Corporación para la Asignación de Nombres y Números en Internet

Informe sobre Innovación de Tecnología de Identificadores

15 de mayo de 2014 – Versión Final

Índice

1. Introducción

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) encomendó al panel sobre Innovación de la Tecnología de los Identificadores los siguientes objetivos:

1. Desarrollar una hoja de ruta de tecnología para el Sistema de Nombres de Dominio (DNS) y otros identificadores.

2. Desarrollar recomendaciones de mejores prácticas y sistemas de referencia.

3. Brindar pautas de tecnología para las operaciones de la ICANN y las funciones de seguridad, políticas y técnicas.

4. Participar con el público y la comunidad de la ICANN en temas de tecnología.

La selección del panel se realizó durante los meses de septiembre y octubre de 2013, con Paul Mockapetris como presidente. Todos los miembros se desempeñaron a título personal; se mencionan sus afiliaciones sólo a los efectos de identificarlos:

- Jari Arkko, Presidente del Grupo de Trabajo de Ingeniería en Internet (IETF).
- Rick Boivie — Centro de Investigación Thomas J. Watson de IBM.
- Anne-Marie Eklund-Löwinder — Gerente de Seguridad, Fundación de Infraestructura de Internet.
- Geoff Huston — Investigador Principal, Centro de Información de Redes para la Región de Asia y el Pacífico.
- James Seng — Director Ejecutivo, Zodiac Holdings.
- Paul Vixie — Director Ejecutivo, Farsight Security.
- Lixia Zhang — Cátedra Postel de Ciencias Informáticas, Universidad de California, Los Ángeles.

Se realizaron reuniones presenciales en el IETF en Vancouver (noviembre de 2013), ICANN Buenos Aires (noviembre 2013) y en la oficina de la ICANN en los Ángeles (enero de 2014). La Reunión de Buenos Aires fue abierta al público y también se presentó un resumen de las actividades del panel en dos seminarios web en enero de 2014. Hubo debates vía correo electrónico, *et al*, que complementaron estos encuentros. Se presentaron informes preliminares para comentario público a partir de febrero de 2014.

El presidente desea agradecer al panel por todas sus contribuciones e ideas y a la ICANN por apoyar a este panel. Un agradecimiento a Elise Gerich y Alice Jansen de la ICANN, quienes aportaron ideas y brindaron su apoyo a todo el trabajo del panel.

2. Estrategia del Panel

El nombre de este panel no es casual. El ámbito de aplicación se extendió más allá del DNS *per se*, en reconocimiento de la creciente importancia de los identificadores de todas las clases en Internet, así como el papel de la ICANN en la gestión de otros identificadores. La lista parcial de los porfolios actuales de la ICANN comprende:

- Nombres de dominio
- Números del sistema autónomo
- Direcciones de protocolo de Internet versión 4 (IPv4)
- Direcciones de protocolo de Internet versión 6 (IPv6)
- Direcciones multicast
- Números de puertos
- Números de protocolos
- Registro de Identificadores Uniformes de Recursos (URI)
- Base de Información de Gestión (MIB)
- Base de datos de zonas horarias

Sin embargo, paralelamente a esta expansión, el plazo del panel se redujo de un año, que era el plazo original, a aproximadamente seis meses. Esto dio como resultado un enfoque más orientado al DNS de lo esperado.

Para compensar, el panel adoptó los siguientes principios:

- Intentar documentar todas las ideas consideradas, pero centrarse en unas pocas.
- Buscar tendencias principales específicas (por ejemplo, la expansión de Internet, tendencias en la arquitectura de procesadores)
- Buscar necesidades "candentes"
- Evitar centrase en campos sobre los que se ha trabajado previamente (por ejemplo, implementación de DNSSEC, estrategias existentes para las colisiones) y buscar nuevas ideas.

El propósito central del panel es aportar información a los procesos de planificación estratégica de la ICANN. Si bien el panel consideró ideas muy relacionadas a las necesidades operacionales de la ICANN, no se limitó a las que serían implementadas por la ICANN *per se*. La implementación de muchas de las ideas analizadas en este informe estaría naturalmente dentro del ámbito del IETF o en de otra entidad. Algunas de las ideas plantean cuestiones de políticas que no fueron abordadas por el panel, pero que sí se señalan.

Finalmente, dada la gran cantidad de actividad en el campo de los identificadores de sistemas distribuidos, el panel meramente realizó un muestreo de este espacio. El lector no debe asumir que el panel conocía todas las actividades en curso, o que las ideas no abordadas en este informe son menos importantes que las que sí fueron abordadas.

3. Hoja de Ruta

Los identificadores continúan siendo un área de gran demanda en la comunidad de Internet. En el corto plazo, los Dominios de Alto Nivel (TLD) comenzarán a estar *online.* Su cuenta de Facebook intenta convertirse en su credencial de inicio de sesión única para Internet - como lo es su cuenta de Google. A largo plazo, la comunidad de investigación tiene una gran cantidad de diferentes proyectos, que incluyen Redes Centralizadas de Contenido (CCN), Redes Centralizadas de Información (ICN), Redes de Datos Nominados (NDN), y muchas otras variantes. Si bien la comunidad de investigación no puede ponerse de acuerdo con respecto a la denominación para el campo, todos sus miembros concuerdan en que el contenido debería ser identificado por nombre, no por dirección o ubicación, y que el almacenamiento en el caché deber ser oportunista. Otras propuestas han insistido en que los nombres no jerárquicos son la tendencia futura, y los nombres de auto-certificación deben ser la base de cualquier nuevo sistema.

Los Identificadores son fundamentales para cualquier red en términos de la identificación de los componentes de la red con respecto a todos los otros componentes de la misma. Además, las redes modernas no son un único dominio homogéneo, sino que se construyen como una amalgama de una serie de tecnologías, y hay un requisito para llevar a cabo el mapeo entre los dominios de identidad. Esta función de mapeo puede llevarse a cabo de varias maneras. En el contexto de Internet, uno de los dominios de identidad más visibles es el ámbito de los nombres de dominio, que es un espacio de nombres de estructura jerárquica. Asociada a este espacio de nombres, se encuentra una función de mapeo que puede asignar los nombres de dominio a otras identidades (como por ejemplo, las direcciones IP). Cuando observamos una hoja de ruta para los identificadores, es necesario estar al tanto de la distinción entre el ámbito del identificador y la función de mapeo, y considerar la hoja de ruta para cada uno.

En la Internet actual, el panel identificó varios factores que tenderán a ampliar el uso del DNS, así como varios que actuarán para contraerlo. No todos estos factores son técnicos, y la lucha parecería más darwiniana que basada en la elegancia o en alguna otra virtud.

<u>Factores Actuales de Expansión</u>

- El DNS goza de una ventaja legada dado que se implementa en cada dispositivo que se conecta a Internet. El simple crecimiento en la base existente expandirá su uso. Por ejemplo, una aplicación que desea traspasar los servidores de seguridad y almacenarse en el caché a través de Internet se encuentra con el DNS como base existente.
- Los nuevos TLD intentarán monetizar sus marcas. En tanto que existe mucho escepticismo en la comunidad técnica, más de mil nuevas marcas se esforzarán por prosperar, y es probable que haya innovación y varias sorpresas.
- El surgimiento de nuevas capacidades, como las capacidades de seguridad de las Extensiones de Seguridad del Sistema de Nombres de Dominio (DDNSSEC) o la autenticación basada en el DNS de Entidades con Nombre (DANE), puede motivar un uso adicional.

- Los nuevos datos en el DNS podrían ampliar su uso, especialmente cuando se combina con DNSSEC para garantizar la autenticidad. Uno de los panelistas estuvo a favor de publicar la "fecha de creación ", el registrador y el "intervalo desde los cambios de delegación" de los dominios como información básica sobre su reputación. Otras propuestas han utilizado el DNS como un registro de los bloques de direcciones, los sistemas autónomos, etc. La ICANN ha restringido el uso de algunas etiquetas en los nombres de dominio, y podría ser conveniente un registro de tiempo real, en especial, cuando las especificaciones escritas se encuentran en varios alfabetos. En la práctica, estas bases de datos pueden ser públicas o privadas.
- La "Internet de las Cosas" (IOT) tiene distintos significados para distintas personas, pero suele incluir una gran cantidad de ítems en una o más grandes bases de datos distribuidas. El DNS fue propuesto como un componente fundamental en la construcción de arquitecturas y prototipos, como parte del DNS público y como una o más bases de datos privadas del DNS. El panel desearía haber tenido el tiempo de analizar esta cuestión en mayor profundidad, recomienda su consideración en instancias posteriores, y considera que el DNS puede tener una función al respecto.

