Servidor de DNS

Preguntas

1. ¿En qué consiste DNS? ¿Qué puertos y protocolo en la capa de transporte utiliza?

DNS funciona sobre UDP y algunas veces sobre TCP, utilizando el puerto 53.

La función más conocida de los protocolos DNS es la asignación de nombres a direcciones IP. Por ejemplo, si la dirección IP del sitio FTP de prox.es es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.es y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Cada dominio debe tener un servidor DNS autorizado responsable de dicho dominio (también llamado zona de autoridad), que a su vez puede tener otros servidores DNS autorizados responsables de subdominios. De tal manera el servicio de DNS queda distribuido, sin un registro central donde consultar o actualizar cambios. La información de los nombres de máquinas está repartida por todos los servidores de DNS del mundo.

Si un cliente formula una pregunta recursiva a un servidor DNS, éste debe intentar por todos los medios resolverla aunque para ello tenga que preguntar a otros servidores. Si, en cambio, el cliente formula una pregunta iterativa a un servidor DNS, este servidor devolverá o bien la dirección IP si la conoce o si no, la dirección de otro servidor que sea capaz de resolver el nombre.

Nombre de dominio = nombre de máquina + subdominios + dominio de nivel superior

www.xtec.cat = www (nombre de máquina) + xtec (subdominio) + cat (dominio nivel superior)

2. ¿Qué es un servidor DNS primario? ¿Qué es un servidor DNS esclavo? ¿Qué es un servidor DNS caché?

Los tres responden a peticiones de DNS.

Los servidores DNS primarios o maestros guardan los datos de uno o más espacios de nombres en sus ficheros, que utilizan para resolver las peticiones de información sobre dichas zonas.

Los servidores DNS secundarios o esclavos obtienen la base de datos para la resolución de nombres desde los servidores primarios a través de una transferencia de zona, y mantienen dicha copia actualizada y la utilizan para resolver las peticiones de información sobre dichas zonas.

Los servidores DNS locales o caché no contienen la base de datos para la resolución de nombres, sino que 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.

3. En una pequeña red local ¿Cómo resuelve el servidor de DNS el nombre de una máquina externa a la red? ¿Cómo resuelve el servidor de DNS el nombre de una máquina interna de la red?

El servidor local de DNS resolverá el nombre de una maquina externa a la red reenviando la pregunta a otro servidor, mientras que resolverá el nombre de la máquina interna utilizando

su lista de nombres asociados a IPs.

De todas maneras, el cliente antes de enviar su petición al servidor de DNS intentará resolverla mediante el fichero *hosts* y mediante su caché de DNS.

4. ¿Viene algún software de servidor de DNS con Windows Server? ¿Desde dónde se instala y desde dónde se administra?

Se instala desde "Agregar y quitar programas → Agregar y quitar componentes de Windows → Servicios de red → Sistema de Nombres de Dominio (DNS)".

Se administra desde "Herramientas Administrativas → DNS"

5. ¿Cuál es el software de servidor de DNS más conocido para Unix/Linux?

***bind* del ISC, pero hay otros más sencillos como *dnsmasq*, que además integra el servicio de DHCP con el de DNS.**

6. Al instalar un servidor de DNS en una pequeña red local, ¿Qué parámetros a configurar piensas que serán los más importantes? ¿Qué son los registros A, AAAA, CNAME, NS, MX, PTR y SOA?

- nombre de dominio,

- nombre de los equipos asociado a sus correspondientes IPs,

- nombre del servidor de correo,

- IP del servidor de DNS para la resolución de nombre externos a la red.

En el fichero de configuración, los registros más importantes son:

- A: traduce nombres de hosts a direcciones IPv4.

- AAAA: traduce nombres de hosts a direcciones IPv6.

- CNAME: Se usa para crear nombres de hosts adicionales, o alias.

- NS: Asocia un nombre de dominio a los servidores de nombres de dicho dominio.

- MX: Asocia un nombre de dominio a los servidores de intercambio de correo del dominio.

- PTR: funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.

- SOA: Proporciona información sobre la zona.

7. ¿De qué tres maneras se puede integrar el servicio de DHCP con el de DNS para conseguir que el servidor de DNS resuelva nombres de máquinas cuya IP fue dada por un servidor de DHCP?

