

TECNOLOGIA WEB

DNS

DNS – DOMAIN NAME SYSTEM

- DEFINICION

- Es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa.
- Aunque Internet sólo funciona en base a direcciones IP, el DNS permite que los humanos usemos nombres de dominio que son bastante más simples de recordar
- Los equipos que ejecutan DNS son llamados servidores de nombres

DNS

- El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.
- Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio

COMPONENTES DNS

- Para la operación práctica del sistema DNS se utilizan tres componentes principales:
 - Los Clientes fase 1: 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?);
 - Los 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.
 - Y las Zonas de autoridad, porciones del espacio de nombres raros de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad

TERMINOS UTILIZADOS

- Zona
 - Conjunto de dominios y subdominios que son administrados por el servidor DNS, es un concepto distinto al de dominio
- Servidor de nombre (Name Server)
 - Responsable de dar respuesta a las peticiones DNS, tales como “cual es la dirección IP para el nombre de dominio `www.xxxxx.com`?” y del mismo modo responde a peticiones DNS tales como “cual es el nombre de dominio para la dirección IP `XXX.XXX.XXX.XXX`”

TERMINOS UTILIZADOS

- Servidor de nombre autoritativo
 - Es el servidor de nombres que provee la respuesta de resolución de nombre desde su base local. Esta respuesta se llama respuesta autoritativa.
- Servidor de nombre (Name Server)
 - Responsable de dar respuesta a las peticiones DNS, tales como “cual es la dirección IP para el nombre de dominio `www.xxxxx.com`?” y del mismo modo responde a peticiones DNS tales como “cual es el nombre de dominio para la dirección IP `XXX.XXX.XXX.XXX`”

TIPOS DE REGISTROS DNS

- A = Address – (Dirección) Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.
- AAAA = Address – (Dirección) Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.
- CNAME = Canonical Name – (Nombre Canónico) Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como ftp y servidor web) en un servidor con una sola dirección ip. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). esto también es usado cuando corren múltiples servidores http, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real. Ej. Ejemplo1 IN CNAME ejemplo2
- NS = Name Server – (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.

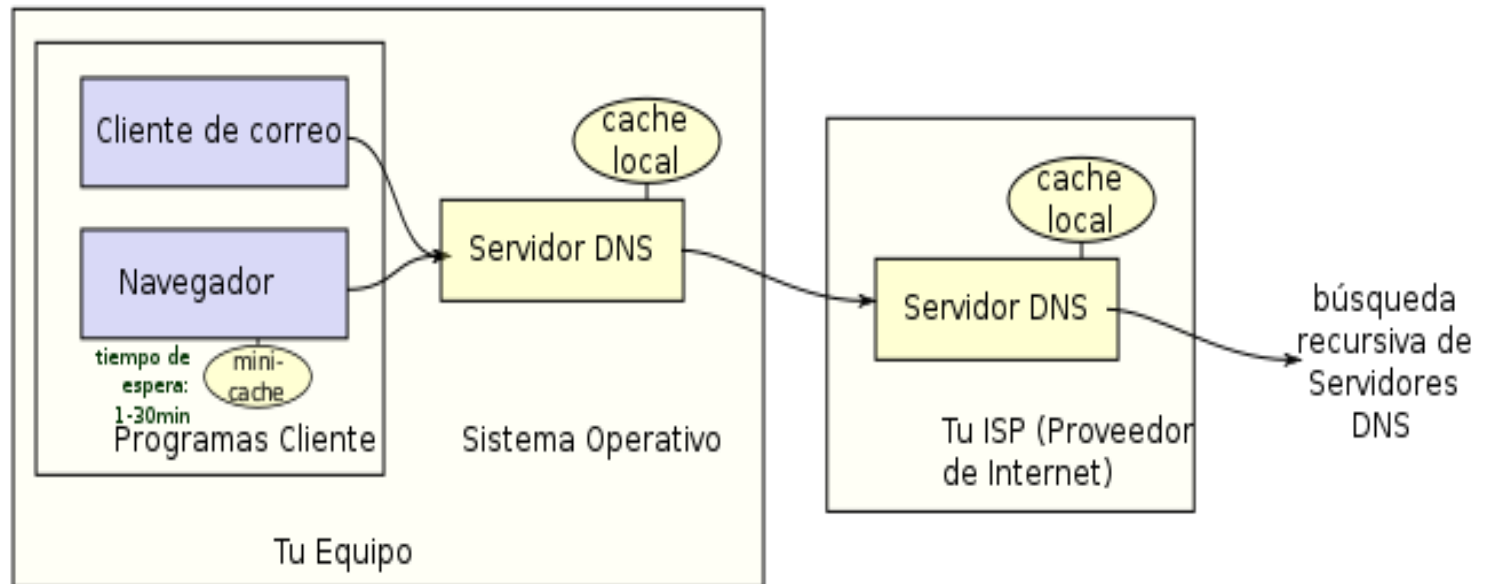
TIPOS DE REGISTROS DNS

- MX (registro) = Mail Exchange – (Registro de Intercambio de Correo)
Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
- PTR = Pointer – (Indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración del Dns reversiva.
- SOA = Start of authority – (Autoridad de la zona) Proporciona información sobre el servidor DNS primario de la zona.
- HINFO = Host INFOrmation – (Información del sistema informático)
Descripción del host, permite que la gente conozca el tipo de máquina y sistema operativo al que corresponde un dominio.
- TXT = TeXT - (Información textual) Permite a los dominios identificarse de modos arbitrarios.
- LOC = LOCalización - Permite indicar las coordenadas del dominio.

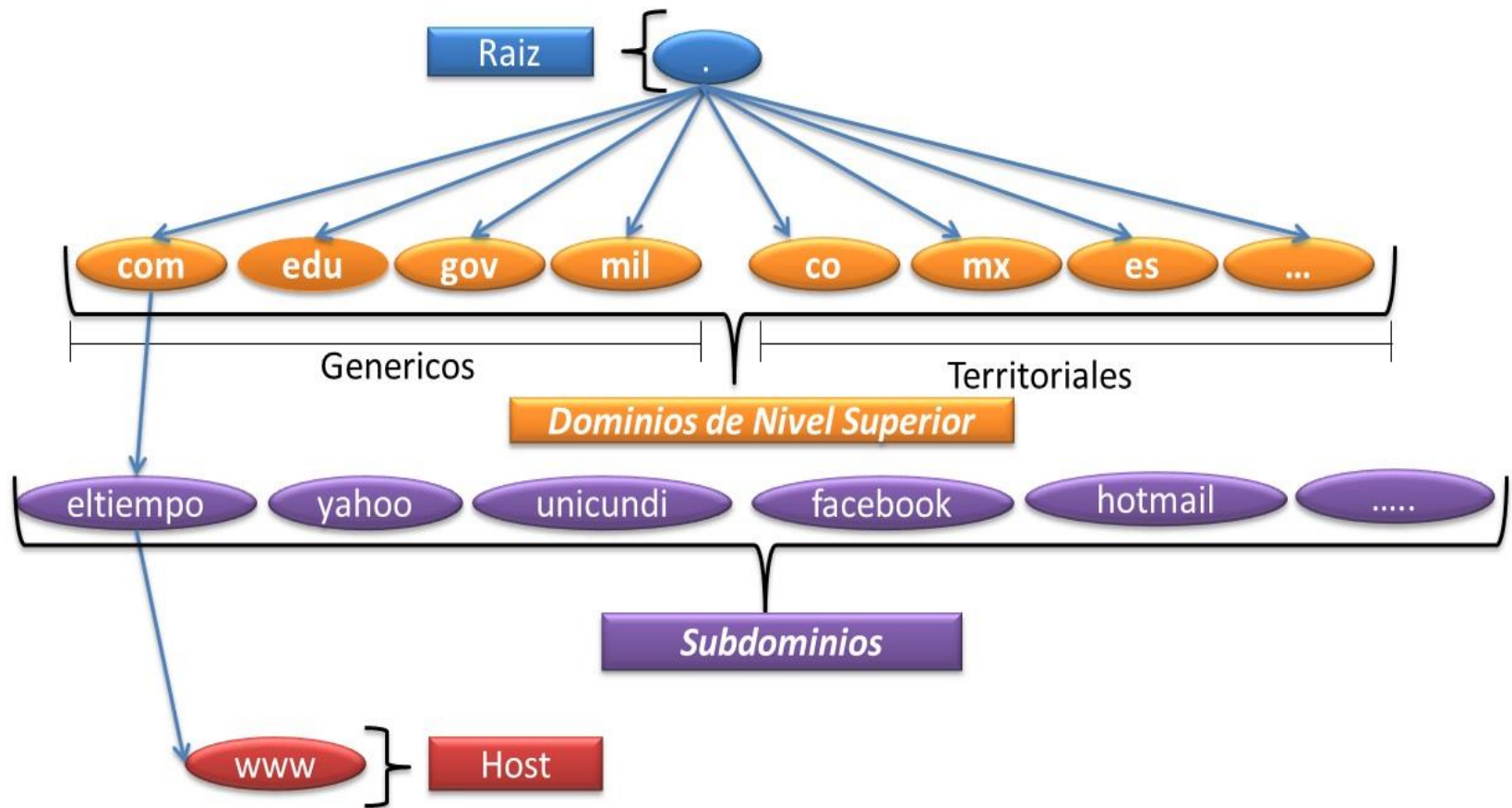
TIPOS DE REGISTROS DNS

- WKS - Generalización del registro MX para indicar los servicios que ofrece el dominio. Obsoleto en favor de SRV.
- SRV = SeRVicios - Permite indicar los servicios que ofrece el dominio. RFC 2782. Excepto Mx y Ns. Hay que incorporar el nombre del servicio, protocolo, dominio completo, prioridad del servicio, peso, puerto y el equipo completo. Esta es la sintaxis correspondiente.

DNS – COMO FUNCIONA



DNS - JERARQUIA



TIPOS DE SERVIDORES DNS

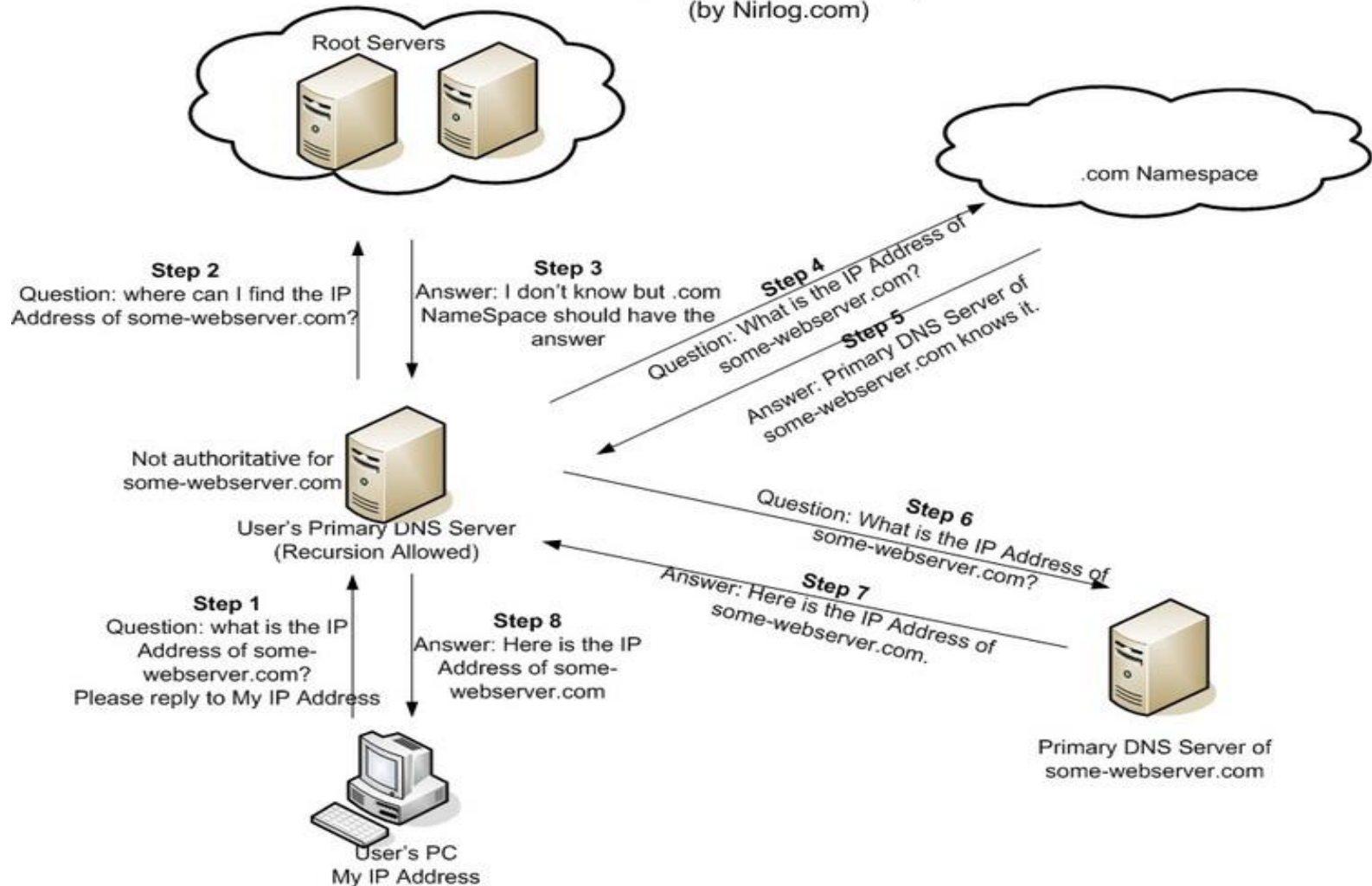
- Primarios o maestros: Guardan los datos de un espacio de nombres en sus ficheros
- Secundarios o esclavos: Obtienen los datos de los servidores primarios a través de una transferencia de zona.
- Locales o caché: Funcionan con el mismo software, pero no contienen la base de datos para la resolución de nombres. Cuando se les realiza una consulta, estos a su vez consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre

TIPOS DE RESOLUCIONES DE NOMBRE

- RESOLUCION ITERATIVA
 - Respuesta completa que el servidor de nombres pueda dar, consultando sus datos locales.
- RESOLUCION RECURSIVA
 - El servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta

DNS - BUSQUEDA RECURSIVA

DNS Query (Recursive)
(by Nirlog.com)



CONFIGURACION DNS BASICA EN UBUNTU

- `sudo apt-get install bind9 dnsutils`
- Sacar backup de `named.conf.local` que está en el directorio `/etc/bind`.
- Agregar la configuración para una nueva zona (directa y para la inversa) en el archivo `named.conf.local`. El contenido podría ser:

```
//Directa para home.com.bo
```

```
zone "home.com.bo" {  
    type master;  
    file "db.home.com.bo";  
};
```

```
//inversa para home.com.bo
```

```
zone "137.168.192.in-addr.arpa" {  
    type master;  
    file "db.192.168.137";  
};
```

CONFIGURACION DNS BASICA EN UBUNTU

- Verificar que lo que se hizo está bien ejecutando el comando:
 - `sudo named-checkconf`
- Crear el archivo para la resolución directa en el directorio `/var/cache/bind`. Se puede usar como base `db.local`
 - `sudo cp /etc/bind/db.local /var/cache/bind/db.home.com.bo`

CONFIGURACION DNS BASICA EN UBUNTU

- Editar el archivo cambiando localhost por el nombre del dominio y agregando los registros que se necesiten

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@          IN      SOA      dns.home.com.bo. root.home.com.bo. (
                                2013030601          ; Serial
                                6H                   ; Refresh
                                1H                   ; Retry
                                2W                   ; Expire
                                3H )                ; Negative Cache TTL
;
@          IN      NS       dns.home.com.bo.
@          IN      MX       10      mail
@          IN      A        192.168.137.10
dns        IN      A        192.168.137.10
cliente    IN      A        192.168.137.129
server01   IN      CNAME    dns
mail       IN      A        192.168.137.10
```

CONFIGURACION DNS BASICA EN UBUNTU

- Verificar el archivo de zona con el comando:
 - `named-checkzone home.com.bo /var/cache/bind/db.home.com.bo`
- Crear el archivo para la resolución inversa de la zona. Se puede tomar como base db.127:
 - `sudo cp /etc/bind/db.127 /var/cache/bind/db.192.168.137`

CONFIGURACION DNS BASICA EN UBUNTU

- Modificar localhost por el nombre del dominio y agregar los registros de resolución inversa necesarios:

```
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      dns.home.com.bo. root.home.com.bo. (
                        2013030601          ; Serial
                        6H                   ; Refresh
                        1H                   ; Retry
                        2W                   ; Expire
                        3H )                 ; Negative Cache TTL

;
@         IN      NS       dns.home.com.bo.
10        IN      PTR      dns.home.com.bo.
129       IN      PTR      cliente.home.com.bo.
```

CONFIGURACION DNS BASICA EN UBUNTU

- Se puede verificar el archivo de zona con el siguiente comando:
 - `sudo named-checkzone 137.168.192.in-addr.arpa /var/cache/bind/db.192.168.137`
- Reiniciar servicio bind
 - `sudo service bind9 restart`
- Testear: Usar nslookup, ping, etc.