Factores Actuales de Contracción

- El DNS es el estándar legado, pero además, es un impedimento en cuanto a que esa lógica del DNS incorporada en los puntos de acceso WIFI, cable módems y módems de Línea de Abonado Digital (DSL), servidores de seguridad, enrutadores y la base de software de Internet, a menudo, limitan el alcance del uso y restringen la innovación. Las implementaciones del DNS a veces no son tan completas o actualizadas, ni cumplen con los estándares. Estos problemas han dificultado la implementación de DNSSEC y hacen que la implementación de cualquier tipo de datos nuevos o características del DNS resulte problemática. Esto lleva a diseñar prácticas sobre cómo limitar todo uso de registros de direcciones y de texto (TXT). Esta osificación no se aplica únicamente al DNS.
- Existe un interés comercial en tener el control ("poseer") de la ventana de búsqueda y/o el espacio de identificadores. El interés, aquí, se da al ver la intención del usuario en forma libre y mantenerla oculta de la Internet abierta. El panel ha tomado nota de la tendencia hacia dispositivos con codificación fija a un servicio específico de DNS, como también a las extensiones propietarias, como un camino hacia la balcanización.
- Los usuarios están a favor de una interfaz más poderosa. En lugar de ingresar nombres de DNS, los usuarios y las aplicaciones, a menudo, emplean la búsqueda y otros mecanismos para obtener información específica. La barra del Localizador Universal de Recursos (URL) en los navegadores es mayormente una herramienta de búsqueda en la actualidad, por ejemplo. La interfaz del usuario más común en la actualidad es el dispositivo móvil, que no favorece el tipeo. El reconocimiento de voz y otros tipos de Inteligencia Artificial (AI) en la barra del navegador conducen a la existencia de incompatibilidades entre diferentes proveedores. A modo de ejemplo, en un experimento que llevó a cabo Geoff Huston (véase su contribución), éste observó la búsqueda desencadenada por "Geoff.Huston" en varios navegadores y observó que prácticamente NO había coherencia entre los proveedores. Esta falta de consistencia puede ser

tolerable en una búsqueda en un navegador en la que se espera que el usuario vete resultados, pero puede ser peligrosa en los archivos de configuración en los sistemas - una de las preocupaciones son las re-colisiones.

La sensación del panel era que, si bien el uso del DNS puede desaparecer de la interfaz de usuario, es probable que continúe siendo un parte de la infraestructura fundacional. Una analogía era que el DNS no es de papel al enfrentar el ataque de los libros electrónicos, sino más bien un conjunto de instrucciones informáticas al que se accede mediante niveles lingüísticos superiores.

Las opiniones difieren sobre si era posible o recomendable buscar un renacimiento o reestructuración del DNS. La tecnología se discute en la sección denominada "Fundamentos del DNS" en este informe. Ahí está la cuestión sobre política respecto de si la ICANN debería tratar de preservar y extender el sistema de DNS. Si es así, ¿cómo se logra una arquitectura coherente basada en los diversos puntos de vista de la unidad constitutiva de la ICANN, el IETF (donde presumiblemente se llevaría a cabo el trabajo) y otras partes en Internet?

El largo plazo

Un conjunto de ideas sobre el largo plazo es el Modelo de Redes de Datos Nominados. Sus ideas clave son el acceso al contenido por nombre, autenticación digital en todas partes, el almacenamiento en caché oportunista, y un esquema de flujo en el que las solicitudes de contenido y las respuestas siguen el mismo camino. El modelo para direccionar las consultas se expresa, a veces, simplemente mediante la utilización de una jerarquía de nombres para las decisiones relacionadas con el direccionamiento de las coincidencias de los prefijos más largos, que para los escépticos no es escalable. En cualquier caso, se implementan el software, el hardware, y varios bancos de pruebas de red. Las aplicaciones más obvias son la distribución de contenido, pero los defensores afirman que el modelo es bueno para el control de procesos, redes de automoción, etc.

En cierto sentido, el DNS fue la primera de las alternativas preliminares para depurar la ICN, al igual que los enfoques más actuales [Fayazbakhsh 2013] que intentan conservar sólo las partes más importantes del modelo del ICN. La importancia aquí está en el ojo del espectador.

El DNS recupera datos mediante nombres. No intenta direccionar por nombre y, en lugar de ello, utiliza la capa de direcciones de Internet para acceder al contenido; este sistema corrige lo que algunos consideran es el problema de escalamiento central para ICN. El DNS ha sido infamemente conocido como un vehículo para tunelizar video [Kaminsky 2004] y el entunelado ilícito del acceso a través de las consultas al DNS que se realizan antes de la autenticación por parte de algunos puntos de acceso WIFI. (El "túnel de DNS" de Google devuelve unos 1.620.000 accesos).

La ICN posee coincidencias de prefijos más largas y selectores que permiten el transporte en los medios, facilidades que fueron anticipadas en la sección de consultas de la especificación del protocolo del DNS original, pero que nunca se desarrollaron.

En cualquier caso, suponiendo que se pudiesen agrandar los paquetes del DNS y agregar campos de consulta adicionales, los servicios de contenido podrían replicarse en el DNS. La coincidencia de las solicitudes y respuestas autenticadas de ICN puede ser la mejor manera de evitar los ataques de amplificación de DNS.

En conclusión, se podría imaginar un esquema NDN que reemplace al DNS, probablemente que comience como un superconjunto de facilidades del DNS en una transición que llevaría años o décadas en completarse. Todo intento por mejorar la arquitectura del DNS debe tener la libertad de tomar características del NDN.

ICN no es, en modo alguno, el único modelo para el futuro; simplemente es uno de los más desarrollados. El panel considera que siempre es útil intentar y extraer los principios básicos y luego estudiar la composición. [Ghodsi2011] es un buen ejemplo de la forma en que se relaciona la trinidad de nombre, la identificación en el mundo real y la Infraestructura de Clave Pública (PKI).

Más recientemente, se ha puesto de manifiesto el énfasis en la distribución del control [Newyorker 2014] y en la privacidad, con el sistema Namecoin que continúa siendo el ejemplo más conocido. En la Internet de hoy en día, la PKI representa un recurso para la vigilancia a gran escala y, por tanto, un problema para la vida privada. Una mezcla de objetos de autocertificación y una PKI opcional, o tal vez sistemas paralelos de PKI y de pares (P2P) puede ser la respuesta. El Panel sobre ITI no incluyó el análisis de este campo dentro de su labor, si bien le resulta sumamente interesante.

4. Cuestiones sobre las Operaciones

Muchas cuestiones surgen en el día a día de las operaciones de la ICANN. Estas giran principalmente en torno a la raíz.

4.1.Endurecimiento de la Raíz

Dada la importancia central de la infraestructura de la raíz, hubo varias sugerencias externas para que el panel considere una tecnología informática confiable. El panel pensó que este tipo de tecnología podría tener fundamento en los sistemas que se utilizan para editar y firmar la raíz, pero pensaba que el considerar mejorar la distribución de los datos firmados sobre hardware comercial era una prioridad más adecuada para el panel. Las revelaciones de Snowden plantean algunas preocupaciones de seguridad relacionadas con el hardware que es posible que no se hayan considerado en el diseño de los sistemas actuales, como las infecciones del BIOS, software espía en el disco duro, *et al* [Spiegel 2014].

4.2.Replicación

El DNS ha tenido siempre dos mecanismos complementarios para la distribución de datos: la replicación previamente planificada de las zonas, y las consultas a solicitud. Desde el punto de vista de una pieza individual de datos del DNS, un registro de recurso (RR), se inicia en su última fuente como parte de una zona, viaja con esa zona en una o más transferencias de zona, y luego completa su viaje a su destino final cuando se arroja mediante una consulta.

Por ejemplo, la zona raíz es generada por la ICANN en sociedad con Verisign y el Departamento de Comercio de los EE.UU., y luego se distribuye a todos los servidores raíz mediante transferencias de zona. Conceptualmente, esta distribución, al igual que la distribución de cualquier otra zona en el DNS, puede hacerse mediante cualquier mecanismo: cintas magnéticas y entregas por Federal Express (FedEx), transferencias de archivos a través del Protocolo de Transferencia de Archivos (FTP) o Rsynch, o de manera más óptima por transferencia de zona incremental que envía cambios de una versión anterior en lugar de toda la zona. Las copias se pueden mandar a través de una notificación del DNS o a través de una estrategia de sondeo que busca cambios. La seguridad para las transferencias de zona puede realizarse mediante la Firma de Transacciones del DNS (TSIG) y / o mediante cualquier número de protocolos de transporte, por ejemplo, Protocolo de Seguridad de Internet (IPSEC), Protocolo de Transferencia de Hipertexto Seguro (HTTPS), etc. Hay cientos de ejemplos de servidores raíz con copias en la zona raíz.

