de .COM y le va a preguntar cuál es la dirección IP de www.example.com. El

servidor de .COM: “Lo desconozco pero sí conozco cuál es la dirección de IP del servidor de nombre de example.com”. El servidor de nombres recursivo ahora va a ir a este example.com y le va a dar la dirección IP o le va a dar la dirección definitiva o final y el servidor de nombres recursivo entonces va a dar la dirección de IP a este resolutor terminal.

Esto sucede en segundos, no en minutos. Es lo mismo que si abren una aplicación desde la laptop o del teléfono, que a veces lleva un tiempo abrir la página o abrir la aplicación pero si están tratando de volver a cargarla nuevamente, es mucho más fácil. ¿Por qué? Porque la información ya quedó en la memoria caché del cliente.

La memoria caché obviamente acelera el proceso de resolución porque ahora sabe cuál es el nombre, la dirección IP de la zona raíz y de los servidores de nombre. Si están tratando de acceder o si están tratando de solicitar cuál es la dirección IP de ftp.example.com cuando yo estoy haciendo la pregunta de www.example.com, ahora le está preguntando cuál es la dirección de ftp.example.com. El safari o el resolutor va a ir nuevamente al servidor de nombres recursivo pero esta vez no va a volver al servidor de la zona raíz sino que va a ir directamente no a la zona raíz sino al servidor de nombres porque ya tiene la memoria caché. Entonces, utilizando esta

información que tiene en caché, va a acelerar el proceso, lo hace más eficiente y más rápido.

Aquí está cómo se da el proceso de resolución, cómo funciona. Creo que tenemos una página nada más de DNSSEC pero si quieren entender bien lo que son las extensiones de seguridad del DNS, creo que hay algunas sesiones que van a hablar sobre este tema específicamente. ¿Hay una esta semana para las DNSSEC a la que puedan asistir?

JOHN CRAIN: Me parece que el miércoles hay una sobre el DNSSEC. Lo voy a buscar y lo voy a avisar antes de que terminemos.

ORADOR DESCONOCIDO: Hubo un tutorial ayer.

RACHEL REYES: Básicamente entonces estos son los puntos básicos de DNSSEC. Los voy a leer en voz alta. Los datos del DNS pueden firmarse digitalmente para ser autenticados. Cada zona tiene un par de clave pública y privada que funciona con DNSSEC. Hay distintos tipos de registros. Tenemos el DNSKEY, que es la clave pública para una zona, el RRSIG, o la firma digital. NSEC o NSEC3, que es

quien señala el nombre siguiente en una zona y DS que es el firmante de la delegación.

Si ustedes quieren conocer más sobre DNSSEC pueden asistir entonces a alguna de las sesiones de DNSSEC que se van a dar esta semana. Vamos a hablar entonces del ecosistema del nombre de dominio que tiene esta apariencia. Tenemos un registro que tiene la base de datos de los nombres de dominio y los registratarios. Después tenemos el registrador, que es el agente primario entre el registratario y el registro y después tenemos el registratario, que es el titular de la registración de un nombre de dominio.

Así se procesan estos nombres de dominio. No vamos a hablar exactamente de cómo sucede esto sino de lo que nosotros hablamos tiene que ver con el registro de nombres de dominio. Está todo aquí. Los servidores de nombres autoritativos, los servidores de nombres recursivos y los usuarios de Internet. Con esto termino la presentación para la sesión de hoy. No sé si hay preguntas en la sala.

JOHN CRAIN: El DNSSEC es el miércoles de 9:00 de la mañana a 3:00 de la tarde. Es todo un día de DNSSEC. Más de lo que necesitan.

SIRANUSH VARDANYAN: Gracias. Vamos entonces a empezar con las preguntas, por favor.

NICOLAS FIUMARELLI: Nicolas Fiumarelli, de Uruguay. Ustedes mencionaron que el DNS no está afectado por el tipo de letra, mayúscula o minúscula. ¿Qué pasa con los nombres de dominio internacionalizados?

RACHEL REYES: Matt puede responder eso.

MATT LARSON: El DNS en sí mismo realmente no responde a mayúsculas y minúsculas. Los IDN son una capa por encima del DNS. Rachel, ¿podrías volver a las primeras imágenes que vimos? Aquí, por favor. Si miramos aquí esta imagen, ustedes pueden ver el nodo que tenemos a la izquierda. Cuando implementamos los IDN, los implementamos por encima de esto. Desde la perspectiva del usuario, si tenemos una aplicación que permite los IDN que puede utilizar los caracteres internacionalizados, esta aplicación los tiene que convertir en LDH, que es el formato. Desde la perspectiva del DNS se ve como algo más cómico. Ustedes pueden ver que esto se llama PUNYCODE. Se basa en Unicode pero está específicamente diseñado para los caracteres Unicode para las etiquetas dentro del DNS.

NICOLAS FIUMARELLI: Gracias.

MATT LARSON: Hubo gente cuando estábamos haciendo esto que dijo: "¿Por qué necesitamos esta capa por encima del DNS? ¿Por qué no ponemos etiquetas UTF-8 dentro del DNS?" Hubo una preocupación, una inquietud porque el sistema DNS no lo iba a esperar. No fue diseñado para hacer eso. Es por eso que teníamos que hacer una actualización de toda la infraestructura y de todos los clientes. Lo hicimos con los IDN. Tenemos todos los clientes en el mismo lugar pero no tenemos que tocar el resto de la infraestructura del DNS. ¿Queremos tocar todas las aplicaciones y la infraestructura del DNS o solo las aplicaciones? Por eso decidimos esta última opción.

SIRANUSH VARDANYAN: Tenemos una pregunta aquí.

ABDULKARIM OLOYEDE: Yo querría hacer una pregunta porque dijeron que había una capa por encima del DNS. Al mismo tiempo, desde lo que yo entiendo, esto significa que si envían una consulta al servidor DNS le envían todo al servidor DNS. ¿Cómo saben si esta capa

está por encima del DNS? Es una pregunta de seguimiento antes de hacer mi pregunta.

MATT LARSON: Cuando decimos una capa por encima del DNS, un nivel por encima del DNS, esto es conceptual pero dentro de cualquier aplicación que entiende los IDN, por ejemplo, en un navegador que entiende los IDN o puede tipear caracteres no latinos y los va a convertir en algo que se vea como ve ahí xn--. Puede ser xn—y algo más. Es una etiqueta por etiqueta que está internacionalizada. Este navegador se lo mando al resolutor final que se lo manda al servidor de nombres y esa consulta que tiene xn—lo va a hacer dentro de la aplicación y no en los resolutores o en el DNS.

ABDULKARIM OLOYEDE: Ahora voy a formular mis dos preguntas. Cuando se hizo la presentación, no sé si yo me perdí una parte o usted habló demasiado rápido pero con respecto a los servidores de la zona, usted dijo que iba a ser un poco complicado. Yo estaba un poco confundido con los servidores de zona. ¿Qué significa los servidores de zona? Especialmente cuando hablamos de los servidores de zona primarios, secundarios. Algunos que pueden funcionar como maestros y esclavos. ¿Puede explicar eso nuevamente? Con respecto a 4.2.2.2, si se envía una consulta,

¿eso es como el servidor recursivo por defecto, para todas las consultas?

JOHN CRAIN: Si hablamos de los distintos tipos de servidores de nombres, porque en general no decimos servidores de zona, a ver, ¿podemos volver a atrás? Básicamente, hay tres tipos de servidores. Tenemos el servidor terminal o stub, que es el que está aquí en la laptop o en el teléfono y puede estar en el sistema operativo o en la aplicación en sí mismo como en el buscador, por ejemplo. Estos solamente responden preguntas. Después tenemos los recursivos que normalmente son manejados por un ISP o los tienen ustedes en un dispositivo en su casa. Estos son los que pasan a los servidores autoritativos para buscar la respuesta. Estos son los que tienen las respuestas. Por eso decimos que son autoritativos, porque tienen la autoridad para darles la respuesta. Allí es donde está el archivo de la zona, en el servidor autoritativo.

En el recursivo hay un motor de consultas que hace las consultas. Lo único que se guarda está en la caché. Los resolutores terminales también pueden tener eso. Tenemos una trayectoria que se sigue desde el dispositivo hacia arriba. Hubo otro comentario que creo que lo hizo Rachel con respecto a la complejidad de cómo se aprovisiona el servidor raíz. No sé si se

refiere a eso. Eso es algo totalmente diferente. Es un sistema de aprovisionamiento, no un sistema de servidores de nombres. Le voy a dejar a Matt que conteste esto porque él trabajó más de ese lado. Al igual que con los servidores recursivos, el servidor recursivo está definido cuando ustedes configuran su computadora portátil o de escritorio. Ustedes pueden decirle a la red: "Vaya para aquí". Allí se usó un protocolo de configuración dinámica del host que les dice qué dirección de IP tienen que usar y también los servidores recursivos de los nombres de dominio. Pueden tener dos o uno o cuatro de estos. Todas las consultas luego deberían ir a estos que están configurados.

SIRANUSH VARDANYAN: Tenemos una pregunta de un participante remoto. Terminamos antes con esta.

MATT LARSON: Específicamente hizo preguntas sobre 4.2.2.2. Es un servidor operado por un ISP de comunicaciones de nivel 3. Es lo que llamamos un servidor abierto recursivo. Ustedes pueden tener un grupo de clientes, como en cualquier red. Puede ser un ISP para sus clientes de banda ancha o en este edificio la red de ICANN puede tener un grupo de clientes con resolutores

terminales, los que están aquí en la parte inferior izquierda. Necesitan un servidor recursivo por encima.

Como dijo John, el operador de la red es responsable de utilizar ese servidor recursivo y cuando se conecta a la red, el dispositivo obtiene la dirección IP de ese servidor recursivo pero ustedes, si no tienen ese servidor recursivo, pueden utilizar otros. Hay algunos abiertos muy populares que aceptan consultas de terceros. Hay servidores recursivos públicos. Tal vez el más popular sea el Google Public DNS, que es 8.8.8.8. Ustedes pueden configurar este resolutor terminal en su teléfono, por ejemplo. Pueden cambiar a qué servidor recursivo quieren que vaya. Por ejemplo, este de Google. Hubo algunos que fueron los primeros en decir: "Vamos a poner servidores recursivos fuera de la red y nosotros vamos a ofrecer este servicio". Verisign los tiene. PCH tiene algo que se llama Quad9, 9.9.9.9. Hay varios públicos. Ese 4.2.2.2 es el de nivel 3 que existe desde hace mucho tiempo.

SIRANUSH VARDANYAN: Muchas gracias. Hay una pregunta de un participante remoto. Es [inaudible], de África. "África parece estar desarrollándose gradualmente y existe la necesidad de aumentar su capacidad. Además del programa de becarios que está llenando esta brecha de capacidad en los países en desarrollo, ¿qué es lo que está

haciendo la ICANN para el tema de DNSSEC, para aumentar su capacidad y qué es lo que tenemos que hacer en África en términos de política?".

JOHN CRAIN: El desarrollo de capacidad en términos del DNS, normalmente trabajamos con la comunidad. Mi grupo específicamente hace mucho trabajo de capacitación y de desarrollo de capacidades. En África específicamente es más probable que ustedes vean organizaciones como AfriNIC o si van a AFNOG o AfTLD, como el nombre de dominio de primer nivel, ellos los que están dando este tipo de capacitación y nosotros los apoyamos.

Hay otro que se llama Network Startup Resource Center, que es una organización muy activa en África que enseña sobre DNS y las cuestiones de infraestructura. Con respecto a DNSSEC específicamente, hemos hecho varios cursos de capacitación en la región africana, tanto con AFNOG como con todas las organizaciones de África. No estoy seguro de cuándo está programado el próximo pero creo que hay una capacitación de DNSSEC práctica para África programada. Estamos muy activos en ese sentido.

Nos apoyamos mucho en los que tienen el conocimiento especializado a nivel local. Si uno trabaja en distintas partes del mundo, sabe que esta no es la tarea de la ICANN. La ICANN es

una organización pequeña. Algunos piensan que es demasiado grande pero sigue siendo una organización pequeña. Nosotros tratamos de comunicarnos con las comunidades técnicas a nivel local y colaboramos con ellos con el material y esto funciona mucho mejor que otras opciones. También trabajamos mucho en unas plataformas de aprendizaje en línea que nos permiten dar una funcionalidad de educación a distancia y también nos permite traducir esto de manera más razonable a distintos idiomas.

