Nombre: Sara María Castrillón Ríos
Curso: ST0263 – Tópicos Especiales en Telemática
Semestre: 2023-2
Fecha de entrega: 8 de agosto 2023

RETO 1: Domain Name System – DNS.

Elementos conceptuales:

El sistema de nombres de dominio (DNS), trabaja sobre el protocolo UDP debido a que no se necesita manejar integridad en los datos (no son sensibles), entonces prefiere apostarle a la velocidad en tiempo de respuesta. DNS se encarga de vincular los nombres de dominio con sus respectivas direcciones de Protocolo de Internet (IP) de tal forma que cuando los usuarios introducen un nombre de dominio en la barra de direcciones de su navegador web, sin saberlo, están enviando una solicitud de DNS; En la cual, inicialmente el ordenador comprobará si ya ha almacenado un registro DNS (dirección IP que corresponde con el nombre de dominio buscado) del dominio que has enviado localmente.
Las direcciones IP correspondientes del servicio DNS suelen encontrarse en la caché del navegador o en la caché del proveedor de servicios de Internet (ISP).
Sin embargo, si no se encuentra ninguna dirección IP que coincida en el archivo hosts y/o en la caché, se enviará la consulta o petición DNS a una red con cuatro tipos de servidores DNS, los cuales funcionan de la siguiente manera:

1. **Resolutor recursivo:** Actúa como intermediario principal entre un ordenador y otros servidores DNS. Su propósito es reenviar una petición a otros servidores DNS y luego devolverla una vez completada.
   Cuando el resolutor recursivo recibe una petición, primero busca en su caché una dirección IP que coincida con el nombre de dominio. Si se encuentra esa dirección IP, la petición enviada a los servidores DNS termina aquí, y se verá inmediatamente el sitio que se quiere visitar.
   Sin embargo, si no encuentra ninguna coincidencia en la caché, el resolutor recursivo enviará la solicitud al siguiente servidor DNS: el root server.
2. **DNS root server:** No guarda las direcciones IP asociadas a nombres de dominio, pero da indicaciones de dónde pueden encontrarse.
   Una vez que el root server recibe una petición del resolutor recursivo, identificará el dominio de nivel superior del nombre de dominio. Entonces, le dirá al resolutor recursivo con qué servidor TLD se debe comunicar.
3. **Servidor de nombres de dominio de nivel superior (TLD):** Es el responsable de almacenar y gestionar la información sobre los nombres de dominio que utilizan un dominio de nivel superior (TLD) específico. Un TLD es la última parte de un nombre de dominio, como .com, .org y .net.
4. **Servidor de nombres autoritativo:** Es la autoridad final en el proceso de resolución DNS. almacena toda la información relacionada con el nombre de dominio que deseas visitar, incluida su dirección IP. El resolutor recursivo obtendrá la dirección IP y la enviará de nuevo al ordenador, dirigiéndolo al sitio.

   Por último, el resolutor del sistema de nombres de dominio realiza el almacenamiento en caché de DNS, almacenando las direcciones IP recogidas de los servidores de nombres autoritativos como datos temporales. En otras palabras, el almacenamiento en caché del DNS hace que la próxima vez que se quiera visitar el mismo sitio, solo tendrá que devolver la coincidencia de la dirección IP obtenida anteriormente.

Como se puede observar, este es un sistema distribuido (o base de datos distribuida) ya que cuenta con múltiples servidores al rededor del mundo en diferentes zonas, cada uno con información diferente y espacios de alojamiento de memoria separados, pero que trabajan en conjunto para proporcionar la información solicitada.
A continuación, se analiza cómo funciona este sistema distribuido desde diferentes perspectivas:

- **Perspectiva arquitectural:** Desde el punto de vista arquitectural, al hablar de la comunicación server-to-server, el DNS se basa en una jerarquía de servidores distribuidos que colaboran para proporcionar respuestas rápidas y eficientes a las consultas de resolución de nombres. Ya que se tienen varios servidores distribuidos alrededor del mundo que siguen la jerarquía explicada en el punto anterior: En la parte superior se encuentran los servidores raíz que contienen información sobre los servidores de nombres de dominio de nivel superior o Top Level Domain. Después están los servidores de nombres de dominio de segundo nivel, que a su vez contienen información sobre los servidores de nombres de dominio de tercer nivel.