Cuando los usuarios desean acceder a los datos en la zona raíz, envían consultas a la misma. Las consultas son direccionadas por dos mecanismos: en primer lugar, la dirección de IP de destino en la consulta identifica un conjunto de servidores raíz que comparten una dirección anycast común, y en segundo lugar, el sistema de direccionamiento decide qué servidor en el conjunto anycast recibirá, en realidad, la consulta. Este esquema es el resultado de una evolución que comenzó con 3 servidores raíz con direcciones unicast, luego se amplió a 13 organizaciones de servidores raíz, con grupos de carga compartida, y luego, el esquema actual (con muchos pasos pequeños en el medio). En términos más simples, los "13 servidores raíz" son en realidad "13 organizaciones de servidores raíz" que finalmente entregan la zona a cientos o miles de servidores individuales[1]. La razón por la que sólo tenemos 13 organizaciones de servidores raíz, y se utiliza anycast, es que resultó mucho más sencillo de realizar en lugar de atenuar la limitación del tamaño de los paquetes del Protocolo de Nivel de Transporte (UDP) del DNS. Además, existen otros problemas relacionados con el agregado de las direcciones de IPv6. En el camino que va desde el servidor raíz hasta el usuario, la seguridad puede ser proporcionada por DNSSEC de manera opcional.

Con los años, los servidores raíz han sido objeto de ataques, en su mayoría en relación a la Denegación de Servicio Distribuido (DDoS). Para que un ataque de ese tipo contra un usuario en particular tenga éxito, debe interrumpir las consultas a todas las direcciones anycast de las distintas 13 organizaciones de servidores raíz. La interrupción de un subconjunto ralentizará el rendimiento, en tanto que el emisor se entera de los servidores raíz que debe evitar. La interrupción puede darse al sacar el servidor o la ruta de acceso de la red al servidor, generalmente con sobrecarga. De este modo, por ejemplo, en un ataque de este tipo, los usuarios en California pensaron que el servidor raíz en Estocolmo se había caído, y en

[1] Actualmente, dos de las organizaciones de servidores raíz son operadas por la misma entidad: Verisign.

Estocolmo los usuarios observaron lo contrario. La respuesta de las organizaciones de servidores raíz a una reciente amenaza de la organización hacker *Anonymous* fue desplegar más ancho de banda, servidores y fanfarria.

Por supuesto, no es necesario que el ataque esté dirigido contra la constelación de servidores raíz, puede estar dirigido contra la/s conexión/es del usuario de Internet. Si bien el daño es más limitado, la correlación de fuerzas entre un botnet atacante y una sola empresa suele favorecer mucho más al atacante, incluso en el caso de las empresas más grandes.

Algunos panelistas han adoptado la práctica de recomendar a las empresas que distribuyan internamente copias de la raíz, y **cualquier otra zona crítica**, para que durante un ataque, sea posible continuar con el funcionamiento normal, al menos para el DNS. La ICANN hace que sea sencillo para cualquier organización obtener una copia de la zona raíz, y con un poco más de esfuerzo, transformarse en una instancia del servidor raíz en la organización de "servidores de la raíz L" de la ICANN. Resulta, también, una buena idea para una empresa ser internamente autosuficiente en materia de DNS, y no verse amenazada por la falta de acceso a servidores externos o las acciones llevadas a cabo por el registro, registrador, operadores de servidores raíz, etc., ya sea accidental o intencionalmente.

Con DNSSEC, tenemos una manera de distribuir una zona que puede ser verificada mediante el uso de firmas digitales integradas. El panel cree que este principio puede extenderse aún más, por ejemplo, mediante la protección de la delegación y los datos glue. Por otro lado, es posible eliminar o reducir la organización del servidor raíz y datos de direcciones. En la contribución realizada por el panelista Paul Vixie, se incluye un esquema detallado incluido en la sección de Contribuciones del presente informe.

También hay aspectos políticos significativos. Existen 13 organizaciones de servidores raíz, y varios países que se sienten excluidos, aun cuando puedan tener tantas instancias del servidor de la raíz L de la ICANN en su país como deseen instalar. (Ni que decir con respecto a que varias de las demás organizaciones de servidores raíz están dispuestas a extender sus constelaciones anycast.) Así que, simplemente, minimicemos el problema.

Cabe señalar que no hay ninguna necesidad técnica para sustituir el sistema de servidores raíz existente para aquellos que lo prefieran; simplemente facilitemos la replicación de la raíz, y también establezcamos un ejemplo para otras zonas.

4.3.Control de Zona Compartida

En la sección anterior, hablamos de las sensaciones políticas que hacen que los países quieran poseer una organización de servidores raíz. Estas preocupaciones pueden o no estar bien fundadas, pero no caben dudas de que la operación en la raíz actual se ubica en los Estados Unidos y se encuentra sujeta a la Jurisdicción de este país.

De un modo más simple, la raíz se actualiza en una secuencia:

- La ICANN recibe las solicitudes de actualización de los TLD, y las examina para detectar errores.
- La ICANN envía los cambios al Departamento de Comercio.
- La ICANN envía los cambios aprobados a Verisign.
- Verisign genera una raíz firmada y la distribuye.

¿Existe una forma técnica para considerar compartir el control sobre la raíz? Algunas teorías han avanzado. Una línea de pensamiento sostiene que los datos deben tener N múltiples firmas. Y luego M / N; se requieren firmas para autenticar los datos. Por supuesto, que hay argumentos sobre el tamaño M y N, y respecto de si se necesita o desea un cripto diferente.

No es nuestra intención expedirnos a favor de un sistema específico aquí, pero el panel piensa que un buen diseño puede dar lugar al comienzo de un proceso político para decidir cómo compartir el control. Nuestra visión es la creación de una caja de herramientas para el control de la zona compartida, no sólo para la raíz, sino también para abordar otros problemas de coordinación de zona. El panel nota que el Grupo de Trabajo sobre las operaciones de DNS (DNSOP) en el IETF tiene dos propuestas para la coordinación de la información de firma de DNSSEC, pero nos preguntamos si no sería mejor crear un recurso general, en lugar de una solución a este problema puntual. La coordinación de direcciones directas y reversas podría ser de otra aplicación.

Entonces, ¿qué se necesita? Creemos que el modelo adecuado es aquel en el que todas las partes que comparten el control tienen un conjunto de capacidades:

- Un sistema para el inicio de una zona compartida que consiste en la zona en sí, reglas y registros individuales para cada uno de los participantes a fin de que publiquen sus solicitudes y acciones.
- Verificaciones técnicas automáticas apropiadas para la zona en particular.
- Cada tipo de solicitud es visible para todos los demás participantes quienes pueden aprobar, rechazar o desestimar.
- Las reglas definen lo que ocurre con una solicitud.
    - Un tipo de regla consiste en un voto que define las condiciones para que la solicitud sea exitosa. Esto podría incluir un retraso para que todas las partes tengan tiempo de considerar la solicitud.
        - Para los ccTLD las reglas de la Cumbre Mundial sobre la Sociedad de la Información (WSIS) dictarían 1 de N, por lo que cada Dominio de Alto Nivel con Código de País (ccTLD) podría cambiar unilateralmente sus propios datos.
        - Otros dominios podrían utilizar la mayoría simple.
    - Los retrasos especificados podrían ser relevantes para que otros puedan especificar cuestiones operativas y permitir a los solicitantes reconsiderarlas.
    - Se podrían aplicar diferentes condiciones para operaciones distintas, como por ejemplo, crear una nueva en lugar de editarla, etc.

Los participantes podrían, entonces, cada uno crear un algoritmo estándar para generar un estado uniforme. Esto puede parecer una fantasía, pero los algoritmos bizantinos como Bitcoin [Andreesen 2014] y Namecoin demuestran que estos sistemas son posibles en la actualidad.

(Se debe tener en cuenta que el panel no está proponiendo las reglas, sólo un sistema distribuido para la implementación de toda regla que la comunidad desee).

4.4.Operaciones de Registros /Registradores

Algunos panelistas sostienen que las operaciones de la ICANN deben proporcionar garantías de nivel de servicio, pero el panel no consideró que esto fuese un asunto con el que pudiese avanzar.

4.5.¿Qué Datos debería publicar la ICANN?

4.5.1. Parámetros de la ICANN

La ICANN tiene muchos conjuntos de parámetros que administra como parte de las funciones de la Autoridad de Números Asignados en Internet (IANA), así como el proceso de nuevos TLD y, entre otros, por ejemplo, las etiquetas reservadas en varios idiomas. Todo esto debe estar disponible online, tal vez en el DNS, y desde luego, en forma segura, de modo que pueda ser utilizado directamente por cualquier persona en la comunidad de Internet. Otras propuestas han recurrido al DNS como un registro de bloques de direcciones, sistemas autónomos, etc.

4.5.2. Fecha de Creación de los Dominios, Actividades y Bailías

La reputación del DNS es una valiosa herramienta de seguridad. En la actualidad, la fecha de la creación de un dominio es, tal vez, la información más indicativa sobre la reputación de un dominio. Otra información de ese tipo es la tasa de actualización de un dominio para los servidores de nombres y direcciones. En ocasiones, también es importante saber cuál fue el registrador al cual se recurrió para la creación y administración de un nombre de dominio. Los nuevos dominios, la alta tasa de actualización y algunos registradores resultan sospechosos. Sería deseable que esta información esté disponible en tiempo real.