1) Las IPs pueden estar reservadas a las MAC, y por lo tanto DHCP siempre da las mismas.

2) Con un servidor DNS dinámico, y un servidor DHCP que de la dirección del servidor DNS dinámico. Cuando un cliente reciba los parámetros IP del servidor de DHCP, lo anunciará al servidor DNS dinámico.

3) Con algún programa que ya traiga un servidor de DNS y DHCP integrados.

8. ¿Para qué sirve el fichero *hosts*? ¿Cómo se vacía la caché de DNS del cliente en Windows,

MacOS X y Linux?

El fichero *hosts* se utilizaba -y todavía se utiliza- para asociar en un cliente nombres de máquinas a IP. Los clientes todavía consultan este fichero antes de lanzar una petición a un servidor DNS.

La caché de DNS en el cliente se vacía reiniciando la máquina o bien escribiendo el comando:

En Windows: `ipconfig /flushdns`

En Linux: `systemctl restart nscd`

En MacOS X: `dscacheutil -flushcache`

Datos de la práctica

Nuestro servidor de DNS será un servidor primario para búsquedas directas.

Nuestra red se llama *mired.org*.

Los nombres que el servidor de DNS servirá son:

- *obelix* (cliente con reserva DHCP): IP 192.168.100.150
- *asterix* (servidor): IP 192.168.100.2
- *panoramix* (router): IP 192.168.100.1

El servidor de correo será *asterix*, que también se llamará *www*, *ftp* y *mail*.

El servidor de nombres será *asterix*, que también se llamará *dns*.

Una vez realizado el ejercicio necesitaremos asegurarnos que el servidor de DHCP esté sirviendo a los clientes la IP del servidor de DNS que hemos configurado.

También deberemos asegurarnos de que los servidores cuyos parámetros IP se han configurado manualmente (DHCP, router), también tengan configurada la dirección IP del servidor de DNS que hemos instalado para que puedan acceder a los equipos de nuestra red por su nombre.

Práctica con Windows

Instalaremos DNS para Windows Server. Exploraremos la interfaz gráfica de administración del servidor DNS, configurando los parámetros básicos. Configuraremos DNS para una pequeña red local y probaremos el servidor.

1. Manipula la configuración de las tarjetas de red de las máquinas virtuales del servidor y el cliente para que compartan la misma red interna.

2. Instala y configura el servidor DHCP. Paso a paso , para Windows 2016:

   https://www.solvetic.com/tutoriales/article/3284-instalar-y-configurar-servidor-dns-windows-server-2016/

3. Configura el servidor de DHCP para que incluya dirección del nuevo servidor de DNS entre los parámetros que da a los clientes.