  Sin embardo, también podemos notar una arquitectura cliente/servidor en el momento en el que el browser realiza una petición DNS y la solicitud se envía al servidor DNS local, que verifica su caché local para ver si tiene la información solicitada. Si la información no se encuentra en la caché local, el servidor DNS local envía una solicitud de consulta recursiva a otro servidor DNS, avanzando en la red de servidores jerárquica de DNS hasta encontrar la información solicitada. Una vez que se encuentra la información, el servidor DNS local almacena la información en su caché local, acelerando búsquedas futuras de la misma información.

  Es importante destacar que el DNS opera en un modelo cliente-servidor en el que el cliente envía consultas a los servidores DNS para obtener respuestas. La arquitectura jerárquica y distribuida del DNS permite una resolución eficiente de nombres en todo Internet.

Perspectiva de procesos/concurrencia: El DNS maneja la concurrencia mediante su arquitectura distribuida y jerárquica, el uso de caché local, la replicación de servidores autorizados, el uso de anycast y el balanceo de carga. Estas estrategias permiten que el DNS resuelva consultas de manera eficiente y confiable, incluso en entornos de alta concurrencia y tráfico intenso:

- **Arquitectura distribuida y jerárquica:** Como se analizó en el punto anterior, el DNS se basa en una red distribuida de servidores que trabajan en conjunto. Los servidores DNS están distribuidos en todo el mundo y organizados en una jerarquía. Los servidores raíz están en la cima, seguidos por los servidores TLD y luego los servidores autorizados para dominios específicos. Esta arquitectura permite distribuir la carga de consultas en muchos servidores, evitando así cuellos de botella y mejorando la escalabilidad del sistema.
- **Caché local:** Los servidores DNS locales y los resolutores implementan una caché local para almacenar temporalmente las respuestas a las consultas que han sido resueltas recientemente. Cuando otro cliente realiza la misma consulta, el servidor puede recuperar la respuesta de su caché local sin tener que enviar la consulta a servidores superiores, lo que reduce la carga y mejora la velocidad de respuesta.
- **Replicación de servidores autorizados:** Los dominios populares a menudo tienen varios servidores autorizados replicados en diferentes ubicaciones geográficas. Esta replicación permite distribuir la carga de consultas entre los servidores autorizados, lo que aumenta la capacidad de manejar un mayor número de solicitudes concurrentes.
- **Anycast:** Algunos servidores DNS utilizan la técnica de "anycast" para responder a las consultas de manera más eficiente. Con anycast, una dirección IP se asigna a múltiples servidores DNS distribuidos geográficamente. Cuando un cliente realiza una consulta, la red dirige la solicitud al servidor más cercano geográficamente, reduciendo el tiempo de respuesta y ayudando a distribuir la carga de manera más equitativa.
- **Balanceo de carga:** Algunos proveedores de servicios de DNS implementan técnicas de balanceo de carga en sus servidores para distribuir las consultas entrantes de manera uniforme entre varios servidores disponibles. Esto garantiza que ningún servidor esté sobrecargado y mejora la resiliencia del servicio.

- **Perspectiva de comunicación entre procesos:** A la hora de llevar a cabo los procesos de DNS, es necesario establecer una comunicación clara entre servidores únicamente a través del paso de mensajes, un aspecto muy importante para los sistemas distribuidos. Por lo cual se utilizan dos mecanismos de comunicación cuando un cliente solicita una consulta:

  Inicialmente tenemos la consulta recursiva, la cual se encarga de realizar solo primera solicitud de la dirección IP al dominio correspondiente y en caso de no obtenerla, las solicitudes serán generas por servidores que la recibieron, hasta encontrarla. Mientras que la consulta iterativa realiza una búsqueda en la base de datos de la dirección IP relacionada con el nombre de dominio, y en caso de no encontrarla este se encarga de enviar consultas a diferentes servidores hasta que se resuelva la consulta.

  La comunicación entre procesos DNS generalmente ocurre mediante el uso de protocolos específicos diseñados para facilitar la resolución de nombres y el intercambio de información en el sistema de nombres de dominio, como son:
  - **Protocolo de resolución de nombres (DNS):** Este es el protocolo principal utilizado para la comunicación entre clientes y servidores DNS. Los clientes envían consultas DNS a los servidores DNS para obtener la dirección IP correspondiente a un nombre de dominio. Los servidores responden con la dirección IP o un error si no pueden resolver la consulta. DNS opera en el puerto UDP 53 y, en algunos casos, en TCP cuando las respuestas exceden el tamaño máximo de UDP.
  - **Protocolo de transferencia de zona (AXFR y IXFR):** Estos protocolos se utilizan para la replicación y sincronización de datos entre servidores DNS autorizados. AXFR (Transferencia de Zona Completa) se utiliza para transferir toda la zona de un servidor autorizado a otro, mientras que IXFR (Transferencia de Zona Incremental) se utiliza para transferir solo las actualizaciones incrementales desde la última transferencia. Esto permite mantener actualizados los datos de la zona entre servidores autorizados y garantizar la coherencia de la información.
  - **Protocolo de notificación de DNS (DNS NOTIFY):** Este protocolo permite a los servidores DNS autorizados informar a otros servidores sobre cambios en las zonas de dominio que gestionan. Cuando se producen cambios en una zona, el servidor que realiza el cambio notifica a los servidores secundarios que deberían actualizar sus copias de la zona mediante una notificación DNS NOTIFY.

  Estos protocolos permiten que los diferentes procesos DNS se comuniquen entre sí para proporcionar resolución de nombres, replicación de datos y actualización de registros en todo el sistema de nombres de dominio. Al trabajar juntos, estos protocolos permiten que el DNS funcione de manera eficiente y confiable en toda la infraestructura de Internet.

- **Perspectiva de coordinación:** En los sistemas distribuidos es indispensable la coordinación, pues al tratarse de tantos elementos independientes interactuando entre sí, es fundamental que la comunicación se dé de manera organizada. En cuanto a la coordinación de los diferentes componentes del DNS, las principales estrategias son la jerarquía de servidores, y las autoridades de zona. el DNS utiliza una jerarquía de servidores para manejar las solicitudes de los clientes, en la que cada uno es responsable de manejar las solicitudes de los servidores en niveles inferiores, reenviando las solicitudes a servidores en niveles superiores si no se puede responder a la solicitud. Y las autoridades de zona, en la que cada una hay un servidor que es responsable de mantener y actualizar la información de los registros de recursos en esa zona.

  En general, la coordinación en el DNS se realiza a través de estándares y políticas definidas por organizaciones como IANA e ICANN, así como mediante la colaboración y comunicación entre las diferentes entidades que operan servidores DNS y gestionan los dominios en todo el mundo. Esta coordinación garantiza la estabilidad y funcionalidad del DNS, lo que es esencial para el correcto funcionamiento de Internet.

- **Perspectiva de naming:** El DNS utiliza el sistema jerárquico del que se ha venido hablando, donde cada parte del árbol de nombres es gestionada por diferentes servidores que contienen el recurso (RR):
  - A (dirección IPv4).
  - AAAA (dirección IPv6).
  - CNAME (Para asociar a un alias).
  - MX (servidor de correo electrónico).
  - NS (servidor de nombres).

  Perspectiva de consistencia y replicación: Para garantizar la consistencia y manejar la replicación de la información, el DNS utiliza algunos mecanismos y técnicas que aseguran que todos los servidores autorizados estén actualizados y sincronizados:

  - **Transferencia de zona:** Es un proceso mediante el cual los servidores DNS secundarios obtienen una copia actualizada de los datos de nombres de dominio del servidor DNS maestro (autorizado) cuando se realizan cambios en la zona.
  - **Actualizaciones dinámicas de DNS:** Los servidores DNS pueden permitir actualizaciones dinámicas, lo que significa que los clientes pueden modificar directamente los registros DNS en el servidor maestro. Esto es útil en situaciones en las que las direcciones IP cambian con frecuencia, como en conexiones de Internet con dirección IP dinámica.
  - **TTL (Tiempo de vida del registro):** Cada registro de DNS tiene un valor de TTL asociado, que especifica cuánto tiempo se mantendrá en caché una respuesta antes de que deba ser considerada obsoleta y se deba buscar una actualización.
  - **Replicación geográfica:** Algunas organizaciones implementan replicación geográfica, donde mantienen copias de los servidores DNS en diferentes ubicaciones geográficas. Esto ayuda a mejorar la disponibilidad y la resistencia frente a desastres o problemas en una ubicación específica.
  - Anycast y Protocolo de notificación de DNS (DNS NOTIFY), de los cuales se habló en secciones pasadas.

- **Perspectiva de tolerancia a fallos:** Gracias a las técnicas de replicación mencionadas en el punto anterior, se puede garantizar la tolerancia a fallos mediante la redundancia y replicación de datos con protocolos como el de transferencia de zona, pues los servidores de nombres de nivel superior suelen tener múltiples réplicas en diferentes ubicaciones geográficas.
  También se utilizan otras técnicas como el caché, que permite que los servidores almacenen temporalmente información de nombres de dominio y otros servidores pueden utilizar esta información en caso de que el servidor responsable falle o sea inaccesible.
  Finalmente, podemos hablar de la distribución de carga (Proxy inverso), quien ayuda a equilibrar la carga de trabajo entre los servidores de nombres y redistribuirla automáticamente si un servidor falla, además de que La distribución equitativa de las consultas DNS entre múltiples servidores mediante técnicas de balanceo de carga garantiza que ningún servidor esté sobrecargado y permite una mejor utilización de los recursos.

