DNS

Domain Name Server

Servidor de Nombres de Dominio

Términos que se usan en un DNS:

Servidores de DNS . Estos pueden ser *primarios* o *secundarios*. Un servidor primario es aquél que puede modificar la información en la base de datosa. Un solo servidor de DNS puede contener múltiples zonas primarias y secundarias.

Clientes . Cualquier máquina que hace una consulta a un servidor de DNS. El cliente puede o no puede estar registrado en una base de datos de un servidor de nombres. El cliente realiza la requiza al DNS a través de procesos llamados *resolvedores*.

El Servidor de Nombres de Dominio: es una base de datos distribuida jerárquicamente.

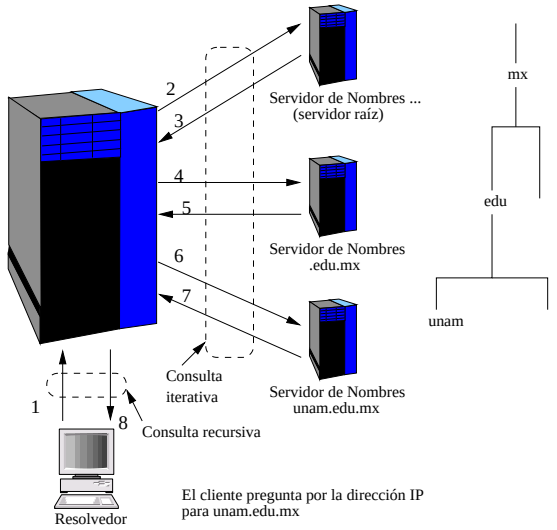
Por su funcionamiento, es un conjunto de protocolos que definen lo siguiente:

- Un mecanismo para consulta y puesta al día de información de direcciones en la base de datos.
- Un mecanismo para replicar la información en la base de datos entre servidores.

Resolvedores . Manejan el proceso de mapear un nombre simbólico a una dirección de red actual. El resolvedor (que puede recidir en otra máquina) realiza consultas a servidores de nombres. Cuando resuelve la informaciñon desde un servidor de nombres, este cachea (guarda) esa información localmente para el caso de que la misma información sea requerida de nuevo.

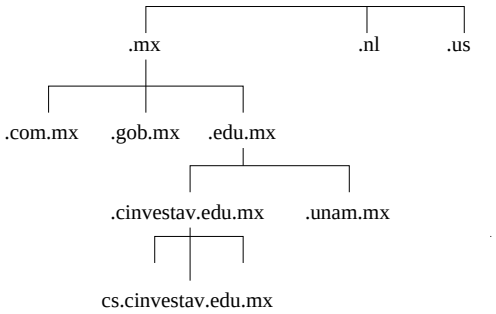
Consultas (a un servidor de DNS) pueden ser *recursivas* e *iterativas*.

Servidores raíz . Cuando un servidor de DNS procesa una consulta recursiva y esta consulta no puede ser resuelta a partir de los archivos de zona locales, la consulta debe ser escalada a un servidor DNS raíz. El servidor raíz es responsable de retornar una respuesta autoritativa para un dominio en particular o una referencia a un servidor que pueda proporcionar una respuesta autoritativa. Se puede configurar un servidor de DNS para contener su propia zona raíz, esto permite que el servidor no sea capaz de contestar consultas para nombres fuera de nuestra red.



Estructura del DNS

El Sistema de Nombres de Dominio es una base de datos jerárgica y distribuida. Estos datos incluyen nombres de hosts y nombres de dominios. Los nombres en la base de datos del DNS forman una estructura de datos jerárgica llamada el *espacio de nombres de dominio*.



De la figura anterior:

- En el paso 1 existe una consulta recursiva para unam.edu.mx, buscando for un registro de recursos tipo 'A' (A RR)
- Se nota también que sigue la consulta iterativa para unam.edu.mx al servidor de nombres raíz in los pasos 2 y 3.
- Hay la referencia para el servidor de nombre .mx (NS RRs, para mx); por simplicidad se han omitado la consulta iterativa A por el servidor DNS (a la izquierda) para resolver la dirección IP de los nombres de host de los servidores de nombres retornados por otros servidores DNS. Esto se muestra en los pasos 4 y 5.
- La consulta iterativa para unam.edu.mx (A RR)

- Referencia al servidor de nombres edu.mx (NS RR, para edu.mx)
- Consulta iterativa para unam.edu.mx (A RR) en los pasos 6 y 7.
- Respuesta del servidor edu.mx (dirección IP de unam.edu.mx)
- Respuesta del servidor DNS local al resolvedor (dirección IP de unam.edu.mx) en el paso 8.

Descripción	Tipo	Dato
Name Server	NS	El registro NS contiene el nombre del propietario, así como también el nombre DNS del servidor de nombres.
Mail Exchanger	MX	El registro MX contiene el nombre del propietario, el nombre DNS del servidor intercambiador de correo, un número de preferencia y cualquier nombre canónico.

Tipos de Registros de Recursos (RRs)

Descripción	Tipo	Dato
Start of Authority	SOA	El SOA contiene el nombre primario del servidor de DNS, el nombre de la persona responsable del servidor de DNS, el número serial, el intervalo de reintento, el tiempo de expiración, y el mínimo TTL (Time To Live).
Host	A	El nombre del host contiene el nombre propietario o el nombre DNS del host, y la dirección IP del host.

Registro Start of Authority (SOA)

Este es un ejemplo de un registro SOA:

```
; Start of Authority (SOA) record
dns.com.    IN SOA dns1.dns.com.   owner.dns.com. (
        00000001    ; serial (contador)
           10800    ; refresh (3 horas)
            3600    ; retry (1 hora)
          604800    ; expire (1 semana)
           86400 )  ; TTL (1 día)
```

`owner.dns.com` debería ser leído como owner@dns.com. Los paréntesis del registro se cierran en la última línea, después del valor del TTL. Un punto y coma (;) indica que se inicia un comentario.

Número Serial Este número identifica la versión activa de la base de datos del DNS. Cuando se levanta la base de datos, este debe ser aumentado en uno para que los servidores secundarios sepan cual usar. En el ejemplo se usa un contador, aunque se puede usar la fecha o cualquier otro sistema numérico.

Refresco Este dice a los servidores de nombres secundarios que tan frecuentemente debe checar por la información actualizada.

Reintento Si el servidor de nombres secundario no puede contactar al servidor primario, entonces el secundario reintentará una conección cada *reintento* segundos.

Archivos de configuración en Linux para un DNS

- `/etc/named.boot` Usado para poner la localización de los archivos de configuración y de la base de datos
- `/etc/named.conf` El archivo de configuración de la base de datos.
- `named.hosts` Define el dominio con el mapeo de hosts a IPs
- `named.rev` Usado IN-ADDR-ARPA para mapear IPs a nombres de hosts.
- `named.local` Usado para resolver el manejo de lazo cerrado (loopback)
- `named.ca` Lista de los servidores raíz

Expiración Si un servidor de nombres secundario no puede contactar a un servidor primario por *expiración* segundos, el secundario parará de contestar cualquier consulta sobre su dominio. La teoría aqui es que en este punto, los datos son tan viejos que pueden causar algún daño, de forma que es mejor no contestar que dar una mala respuesta.

TTL Este valor es retornado en todas las respuestas a las consultas a la base de datos, y le dice al requisidor (o a otros servidores) que tanto tiempo puede guardarse (cached). Este valor es el valor por defecto para todos los registros en el archivo; y puede ser sobreescrito por un valor TTL proveído en un RR.

Referencias:

Networking Complete
2nd. Edition
Ed. Sybex.

TCP/IP, T. Parker and M. Sportack
Ed. SAMS, 2000