**Alumnos: Joaquin Berzunces y Nahuel Gonzalez Aran**

**Trabajo Práctico Nº2**



# **Protocolo: DNS (Domain Name System)**

**¿Qué es el protocolo DNS?**

El DNS es un sistema de nomenclatura jerárquica descentralizado para dispositivos conectados a redes IP. Este sistema asocia información variada con nombres de dominio a cada uno de sus participantes.

**¿Cómo funciona?**

Los servidores DNS traducen request de nombres en direcciones IP, controlando que servidor el usuario final va a llegar cuando tipeen un nombre de dominio en su navegador

**¿Dónde se implementa?**

DNS se implementa en servidores que actúan como una base de datos jerárquica y distribuida para traducir nombres de dominio en direcciones IP. Los usuarios interactúan con el DNS principalmente mediante aplicaciones como navegadores web y clientes de correo electrónico

**¿Quien o quienes lo implementan?**

La Corporación de Internet para la Asignación de Nombres y Números (ICANN) es la responsable de la administración e implementación del protocolo DNS. Se asegura que cada nombre de dominio sea único y que todos los usuarios de internet puedan encontrar las direcciones válidas.

**¿En qué se diferencia de otros protocolos de red?**

DNS se diferencia de otros protocolos que se usan para administrar y distribuir dirección IP en redes como DHC). DHCP asigna las direcciones IP a las computadoras cliente., mientras que el servidor DNS las resuelve.

# **Historia:**

## **Orígenes del uso de nombres de host en ARPANET**

Durante los inicios de ARPANET, la identificación de computadoras no se hacía mediante direcciones numéricas, sino a través de nombres de host. Para facilitar esta tarea, se utilizaba un archivo llamado HOSTS.TXT, mantenido manualmente por el Instituto de Investigación de Stanford (SRI International).

## **El papel de Elizabeth Feinler y el SRI**

Elizabeth Feinler, quien dirigía el primer directorio de ARPANET desde el SRI, fue la principal responsable de la gestión del archivo HOSTS.TXT, junto con el Centro de Información de Red (NIC).

* Las asignaciones de nombres se realizaban de forma manual.
* Los administradores de red debían comunicarse telefónicamente con el NIC para registrar un nuevo nombre.

Feinler también tuvo un rol clave en:

* La creación del directorio WHOIS.
* La propuesta de dominios basados en la función o ubicación, como .edu para instituciones educativas.
* La administración del Registro de Nombres de Host entre 1972 y 1989.

## **Jon Postel y la Lista de Números Asignados**

En paralelo, Jon Postel, desde el Instituto de Ciencias de la Información (ISI) de la Universidad del Sur de California, era responsable de la Lista de Números Asignados (Assigned Numbers List). Colaboró estrechamente con el SRI en la gestión de recursos de red.

## **Surgimiento de DNS**

A principios de los años 80, el sistema manual y centralizado comenzó a volverse ineficiente, debido al crecimiento de la red. Como respuesta, se encargó a Paul Mockapetris el diseño de un sistema automatizado y más escalable.

* En 1983, Mockapetris propuso y desarrolló el Sistema de Nombres de Dominio (DNS) desde la Universidad del Sur de California.
* En noviembre de ese mismo año, el IETF publicó las especificaciones del protocolo en los documentos RFC 882 y RFC 883.
* Estas especificaciones fueron actualizadas en enero de 1986 mediante el RFC 973.

**¿Qué características tiene?**

Como DNS es una base de datos distribuida, es decir que está repartida entre muchos servidores diferentes, lo hace más resistente a los fallos que una base de datos centralizada.Significa que si un servidor se cae, se podrá acceder a los datos mediante otro sitio.

Otra característica del DNS es que está jerarquizado. En el nivel más alto están los dominios de nivel superior(TLD), como .com y .org. Debajo de estos están los dominios de segundo nivel, como [google.com](http://google.com) o [apple.com](http://apple.com). Por ultimo estan los de tercer nivel como [gmail.google.com](http://gmail.google.com)

# **Tipos de servidores DNS**

Hay 4 tipos de categorías de servidores DNS

* **DNS recursive resolver**: Actúa como intermediario entre el dispositivo y los otros 3 tipos de DNS nameserver. Estos nameserver contienen toda la información necesaria sobre los dominios online. Ni bien tipeas el nombre de dominio en el navegador, el DNS recursive resolver primero chequea la cache para saber si entraste previamente a ese sitio y, si lo hiciste, va a buscar la dirección IP del caché e instantáneamente conectarte al sitio web. Si es la primera vez que visitas el sitio web, el recursor DNS va a realizar distintas queries para obtener la dirección IP del dominio solicitado.
* **DNS root nameserver**: Es la primera parada que hace el DNS recursor en su búsqueda de la dirección IP del sitio web. El recursor envía una query al root server dándole el nombre de dominio y preguntando sobre el correcto TLD nameserver de ese dominio. El root nameserver examina la extensión de dominio e informa el DNS resolver cual TLD nameserver tiene que examinar para acercarse a la dirección IP del sitio web
* **TLD nameserver**: Mantienen la información acerca de los dominios con las mismas extensiones. “.com”, “.org”. Cada TLD nameserver es responsable de los sitios web con una extensión manual.
* **Autoritativos**: Es el servidor DNS final que contiene la información oficial y actualizada sobre el dominio. Una vez que el DNS resolver llega, el servidor responde con la dirección IP real del dominio solicitado. Guarda los registros DNS que indican cómo debe funcionar ese dominio. Sin este servidor, no se podría encontrar la dirección IP de un sitio, tiene la última palabra

# **Tipos de registros DNS**

Los registros DNS son un conjunto de instrucciones que se utilizan para conectar nombre de dominio con direcciones IP dentro de servidores DNS

**Registros A**

Los registros de direcciones, o registros A, son los registros DNS más utilizados. Crean una conexión directa entre una dirección IPv4 y un nombre de dominio. Las direcciones IPv4 tienen el siguiente formato: 93.184.216.34.

**Registros AAAA**

Al igual que los registros A, este tipo de registro conecta nombres de dominio con direcciones IPv6. Las direcciones IPv6 tienen más números que las direcciones IPv4 y se están volviendo más comunes a medida que se agotan las opciones para las direcciones IPv4.

**Registros CNAME**

Los registros de nombres canónicos, o registros CNAME, dirigen un dominio de alias a un dominio canónico. Esto significa que este tipo de registro se utiliza para vincular subdominios a

registros de dominio A o AAAA.  
Por ejemplo, en lugar de crear dos registros A para www.example.com y product.example.com, puede vincular product.example.com a un registro CNAME que luego se vincula a un registro A para example.com. El valor es que si la dirección IP cambia para el dominio raíz, solo se tendrá que actualizar el registro A y el CNAME se actualizará en consecuencia.

**Registros MX**

El intercambio de correo, o registros MX, dirige los correos electrónicos al servidor de correo de su dominio. Estos registros, junto con un servidor de correo electrónico, permiten la creación de cuentas de correo electrónico individuales, como user@example.com, que están vinculados al dominio.

**Registros NS**

Los registros de servidor de nombres, o NS, muestran qué servidor DNS actúa como servidor de nombres autorizado para su dominio. Los servidores de nombres autorizados contienen la información final sobre un dominio específico y su dirección IP correspondiente. Un registro NS apunta a todos los diferentes registros que contiene su dominio. Sin registros NS, los usuarios no podrán acceder a su sitio web.

**Registros SOA**

Los registros de inicio de autoridad, o registros SOA, almacenan información administrativa importante sobre un dominio. Esta información puede incluir la dirección de correo electrónico del administrador del dominio, información sobre las actualizaciones del dominio y cuándo un servidor debe actualizar su información.

**Registros PTR**

Los registros de puntero, o registros PTR, funcionan en la dirección opuesta a los registros A. Se utilizan para conectar una dirección IP con un nombre de dominio, en lugar de un nombre de dominio con una dirección IP. Cuando una búsqueda de DNS comienza con una dirección IP, encuentra el nombre de host correspondiente. Estos registros se utilizan para detectar spam comprobando si las direcciones IP y las direcciones de correo electrónico asociadas son utilizadas por servidores de correo electrónico legítimos. El host del servidor debe configurar los registros PTR.

**Registros TXT**

Los registros de texto, o TXT, almacenan información textual relacionada con dominios y subdominios. Los registros de texto permiten el almacenamiento de registros SPF y registros de verificación de correo electrónico. Los registros DKIM y DMARC, que se almacenan en los registros TXT, ayudan a los servidores de correo electrónico a confirmar que un mensaje proviene de una fuente fiable.

# **Problemas y ataques comunes**

Algunos de los problemas más comunes son:

1. **DNS\_PROBE\_FINISHED\_NXDOMAIN**  
 Causa:  
 El dominio no existe o hay una mala configuración en los ajustes de DNS.