4. Prueba el servicio de DNS desde un cliente, tanto para direcciones internas como externas.

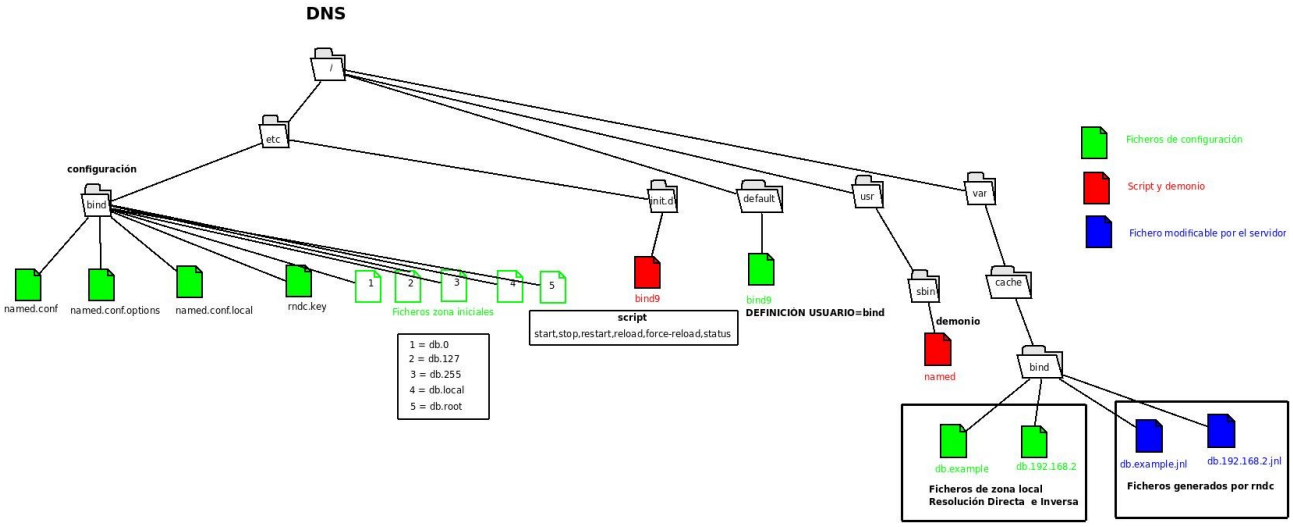
Práctica con Linux

Instalaremos DNS para Linux. Exploraremos el fichero de configuración. Configuraremos DNS para una pequeña red local y probaremos el servidor.

- https://ubuntu.com/server/docs/service-domain-name-service-dns

- https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-debian-9

- https://wiki.debian.org/Bind9



1. Instalamos y configuramos el servidor DNS:

   # **apt install bind9**

   Editamos los servidores de DNS externos para reenviar consultas:

   # **nano /etc/bind/named.conf.options**

```
options {
  forwarders { 8.8.8.8; };
  dnssec-enable no;     # Por problemas con dns-caché de mi instituto
};
```

Especificamos donde está el archivo para búsquedas directas:

nano /etc/bind/named.conf.local

```
zone "mired.org" {
  type master;
  file "/etc/bind/db.mired.org";
};
```

Editamos el archivo para búsquedas directas:

nano /etc/bind/db.mired.org

```
$ORIGIN mired.org.
$TTL 3D
@ IN SOA dns.mired.org. admin.mired.org. ( 1  8H  2H  1W  1D )

                NS          asterix
                MX 10       asterix

panoramix       A           192.168.100.1
asterix         A           192.168.100.2
obelix          A           192.168.100.150

www             CNAME       asterix
ftp             CNAME       asterix
mail            CNAME       asterix
dns             CNAME       asterix
```

y a continuación reiniciamos el servicio:

systemctl restart bind9

Si parece que el servicio no funciona y es difícil detectar si hemos escrito mal la configuración, podemos probar con:

ss -upna

cat /var/log/syslog | grep named

named-checkconf

named-checkzone mired.org /etc/bind/db.mired.org

(Si quieres profundizar en la sintaxis y parámetros del fichero de configuración de zona, lee el capítulo 5 del manual de referencia de Bind: https://ftp.isc.org/isc/bind9/cur/9.17/doc/arm/html/)

2. Prueba el servicio desde un cliente, tanto nombres de la red local como nombres externos:

   $ **cat /etc/resolv.conf**

   # **apt install dnsutils**

   $ **nslookup asterix** o bien $ **dig asterix -trace**

   $ **nslookup www.mired.org** o bien $ **dig www.mired.org -trace**

   $ **nslookup www.google.es** o bien $ **dig www.google.es -trace**

   ¿Te atreves a interpretar las respuestas del comando `dig`?

   Recuerda que **para que el cliente utilice el servidor de DNS, ¡debe estar configurado para utilizar el servidor de DNS!** Esto quiere decir que:

   (a) en los ordenadores que tienen parámetros IP configurados manualmente deberás editar a mano su configuración de red para especificar cual es el nuevo servidor de DNS; y

(b) deberás cambiar la configuración en el servidor de DHCP para que entregue al resto de ordenadores los parámetros de red con el nuevo servidor de DNS.

Práctica adicional con Linux

En una oficina de la empresa "mired.org" tenemos el despacho de los administrativos. También tenemos un datacenter.

- Los administrativos son 10, y uno de ellos es el responsable.
- En el datacenter hay tres servidores: www, bbdd i mail.
- Cada estancia está en una red IP diferente. (Aprovecha las redes del ejercicio anterior de DHCP)

