DNS

Domain Name System

Integrantes:

Gian Franco Fioriello,

Octavio Gonzalez,

Román Rizzi.

Sumario

DNS - Motivación

El concepto de DNS surge de la necesidad de renombrar los sitios web, generando así nombres más fáciles de recordar.

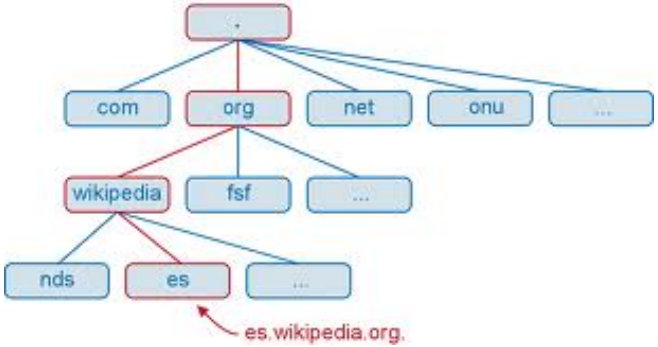
- Direcciones de hosts mnemotécnicas.
- Base de datos distribuida.
- Esquema de nombres jerárquico basado en dominios.

Qué es DNS?

DNS es un sistema de nombres de dominio. Esto se logra mediante la aplicaciòn de una base de datos distribuida y jeràrquica, que almacena informaciòn asociada a nombres de dominio, en redes como Internet.

Se encarga de traducir nombres inteligibles de dominio a identificadores binarios asociados con los equipos conectados a la red, con el propósito de poder localizar y direccionar estos equipos mundialmente.

Qué es DNS?



La organización jerárquica de dominios puede ilustrarse en forma de diagrama de árbol; de arriba hacia abajo, los dominios van haciéndose más específicos. En el ejemplo vemos como, si recorremos el diagrama en sentido inverso (de abajo hacia arriba), pueden leerse algunos nombres de dominio (en el ejemplo, es.wikipedia.org).

Para qué sirve DNS?

- Principalmente se encarga de traducir nombres de hosts a direcciones IP.

  (HTTP, SMTP y FTP emplean DNS.)

Ejemplo

Un cliente HTTP, que se ejecuta en un determinado host de usuario, solicita el URL www.unq.edu.ar.
Para que el host del usuario pueda enviar un mensaje de solicitud HTTP al servidor web www.unq.edu.ar, el host del usuario debe obtener en primer lugar la dirección IP de www.unq.edu.ar.

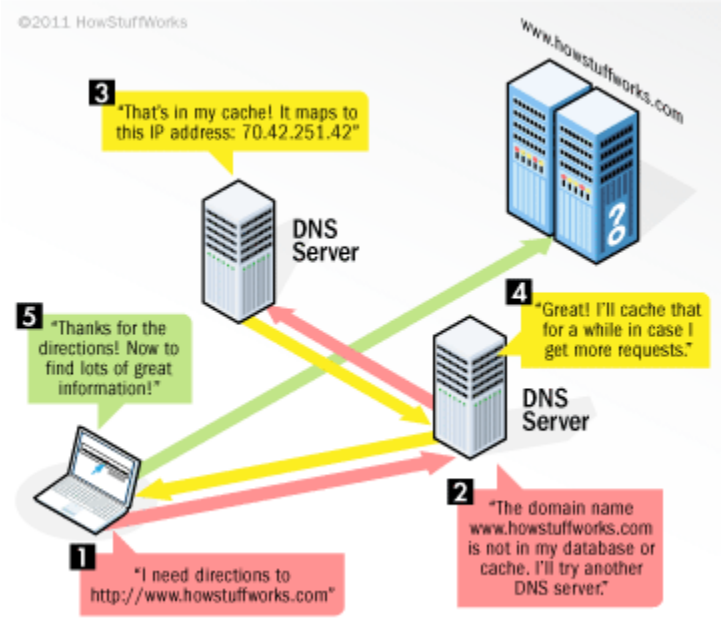
Esto se hace del siguiente modo:

Ejemplo

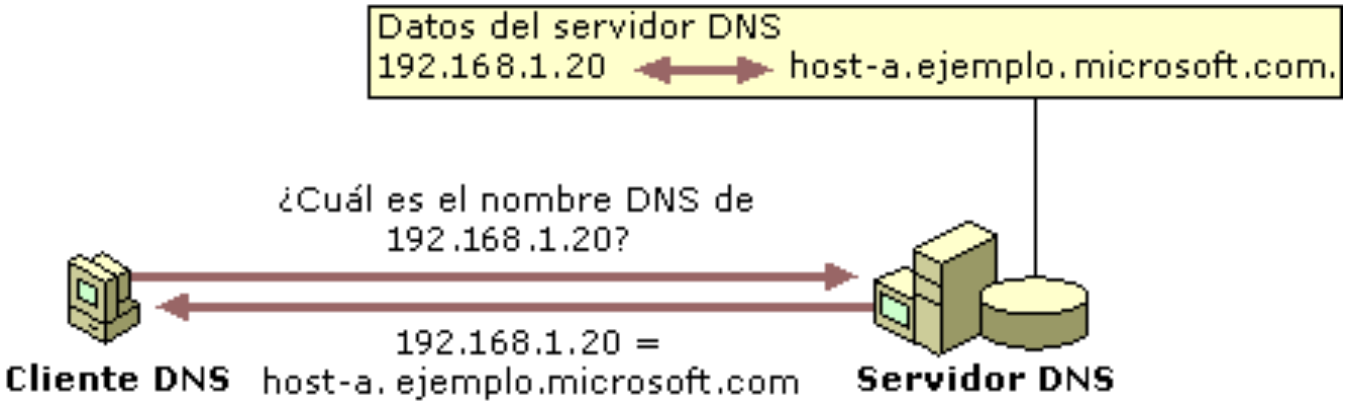
1. La propia máquina cliente ejecuta el lado del cliente de la aplicación DNS.
2. El navegador extrae el nombre de host, www.unq.edu.ar, del URL y pasa el nombre de host al lado del cliente de la aplicación DNS.
3. El cliente DNS envía una consulta que contiene el nombre de host a un servidor DNS.
4. El cliente DNS recibe finalmente una respuesta, que incluye la dirección IP correspondiente al nombre del host.
5. Una vez que el navegador recibe la dirección IP del servidor DNS, puede iniciar una conexión TCP con el proceso servidor HTTP localizado en el puerto 80 en esa dirección.

Para qué sirve DNS?

Ejemplo de funcionamiento de DNS



Ejemplo



Ejemplo de una petición inversa. Dada la dirección IP, se busca el nombre de dominio asociado a dicha dirección.

Para qué más sirve DNS?

- Además de la traducción de nombres de host a direcciones IP, DNS aporta otros servicios:
  - Alias de host,
  - Alias del servidor de correo,
  - Distribución de carga.

Alias de host

- Existen direcciones de host llamadas *canónicas* que tienen la particularidad de tener uno o más alias.

  Una aplicación puede invocar DNS para obtener el nombre de host canónico para un determinado alias, así como la dirección IP del host.

Ejemplo

Nombre canónico: *www.facebook.com*

Alias: *facebook.com* y *fb.com*.

Alias de servidor de correo

- Al igual que antes, los servidores de correo también tienen direcciones canónicas y alias.
- Una aplicación de correo puede invocar al servicio DNS para obtener el nombre de host canónico para un determinado alias, así como la dirección IP del host.

Ejemplo

Fulano De Tal podría tener una cuenta en hotmail como fulanitoDeTal@hotmail.com.

Sin embargo, el nombre de host del servidor de correo de Hotmail es más complicado y mucho menos mnemotécnico que simplemente hotmail.com (por ejemplo, el nombre canónico podría ser algo parecido a *relayl.west-coast.hotmail.com*).

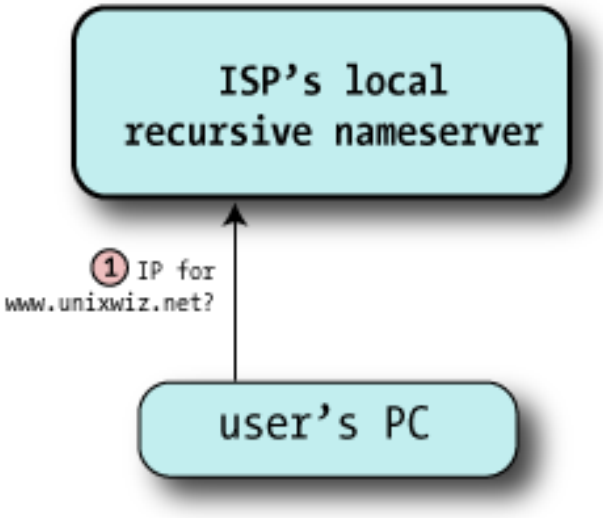
Distribución de carga

Al haber servidores replicados de algunas aplicaciones web (google.com o cnn.com), DNS se encarga de mostrar todas las direcciones IP asociadas a esta dirección de host, pero rotándolas.

Esto provoca que cada vez se realiza una solicitud de conexión, el servidor DNS entrega una dirección IP diferente, dentro de las existentes para la aplicación solicitada.

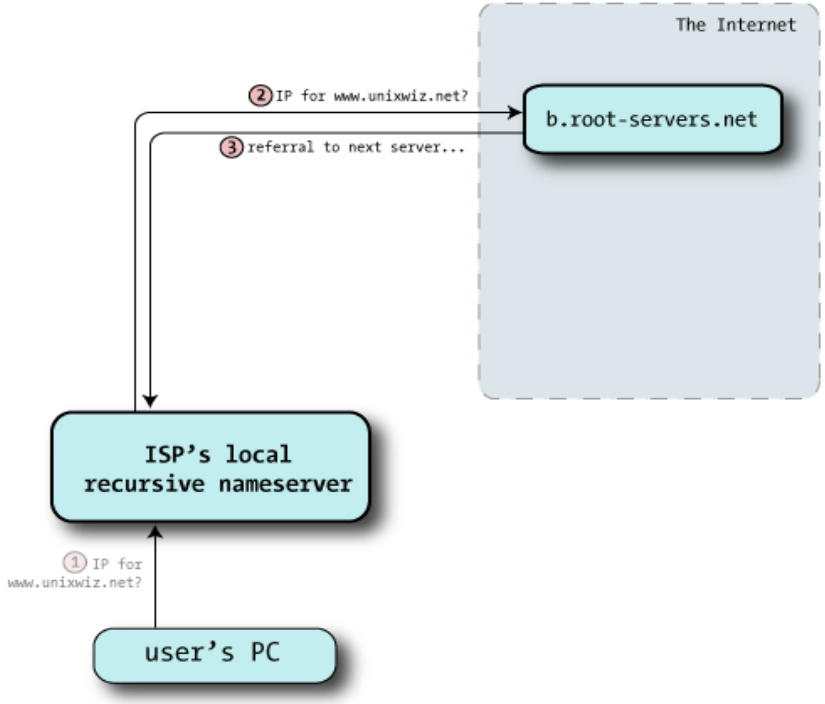
Ejemplo de una petición

En primera instancia, nuestro usuario pregunta por la ip de la página web al servidor DNS de nuestro proveedor de internet



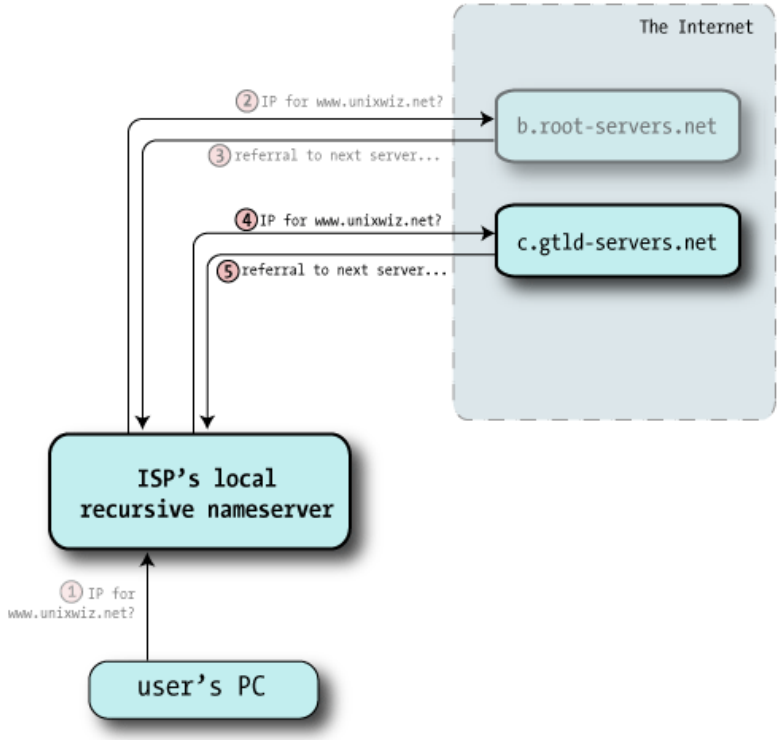
Ejemplo de una petición

Como este servidor no tiene la capacidad de responder a esta petición por su cuenta , delega en uno de los servidores maestros de los cuales tiene conocimiento.



Ejemplo de una petición

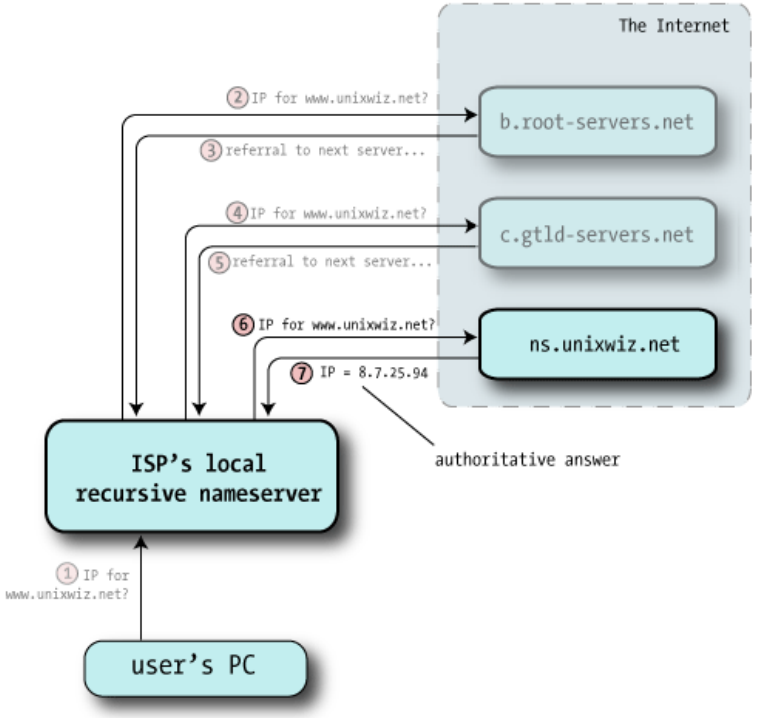
Nuevamente el servidor maestro nos deriva hacia otro servidor encargado de los dominios .net (el nivel más alto en la jerarquía)



Ejemplo de una petición

Este último servidor nos indico la dirección del servidor de dominio al que dirigirnos con el fin de conseguir nuestra dirección.

El flag de “Authoritative answer” nos indica que es la información deseada y no hace falta seguir buscando.

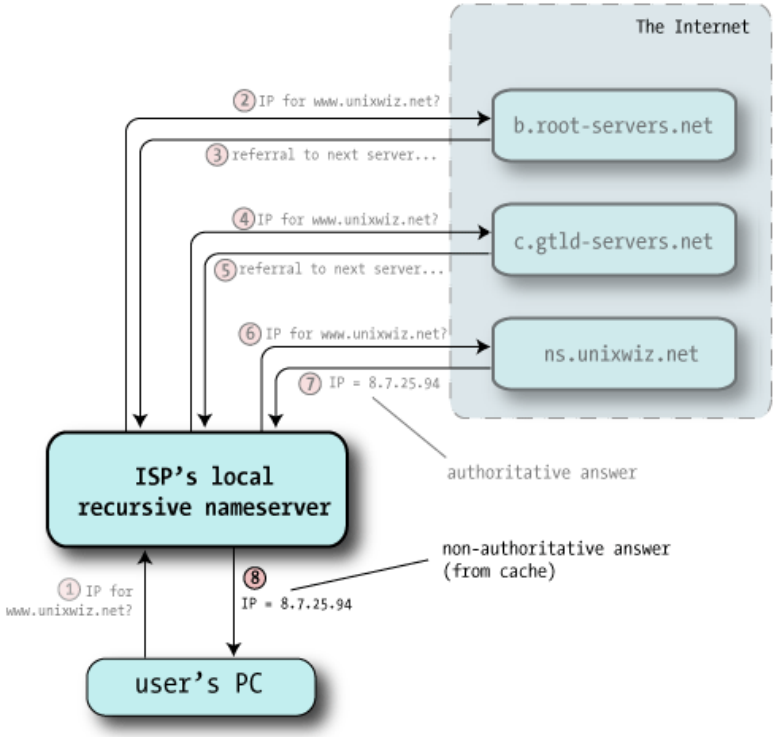


Ejemplo de una petición

Una vez el servidor encontró la información, procede a entregarlo al usuario.

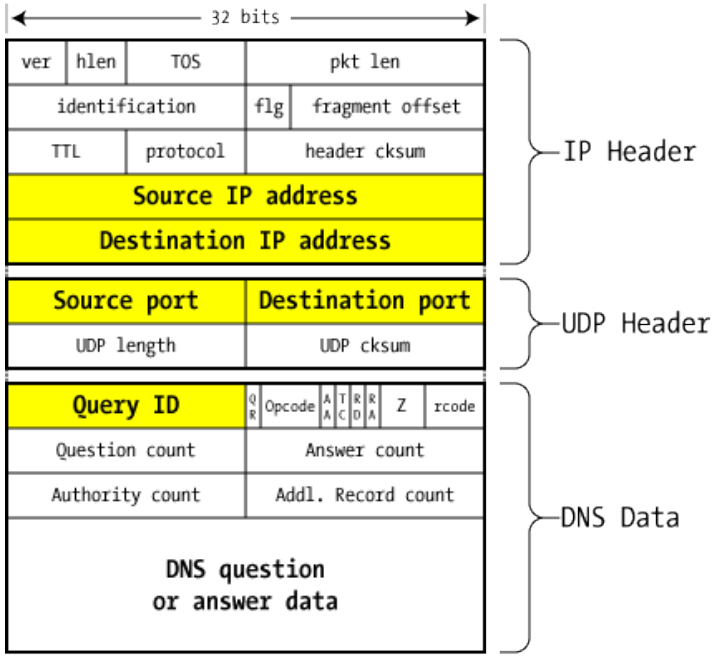
Es importante remarcar que el flag es diferente ya que el servidor ISP no es el que contiene la información sino quien la está comunicando.

El servidor la almacena en su caché para agilizar las peticiones al sitio durante cierto tiempo.



¿Como esta conformado un paquete DNS?

El paquete DNS esta conformado como se muestra en la siguiente imagen, encapsulado con las respectivas capas.



DNS packet on the wire

Memoria caché

Por una cuestión de performance, el servidor guarda en memoria las direcciones ip que buscó debido a las peticiones, disponibles para todos los usuarios que acceden a ese servidor.

Los elementos en la caché tienen un tiempo indicado por el servidor de donde viene la información(TTL), evitando que queden elementos obsoletos y erróneos.

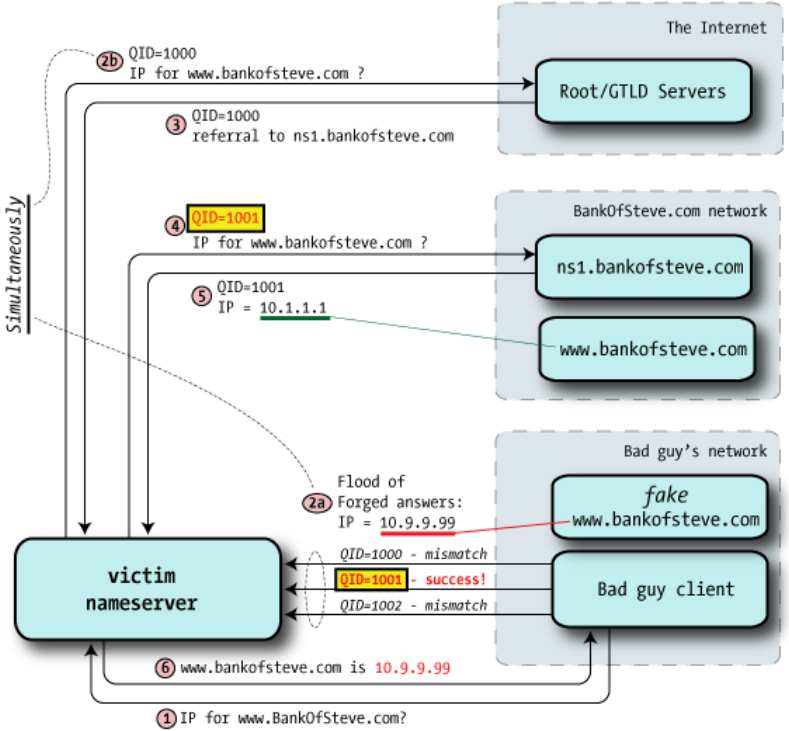
Envenenamiento de caché

Es una vulnerabilidad que busca inyectar información modificada en la caché local del servidor DNS.

Si se consigue explotar esta vulnerabilidad puede lograrse que los usuarios ingresen a la ip deseada por el atacante sin sospecharlo.

Envenenamiento de caché

El ataque consiste en enviar paquetes que cumplan con los requisitos (en este caso, la QueryID) para que el servidor lo tome como una respuesta válida y se pueda alterar la información que esperábamos recibir.



Envenenamiento de caché

Solución a esta vulnerabilidad

La estrategia utilizada para mitigar esta vulnerabilidad es la de randomizar los puertos que vamos a utilizar para establecer nuestra comunicación.

Los servidores DNS de Microsoft traen preestablecidos 2500 puertos udp para ser utilizados por querys aleatorias, si redondeamos el número a 2048, tenemos la siguiente ecuación (número de combinaciones posibles teniendo en cuenta los 16 bits de Query ID).