2. **SERVFAIL (Fallo del Servidor)** Causa:  
 El servidor DNS no pudo completar la consulta.

3. **Error REFUSED (Rechazado)** Causa:  
 El servidor DNS se negó a procesar la consulta.

4. **Tiempos de Espera de DNS (DNS Timeouts)**  
 Causa:  
 La consulta DNS tardó demasiado en responder.

5. **Desajuste entre los Servidores DNS Primario y Secundario**  
 Causa:  
 El servidor secundario tiene archivos de zona desactualizados.

6. **Registros MX Incorrectos o Faltantes** Causa:  
 Los servidores de correo no están correctamente definidos en DNS.

7. **Fallos en la Búsqueda Inversa de DNS (Reverse DNS Lookup Failures)** Causa:  
 El registro PTR está faltando o mal configurado.

8. **Retrasos en la Propagación**  
 Causa:  
 Los cambios en DNS tardan tiempo en propagarse globalmente.

Secuestro de DNS

El secuestro de DNS implica la redirección no autorizada de consultas DNS a sitios malintencionados. Los atacantes manipulan los registros DNS para redirigir a los usuarios hacia sitios web fraudulentos, lo que puede llevar al robo de datos o a la propagación de malware. Esto puede ocurrir a través de varios métodos, como comprometer los servidores DNS, es decir el atacante logra **acceder o controlar el servidor DNS** de forma no autorizada o mediante «ataques de intermediario» en los que el atacante intercepta y modifica consultas DNS.

Ataque por inundación DNS

Un ataque por inundación DNS es un tipo de ataque de denegación de servicio en el que el atacante envía muchas solicitudes DNS a un servidor de destino con la intención de sobrecargarlo y provocar una denegación de servicio. Esto puede impedir que los usuarios legítimos tengan acceso a los servicios proporcionados por el servidor DNS de destino.

**¿Qué significan realmente siglas como ".com" o ".org"?**

Un dominio .com es una extensión de dominio de nivel superior(TLD) que se utiliza para sitios webs comerciales “com” significa “comercial”. “.org” también es un TLD pero al principio fue creado para que lo usen organizaciones sin fines de lucro, “org” significa “organización”, pero a día de hoy lo usan organizaciones de todo tipo como empresas, instituciones educativas, etc.

# **Implementación:**

Mostramos dos implementaciones que representan el funcionamiento y uso de un servidor DNS. La primera implementación: En Packet Tracer se hace la simulación de un servidor DNS. Se diseña utilizando un servidor configurado como DNS server, una PC conectada al mismo switch y un Switch para interconectar los dispositivos. Se simula como una PC dentro de una red local consulta a un servidor DNS para resolver un nombre de dominio y obtener la dirección IP correspondiente.

La segunda implementación: Código en python - Simulación de resolución DNS. Se desarrolló un script en Python que simula la resolución de nombres y direcciones IP usando herramientas como dnspython y subprocess.

**Funcionalidad:**

* La función resolver\_dominio() permite al usuario ingresar un dominio (por ejemplo, www.google.com) y devuelve su IP utilizando consultas tipo A.
* La función resolver\_ip() permite ingresar una dirección IP, realiza una consulta PTR para obtener el nombre de dominio asociado (resolución inversa) y ejecuta un nslookup para mostrar información adicional.
* Se usa subprocess para ejecutar el comando nslookup desde la consola y mostrar su salida en Python.

Esta implementación permite entender cómo funcionan las consultas DNS reales fuera de un entorno simulado. A diferencia de Packet Tracer, aquí las consultas se hacen contra servidores DNS públicos (como los de Google, Cloudflare, etc.) dependiendo de la configuración del sistema operativo.

**Bibliografía**

[**DNS: Definición, tipos y características**](https://informatecdigital.com/dns-definicion-tipos-y-caracteristicas/)

<https://informatecdigital.com/dns-definicion-tipos-y-caracteristicas/>

<https://www.defectodigital.com.mx/dns-explicado/>

<https://www.fs.com/es/blog/dhcp-and-dns-difference-2676.html>

<https://en.wikipedia.org/wiki/Domain_Name_System#>

<https://dnsspy.io/learning/dns-troubleshooting/common-dns-errors>

[DNS: Definición, tipos y características](https://informatecdigital.com/dns-definicion-tipos-y-caracteristicas/)

<https://www.dnspython.org/>

<https://www.nslookup.io/>

<https://docs.python.org/es/3.13/library/subprocess.html>