1. Instala un servidor DNS con los siguientes requisitos:

   - Las máquinas de los administrativos se deben llamar: "adm1", "adm2", ...
   - Todas las máquinas del datacenter también tendrán nombre.
   - Define alias para las máquinas significativas.

```
# apt update
# apt install bind9
```

```
# nano /etc/bind/named.conf.options
```

```
acl corpnets { 192.168.100.0/24; 192.168.200.0/24; };
options {
  allow-query { corpnets; };
  forwarders { 8.8.8.8; };
  dnssec-enable no;     # Por problemas con dns-caché de mi instituto
};
```

```
# nano /etc/bind/named.conf.local
```

```
zone "mired.org" {
  type master;
  file "/etc/bind/db.mired.org";
};
```

```
# nano /etc/bind/db.mired.org
```

```
$ORIGIN mired.org.
$TTL 3D
@         IN    SOA        dns.mired.org. admin.mired.org. (
                              2018120101    ;   serial
```

```
                              8H            ;   refresh after 8 hours
                              2H            ;   retry after 1 hour
                              1W            ;   expire after 1 week
                              1D )          ;   minimum TTL of 1 day

@         IN    NS         dns.mired.org.
@         IN    NS         dns2.mired.org.

@         IN    MX   10    server.mired.org.

adm01     IN    A          192.168._tu-ip_.201
adm02     IN    A          192.168._tu-ip_.202
adm…      IN    A          192.168._tu-ip_.…
adm10     IN    A          192.168._tu-ip_.210
boss      IN    CNAME      adm01

dns       IN    A          192.168._tu-ip_.1
router    IN    CNAME      dns

server    IN    A          192.168._tu-ip_+100.201
dns2      IN    A          192.168._tu-ip_+100.202
www       IN    CNAME      server
bbdd      IN    CNAME      server
mail      IN    CNAME      server
```

y a continuación reiniciamos el servicio:

systemctl restart bind9

2. Además de la resolución directa, también habrá resolución inversa.

nano /etc/bind/named.conf.local

```
zone "168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.192.168";
};
```

nano /etc/bind/db.192.168

```
$ORIGIN 168.192.in-addr.arpa.
$TTL 3D
@         IN    SOA        dns.mired.org. admin.mired.org. (
                              2018120101    ;   serial
                              8H            ;   refresh after 8 hours
                              2H            ;   retry after 1 hour
                              1W            ;   expire after 1 week
                              1D )          ;   minimum TTL of 1 day

@         IN    NS         dns.mired.org.
@         IN    NS         dns2.mired.org.

201._tu-ip_     IN    PTR   adm01.mired.org.
202._tu-ip_     IN    PTR   adm02.mired.org.
20…._tu-ip_     IN    PTR   adm….mired.org.
210._tu-ip_     IN    PTR   adm10.mired.org.
```

```
1._tu-ip_       IN    PTR   dns.mired.org.
1._tu-ip_+100   IN    PTR   dns.mired.org.

201._tu-ip_+100 IN    PTR   server.mired.org.
202._tu-ip_+100 IN    PTR   dns2.mired.org.
```

y a continuación reiniciamos el servicio:

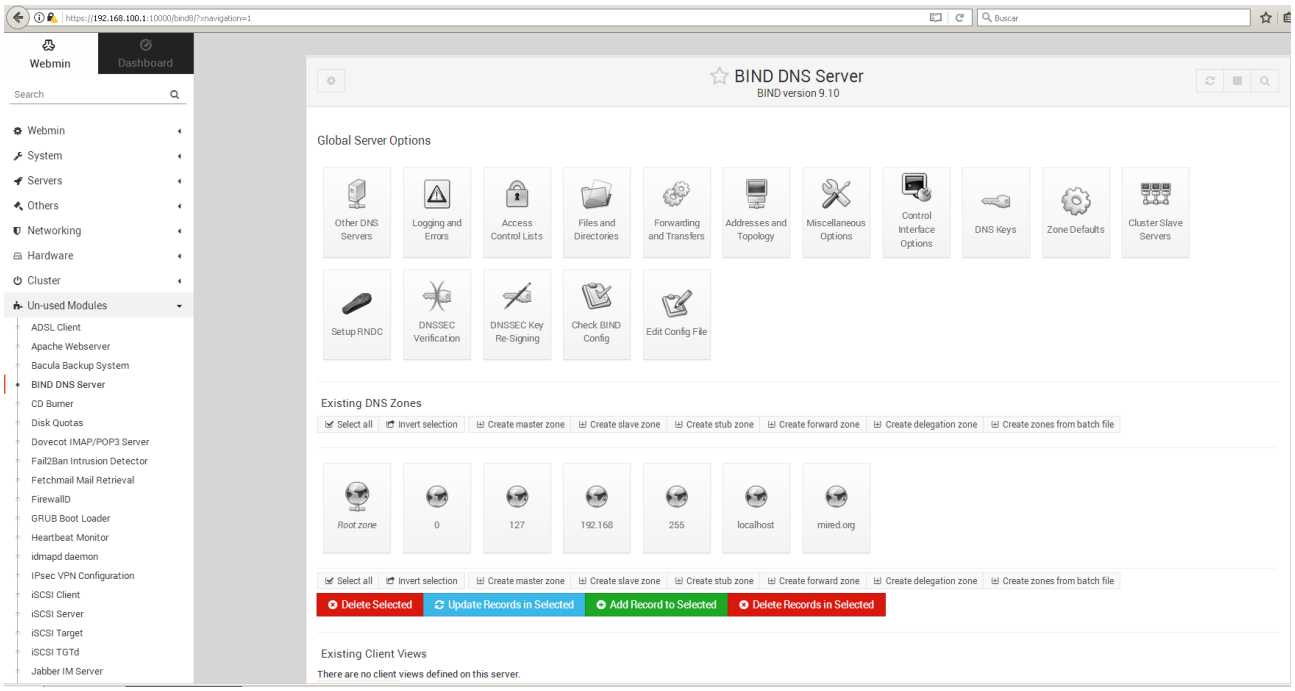
```
# systemctl restart bind9
```

3. Instala en el servidor el módulo de Webmin para administrar DNS.

   https://*IP_servidor*:10000/ → Un-used modules → BIND DNS Server

   https://*IP_servidor*:10000/ → Refresh modules

   https://*IP_servidor*:10000/ → Servers → BIND DNS Server



4. Instala un servidor DNS esclavo del primero.

Creamos una nueva máquina con BIND9 en 192.168.200.2. En el servidor primario (192.168.200.1) añadimos:

```
# nano /etc/bind/named.conf.local
```

```
zone "mired.org" {
  type master;
  file "/etc/bind/db.mired.org";
};

zone "168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.192.168";
};
```

```
options {
  allow-transfer { 192.168.200.202; };
  notify yes;
  also-notify { 192.168.200.202; };
};
```

Y en el servidor esclavo (192.168.200.2) añadimos:

nano /etc/bind/named.conf.local

```
zone "mired.org" {
  type slave;
  file "/etc/bind/db.mired.org";
  masters { 192.168.200.1; };

zone "168.192.in-addr.arpa" {
  type slave;
  file "/etc/bind/db.192.168";
  masters { 192.168.200.1; };
};
```

En el servidor esclavo no hace falta transferir los ficheros /etc/bind/db.mired.org y /etc/bind/db.192.168, si no que se deberían crear a partir de una copia del primario. Para que se puedan crear, asegurate de que el usuario o el grupo bind tenga permisos de escritura en la ruta de dichos ficheros.

5. Entrega un script para comprobar todos los registros, detectando qué servidor de DNS (maestro o esclavo) está activo.

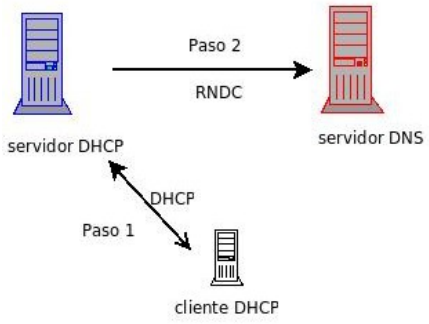
   Poner todos los nslookup o dig en un archivo Bash.

6. ¿DNS dinámico?

   https://wiki.debian.org/DDNS

   https://help.ubuntu.com/community/DynamicDNS

   http://systemadmin.es/2014/02/actualizacion-zonas-dns-con-las-concesiones-dhcp



   ¿Subdominios?

   http://www.zytrax.com/books/dns/ch9/subdomain.html

   http://www.zytrax.com/books/dns/ch9/delegate.html

Referencias

- http://en.wikipedia.org/wiki/Domain_Name_System
- https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- https://howdns.works/
- http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
- http://www.zytrax.com/books/dns/
- https://en.wikipedia.org/wiki/Comparison_of_DNS_server_software
- https://tools.cisco.com/security/center/resources/dns_best_practices
- https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks