DNS / PUERTO 53

Martinez Jean, Armijos Manuel, Sanchez Carlos, Curimilma Jhonathan
Carrera de Ingeniera en Ciencias Computacionales
Universidad Nacional de Loja
Loja-Ecuador
jean.martinez@unl.edu.ec
carlos.d.sanchez.b@unl.edu.ec
jhonathan.curimilma@unl.edu.ec
manuel.i.armijos@unl.edu.ec

***Abstract*—The Domain Name System (DNS) is a fundamental infrastructure on the Internet that enables the translation of human-readable domain names into numeric IP addresses used by machines. This report aims to provide a comprehensive overview of how DNS works, its architecture, its key components and the protocols involved.By understanding the fundamentals and key concepts of DNS, IT professionals will be able to make informed decisions and implement appropriate measures to ensure the availability and reliability of domain name services.**

***Keywords*—** *Domain Name System (DNS), Domain Name Translation, Numeric IP Addresses, DNS Operation, DNS Architecture, Availability, Reliability, Domain Name Services.*

***Resumen*—El Sistema de Nombres de Dominio (DNS) es una infraestructura fundamental en Internet que permite la traducción de nombres de dominio legibles por humanos en direcciones IP numéricas utilizadas por las máquinas. Este informe tiene como objetivo proporcionar una visión general exhaustiva del funcionamiento del DNS, su arquitectura, sus componentes clave y los protocolos involucrados. Al comprender los fundamentos y los conceptos clave del DNS, los profesionales de TI podrán tomar decisiones informadas y implementar medidas adecuadas para garantizar la disponibilidad y la confiabilidad de los servicios de nombres de dominio.**

***Keywords*—** *Sistema de Nombres de Dominio (DNS), Traducción de nombres de dominio, Direcciones IP numéricas, Funcionamiento del DNS, Arquitectura del DNS, Disponibilidad, Confiabilidad, Servicios de nombres de dominio.*

I. Introducción

El Sistema de Nombres de Dominio (DNS) es una infraestructura fundamental en Internet que desempeña un papel vital en la traducción de nombres de dominio legibles por humanos en direcciones IP numéricas utilizadas por las máquinas. Desde sus inicios en la década de 1980, el DNS ha sido un componente esencial en la navegación web, el envío de correos electrónicos, la comunicación en línea y muchas otras actividades en Internet. En esta guía, exploraremos la jerarquía del DNS, desde el nivel raíz hasta los subdominios, y analizaremos el papel de los servidores de nombres de dominio, los registros DNS y los diferentes tipos de consultas y respuestas DNS. También examinaremos las medidas de seguridad y las mejores prácticas para proteger el DNS contra ataques y garantizar su integridad y disponibilidad. El DNS continúa evolucionando en respuesta a los desafíos emergentes y los avances tecnológicos. Con el advenimiento de nuevas extensiones de dominio, la implementación de DNSSEC y los esfuerzos en curso para mejorar la privacidad y la seguridad, es fundamental estar al tanto de las últimas tendencias y desarrollos en el campo del DNS.

Al final de este informe, aquellos interesados en comprender mejor el funcionamiento del DNS tendrán una base sólida para tomar decisiones informadas, resolver problemas relacionados con el DNS y garantizar la eficiencia y seguridad de los servicios de nombres de dominio en sus entornos de red.

II. Desarrollo

1) *ORIGEN:*

El Sistema de Nombres de Dominio (DNS) se originó a principios de la década de 1980 como una solución para facilitar la navegación y la comunicación en la incipiente Internet. Antes de la implementación del DNS, se utilizaba un archivo de texto centralizado llamado ”hosts.txt” que almacenaba una lista de nombres de dominio y sus direcciones IP correspondientes. Sin embargo, a medida que la Internet crecía rápidamente, mantener y actualizar manualmente este archivo se volvió cada vez más difícil y poco práctico.

