Gestión e Implantación de Redes de Computadores

Práctica 2

Configuración de un servicio de DNS

Objetivo

Cuando se conecta un sistema a una red, una de las principales tareas que debe realizar el administrador del sistema es garantizar que se puede resolver los nombres nemotécnicos por su correspondiente IP. Esta práctica pretende introducirnos en la instalación y mantenimiento de un servidor de DNS.

Conocimientos previos

Aunque en clase de teoría ya se han impartido los puntos más importantes para poder efectuar esta práctica, como referencia, se puede usar la múltiple información que sobre servicios DNS aparece en Internet.

Introducción

La gran cantidad de ordenadores que están conectados a Internet y el objetivo de identificarlos con una cadena de caracteres determinada en vez de con números, siempre más difíciles de recordar, llevaron a la especificación de un sistema cliente servidor que permitiera la identificación de las máquinas mediante un nombre y que dado éste pudiera obtenerse su dirección IP asociada.

Un primer paso para la resolución del problema de asignación de nombres en una red (ya sea local o la propia Internet) fue considerar un fichero donde se registraran los pares nombre-dirección IP. Este sistema tiene el gran inconveniente de la posible creación de conflictos. Aún así, este sistema se soporta en todos los sistemas que permiten que cada computadora tenga un fichero (/etc/hosts en Unix y /windows/lmhosts en windows) que puede usarse en la resolución de nombres.

Para mejorar el sistema de resolución de nombres, se introdujo el servicio de DNS, mecanismo implementado para la asignación de nombres a direcciones IP y que es una base de datos distribuida donde se identifican los objetos de una red de computadoras. Se basa en la arquitectura cliente servidor, disponiendo por tanto de un servidor que atiende peticiones de resolución de nombres y un cliente, normalmente una función de librería denominada **resolver** y cuya función es la de ponerse en contacto con el servidor y preguntarle la dirección IP para un nombre dado.

El DNS proporciona un servicio de resolución de nombres distribuido, eficiente, confiable y de propósito general. Es distribuido porque la resolución de nombres se divide entre los distintos servidores encargados de cada zona, eficiente porque la resolución, normalmente, se asocia a procesos locales no requiriendo tráfico de red y es de propósito general porque no está restringido a nombres de máquinas.
La resolución de nombres consiste en, dado una petición del cliente, el servidor buscará en su base de datos (si pertenece a su espacio de nombres) o realizará consultas otros servidores.

El primer paso a realizar por un servidor de nombres cuando recibe una petición de un resolver será comprobar si el nombre pertenece a un subdominio sobre el que tiene autoridad (es capaz de resolverlo). Si es así, envía al cliente la dirección que indica su base de datos. Si el nombre pertenece a otro dominio, entonces empieza el proceso de resolución, existiendo 2 métodos:

1. Recursiva
El servidor, a no disponer de la dirección IP, consulta a otros servidores para obtener la dirección. A medida que el servidor va realizando preguntas, va guardando en caché los nombres encontrados para evitarse futuras búsquedas.

2. Iterativa.
El servidor de nombres no realiza la búsqueda sino que le devuelve al cliente la dirección del siguiente servidor al que debe preguntarle por la dirección IP, tras comprobar que no está ni en sus tablas ni en la caché.

Los clientes: resolver

Son programas de biblioteca que se encargan de la petición de resolución de nombres y direcciones. Sus tareas principales:

Preguntar al servidor de nombres
Interpretar las respuestas
Devolver la información al programa que la solicita
Resolución de nombres de dominio a direcciones IP

La configuración de un cliente DNS consiste en la configuración del fichero /etc/resolv.conf en el que, a grandes rasgos, se introduce el dominio y el servidor de

nombre necesario.

/etc/resolv.conf

Este archivo se ha analizado en la práctica anterior.

Servidor DNS.

El espacio de nombres del DNS sigue una estructura jerárquica, basada en dominios y con una base de datos que implementa el esquema. Esto se conoce como nombre de dominio.
Con esta estructura se consiguen 2 objetivos claros: la transformación eficiente de los nombres en direcciones IP y garantiza un control autónomo de la asignación de nombres a los diferentes dominios. Ésta es una de las principales características del DNS: la delegación de autoridad para la asignación de nombres en subdominios. Cada dominio controla en modo de asignación de los dominios que están bajo él. Para crear un dominio, se requiere el permiso del dominio en el que se incluirá (de esta forma se evitan los conflictos de nombres y cada dominio lleva registro de todos sus subdominios sin necesidad de obtener permiso de nadie más de la jerarquía).
Esta organización se representa habitualmente por un árbol donde la raíz se etiqueta con una cadena vacía (" ") y las hojas representan los dominios que no contienen subdominios pero sí computadoras (desde una a cientos de ellas).

En el primer nivel, aunque existen muchos más, se distinguen 2 tipos de dominios:

- Genéricos (organizativos): los dominios se dividen en función de la organización que va a representar. Se distinguen los siguientes subdominios:
  - edu: organizaciones educacionales como universidades, ...
  - com: para organizaciones comerciales.
  - net: proveedores de red.
  - gov: Instituciones gobernamentales
  - mil: instituciones militares
  - org: Organizaciones no incluídas en los casos anteriores.
  - int: Organizaciones internacionales.
- Países (geográficos): divide los dominios en países, asignando un dominio por país (es para España, fr para Francia, us para USA,...)

Un nombre de dominio bien cualificado, se forma con los nombres de los distintos dominios, recorridos de abajo a arriba en el árbol, separados por un punto, recibiendo cada uno por separado el nombre de etiqueta. Se distinguen los nombres de dominio absoluto (acabados en un punto) o relativos (que deben interpretarse en un contexto para determinar de forma unívoca su significado verdadero). Veamos un ejemplo:
origin.eps.ua.es. es un nombre de dominio absoluto (FQDN, Full Qualified Domain Name) que hace referencia a la computadora llamada origin dentro del subdominio eps de la Escuela Politécnica Superior de la UA, que a su vez está dentro del dominio ua, de la Universidad de Alicante, dependiente del dominio es (España).

Otras características genéricas de este sistema son:

1.- No es "case-sensitive", es decir, no hace distinción entre mayúsculas y minúsculas.
2.- Los nombres de componentes no pueden exceder de 63 caracteres y la trayectoria completa (el nombre de dominio entero) no puede exceder de 255 caracteres de longitud.

Es un sistema general permitiendo que múltiples jerarquías de nombres se incorporen al sistema.

Zonas. Registros de recursos (RR)

Cada servidor DNS se encarga de resolver nombres de uno o varios dominios. A la/s ramas del árbol jerárquico de nombres que resuelve un servidor se le denomina zona. Lo normal es que cada zona tenga un servidor primario que obtiene los datos de un fichero y uno o más secundarios que obtienen los datos de un servidor primario. Los servidores de nombres que estén situados inmediatamente por encima en el árbol del espacio de nombres, apuntarán a los servidores encargados de resolver estas zonas, de tal forma que estos servidores responderán directamente a peticiones de nombre que pertenezcan a su zona.
Normalmente, además del servidor primario de zona, se dispone de uno o más servidores secundarios. Para que estas computadoras trabajen con datos correctos, lo que hacen es pedírselos al servidor primario mediante lo que se llama una transferencia de zona.

Datos del DNS. Registros de recursos

Los datos que maneja un DNS serán aquellos que son necesarios para poder realizar su labor:

Lista de nombres con la dirección asociada.
Lista de direcciones con sus nombres asociados
Lista de servidores raíz mundiales para saber a quién debe enviarle consultas externas

Todos estos datos deben guardarse de alguna forma en el servidor de nombres. La opción escogida es la almacenarlos como una serie de entradas de texto, formando lo que se conoce como un registro de recursos (RR).
Un registro de recursos está compuesto por 5 tuplas cuyo formato es:

[nombre] [TTL] [clase] Tipo de Registro Valor del dato
Nombre: indica el índice con el que se referenciará al registro. Si se omite se toma el último.
TTL: tiempo de vida. Indica cuánto tiempo ha de guardarse un registro en caché.
Clase: la única clase usada actualmente es la IN (de Internet)
Valor: puede ser un número, un nombre de dominio o una cadena ASCII.
Tipo de registro. Puede ser uno de los enumerados en la siguiente lista:

SOA Inicio de autoridad. Fija los parámetros de la zona
NS Servidor de Nombre. Nombre de un servidor autorizado para el dominio
A Dirección de anfitrión. Asigna a un nombre una dirección
CNAME Nombre canónico. Establece un alias para un nombre verdadero
MX Intercambio de correo. Especifica qué máquinas intercambian correo

PTR Puntero. Permite la conversión de una dirección a nombre.

Registro SOA

Proporciona la información sobre la zona indicando el servidor de nombres primario, la dirección de correo del administrador de la zona y varios temporizadores útiles para los servidores secundarios. Un ejemplo de este registro es:

```
eps.ua.es IN SOA  origin.eps.ua.es   root.origin.eps.ua.es (
1998072701 ; Serial
86400 ; Refresh 24 hours
3600 ; Retry 1 hour
3600000 ; Expire 1000 hours
86400 ) ; Negative TTL
```

Con este registro se indica que el dominio eps.ua.es está controlado por la computadora origin, que el correo lo envíe al root de dicha máquina. Los secundarios se conectarán cada 24 horas al primario y, si el número de serie es menor que el del primario, se realizará una transferencia de zona. Si el secundario no logra conectarse, se le indica que lo reintente dentro de una hora y, si no es capaz de hacerlo en 1000 horas, que deje de responder a consultas de resolución.
El valor de 86400 (24 horas) que se indica en el registro SOA, es el valor por defecto usado para mantener en caché las respuestas.

Registro NS

Este tipo de registro indica qué servidores son los servidores de nombres.

Registro A

Asocia a un nombre una dirección IP. Si un host dispone de más de una interface de red, deberá tener un registro A por cada una de ellas.

Registro CNAME

Permite crear alias (nombres canónicos) para computadoras que tienen un nombre real. El ejemplo más usado es para añadir el alias de Web a un servidor (origin.eps.ua.es como www.eps.ua.es)

Registro MX

Indican el servidor de correo para el dominio especificado.

Resolución Inversa: de dirección a nombre

Otra característica que cumple un servidor de nombres es responder a peticiones de resolución de nombres dadas direcciones IP. Recordemos que el espacio de direcciones del DNS, está indexado mediante nombres y no por números. Para la resolución inversa, se ha creado un dominio que usa números como nombres. Este dominio es el in-addr.arpa. Junto con los números de la dirección en orden inverso (ya que los nombres se

componen de abajo hacia arriba).
Tanto para la resolución inversa como para la directa, los clientes saben qué servidor de nombres usar gracias a la configuración de red. Tanto en las computadoras Unix como en la basadas en el Windows de Microsoft, con la configuración de la red se le indica al sistema cuál es el servidor de nombres (el fichero /etc/resolv.conf indica, entre otras informaciones que se verán más adelante, el servidor de nombres a usar). Los clientes sólo necesitan conocer la dirección del servidor de nombres ya que el puerto es uno de los reservados y siempre el mismo (53)
Los servidores, para encontrar el resto de servidores a los que deben preguntar por nombres externos, disponen en su base de datos de los servidores de nombres raíz (varios, para asegurar un balance de carga) a partir de los cuales podrá encontrar cualquier nombre de Internet.

Configuración

named.conf

El fichero **named.conf** por defecto posee un contenido similar a este:

```
options {
directory "/var/named";
listen-on { 127.0.0.1; };
};

zone "localhost" {
type master;
file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
```

Las posibilidades de configuración que brinda este fichero son enormes, basta con mirar rápidamente el “man" del mismo para percibir esto. Sin embargo básicamente se puede decir que está formado por un conjunto de sentencias y de comentarios. Las sentencias se terminan con el caracter “;" y pueden contener dentro de sí a otras sentencias, en estos casos el contenido de la sentencia va encerrado entre {}.

Existen muchos tipos de sentencias. De ellas las principales se explican a continuación:

acl : es una sentencia que permite definir listas de direcciones IP con el objetivo de utilizarlas para indicar reglas de acceso en otras sentencias. Su nombre significa Access Control List. Por defecto existen cuatro acl definidas:

any : acceso permitido a todos los hosts.
none : acceso denegado a todos los hosts.
localhost : acceso permitido sólo a las direcciones IP locales.

localnets : acceso permitido a todos los hosts de todas las redes con las cuales el sistema tenga al menos una interface.

El siguiente es un ejemplo que define una lista de acceso con nombre “peligrosos" y que incluye a todos los hosts pertenecientes a las redes 192.168.11.0 y 192.168.12.0, así como al host independiene 192.168.13.2

```
acl “peligrosos” { 192.168.11.0/24; 192.16812.0/24; 192.168.13.2; };
```

options : esta sentencia controla toda la configuración del servidor y define las opciones por defecto de otras sentencias. Sólo debe aparecer una vez en el fichero de configuración. Puede apreciarse su utilización en el ejemplo anterior. En el que se da a continuación se muestran y comentan otras opciones.

```
options {
directory /var/named;
        # indica el directorio de trabajo del servidor. Toda referencia
        # a fichero relativa lo será a partir de este directorio

allow-query {192.168/16; };
        # indica que se permiten las consultas de todos los hosts con
        # direcciones que comiencen con 192.168

blackhole { peligrosos; };
        # especifica que no se les responda ninguna consulta a los hosts de
la lista peligrosos

listen-on port 1054 {!10.20.30.40; };
       # indica que el servidor escuche las consultas por el puerto 1054 y a
través de todas sus interfaces de red excepto la de dirección 10.20.30.40
```

zone : es una de las sentencias más importantes pues permite definir las zonas y describir sus respectivas configuraciones. Los tipos de zonas más importantes son:

Master zone
Es aquella donde el servidor tiene la copia primaria o principal de los datos de la zona y es capaz de dar respuestas autorizadas acerca de esta.

Slave zone
Es la zona cuyos datos son resultado de la réplica de la información de una zona master.

A continuación se muestra a través del ejemplo descrito hasta el momento como se definen las zonas eps.ua.es, 11.168.192.in-addr.arpa y 12.168.192.in-addr.arpa.

```
zone "eps.ua.es" {
type master;
file "named.date.eps";
};

zone "11.168.192.in-addr.arpa" IN {
type master;
file "named.rev.11";
};

zone "12.168.192.in-addr.arpa" IN {
type master;
file "named.rev.12";
};
```

Los siguientes atributos pueden ser indicados al caracterizar una zona:

type : indica el tipo de zona.

file : para el caso de las zonas cuya información se almacene localmente indica el nombre del fichero donde esta se encuentra.

allow--update : indica los hosts autorizados a hacer actualizaciones dinámicas a la zona.

allow-transfer : indica los hosts autorizados a transferir la información de la zona. Este atributo también se puede especificar de forma global en la sentencia options.

allow-query : indica los hosts autorizados a hacer consultas sobre la zona. Este atributo también se puede especificar de forma global en la sentencia options.

Resolución directa de nombres

El fichero "named.data.eps" que, como hemos visto en el ejemplo anterior, es el que contiene los datos para la resolución directa, tendrá, por ejemplo, el siguiente contenido:

```
eps.ua.es. IN SOA dns.eps.ua.es. admin.eps.ua.es. (
2015030201; número de serie
10800 ; 3 horas - Tiempo de refresco
900 ; 15 minutos - Tiempo de reintento
604800 ; 1 semana - Tiempo de expiración
86400) ; 1 día – TTL Negativa


; Servidores del dominio
eps.ua.es. IN NS dns.eps.ua.es.
eps.ua.es. IN NS origin.eps.ua.es.

; Direcciones de las máquinas de la subred 192.168.11.0
rt11.eps.ua.es.      IN    A    192.168.11.1
pc1-11.eps.ua.es.  IN    A    192.168.11.2

; Direcciones de las máquinas de la subred 192.168.12.0
rt12.eps.ua.es.      IN    A    192.168.12.1
pc1-12.eps.ua.es.  IN    A    192.168.12.2

router-L25          IN    CNAME     rt11.eps.ua.es.
```

Resolución inversa

El fichero "named.rev.11" que, como hemos visto en el ejemplo anterior, es el que contiene los datos para la resolución inversa de la red 192.168.11.0/24, tendrá, por ejemplo, el siguiente contenido:

```
11.168.192.in-addr.arpa. IN SOA dns.eps.ua.es. admin.eps.ua.es.(
1; número de serie
10800 ; 3 horas - Tiempo de refresco
900 ; 15 minutos - Tiempo de reintento
604800 ; 1 semana - Tiempo de expiración
86400) ; 1 día – TTL negativa


; Servidores del dominio
11.168.192.in-addr.arpa. IN NS dns.eps.ua.es.
11.168.192.in-addr.arpa. IN NS origin.eps.ua.es.

; Direcciones de las máquinas de la subred 192.168.11.0
1 IN PTR rt11.eps.ua.es.
2 IN PTR pc1-11.eps.ua.es.
```

Enunciado

La práctica consistirá en la configuración y prueba de un servidor de DNS local.

Nuestro DNS debe ser capaz de resolver las IP´s de nuestra red local. Los nombres y las direcciones serán las mismas que la práctica anterior de configuración de TCP/IP.

La configuración a realizar debe soportar los siguientes servicios:

1. Se tendrán dos servidores de nombres, uno actuando como maestro y el otro como esclavo.
2. Los servidores atenderán múltiples zonas (sólo dos) mediante resolución directa.
3. Los servidores atenderán múltiples zonas (sólo dos) mediante resolución inversa.
4. Se soportarán vistas. Es decir, ante la misma consulta sobre el router virtual, se devolverán distintas respuestas, dependiendo de si el origen de la consulta es interno a nuestra red o externo. Según la práctica anterior, se considerará la Red-A interna y la Red-B externa.
5. Se soportará distribución de carga Round Robin para el recurso “www.midominio.es” entre tres servidores Web.
6. Se podrá acceder al recurso “atlético.midominio.es” desde un navegador Web.
7. Por supuesto, si las consultas no están en nuestra base de datos se redirigirán a otro servidor de nombres.

Para probar el funcionamiento de nuestro servicio, disponemos de las herramientas **nslookup** o **dig**, con la que probaremos la configuración realizada.

Para la realización de esta práctica se dispone de **cuatro sesiones** de laboratorio.