La Información de bailía se discutió de manera similar, pero fue abordada por el IETF en su siguiente reunión en Londres, en marzo de 2014.

4.5.3. El Ejemplo de LISP

En sus comienzos, se solicitó al panel que considerara la posibilidad de que la ICANN admitiera un servicio de Súper-raíz para el Protocolo de Separación de Localizadores /Identificadores (LISP) [RFC 6830]. Tal como nos explicó Dino Farinacci *et al*, la ICANN podría ejecutar servidores LISP como un

servicio experimental para derivar solicitudes a los servidores LISP existentes que actualmente no ofrecen conectividad universal. La ICANN localizó recursos para cuatro servidores, pero el proyecto nunca comenzó debido a algunas cuestiones no resueltas:

- ¿Cuál sería el alcance (duración, etc.) del experimento? ¿Cuáles fueron los criterios para el éxito?
- ¿Qué software se utilizaría y quién lo admitiría? Existían dos alternativas propietarias disponibles.
- ¿Quién tendría el control operacional y sobre las políticas?
- ¿Debería la ICANN hacer esto o lo deberían hacer los Registros Regionales de Internet (RIR)?
- ¿Cambiaría la respuesta si las direcciones de IP no estuviesen involucradas?

No se llevó a cabo ninguna acción en cuanto a este experimento.

Parte del panel consideró que el "LISP es sólo una instancia de una clase más genérica de las tecnologías de tunelado para el transporte, y como tal, no presentó ninguna tarea nueva de administración de identificadores que quedase fuera de las actuales prácticas de gestión de identificadores operativos, y por lo tanto, el hecho de que esta particular forma de tunelado requiriese especial atención y aval por parte de la ICANN no fue claramente justificado".

La ICANN deberá prever que las políticas y las cuestiones técnicas en torno a los nuevos identificadores surgirán nuevamente y deberá planificar en consecuencia.

4.6. Colisiones

Muchos de los panelistas estaban familiarizados con el problema de la colisión en el DNS, y si bien hubo mucho debate sobre el tema, no surgieron directivas importantes. El panel consideró que el prototipo mundial real del sistema que se describe en [ICANN 2013] es muy recomendable.

5. Fundamentos del Protocolo del DNS

¿Podemos imaginar una revisión sustancial, mejora o renacimiento en el DNS? Muchos, incluidos algunos miembros del panel, creen que la base instalada es demasiado resistente, o que el proceso es problemático[2], o que comenzar de nuevo es la idea correcta.

Sorprendentemente, el panel fue unánime en su idea de que valía la pena realizar un esfuerzo por caracterizar los problemas y buscar soluciones; tal vez aunque sólo sea para dejar descansar el tema. En

[2] Las opiniones difieren. Hay quienes dicen que el proceso del IETF simplemente "estaba dividido" en grupos de trabajo específicos (sobre todo en el pasado). Otros piensan que las API son necesarias, y el IETF no se encarga de las API, entonces, ¿quién lo hace? Otros consideran que la diversidad de grupos de trabajo sobre el DNS es mucho más efectiva que la visión general para acelerar la evolución y la innovación.

esta sección, el panel describe algunas de las cuestiones que han de ser estudiadas si fuese necesario llevar a cabo un mayor esfuerzo.

La historia de la innovación en el DNS ha tenido sus éxitos y fracasos. Una de las lecciones principales es que la tecnología sólo se adopta ampliamente si brinda un beneficio específico. Los administradores son cuidadosos al mantener sus zonas conectadas al DNS global y sus registros A y MX actualizados; de lo contrario, no reciben correo electrónico o tráfico web. Pero de los casi 60 tipos de registros que se han definido, menos de 10 tienen un uso amplio.

Los esfuerzos para crear la aplicación han enfrentado dificultades similares.

Un conjunto inicial de RFC para el DNS sugirió un método para el direccionamiento del correo a buzones específicos, pero nunca se puso en práctica. Un segundo esquema, el MX RR, resolvió el problema de proporcionar servidores de correo redundantes, así como brindar direccionamiento de correo a través de las fronteras organizacionales - es la base del direccionamiento de correo en la actualidad. Las bases de datos anti-spam fueron ampliamente adoptadas sin estandarización. Un esfuerzo por implementar estándares competentes para la autenticación de correo electrónico condujo a dos implementaciones con la utilización de TXT RR, y a un debate sobre si la estandarización de nuevos tipos sería, alguna vez, de utilidad.

El esfuerzo de mapeo del número E.164 (ENUM) para estandarizar el direccionamiento telefónico y de otros medios con la utilización del DNS también tuvo un éxito muy limitado. A pesar de que la tecnología del Puntero a la Autoridad de Asignación de Nombres (NAPTR) es considerada una verdadera innovación, los diseñadores de ENUM ignoraron la necesidad de direccionar la información distinta de los números telefónicos de destino, y los fabricantes de equipos prefirieron mantener el valor de sus sistemas propietarios.

5.1.Principios Generales

Todo nuevo diseño debería:

- Eliminar las limitaciones de tamaño - La Unidad Máxima de Transferencia (MTU) de 576 bytes, probablemente ha hecho más para retrasar el DNS que cualquier otro factor, DNSSEC no encaja y, a pesar del mecanismo de extensión para el DNS (EDNS0), una gran cantidad de hardware y software no transmitirá paquetes grandes.
- Preservar la conectividad a todos los nombres y datos del DNS existentes.
- Trata de fomentar implementaciones uniformes - Si los diferentes ejecutores no siguen las especificaciones, el usuario queda limitado a cualquier solapamiento común que pueda existir.
- Permitir la expansión futura.
- Proporcionar incentivos para la adopción.

5.2.Modelo de Datos

Las primeras RFC del DNS imaginaban espacios de nombres paralelos para diferentes "clases" de información y nuevos tipos de datos construidos a partir de componentes simples. La noción de clase nunca fue explorada. Se definieron nuevos tipos de datos, pero más recientemente, muchos se han pronunciado a favor de usar el registro genérico TXT para cadenas de caracteres de texto arbitrarias para transportar datos, junto con otro nivel de la etiqueta como sustituto para el tipo RR.

El panel podría alegar que el DNS debería definir sus propios tipos y formatos de RR en los metadatos transportados en el DNS, o bien, el DNS debería formalizar etiquetas secundarias como el último tipo de datos y ampliar la consulta para permitir una adaptación más flexible.

Por último, es necesario que exploremos los objetos de datos auto-firmados que pueden existir independientemente del nombre de dominio.

5.3. Distribución

La estructura de la zona de datos y almacenamiento en caché mediante el registro de recursos se implementa con "mejoras" un tanto irregulares al estándar Tiempo de Vida Útil (TTL), y la obtención previa de información de expiración. Quizá valga la pena tomar en cuenta nuevas formas de agrupar datos con números de serie que podrían actualizar los grupos de datos en caché sin tener, en realidad, que transferir los datos.

El panel también piensa que la seguridad puede mejorarse mediante una replicación más frecuente de zonas (posiblemente más pequeñas), usando los mecanismos de transferencia de zona existentes, *et al.* No es necesario asegurar estos datos mediante DNSSEC, y por lo tanto, es posible mejorar la seguridad en aquellos sitios en los que DNSSEC no se implementa.

5.4. Interfaz de Programa de Aplicaciones (API)

La API del DNS se presenta de dos formas: una interfaz de usuario y los nombres a nivel de la API. En ambos casos nos beneficiaríamos de una sintaxis estándar que permitiría un Nombre de Dominio Totalmente Calificado (FQDN). La comunidad de usuarios tendría un mejor servicio mediante un conjunto de políticas de búsqueda acorde a través de UI, pero no queda claro si existe alguna forma de hacer que los proveedores implementen esto.

La API de programación ha tenido varios intentos de revisión, pero en su mayoría fracasaron. Recientemente, el panel vio una presentación a cargo de Paul Hoffman sobre un nuevo diseño que presenta interfaces asíncronas y soporte de DNSSEC. El trabajo fue publicado por el IETF en Londres, en marzo de 2014. Ver http://vpnc.org/getdns-api/.

No obstante, independientemente de la API, hay una cuestión conexa sobre dónde se debe realizar la validación de DNSSEC y el filtrado de DNS (en caso de existir). El panel coincidió en forma unánime en que, técnicamente, la terminación de DNSSEC debería permitirse en el sistema final (que podría ser una máquina virtual, un ordenador portátil, un servidor en el entorno del usuario, etc., según la preferencia del usuario) a pesar de que esto podría resultar imposible debido al enrutador, servidor de seguridad

(firewall) u otras restricciones legadas. Del mismo modo, en tanto que el filtrado del DNS no es una elección de todos, debe estar bajo el control del usuario.

Nada de esto debe entenderse como que el usuario tenga prohibido confiar estas tareas a un ISP u otro servicio.

Las políticas y restricciones legales pueden expresar lo contrario.

