Servidor DNS

Proyecto 2 - Segunda Entrega

Juan C. Chafloque Mesia
Ingeniería de Sistemas
Pontificia Universidad Javeriana
Bogotá, Colombia
juanchafloque@javeriana.edu.co

Julio Andrés Mejía Vera
Ingeniería de Sistemas
Pontificia Universidad Javeriana
Bogotá, Colombia
julio.mejia@javeriana.edu.co

Sergio Posada Henao
Ingeniería de Sistemas
Pontificia Universidad Javeriana
Bogotá, Colombia
sergio_posada@javeriana.edu.co

***Abstract*— When you want to access a web page on the Internet you need the IP address of the server where it is stored, but, as a rule, the user only knows the domain name. The reason is none other than the difficulty of remembering the numerical series of the type 93.184.216.34 that compose them, which are precisely those that constitute the basis of communication on the Internet.**

***Keywords*— IP address, domain, user, Internet, Communication, server.**

DNS

El Sistema de Nombres de dominio DNS (Domain Name Space) es un sistema de nomenclatura el cual se ocupa de administrar el espacio de nombres de dominio. Su tarea principal consiste en resolver las peticiones de asignación de nombres. Cada vez que un usuario registra un dominio, se crea una entrada en el registro correspondiente y esta queda almacenada como un "resource record". La base de datos de un servidor DNS se convierte en la compilación de de todos los registros de la zona del espacio de nombres de dominio que se gestiona.

PETICIONES DNS

Cuando se introduce la dirección de una página web (URL) en el campo de búsqueda del navegador, éste realiza una petición al resolver, un componente especial del sistema operativo cuya función se basa en almacenar en caché direcciones IP ya solicitadas anteriormente y proporcionarles cuando la aplicación cliente lo solicita.

Si un servidor DNS no puede responder a una petición con la información que se dispone en su base de datos, puede solicitar la información a otro servidor o reenviar la petición al servidor DNS que corresponda. Esta resolución se puede lograr de 2 formas:

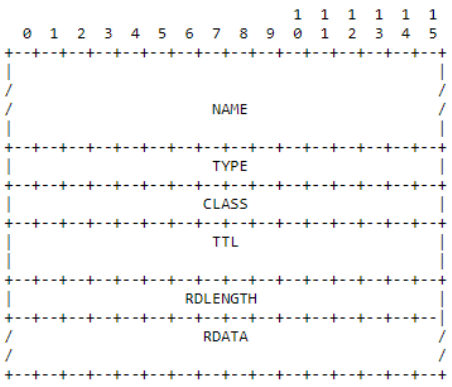
- **Resolución Recursiva**: Es la que se produce cuando el servidor DNS no puede responder por sí mismo a una petición y toma la información de otro servidor. El resolver transfiere la petición completa a su servidor DNS, que proporciona a su vez la respuesta al resolver con el nombre de dominio, si se ha resuelto.

- **Resolución Iterativa**: Cuando el servidor DNS no puede resolver la petición, envía como respuesta la dirección del siguiente servidor DNS de la jerarquía. El resolver tiene que enviar él mismo una nueva petición y repetir la maniobra hasta que se resuelve el nombre de dominio.

Según el RFC 1035 todas las comunicaciones dentro del protocolo de dominio se llevan a cabo en un solo formato llamado mensaje. El formato de mensaje está dividido en 5 secciones que se muestran a continuación:

```
+---------------------+
|        Header       |
+---------------------+
|       Question      | the question for the name server
+---------------------+
|        Answer       | RRs answering the question
+---------------------+
|      Authority      | RRs pointing toward an authority
+---------------------+
|      Additional     | RRs holding additional information
+---------------------+
```

En la mayoría de los casos de prueba, los campos de "authority" y "additional" estaban vacios. El paquete de "answers" siguió el estándar del RFC 1035 y se implementó con la siguiente estructura:



En donde el “name” es el nombre del dueño de la petición, el “type” son dos octetos que contienen el tipo de RR que en este caso es tipo A (Toma el valor de 1 e indica que es una dirección IP de host), el “class” son dos octetos que contienen la clase del RR que en este caso es IN (Internet), el “ttl” son 32 bits que muestran el time to live y por último el “rdlength” que es la longitud de toda la trama de respuesta.

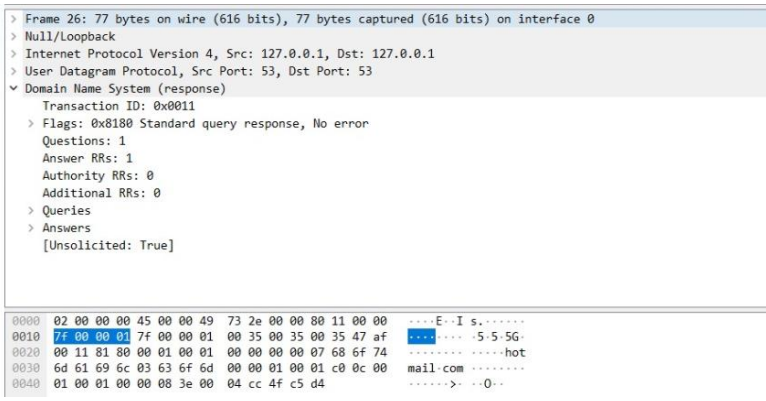
SERVIDOR DNS

Un servidor DNS consiste en un software para servidores que recurre a la base de datos de un DNS para responder a las peticiones que guardan relación con el espacio de nombres de dominio. Como, por regla general, se alojan en hosts dedicados. Hay una diferenciación entre servidores DNS primarios y secundarios:

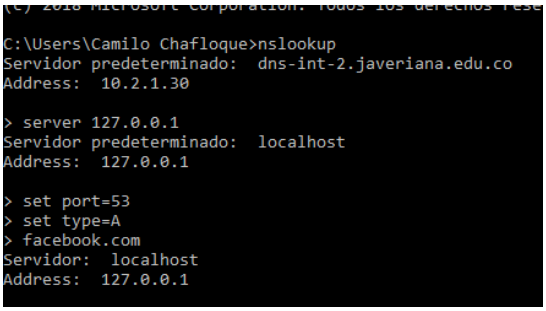
- **Servidor Maestro:** Toma esta denominación cuando guarda la información sobre una zona determinada del espacio de nombres de dominio en su propia base de datos. El sistema de nombres de dominio está construido de tal forma que cada zona dispone de un servidor de nombres primario.
-
- **Servidor Secundario:** cuando la información de un servidor de nombres no procede de los archivos de zona propios, sino que son de segunda o de tercera mano, este servidor se convierte en secundario o esclavo para esta información. Esta situación se produce cuando un servidor no puede resolver una petición con su propia base de datos y ha de recurrir a la información disponible en otro servidor de nombres.

ESCENARIO DE PRUEBAS

Para los escenarios de pruebas se utilizaron los computadores de los estudiantes de grupo. Se tuvieron inconvenientes a la hora de devolver el paquete con las respuestas de las peticiones de los usuarios debido a que en Wireshark aparecía el mensaje “Unsolicited: True”. Al investigar esto en el RFC, se vio que era un problema de seguridad y el computador del cliente rechazaba la llegada del paquete ya que este piensa que el paquete es maligno y no es seguro. Dado este inconveniente, el paquete con la información requerida por el cliente se mostró en la consola del servidor para que se vea que el paquete tenía en verdad lo que pedía el cliente.



Se realizaron pruebas para los dos casos posibles. El primer caso fue que el cliente enviará una petición para un dominio que se encontrará en el Master File del servidor interno. El segundo caso fue que el cliente enviará un dominio que no se encontrará en el Master File interno y el servidor tuviera que acudir al servidor de Google para recuperar la información requerida.



La imagen anterior muestran los datos de entrada que se tienen que hacer en la consola del computador “cliente” para poder realizar las peticiones al servidor DNS implementado.

- Caso 1:

Para el primer caso se utilizó el dominio yahoo.com que se encontraba en el Mater File interno. Al correr el servidor, este entra en un loop infinito en espera de que algún cliente realice una petición al DNS. Una vez este la hace, se verifica que el dominio solicitado se encuentre en el Master File interno. En caso de que este si lo tenga, se creará el paquete según el RFC 1035

y se le enviará al cliente las respectivas respuestas. Como en este caso, el dominio si se encuentra dentro del Master File, se retorna el paquete con la información que tiene el servidor DNS implementado.

```
Datagrama recibido del host: /127.0.0.1 desde el puerto remoto: 56366
**********Domain: yahoo.com
Se encontró el dominio en el MasterFile Interno
Transaction ID: 0x5
Flags: 0x8180
Questions: 0x1
Cantidad de respuestas: 6
Authority RRs: 0x0
Additional RRs: 0x0
Record: yahoo
Record: com

********** Answer 1 **********
Name: 7961
Record Type: 0x494e
Class: 0x1
TTL: 0x557
Len: 0x4
Address: 72.30.35.9
**********End of Package**********
```

- Caso 2:

Para el segundo caso se utilizó el dominio hotmail.com que no se encontraba en el Mater File interno. Al correr el servidor, este entra en un loop infinito en espera de que algún cliente realice una petición al DNS. Una vez este la hace, se verifica que el dominio solicitado se encuentre en el Master File interno. En caso de que este si lo tenga, se creará el paquete según el RFC 1035 y se le enviará al cliente las respectivas respuestas. Como este no es el caso, el servidor implementado tiene que recurrir a un servidor DNS externo, que para el caso de este proyecto es el servidor DNS de google (8.8.8.8). Para esto, el servidor interno arma la trama según el RFC, se la envía al servidor de Google y luego recibe un paquete de respuesta para que esta sea enviada al cliente.

```
Datagrama recibido del host: /127.0.0.1 desde el puerto remoto: 58191
**********Domain: hotmail.com
Se encontró el dominio en el MasterFile Externo
Transaction ID: 0x11
Flags: 0x8180
Questions: 0x1
Cantidad de respuestas: 1
Authority RRs: 0x0
Additional RRs: 0x0
Record: hotmail
Record: com

********** Answer 1 **********
Name: c00c
Record Type: 0x1
Class: 0x1
TTL: 0x83e
Len: 0x4
Address: 204.79.197.212
**********End of Package**********
```

REFERENCIAS

[1] P. Mockapetris “RFC 1035 - Domain names - Implementation and Specification” Network working group 1997. [Online]. Disponible en https://www.ietf.org/rfc/rfc1035.txt. [Revisado el 15-Nov-2019].