En 1983, Paul Mockapetris, un investigador de la Universidad del Sur de California, desarrolló la idea del DNS como un sistema de resolución de nombres jerárquico y distribuido. Mockapetris propuso un modelo en el que los nombres de dominio se organizarían en una estructura de árbol invertido, en la que los dominios de nivel superior se ubicarían en la parte superior y los subdominios se ramificarían a partir de ellos.

En 1984, se publicó la primera especificación oficial del DNS en el documento RFC 882. Este documento fue seguido por el RFC 883, que proporcionaba detalles adicionales sobre el funcionamiento y la implementación del DNS. Estos estándares sentaron las bases para el desarrollo y la adopción generalizada del DNS como el sistema de nombres utilizado en Internet.

El DNS fue adoptado gradualmente y se convirtió en un componente esencial de la infraestructura de Internet. En la década de 1990, se realizaron mejoras significativas al DNS con la introducción de extensiones de seguridad (DNSSEC) para garantizar la autenticidad de los datos de DNS y proteger contra ataques maliciosos, como el envenenamiento de caché.

A medida que Internet continuaba expandiéndose, se estableció un modelo de gobernanza para la gestión del DNS. La Corporación de Internet para la Asignación de Nombres y Números (ICANN) fue creada en 1998 como una organización sin fines de lucro responsable de la coordinación y administración de los nombres de dominio y las direcciones IP en Internet.

Hoy en día, el DNS sigue siendo la columna vertebral de la navegación web y la comunicación en Internet. Ha evolucionado constantemente para adaptarse a los cambios tecnológicos y los desafíos de seguridad, y continúa desempeñando un papel fundamental en la resolución de nombres de dominio y la traducción de nombres legibles por humanos en direcciones IP utilizables por las máquinas.[1]

2) *SISTEMAS DE NOMBRES DE DOMINIO:*

El Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) es una infraestructura fundamental en Internet que permite la traducción de nombres de dominio legibles por humanos en direcciones IP numéricas utilizadas por las máquinas.
Cuando un usuario ingresa una URL o un nombre de dominio en su navegador web, como "www.ejemplo.com", el navegador necesita obtener la dirección IP correspondiente para poder establecer una conexión con el servidor que aloja ese sitio web. En lugar de recordar y escribir direcciones IP complicadas, el DNS actúa como un directorio telefónico de Internet, permitiendo que se utilicen nombres de dominio más fáciles de recordar.[2]

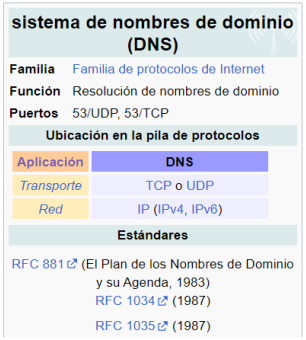

Fig. 1: DNS

3) *FUNCIONAMIENTO:*

Cuando un dispositivo (teléfono, computadora, tablet) necesita conectarse con otro, por ejemplo un servidor web, se inicia el proceso de resolución de ese nombre. El dispositivo cuenta con un resolutor básico que simplemente tiene configurada la dirección IP de uno o más resolutores iterativos.
Un resolutor iterativo tiene configuradas las direcciones IP de los servidores autoritativos de la raíz, de modo de poder comenzar desde la raíz a resolver los nombres de dominio de la siguiente forma:

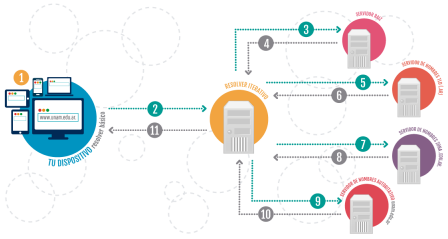

Fig. 2: Resolver Iterativo

1. El usuario ingresa el nombre del servidor al que se quiere conectar. Por ejemplo, en el navegador ingresa www.unam.edu.ar. Éste le solicita al resolutor básico - que es interno al dispositivo - la dirección IP asociada al nombre www.unam.edu.ar.

2. El resolutor básico se conecta a un resolutor iterativo (del cual ya sabe la dirección IP) y le solicita que resuelva el nombre www.unam.edu.ar a una dirección IP.

Fig. 3: Resolver Básico-Resolver Iterativo

3. Suponiendo que el resolutor iterativo no tiene ninguna información más allá de la configuración inicial, contacta a uno de los servidores raíz (que tiene configurados) y le solicita la dirección IP del nombre www.unam.edu.ar en forma autoritativa.

4. Como el servidor raíz no tiene información autoritativa de ese nombre pero sí conoce los servidores de los TLD .ar (porque esa zona está delegada desde la raíz), en su respuesta indica los nombres de los servidores autoritativos de esta zona y las direcciones IP de dichos servidores.

Fig. 4: Resolver Iterativo-Servidor Raíz

5. Conociendo esta información, el resolutor iterativo contacta a uno de los servidores autoritativos de la zona .ar, operados por NIC Argentina, y le solicita la dirección IP del nombre www.unam.edu.ar en forma autoritativa.

6. El servidor de la zona .ar tampoco tiene información autoritativa de ese nombre, pero sí sabe de los servidores de la zona .edu.ar, por ello, al igual que en el caso anterior responde cuáles son esos servidores de nombre.

Fig. 5: Resolver Iterativo-Servidores de Nombres TLD

7. Ahora el resolutor iterativo contacta a uno de los servidores autoritativos de la zona .edu.ar, operados por la Asociación Redes de Interconexión Universitaria – ARIU, y le solicita la dirección IP del nombre www.unam.edu.ar en forma autoritativa.

8. El servidor de la zona .edu.ar tampoco tiene información autoritativa de ese nombre, pero sí sabe de los servidores de la zona .unam.edu.ar, entonces responde indicando cuáles son esos servidores de nombre.

Fig. 6: Resolver Iterativo-Servidores de Nombres de Zona

9. Una vez más, el resolutor iterativo contacta a uno de los servidores autoritativos de la zona .unam.edu.ar (operados por la Universidad Nacional de Misiones) y le solicita la dirección IP del nombre www.unam.edu.ar en forma autoritativa.

10. Como este servidor conoce la información y es responsable de

ella, contesta con la dirección IP asociada a ese nombre indicando que la respuesta es autoritativa.

Fig. 7: Resolver Iterativo-Servidores de Nombres Autoritativo

11. Ahora el resolutor iterativo cuenta con la respuesta a la consulta recibida en el paso 2, entonces le responde al resolutor básico del dispositivo del usuario la dirección IP asociada al nombre www.unam.edu.ar.

Fig. 8: Resolver Iterativo-Básico

Dado lo largo del proceso y la cantidad de consultas que debe hacer el resolutor iterativo, normalmente, dicho servidor incluye una memoria cache local que utiliza para guardar todas las respuestas obtenidas de servidores autoritativos, tanto las intermedias como las finales. De este modo, cada dato autoritativo que obtiene lo almacena en dicha memoria con un detalle de la hora en que se almacenó y el tiempo por el cual será válida esa respuesta.
En base a esto, el proceso de resolución en una primera instancia busca la información en la memoria cache, y de encontrarlo, verifica si la respuesta almacenada aun es válida, caso contrario, inicia el proceso de consulta.

Nota: Típicamente el protocolo DNS transporta las peticiones y respuestas entre cliente y servidor usando el protocolo UDP, ya que es mucho más rápido. Las ocasiones donde se usa el protocolo TCP son: cuando se necesitan transportar respuestas mayores de 512 bytes de longitud (por ejemplo al usar DNSSEC) y cuando se intercambia información entre servidores (por ejemplo al hacer una transferencia de zona), por razones de fiabilidad.[3]

4) COMPONENTES:

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- **Clientes:** Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS *(Por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio?)*
- **Servidores DNS:** Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
- **Zonas de autoridad:** Es una parte del espacio de nombre de dominios sobre la que es responsable un servidor DNS, que puede tener autoridad sobre varias zonas. *(Por ejemplo: subdominio.depratti.ORG, subdominio.COM, etc.)[4]*

5) JERARQUÍA:

- **Root (Raíz):** El nivel más alto de la jerarquía de DNS es el servidor raíz, representado por un punto ".". Los servidores raíz son administrados por organizaciones como ICANN (Corporación de Internet para la Asignación de Nombres y Números) y contienen información sobre los servidores de nombres de dominio de nivel superior (TLD).
- **TLD (Dominio de nivel superior):** Los TLD son la siguiente capa en la jerarquía de DNS y se dividen en dos tipos principales: los TLD genéricos (gTLD) y los TLD de código de país (ccTLD). Los gTLD incluyen extensiones como .com, .org, .net, entre otros, mientras que los ccTLD representan códigos de país, como .us para Estados Unidos o .uk para Reino Unido.
- **SLD (Dominio de segundo nivel):** Los SLD se encuentran directamente debajo de los TLD y forman parte del nombre de dominio principal. Por ejemplo, en el dominio "example.com", "example" sería el SLD. Los SLD son registrados por los propietarios de los dominios y pueden representar marcas, organizaciones o cualquier otro identificador específico.
- **Subdominios:** Los subdominios son extensiones adicionales que se colocan delante del nombre de dominio principal y están separados por puntos. Por ejemplo, en "subdominio.example.com", "subdominio" sería el subdominio. Los subdominios permiten una mayor organización y subdivisión de los sitios web y servicios bajo un dominio principal.

Nota: Un nombre de dominio debe incluir todos los puntos. Tiene una longitud máxima de 255 caracteres y se escribe siempre de derecha a izquierda.[5]

6) SEGURIDAD:

La seguridad en DNS es un aspecto crítico para garantizar la confiabilidad y protección de los servicios de nombres de dominio. A continuación, se presentan algunas consideraciones clave sobre la seguridad en DNS:

1) **Transferencia segura de zona (TSIG):** TSIG es un mecanismo de autenticación y protección de la integridad de las transferencias de zona entre servidores DNS. Utiliza una clave compartida para verificar la autenticidad de las actualizaciones y asegurar que solo los servidores autorizados puedan realizar cambios en la zona DNS.
2) **Firma de zona (DNSSEC):** DNSSEC es una extensión de seguridad que permite la verificación de la autenticidad y la integridad de los datos DNS. Utiliza firmas criptográficas para firmar las respuestas DNS, lo que ayuda a prevenir ataques de envenenamiento de caché y suplantación de identidad.
3) **Prevención de envenenamiento de caché:** El envenenamiento de caché es un ataque en el que se falsifica la respuesta DNS para dirigir a los usuarios a sitios web maliciosos. Para prevenir esto, es importante implementar medidas como la validación DNSSEC, el uso de servidores DNS confiables y la configuración adecuada de la caché DNS.
4) **Monitoreo y registro de actividad DNS:** El monitoreo constante de la actividad DNS puede ayudar a identificar patrones anormales o ataques en curso. Mantener registros detallados de las consultas y respuestas DNS puede facilitar la detección de comportamientos sospechosos y respaldar las investigaciones forenses en caso de incidentes de seguridad.
5) **Protección contra ataques DDoS:** Los ataques de denegación de servicio distribuido (DDoS) pueden afectar la disponibilidad de los servidores DNS al inundarlos con tráfico malicioso. Es fundamental implementar medidas de mitigación de DDoS, como cortafuegos, equilibrio de carga y servicios de protección DDoS, para asegurar la continuidad del servicio.[6]

7) IMPORTANCIA:

1) **Resolución de nombres:** DNS se utiliza para convertir nombres de dominio legibles por humanos (como www.ejemplo.com) en direcciones IP numéricas (como 192.0.2.1) que las computadoras pueden entender. Permite tra-

ducir los nombres de dominio en direcciones IP para establecer conexiones y acceder a recursos en Internet.