Si bien no somos la universidad del mundo, dedicamos mucho tiempo a tratar de educar a las personas. Por un lado, si ustedes ven mi título, yo me ocupo de la estabilidad, la seguridad y la flexibilidad del sistema, asegurándonos de que el ecosistema funcione bien pero también nos preocupamos porque la gente tenga el conocimiento y la capacidad para desarrollar mejores sistemas.

SIRANUSH VARDANYAN: Gracias. Lendon.

LENDON TELESFORD: Hola. Soy Lendon, de Granada. No es una pregunta de DNS en sí misma. No sé si es posible dar una respuesta a la pregunta que tengo. En la presentación se resaltó el tema de Anycast y las

distintas instancias para los servidores raíz. Mi pregunta es: Dentro del servidor cliente y en el esquema de Anycast, ¿qué mecanismos existen para protegerse de ataques de tipo DDoS que pueden afectar la percepción de proximidad para que no haya confusión con respecto a qué servidor se tiene que recurrir para dar una respuesta a la consulta?

JOHN CRAIN: Estoy tratando de pensar un poquito en esta pregunta. ¿La quiere responder?

MATT LARSON: No estoy seguro de qué quiere decir con que los clientes se confunden con respecto al servidor pero voy a usar un concepto en distintas capas. Anycast es una capa por debajo del DNS. Tenemos DNS y Anycast es parte del sistema de enrutamiento de Internet. Tomemos el sistema de servidores raíz en el que en este momento todas las direcciones de IP tienen Anycast. Supongamos que tenemos un servidor de nombres recursivos que envía una consulta a otro lugar. Desde la capa de DNS dice: "Le estoy enviando una consulta a esta dirección de IP". Cuando llega a la capa de enrutamiento, cuando la red empieza a transportar ese paquete de datos, los enrutadores en la red van a ver que hay múltiples instancias, múltiples lugares en la red donde está disponible esa dirección IP.

Con BGP, que es el protocolo de enrutamiento que utilizamos, hay distintas redes que anuncian la ruta a esa red en particular. Hay múltiples redes en Internet que dicen: “Yo puedo responder esto. Yo puedo responder esto”. Hay enrutadores individuales que toman la información de BGP y toman la decisión. Desde mi perspectiva, cuál es la mejor manera de llegar a ese destino. Todos los enrutadores lo hacen. Cuando uno dice: “Quiero enviar un paquete por esta ruta”, según donde esté ubicado en la red va a llegar al servidor más cercano. No es una distancia geográfica. Hay latencia y muchos otros factores que tener en cuenta en estas políticas de enrutamiento de BGP.

No sé cómo entra en juego la confusión aquí pero si hay un ataque en una instancia y se sobrecarga, los operadores normalmente configuran los servidores de nombres en las configuraciones de Anycast de la siguiente manera. Cuando la red está activa, dice: “Puede publicar mi ruta porque existe” pero si está tan congestionada que colapsa, dependiendo del tipo de falla, si falla masivamente le va a decir a la red: “Ya no estoy más activo. Ya no puedo aceptar consultas del DNS”. La red recalcula y envía el tráfico a otro lugar.

LENDON TELESFORD: Entonces, con respecto a las decisiones de enrutamiento, esa decisión se toma según información prellenada ya de BGP.

MATT LARSON: No diría que está prellenada porque cambia todo el tiempo. Todas las redes, cada red desde la perspectiva de BGP, el sistema autónomo es una red con una recolección de redes que publican sus rutas y dicen: “Yo tengo estas direcciones IP”. Todos los enrutadores con BGP dicen estas son las redes que yo conozco. Los otros enrutadores aquí toman la decisión en tiempo real. Es una versión muy simplificada de cómo funciona pero BGP se produce y cambia en tiempo real constantemente.

JOHN CRAIN: Esto no es algo causado necesariamente por Anycast. Esto ya existe desde antes de Anycast porque hay múltiples vías a un nodo. Un nodo puede publicitar un sitio web. Si yo estoy muy lejos, probablemente vea otra salid pero si estoy bastante cerca, tal vez vea varias rutas. Esto también pasaba al principio. Es un truco de enrutamiento que es reconocido y que se utiliza para agregar más servidores. No hubo un cambio tecnológico por Anycast. Simplemente es un truco del enrutamiento.

LENDON TELESFORD: Quería ver si había alguna forma de engañar a ese truco de enrutamiento.

JOHN CRAIN: No. El enrutamiento tiene sus propias cuestiones de seguridad pero se vinculan con el enrutamiento y no con Anycast. El enrutamiento sí, tiene algunas cuestiones de seguridad, o de falta de seguridad pero no son específicas a Anycast.

SIRANUSH VARDANYAN: Gracias. Por allí.

SHABNIL ANAL SAMI: Shabnil, de Fiji. Si un país quiere ser el host de un servidor raíz cuando se decide quién va a ser el host a partir de esos 13. Por ejemplo, el L, el F, ¿quién lo decide?

JOHN CRAIN: Todo depende de con quién quieren hablar. No es un país sino una red o una cooperación de redes que quiere alojar una instancia. Pueden entrar a root-servers.org para ver la lista de operadores y contactar a uno de los operadores allí. Creo que tenemos uno en Fiji y hay otros también. Pueden comunicarse con esos operadores y preguntarles cuáles son las condiciones para eso. Hay distintas maneras de operar en cada operador pero no es difícil. Hay 990 ubicaciones hoy en día. Sumar algunas más es una cuestión simplemente de ponerse en contacto. Ingrese a ese sitio web: root-servers.org y allí van a ver los enlaces para cada uno de los operadores y pueden ver la

documentación que tienen. Con gusto podemos hablar después de esta reunión y le puedo ayudar en ese proceso.

SHABNIL ANAL SAMI: Me preguntaba cuál tendríamos que alojar. ¿L, F? Puerto Rico tenía L. Fiji también L. Estaba confundido por esa cuestión regional.

JOHN CRAIN: No es una cuestión regional. En general es una cuestión de relaciones. Fiji tiene L, que es el segundo que fue allí. Es porque tenemos un miembro del personal en Fiji. Muchas veces tiene que ver con las relaciones que uno mantiene, cómo desarrollar relaciones. Al entrar a este sitio web dice: "Este se ve bien". A su vez, los criterios, más que nada los financieros, pueden diferir de un operador a otro. Por ejemplo, nosotros en la ICANN tenemos una solución a través de la cual ustedes pagan por el servidor y lo ponen en línea. Nosotros hacemos todo el trabajo. Otros les dan a ustedes el dinero y ellos les envían el servidor. Es un modelo levemente diferente. Ustedes tienen que ver cuál es el que mejor encaja con ustedes. Todos los servidores raíz, desde la perspectiva de DNS, son iguales. Todos les dan las mismas respuestas. Todos funcionan desde la perspectiva de una consulta exactamente de la misma manera. Tiene más que ver con las relaciones comerciales y a quién conocen.

SHABNIL ANAL SAMI: Gracias.

SIRANUSH VARDANYAN: ¿Alguna pregunta más? Adelante.

ORADOR DESCONOCIDO: Tengo dos preguntas. ¿Cómo nos aseguramos de la publicación de las áreas de los registros de los países, que estas sean las correctas y que no haya publicitado zonas incorrectas como ocurrió hace años? Segunda pregunta. ¿Las copias de las raíces de los servidores raíz son parte de las zonas de todo el mundo? Por ejemplo, en la raíz L, ¿es una parte de todas las zonas o tiene todos los registros allí?

MATT LARSON: Todos los servidores raíz tienen la misma información. Solamente hay una zona raíz con información y todos los servidores raíz tienen la misma información. ¿Podría repetir la primera pregunta?

SIRANUSH VARDANYAN: Hay traducción. Lo puede hacer en su propio idioma si quiere. Aprovechen esta oportunidad. Un momentito entonces, por favor, para que se pongan los auriculares.

ORADOR DESCONOCIDO: Cuando los registros en cada país hacen un registro de la zona. Por ejemplo, un ccTLD o cualquiera, y luego eso será publicado o distribuido a lo largo de toda la zona del DNS, ¿cómo se asegura que esas publicaciones serán las correctas y que no haya errores en esa publicación o en la distribución, como ya tengo entendido que ha pasado en el pasado?

JOHN CRAIN: Hay varias preguntas juntas. Una mezcla de terminología y de cuestiones técnicas. Independientemente de los ccTLD o los gTLD, cuando se publica la zona, esa zona está constituida por datos que surgen de la base de datos. Ellos son responsables de asegurase de que los datos sean correctos. Una vez que se han publicado, si el DNSSEC firma la zona y están autenticando las consultas de DNS, pueden asegurarse de tener lo que han publicado. Ahora bien, ahí se termina todo. Es la publicación del lado del DNS. Del otro lado, tenemos las cuestiones de seguridad y base de datos y de la red y la integridad de los datos. Hubo problemas en el pasado donde hubo hackeos de los ccTLD, de estos sistemas, que creo que es a lo que se refiere usted. No hay algo que sea una red verdaderamente segura. Siempre va a haber alguna susceptibilidad a este tipo de cosas. Lo que nosotros hacemos en la ICANN y nuestros amigos en los

registros, mi grupo, el de seguridad específicamente, cuando tienen problema, nos contactan y nosotros los ayudamos con la recuperación y a menudo los ayudamos también a comunicarse con expertos para rediseñar sus sistemas. Creo que a esto se refiere usted.

No lo voy a nombrar pero tuvimos un par de casos en los que hubo un ataque específico de inyección de SQL y esto hizo que la persona que se conduce mal cambiara los registros para una organización muy grande y que apuntara a la dirección del servidor web hacia otro lugar. Si estoy pensando en este caso en particular, esto al mundo exterior le parece que ese servidor web ha sido hackeado pero en realidad no. Es el sistema de registro. Dedicamos mucho tiempo trabajando con los operadores de registros y ellos saben que tienen que tener un sistema totalmente nuevo ahora que impide este tipo de cosas. Han aprendido de sus errores y han avanzado. Eso es lo que se hace cuando está comprometida la información. Se corrige el sistema y se aprende y se mejora ese proceso.

Eso no significa que otro ccTLD o que incluso un gTLD nunca vaya a ser hackeado porque esa no es la realidad. Hemos visto corporaciones realmente importantes con miles de millones de dólares de fondos que han sido víctimas de ataques. Gracias.

SIRANUSH VARDANYAN: Gracias.

JASON HYNDS: Jason Hynds, de Barbados. John, mi siguiente pregunta es: ¿Existe alguna publicación que hicieron como para ayudar a los operadores de registro para evitar este tipo de problemas antes de que sucedan?

JOHN CRAIN: Nosotros estamos trabajando, como dije anteriormente, con algunos socios para generar capacidades. Tenemos miles de horas para ver cómo se monitorea una red, cómo se hace un trabajo de seguridad en la red pero la comunidad que ven aquí, de operadores, también tiene sus propias agrupaciones y comparten lo que son las mejores prácticas. Se ayudan, incluso desde el punto de vista de la ingeniería.

En Jamaica, como parte de la organización LAC, hay una organización que se llama LACTLD e incluye a todos los registros… Bueno, no todos, pero la mayor parte de los registros de la región se reúnen habitualmente. Hay sesiones técnicas y si alguno tiene problemas, hay otro que lo ayuda. No se trata de algo que cada uno enfrenta por sí solo sino que es toda la comunidad la que lo enfrenta. Hay capacitación, hay ayuda mutua.

SIRANUSH VARDANYAN: ¿Alguna pregunta? ¿No hay más preguntas? Entonces los insto a que participen en el taller de DNSSEC el miércoles de 9:00 de la mañana a las 3:00 de la tarde.

ORADOR DESCONOCIDO: Es largo.

SIRANUSH VARDANYAN: En medio vamos a tener sesiones de almuerzo de los becarios. Creo que es un taller importante. ¿Algo más para decir de quienes hicieron las presentaciones?

RACHEL REYES: Muchísimas gracias. Gracias, John y Matt, por ayudarme a responder las preguntas.

SIRANUSH VARDANYAN: Muchísimas gracias a los intérpretes y al equipo técnico. Realmente, muchísimas gracias a Matt, a John y a Rachel por el tiempo. Sé que en esta reunión están muy atareados y les agradezco mucho haber venido aquí, a hacer esta presentación a los becarios. Por favor, un aplauso para ellos.

[Aplausos]

Con esto cerramos la sesión. Gracias.

Tengo un par de anuncios para los becarios.

[FIN DE LA TRANSCRIPCIÓN]