- **Perspectiva de seguridad:** El servicio DNS emplea diferentes mecanismos para contrarrestar los posibles ataques o vulnerabilidades que se puedan presentar. Medidas de seguridad como:
  - **Domain Name System Security Extensions (DNSSEC):** Es una extensión del DNS que proporciona autenticación y protección contra ataques de envenenamiento de caché y suplantación de identidad. Refuerza la autenticación en DNS, ayudando a proteger Internet de los hackers, pues valida las consultas realizadas por un cliente para asegurarse de que no dirijan a un entorno malicioso.
  - **Cifrado TLS o Trasport Layer Security**: Un proceso que encripta los flujos de datos de Internet para que solo sus legítimos destinatarios puedan leerlos.
  - **Restricción de zonas.**

- **La implementación de un proxy inverso** que garantiza que el cliente que realiza la solicitud NO sepa cual o cuales servidores están dando respuesta a ella.
- **Monitoreo y detección de anomalías e la implementación de políticas de seguridad**: Para verificar periódicamente la confiabilidad de los servidores DNS y mantenerse informado sobre posibles cambios en la configuración de DNS. Al hacer esto, sabrá cuándo el rendimiento general de su sitio se ve afectado por un DNS intermitente o defectuoso, o se le advertirá de posibles intentos de ataque a un sitio.
  Las herramientas de monitoreo de DNS prueban la **conectividad** (ping) entre los servidores de nombres autorizados de sus nombres de dominio y los servidores de nombres recursivos. Esta prueba se puede realizar a pedido de forma manual o automática con una frecuencia determinada.
  Un servicio de monitoreo de DNS debe además probar que el servicio de DNS devuelve el conjunto correcto de direcciones IP en todo el camino al servidor DNS raíz. De esta forma, puede detectar el secuestro de DNS o Ataques de suplantación de DNS.
  El monitoreo DNS debe también poder detectar la ralentización del DNS, lo que indicaría un ataque de inundación y proceder a alertar a un administrador de red cuando se esté produciendo.

A modo de **conclusión**, pudimos observar que DNS es un sistema distribuido, pues tiene elementos que trabajan de manera independiente y se localizan en diferentes zonas. Pero todos ellos pertenecen a una misma red de datos que se comunica y coordina desde diferentes perspectivas, a través del paso de mensajes. Garantizando siempre:

1. Heterogeneidad y acoplamiento.
2. Seguridad.
3. Escalabilidad.
4. Manejo de errores.
5. Transparencia.

Si el DNS no manejara una arquitectura jerárquica y distribuida, sería un sistema **imposible de escalar** porque:

- Existiría un único punto de fallo debido a la centralidad.
- Sería un cuello de botella debido a la gran cantidad de datos que se debe almacenar.
- La base de datos con los registros DNS estaría alejada de la mayoría de los host de Internet.
- Una base de datos enorme, en continuo cambio, recaería en una sola máquina y su mantenimiento sería muy costoso.
- No sería posible la respuesta a solicitudes de manera concurrente.

Fuentes:

- Gustavo, B. (2019, mayo 20). ¿Qué es DNS y cómo funciona? Tutoriales Hostinger. https://www.hostinger.es/tutoriales/que-es-dns
- Arquitectura del DNS. (2009, marzo 3). Ual.es. http://www.hpca.ual.es/~vruiz/docencia/redes/teoria/html/texputse63.html
- TLS: cómo se encripta en Internet. (2020, julio 15). IONOS Digital Guide; IONOS. https://www.ionos.es/digitalguide/servidores/seguridad/tls-transport-layer-security/
- ¿Qué es DNSSEC? (s/f). one.com. Recuperado el 2 de agosto de 2023, de https://www.one.com/es/dominios/que-es-dnssec
- DNSSEC – what is it and why is it important? (s/f). Icann.org. Recuperado el 2 de agosto de 2023, de https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en
- 12 Herramientas de supervisión de DNS para cambios de configuración y rendimiento. (2020, enero 25). Geekflare. https://geekflare.com/es/dns-monitoring-tools/