2) **Jerarquía y distribución:** DNS utiliza una estructura jerárquica de servidores distribuidos en todo el mundo para gestionar y almacenar información de nombres de dominio. Esta distribución permite una resolución eficiente y confiable de los nombres de dominio, ya que los servidores DNS se encargan de resolver las consultas de manera descentralizada.
3) **Escalabilidad:** DNS es altamente escalable, lo que significa que puede manejar una gran cantidad de consultas simultáneas y crecientes sin degradar el rendimiento. Esto es esencial para soportar el vasto número de dispositivos conectados a Internet y el crecimiento constante de la red.
4) **Caché y aceleración:** Los servidores DNS pueden almacenar en caché las respuestas de consultas previas, lo que acelera las futuras consultas al evitar la necesidad de buscar la información nuevamente. Esta caché distribuida mejora la eficiencia y la velocidad de las resoluciones de DNS.
5) **Redundancia y disponibilidad:** DNS permite configurar múltiples servidores de nombres para un dominio, lo que proporciona redundancia y mayor disponibilidad. Si un servidor de nombres no está disponible, otros servidores pueden responder a las consultas, evitando interrupciones en el acceso a los recursos en línea.
6) **Gestión de correo electrónico:** DNS también juega un papel crucial en la gestión del correo electrónico al permitir la configuración de registros MX (Mail Exchanger), que especifican los servidores de correo electrónico responsables de recibir mensajes para un dominio específico.
7) **Seguridad y control de acceso:** DNS puede implementar medidas de seguridad, como el uso de registros DNSSEC (DNS Security Extensions), que proporcionan autenticidad e integridad a las respuestas de DNS. También se pueden utilizar registros DNS para controlar y redirigir el tráfico, como los registros SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail) para combatir el correo no deseado y el phishing.

III. Conclusiones

El Sistema de Nombres de Dominio (DNS) es una pieza fundamental de la infraestructura de Internet que permite la traducción de nombres de dominio legibles por humanos en direcciones IP numéricas utilizadas por las máquinas. Sin el DNS, sería difícil y poco práctico para los usuarios acceder a sitios web y servicios en línea utilizando direcciones IP numéricas.

La seguridad del DNS es de vital importancia para garantizar la disponibilidad y la confiabilidad de los servicios de nombres de dominio. La implementación de medidas como la autenticación y la integridad mediante DNSSEC, la protección contra ataques de envenenamiento de caché y la adopción de prácticas sólidas de seguridad son fundamentales para proteger la integridad y la privacidad de las consultas y respuestas DNS.

El DNS continúa evolucionando para adaptarse a los avances tecnológicos y los desafíos emergentes. Las mejoras en la privacidad, como el uso de DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT), y los esfuerzos para mejorar la eficiencia y la resiliencia del DNS, como la implementación de servidores DNS de alto rendimiento y la optimización de las consultas, están moldeando el futuro del DNS y mejorando la experiencia de los usuarios en Internet. Es importante estar al tanto de las últimas tendencias y desarrollos en el campo del DNS para garantizar su eficacia y seguridad en entornos de red.

References

[1] P. Mockapetris, *Domain names: Concepts and facilities*. SRI International, 1988.

[2] M. Liu, Z. Liu, H. Qian, and S. Li, "Security threats and solutions in dns: A survey," *Journal of Network and Computer Applications*, vol. 67, pp. 235–254, 2016.

[3] A. Gupta and S. Vasan, "Understanding the domain name system," *IEEE Potentials*, vol. 33, no. 5, pp. 23–28, 2014.

[4] R. Anderson, A. Blyth, M. Bond, A. Cheung, D. Clifford, D. Dittrich, Z. Durumeric, and et al., *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2008.

[5] P. Mockapetris, "Domain names-concepts and facilities," *RFC 882*, 1983, disponible en: https://tools.ietf.org/html/rfc882.

[6] ——, "Domain names-implementation and specification," *RFC 883*, 1984, disponible en: https://tools.ietf.org/html/rfc883.