5.5. Protocolo de Consulta

El protocolo de consulta del DNS tiene dos tipos de problemas: los relativos al transporte de consultas / respuestas de un solicitante a un servidor, y en segundo lugar, la ampliación de la potencia de la consulta.

Las cuestiones originales del transporte con UDP comienzan con la tradicional limitación de la MTU de 576 bytes. La solución original era recurrir al TCP para las transferencias de mayor volumen. El tamaño de los datos de la raíz fue, tal vez, el primer lugar en el cual las limitaciones de MTU tuvieron un impacto muy generalizado que lleva al límite del servidor raíz 13; posteriormente, la incorporación de firmas de DNSSEC expandió sustancialmente los paquetes de respuesta. Los EDNS0 fueron concebidos para resolver este problema, entre otros, con cierto éxito. Pero hay otros límites, como los diversos tamaños de la trama Ethernet de 1528 o los 1280 de IPv6, etc., que limitan fundamentalmente el UDP.

Por otro lado, el EDNS0 no puede resolver el problema de los puntos de acceso, enrutadores, servidores de seguridad (firewalls) y otro hardware que bloquean el acceso al puerto TCP 53, o limitan el tamaño del paquete, o incluso interceptan las solicitudes de DNS en proxies transparentes, a menudo, en detrimento del servicio. Pueden existir problemas similares en los servidores de nombres con almacenamiento en la memoria caché que no soportan grandes paquetes, todos los tipos de datos de DNS, EDNS0, etc. Algunos problemas pueden ser bastante sutiles. En un ejemplo, los paquetes de DNSSEC normalmente pasan pero no durante el traspaso de la llave de DNSSEC, un proceso de mantenimiento normal, cuando los paquetes son ligeramente más grandes.

Un problema relacionado son los ataques al DDoS del DNS, en particular mediante la utilización de la reflexión y amplificación. En estos casos, se busca alguna forma para identificar el tráfico legítimo de los ataques al tráfico. La validación de direcciones fuente [BCP 38] resolvería una parte importante del problema, tanto para el DNS como para muchos otros protocolos. El panel está de acuerdo con esto[3], pero no se encuentra totalmente implementado. La tasa de configuración y diversas heurísticas pueden ser de ayuda, pero distan de ser una solución definitiva. Se ha pensado en varios mecanismos de autenticación ligeros y aún siguen siendo posibles candidatos.

Una línea de pensamiento sobre la solución al problema del transporte consiste en poner todo el tráfico del DNS en https: la lógica es que todos poseen un interés personal en ver un flujo de tráfico de red seguro, y por lo tanto, es un camino garantizado (algunos sostienen que es el ÚNICO camino

[3] Todos los miembros del panel están a favor del ideal [BCP 38], y algunos miembros del panel consideran que avalar esta opción debería estar entre las recomendaciones principales del panel. Sin embargo, la mayoría señala que su adopción ha sido escasa desde la publicación del BCP en el 2000.

garantizado). El precio es el estado de conexión y la sobrecarga relacionada. Las alternativas incluyen algún nuevo protocolo de transacción o forma de utilizar el UDP, los cuales pueden no funcionar en ciertas partes de la base instalada. En cualquier caso, existe la cuestión de si las transacciones del DNS utilizan un formato tradicional o nuevo.

Independientemente del transporte, el protocolo de consulta al DNS debe ampliarse para permitir consultas más flexibles. Esto podría incluir algún tipo de control de acceso a las etiquetas sucesoras en lugar del NSEC y NSEC3.

Los protocolos mundiales de investigación como el CCN aprendieron del DNS e incorporan todas estas características. El problema de estos nuevos protocolos consiste, más bien, en encontrar la manera de motivar una mejora en la infraestructura existente con cierta compatibilidad reversa, en lugar de generar un nuevo avance en la ciencia de los protocolos.

6. Observaciones y Recomendaciones

- El uso del DNS en la infraestructura seguirá creciendo; el uso del DNS en la Interfaz del Usuario (UI) se ve afectado por las alternativas de búsqueda, las interfaces móviles, etc.
- La ICANN debería publicar más datos firmados con DNSSEC para etiquetas reservadas, etc.
- Realizar un estudio para definir una visión de la arquitectura del DNS para el 2020, en colaboración con el IETF y otras organizaciones.
- Diseñar y publicar un prototipo abierto para la raíz.
- Diseñar un sistema de control compartido para la zona raíz.
- Realizar simulacros de colisiones para evaluar la facilidad de la implementación de ["ICANN 2013"].

7. Referencias

[Andreesen 2014] Andreesen, “Porqué el Bitcoin es Importante”, http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

[BCP 38] Ferguson el al, “Filtrado del Ingreso a Redes: Cómo Vencer los Ataques de Denegación de Servicio que Emplean *Spoofing* de Direcciones Fuente de IP”, RFC 2827, Mayo de 2000.

[DNS/TCP] https://lists.dns-oarc.net/mailman/listinfo/tcp-testing

[Fayazbakhsh 2013] Fayazbakhsh et al, “Menos Dolor, Máximo Crecimiento: ICN que se Implementa en Forma Incremental" Sigcomm 2013.

[Ghodsi 2011] Ghodsi *et al*, “Nombres en una Arquitectura Orientada al Contenido”, Sigcomm 2011

[Huston 2013] Único estudio de DNS-sobre-TCP.

http://www.circleid.com/posts/20130820_a_question_of_dns_protocols/
y el hilo de las operaciones del DNS.

[ICANN 2013] “Guía para la Identificación de Colisión de Nombres y Mitigación para los Profesionales de Tecnología de la Información”, https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

[Kaminsky 2004] D. Kaminsky, “Entunelado de Audio, Video y SSH sobre DNS”, BlackHat 2004

[Fundamento] Secciones sobre los dominios y el DNS

http://www.afnic.fr/en/about-afnic/news/general-news/6391/show/the-internet-in-10-years-professionals-answer-the-afnic-survey.html

[Mockapetris 88] P. Mockapetris y K. Dunlap, “Desarrollo de Sistema de Nombres de Dominio”, SIGCOMM 88

[Newyorker 2013] http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html?goback=%2Egde_1430_member_5817512945197801473#%21

[RFC 881] J. Postel, “Cronograma y Plan de los Nombres de Dominio”, Noviembre 1983

[RFC 882] P. Mockapetris, “Nombres de Dominio --Conceptos y servicios”, Noviembre 1983

[RFC 883] P. Mockapetris, “Nombres de Dominios --Implementación y especificación”, Noviembre 1983

[RFC 1034] P. Mockapetris, “Nombres de Dominio --Conceptos y servicios”, Noviembre 1987

[RFC 1035] P. Mockapetris, “Nombres de Dominios --Implementación y especificación”, Noviembre 1987

[Spiegel 2014] http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

8. Glosario

A: Un tipo de registro de DNS utilizado para alojar una dirección IPv4.

AAAA: Un tipo de registro de DNS utilizado para alojar una dirección IPv6, también conocido como "cuádruple A".

AI: Inteligencia Artificial.

API: Interfaz de Programa de Aplicaciones.

BCP: Mejor Práctica Actual – subconjunto identificado dentro de las RFC.

CCN: Redes Centralizadas de Contenido.

ccTLD: Dominio de Alto Nivel con Código de País - un TLD asignado a un país en particular, en ocasiones operado por un tercero.

DANE: Autenticación Basada en el DNS de Entidades Nominadas.

DDOS: Denegación de Servicio Distribuido.

DNS: Sistema de Nombres de Dominio - El sistema de nombres de Internet.

Operaciones DNSOPS DNS: un equipo de trabajo del IETF que se ocupa de las Operaciones del DNS y cuestiones similares.

DNSSEC: Extensiones de Seguridad del Sistema de Nombres de Dominio.

DSL: Línea de Abonado Digital.

E.164: una Recomendación de la UIT-T, titulada El plan internacional de numeración de telecomunicaciones públicas, que define un plan de numeración para la red telefónica conmutada pública mundial (PSTN) y algunas otras redes de datos.

EDNS0: Mecanismo de extensión para el DNS [RFC 2671] - Un estándar para ampliar el tamaño y los campos de las especificaciones originales del DNS.

ENUM: Mapeo de Número E.164 - un sistema para unificar el sistema de números telefónicos internacional de la red telefónica pública conmutada con las direcciones de Internet y los espacios de nombres de identificación, por ejemplo, para direccionar una llamada telefónica.

FEDEX: Federal Express.

FQDN: Nombre de Dominio Plenamente Calificado.

FTP: Protocolo de Transferencia de Archivos.

HTTPS: Protocolo de Transferencia de Hipertexto Seguro.

HTTPS: Protocolo de Transferencia de Hipertexto Seguro.

IANA: Autoridad de Números Asignados en Internet.

ICANN: Corporación para la Asignación de Nombres y Números en Internet.

ICN: Redes Centralizadas de Información.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

IETF: Grupo de Trabajo en Ingeniería de Internet.

IOT: La Internet de las Cosas.

IP: Protocolo de Internet.

IPSEC: Seguridad del Protocolo de Internet.

IPv4: Protocolo de Internet versión 4.

IPv6: Protocolo de Internet versión 6.

ITI: Innovación sobre la Tecnología de los Identificadores – Un panel de estrategia de la ICANN.

LISP: Protocolo de Separación de Localizador / Identificador [RFC 6830].

MIB: Base de Información de Gestión.

MTU: Unidad Máxima de Transferencia - El tamaño de una unidad de dato máxima que puede pasar con fragmentación o sin la misma.

MX: Mail eXchange - Un tipo de datos del DNS que especifica el intercambio de correo electrónico que maneja el correo de un nombre de dominio específico.

NAPTR: Puntero a la Autoridad de Asignación de Nombres - Un tipo de dato del DNS más comúnmente utilizado en telefonía por Internet.

NDN: Redes de Datos Nominadas.

P2P: Entre pares.

PKI: Infraestructura de Clave Pública.

RFC: Solicitud de Comentarios - Memorandos que documentan las cuestiones técnicas y operativas de Internet.

RIR: Registro Regional de Internet - Una de las organizaciones que administra la asignación y registración de los recursos numéricos de Internet dentro de una región del mundo. Por ejemplo, ARIN, el Registro Norteamericano de Números de Internet administra Canadá, los Estados Unidos y muchas islas del Caribe y el Atlántico Norte.

Rsynch: Protocolo de Sincronización Remota - sincroniza archivos y directorios en tanto que minimiza la transferencia de datos mediante la utilización de codificación delta.

RR: Registro de Recurso - La unidad atómica de información en el DNS.

TSIG: Firma de la Transacción.

TTL: Tiempo de Vida.

TXT: El tipo RR de texto en el DNS, que permite el libre formato en los campos de texto.

UDP: Protocolo de Nivel de Transporte - el Protocolo de Transporte sin conexión de Internet.

UI: Interfaz del Usuario.

URI: Registro de Identificadores Uniformes de Recursos.

URL: Localizador Uniforme de Recursos.

WIFI: Fidelidad Inalámbrica - los estándares de redes móviles definidos por la familia de estándares de IEEE 802.11.

9. Contribuciones de los Miembros del Panel

Nótese que todas las contribuciones son textuales, tal como fueron enviadas por la persona.

9.1.Contribución de James Seng

Arquitectura Técnica

El hacker en mi interior está a favor de la arquitectura de descentralización. Se podría argumentar que la mayor parte de los "problemas políticos" que tenemos en la actualidad derivan de la naturaleza centralizada del DNS con la raíz.

Así que la tecnología como namecoins u otro sistema de identificación descentralizado me resulta difícil de comprender.

Sin embargo, no existe, en realidad, un sistema identificador descentralizado pero que lleve a cabo la coordinación que conozca y que sea ampliamente utilizado. Así que nos guste o no, el sistema del DNS es todavía uno de los sistema de identificación implementados que tenemos. A medida que avanzamos en el IETF, son los "códigos de ejecución" los que ganan, y no necesariamente el mejor diseñado.

Yo no creo en la raíz múltiple o raíz alternativa. Como dije en Buenos Aires, respaldo la RFC 2826. La raíz múltiple o la raíz alternativa y toda propuesta relacionada sólo trasladan el problema político a otro nivel, pero no resuelven el problema político fundamental. Nótese que dije, el problema político, porque no creo que la raíz múltiple resuelva algún problema técnico en absoluto; en todo caso, sólo aumenta la complejidad técnica.

ICANN

El DNS y su naturaleza centralizada de la raíz resultaron, en parte, de la sencilla operación de la función de IANA original para convertirse en la gran organización llamada ICANN, en la actualidad.

He participado en la ICANN desde la primera reunión celebrada en 1999 y he asistido a casi todas ellas. Durante estos años, hay cosas que me habría gustado que la ICANN hubiese hecho otra manera, por ejemplo, nuestra postura no siempre se encuentra alineada.

Sin embargo, la ICANN es el "código de ejecución" en la coordinación de los identificadores del DNS. Quizás haya otros diseños mejores, tal vez más simples y elegantes (como a muchos en la comunidad del IETF, nos hubiera gustado volver a los días de Jon Postel), pero es lo que es hoy, y lo más importante es que, aunque se podría mejorar, funciona. La alternativa propuesta (UIT) que conocemos tiene otros problemas, o incluso peores.

Así que apoyo a la ICANN, ya que es simplemente el mejor sistema de trabajo que tenemos para la coordinación de los identificadores del DNS y la raíz.

Extensión del DNS y su Sistema a Otras Áreas

En consecuencia, no tengo mucho interés en rediseñar el DNS o las propuestas alternativas para nombrar identificadores. Finalmente, alguien, alguna organización tiene que existir para efectuar la coordinación y enfrentaremos los mismos problemas políticos generales.

Avalo y me gusta ver el ecosistema del DNS (estándares del DNS, el funcionamiento de la raíz, la ICANN,...) que tenemos, el cual ha sido originalmente diseñado para DNS y que ha evolucionado hasta extenderse a otras áreas (por ejemplo RFID), de modo que una mayor parte de la comunidad pueda participar. El trabajo que hicimos sobre los IDN, en cierto sentido, incorpora a un grupo de la comunidad de usuarios que tiene que utilizar su lengua materna en el ecosistema del DNS, en lugar de dejar que lo construyeran por sí solos.

Si bien algunos han discutido conmigo respecto de que si hemos creado IDN fuera del ecosistema del DNS, la implementación podría haber sido mucho más rápida (por ejemplo, véase Palabras Claves en Lengua Materna); sostengo que los IDN también son mejores, porque son parte del ecosistema del DNS, donde existen estándares bien definidos, implementaciones abiertas, empresas que se basan en la legitimidad del DNS, y, de manera similar, la protección de los registratarios de IDN y los usuarios finales.

Como tal, no tengo reparos y estoy a favor del hecho de explorar cómo podemos extender el DNS a los identificadores para los cuales no había sido diseñado en un principio. Los ingenieros que diseñaron los identificadores suelen ignorar la política aparejada a los identificadores, especialmente si dichos identificadores se exponen a los usuarios finales. Podrían aprender una o dos cosas de la historia de los identificadores del DNS y la ICANN.

Política de la Raíz

La política de la ICANN, y cuántos la ven como parte de la "gobernanza de Internet" deviene del rol de la ICANN en la coordinación de los servidores raíz.

Lo peor es que 11 de los 13 servidores raíz tienen su sede en EE.UU., debido a un accidente histórico, pero sin embargo, esto hace que se perciba que la ICANN ha estado bajo el control de los EE.UU., lo que es aún peor, en especial, en estos días posteriores al caso Snowden.

Cada vez que alguien se acerca y habla de que tal o cual país debe contar con un servidor raíz, nos desviamos utilizando motivos históricos o técnicos en que no hay manera de extenderse más allá de 13 raíces.

La historia es algo que puedo aceptar como una razón.

Las razones técnicas, no. Es más bien una excusa porque no he sido consciente de todo esfuerzo del IETF por considerar seriamente la forma de extenderse más allá de las 13 raíces. Es por esto que, en Buenos

Aires, señalé que puedo pensar en un par de soluciones técnicas, al menos que sean suficientes como un I-D. No podemos dejar que la ICANN continúe utilizando al IETF / a las razones técnicas como excusa para los problemas políticos que enfrentan. Debemos poder decirle a la ICANN: "Sí, se puede hacer"; sin embargo, la política de hacerlo o no es algo que ustedes deben decidir.

Por otro lado, y más importante, el funcionamiento de los servidores raíz no se promociona.

Tener una raíz no significa, por así decirlo, tener el control inmediato de Internet. De hecho, resulta tan aburrido como una Raíz Anycast. Aunque si el operador raíz no sigue algunas de las Mejores Prácticas de la Operación de Servidores Raíz (por ejemplo, RFC 2010 y RFC 2870), entonces, puede causar mucho daño a Internet.

La mayoría de los ingenieros probablemente entendieron lo que dije anteriormente, pero no la mayoría de los que participan en la ICANN.

Así que existen consideraciones a la hora de seleccionar un operador de servidor raíz, porque es el pináculo de la estabilidad de los identificadores de Internet, y gran parte de ellos se basan en la Confianza. Sin embargo, la Confianza, nos guste o no, no es un problema de ingeniería.

James Seng

http://chineseseoshifu.com/blog/dnspod-in-china.html

¿Por qué el DNSPod es útil en China, a pesar de la forma en que "rompió" el DNS?

9.2. Resolución del DNS y Comportamiento de la Aplicación de Listas de Búsqueda - Geoff Huston

ninguno - NO realiza ninguna búsqueda de DNS

nunca - busca el nombre de la base, pero no se aplica la lista de búsqueda

pre - se aplica la lista de búsqueda, y si devuelve NXDOMAIN, luego buscar el nombre de la base

post- busca el nombre de la base, y si devuelve NXDOMAIN, luego aplica la lista de búsqueda

siempre - NO busca el nombre de la base - sólo aplica la lista de búsqueda

Comportamiento de la librería del resolutor del DNS del sistema operativo base.

Sistema	**Absoluto** *servidor*	**Etiqueta Única Relativa** *servidor*	**Etiqueta Múltiple Relativa** *www.server*
MAC OSX 10.9	Nunca	Siempre	Nunca
Windows XP	Nunca	Siempre	post
Windows Vista	Nunca	Siempre	Nunca
Windows 7	Nunca	Siempre	Nunca
Windows 8	Nunca	Siempre	Nunca
FreeBSD 9.1	Nunca	pre	post
Ubuntu 13.04	Nunca	pre	post

Comportamiento del buscador en plataformas de MAC y Windows

MAC OSX 10.9

	servidor	*servidor*	*www.server*
Chrome (31.0.1650.39 beta)	Nunca	Siempre	pre
Opera (12.16)	Nunca	Siempre	Nunca
Firefox (25.0)	post*	Siempre	post*
Safari (7.0 9537.71)	Ninguno**	Ninguno**	Ninguno**

* Se ha añadido el prefijo "www.", luego se trató de prefijar "www.", y también anexar la lista de búsqueda

** Safari parece estar al tanto de los TLD y no realiza búsquedas de DNS cuando el nombre no es un TLD

Windows 8.1

	servidor	*servidor*	*www.server*
Explorer (11.0.900.16384)	Ninguno	Ninguno	Nunca
Firefox (25.0)	Nunca*	Siempre	Nunca
Opera (17.0)	Ninguno	Ninguno	Ninguno**
Safari (5.1.7 7534.57.2)	Nunca*	Siempre***	Nunca

* Añadió un prefijo "www"

** OPERA está al tanto de los TLD delegados, y sólo requiere que la última etiqueta sea un TLD

*** Añadió el prefijo "www" y el sufijo". com"

9.3. Observaciones sobre la Coherencia y Contribución Derivada - Geoff Huston

Si nos retrotraemos a los orígenes del Sistema de Nombres de Dominio, encontramos los llamados "archivos hosts", como un primer intento de llevar los nombres de uso humano al contexto de las redes informáticas. ARPANET utilizó un modelo de nombres de nodos de red en el que cada nodo conectado tenía un archivo de configuración local, el archivo hosts, que contenía los nombres de todos los demás nodos de ARPANET, y las direcciones de protocolo de cada nodo. No existía una coherencia forzada a través de estas múltiples instancias de este archivo hosts en el conjunto de nodos conectados a ARPANET, ni, en su momento, existió algún método para distribuir una copia del archivo hosts en toda la red. La utilidad de este archivo hosts era proporcionar nombres familiares para los seres humanos en lugar de las direcciones de nivel de protocolo más obtusas. Los usuarios pudieron identificar los nodos de red por su nombre simbólico, que luego se tradujo en una dirección binaria específica del protocolo a través de una búsqueda en el archivo hosts. Conforme ARPANET creció, también lo hizo el tamaño y la velocidad de actualización del archivo hosts y, por otro lado, se incrementó la sobrecarga de mantener un hosts local preciso. El formato de archivo hosts se estandarizó (RFC952) y se definió un servicio de archivo hosts central (RFC953) que podría ocupar el lugar de muchas copias locales de este archivo.

Esto, entonces, fue reemplazado por el Sistema de Nombres de Dominio (DNS), especificado originalmente en 1983 en el RFC 882 y RFC 883. El mecanismo de traducción de un nombre, especificado como una cadena de caracteres familiar para el ser humano, a una dirección de un servicio específico del protocolo se mantuvo en la transición del archivo hosts al DNS.

Este espacio de identificadores tiene un número de propiedades que incluyen la observación de que el DNS se extiende a un espacio de nombres que es adecuado para su uso en el discurso humano, en tanto que, al mismo tiempo, admite una estructura formal suficiente para permitir que los nombres sean manipulados por aplicaciones informáticas de una manera determinista. El espacio de nombres del DNS es un espacio de estructura jerárquica, lo que permite que el espacio de nombres sea examinado de manera eficiente en la búsqueda de coincidencias exactas, y, al mismo tiempo, da lugar a un marco de gestión distribuida del espacio de nombres. Mientras se eviten las colisiones de etiquetas dentro de cualquier zona individual en la jerarquía de nombres del DNS, las colisiones de nombres se pueden evitar en el todo el espacio, lo que permite una singularidad única en cuanto a que los nombres pueden ser fácilmente administrados dentro del contexto del DNS. El DNS es flexible en cuanto a su función de

mapeo, y se puede utilizar para trazar desde un espacio de nombres estructurado hasta cualquier otra forma de recurso de nombre, nuestro punto de servicio. Se busca que el DNS tenga coherencia, en cuanto a que, dada una entrada de nombre compatible en el DNS, las consultas sobre ese nombre deben proporcionar la misma respuesta en las diferentes ubicaciones donde realiza la consulta y en los diversos momentos en que se realiza la misma. Esto da lugar a la coherencia referencial, en el que un nombre de DNS puede pasarse entre las partes y derivar en un recurso congruente de la ubicación de servicio. El DNS no está diseñado para reemplazar a un sistema de directorio o a un sistema de búsqueda. Si hay una coincidencia exacta del nombre que se consulta en el DNS, la consulta del DNS devolverá el valor asignado como resultado de la misma, de lo contrario la consulta devolverá un error de coincidencia.

Este modelo del espacio de nombres del DNS como el espacio de nombres de un identificador usado para dar soporte a una interfaz humana con la red ha sufrido, desde entonces, una serie de cambios, principalmente en respuesta a la modalidad de uso humano de los identificadores en el discurso. Tenemos la tendencia a utilizar los identificadores de maneras que son menos precisas, y en formas que incluyen elementos de contexto local, que utilizan las lenguas y escrituras locales, y con el tiempo, el papel del DNS como forma de interfaz humana con respecto a los recursos y servicios de la red ha sido subsumido por los esfuerzos para soportar interfaces que actúan de una manera más "natural" para el uso humano.

La RFC1034 propuso el uso de una forma de taquigrafía en la especificación de los nombres del DNS, donde los nombres que no finalizaban con una terminación '.' se denominan "nombres relativos", y, como se señala en la RFC1034, los "nombres relativos en su mayoría aparecen en la interfaz del usuario, donde su interpretación varía según cada implementación". Generalmente, tal interpretación local implicaba el aplacamiento de una lista de búsqueda local de sufijos de etiquetas, lo que permite al usuario especificar la parte inicial de un nombre de dominio, y confiar en la aplicación local o las rutinas de software de resolución de nombres para añadir un sufijo definido localmente a fin de formar un nombre de DNS completo.

Esta forma de oclusión selectiva del espacio de identificadores del DNS mediante el uso de sufijos de nombre se llevó un paso adelante en la interfaz de usuario proporcionada por los navegadores web, donde la práctica común con los navegadores web iba a tener el componente del identificador del DNS de una dirección URL y aplicar una transformación del nombre al anteponer la cadena "www." y al agregar un sufijo definido localmente (por lo general ". com."). De esta manera, el identificador que el usuario especificó y el nombre del identificador usado en la posterior consulta al DNS estaban relacionados, pero no necesariamente eran lo mismo.

Este uso de las transformaciones de nombres locales se amplió aún más de modo que los identificadores formados a partir de códigos de escritura distintos del US- ASCII se asignaron en el DNS (IDN: RFC5891). Esto fue un proceso definido de forma explícita en el que el identificador introducido por el usuario se transforma en una cadena de caracteres de etiqueta codificada que forma la consulta al DNS. En este caso, la transformación está precisamente definida, de manera que las múltiples implementaciones del

estándar de IDN tienen como finalidad dar soporte a una visión compatible de la asignación de un identificador en un código de caracteres dado a una forma de nombre de DNS codificado.

Otra evolución del refinamiento del modelo de interacción humana fue la unificación de los términos de búsqueda y los URL como entrada a los navegadores. En este caso, si el usuario no ha utilizado la especificación completa de un URL en el navegador, el navegador intentará asociarlo con una fecha.

9.4.Algunos Problemas con las Tecnologías de Identificadores Actuales – Rick Boivie

1. Flexibilidad de la Zona Raíz

En la actualidad, el sistema del DNS depende en gran medida de la disponibilidad, capacidad y accesibilidad de los servidores raíz. Si una empresa, un ISP, un país o un usuario mantuviera sus propias copias de la zona raíz y las usara para resolver nombres de dominio, en lugar de siempre recurrir a los servidores raíz "reales", esa empresa, ese ISP, país o usurario, tendría una mejor protección contra los ataques a los servidores raíz, y podría continuar funcionando normalmente cuando una empresa, un ISP, un país o un usuario se desconecta de los servidores raíz reales, y cuando los servidores raíz reales no se encuentran disponibles, están sobrecargados, o comprometidos.

2. Uso Fraudulento de Direcciones IP

Los paquetes de direcciones IP con direcciones fuente falsificadas son una de las herramientas más importantes que utilizan los delincuentes en la actualidad para evitar que sus víctimas usen Internet. Al enviar paquetes que aparentemente provienen de la víctima, y al hacerlo desde una gran cantidad de máquinas, el atacante puede causar una gran cantidad de tráfico de "respuestas" que congestionará o sobrecargará los enlaces de red que retornan a la víctima.

3. Cambio Rápido del Relacionamiento entre Nombres y Direcciones en el DNS

En la actualidad, el sistema del DNS suele ser objeto de uso indebido por parte de delincuentes, en formas que les permiten evitar que las autoridades legítimas rastreen y bloqueen sus actividades ilegales. Hoy en día, un "botnet master" puede recurrir a un conjunto de máquinas secuestradas (una "botnet") para varias clases de actividades ilegales, entre las cuales se incluye enviar spam, lanzar ataques DDOS, e infectar otras máquinas con varias clases de software malicioso. Al cambiar rápidamente el relacionamiento entre nombres y direcciones en el sistema del DNS, los botnet masters pueden trasladar rápidamente sus actividades ilegales de un conjunto de máquinas secuestradas a otro, con el fin de evadir los esfuerzos de las autoridades legítimas por rastrear y bloquear sus actividades ilegales.

Recomendamos que la ICANN trabaje con otros integrantes de la comunidad de Internet para:

(1) mejorar la flexibilidad de la zona raíz

(2) abordar el uso fraudulento de direcciones IP

(3) abordar el problema del cambio del relacionamiento entre nombres y direcciones en el DNS

9.5.Anycast Universal para la Zona Raíz

Generalidades

Proponemos que la IANA produzca varias formas adicionales de la zona raíz del DNS, para dar lugar a una dirección anycast universal y la investigación operativa. "Anycast universal", en este contexto, significa una zona raíz cuyos registros NS en el ápex enumeran sólo dos servidores de nombres, cuyas direcciones "conocidas" asociadas (según los registros A y AAAA) pueden ser alojadas por cualquiera. "La investigación operativa", en este contexto, incluye pruebas públicas a gran escala del servicio de nombres de la raíz solo en IPv6 y pruebas públicas a gran escala de los efectos de colisión de los "nuevos gTLD". Este enfoque trata el servicio de nombres de la raíz como una utilidad no administrada y no como una utilidad administrada.

Antecedentes

La dirección anycast universal para la zona raíz no podía ser implementada de manera segura y responsable antes del advenimiento de DNSSEC, ya que sin DNSSEC, cualquier servidor que responda puede ser configurado con los datos raíz de DNS arbitrarios, incluyendo los de los nuevos TLD o los TLD re-delegados existentes. Con DNSSEC, ahora es posible para los operadores de servidores de nombres recursivos configurar la validación de DNSSEC, de tal manera que cualquier información sobre gTLD proveniente de un servidor raíz de dirección anycast universal deba ser aprobado por la IANA, como lo indican las firmas de DNSSEC efectuadas con la clave de la firma en la zona raíz de la IANA.

Las críticas al Sistema de Servidores Raíz actual e histórico incluyen la falta de resistencia a los ataques al DDoS, lo que indica que, incluso con la actual difusión ilimitada a gran escala por parte de cada Operador de Servidores de Nombres Raíz, todavía hay sólo unos pocos cientos de servidores de nombres en el mundo que pueden responder autoritativamente para la zona raíz del DNS. También nos preocupa que se requiera accesibilidad al Sistema de Servidores de Nombres Raíz, incluso para la comunicación puramente local, ya que, de otro modo, los clientes no tienen manera de descubrir los servicios locales. En un sistema mundial distribuido y dimensionado como lo es Internet, los servicios críticos deben estar muy bien distribuidos.

Detalles

Existen varias variaciones útiles para construir. En primer lugar, la dirección anycast básica universal permitirá a cualquier operador de servidor de nombres capturar el tráfico dirigido hacia el sistema de servidores de nombres raíz y responder a nivel local. La IANA generaría y firmaría digitalmente (con DNSSEC) una versión adicional de la zona raíz que tiene un conjunto diferente de registros NS en su

ápex. Estos registros NS denotarán los servidores de nombres cuyas direcciones no estén asignadas a ningún Operador del Servidor de Nombres Raíz (RNSO) en particular, pero que son mantenidas en fideicomiso por la IANA para uso por parte de cualquiera o todas las partes interesadas. La IANA solicitaría micro-asignaciones de infraestructura de un RIR (como ARIN o APNIC), como varios prefijos IPv4 de 24 bits y varios prefijos IPv6 de 48 bits, para su uso en la replicación universal de la zona raíz.

Una segunda variante en la actual zona raíz proporcionaría una dirección anycast universal como la anterior, pero denotaría servidores de nombres que sólo tenían conectividad IPv6 (indicado por la presencia de registros AAAA) y sin conectividad IPv4 (como lo indica la ausencia de registros A). Esta variación facilitaría la investigación operativa en redes de sólo IPv6.

Una tercera variante en la actual zona raíz proporcionaría una dirección anycast universal como la anterior, pero incluiría las delegaciones de todos los nuevos gTLD conocidos, incluyendo aquellos que, de otra manera, no están listos para la delegación (como. CORP y. HOME). Estos nuevos gTLD se delegan a un servidor de nombres operado por la IANA misma, con fines de medición. Cada nuevo gTLD recibirá un comodín A y registros AAAA, cuyas direcciones llegarán a los servidores web operados por la IANA con fines de medición.

Impacto

Dada la naturaleza jerárquica de enrutamiento de Internet, los bloques de direcciones anycast pueden ser objeto de publicidad en múltiples niveles. Una máquina virtual (VM) que se ejecuta en un ordenador portátil podría tener su propio proceso de servidor de nombres que escuche en las direcciones apropiadas conocidas, en cuyo caso no habrá consultas de servicio de nombres raíz que abandonen la VM. La computadora portátil, en sí, también podría capturar el tráfico saliente dirigido a estas direcciones conocidas, que serviría a otra VM u otros procesos que se ejecutan en ese equipo portátil. El enrutador inalámbrico ascendente de esta computadora portátil podría tener servidores que escuchen en estas direcciones, en cuyo caso no habrá consultas de servicio de nombres raíz que abandonen la red LAN inalámbrica. El ISP podría operar servidores que escuchen en estas direcciones conocidas, para dar servicio a todos los clientes que no operen sus propios servidores. Por último, se espera que la Internet global posea muchos operadores que anuncien rutas a estos bloques de direcciones bien conocidas, los cuales, aunque no por ello menos importante, serían los doce operadores de servidores de nombres raíz existentes.

El impacto positivo de esto sería una mayor flexibilidad potencial y la reducción de la latencia del servicio de nombres en la raíz. El impacto negativo estaría dado en una reducción en la capacidad de diagnóstico y el aumento de la vulnerabilidad al "envenenamiento de la ruta"" o "apropiación" del tráfico del servicio de nombres en la raíz. Es, en todo caso, imprescindible que la validación de DNSSEC se torne común a fin de reducir el tipo de recuperación para este tipo de apropiación. Queremos que el resultado para un atacante sea "la "víctima pierde los servicios de nombres en la raíz " y no "la víctima ve un espacio de nombres del DNS diferente".

Ejemplos

Los siguientes ejemplos muestran el conjunto de registros NS del ápex para cada variante de la zona raíz, que incluyen el agregado de direcciones. Estos datos se incluirían en una zona raíz variante antes de la firma de DNSSEC y también se publicarían como un archivo "root hints" Los datos mostrados para iana-servers.net también estarían presentes en la zona de iana-servers.net real. Estos ejemplos requerirían cuatro micro-asignaciones de IPv4 y seis micro-asignaciones de IPv6.

Variante 1: anycast universal

```
. IN NS anycast-2.iana-servers.net.
. IN NS anycast-2.iana-servers.net.
$ORIGIN iana-servers.net.
anycast-1 IN AAAA 2001:?:1::1
anycast-1 IN A ?.?.1.1
anycast-2 IN AAAA 2001:?:2::2
anycast-2 IN A ?.?.2.2
```

Variante 2: anycast universal solo para IPv6

```
. IN NS v6only-1.iana-servers.net.
. IN NS v6only-2.iana-servers.net.
$ORIGIN iana-servers.net.
v6only-1 IN AAAA 2001:?:3::1
v6only-2 IN AAAA 2001:?:4::2
```

Variante 3: estudio de colisión de gTLD anycast

```
. IN NS gtldstudy-1.iana-servers.net.
. IN NS gtldstudy-2.iana-servers.net.
$ORIGIN iana-servers.net.
gtldstudy-1 IN AAAA 2001:?:5::1
gtldstudy-1 IN A ?.?.5.1
```