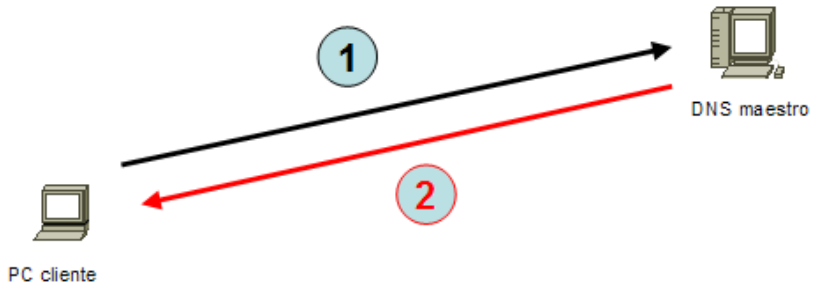
1. Servidor DNS Bind

El servidor de DNS Bind admite tres modos de funcionamiento.

- Servidor DNS maestro
- Servidor DNS esclavo
- Servidor caché DNS

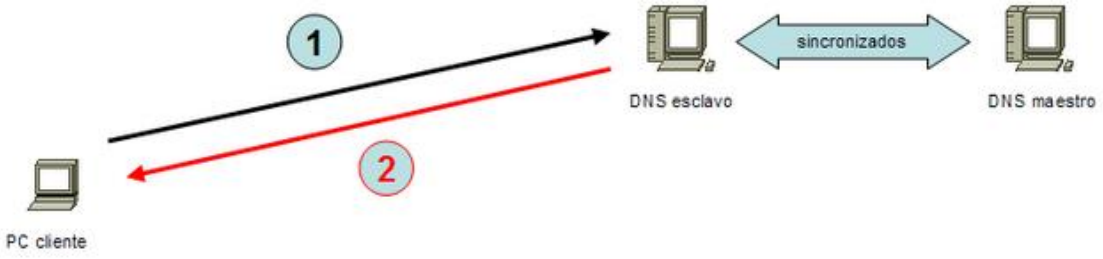
1.1 Servidor DNS Maestro

En este modo de funcionamiento, nuestro servidor se comporta como un auténtico servidor DNS para nuestra red local. Atenderá directamente a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.



1.2 Servidor DNS esclavo

Un servidor esclavo actuará como un servidor espejo de un servidor DNS maestro. Permanecerá sincronizado con el maestro. Se utilizan para repartir las peticiones entre varios servidores, aunque las modificaciones solo se realicen en el maestro. En redes locales salvo por razones de disponibilidad, es raro que exista la necesidad de tener dos servidores DNS ya que con uno será suficiente.



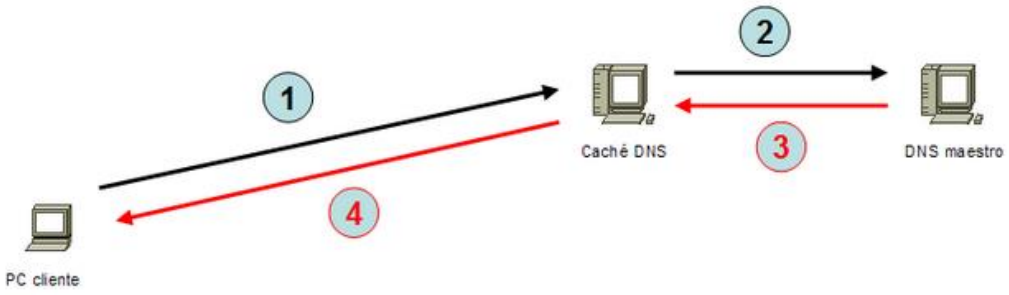
1.3 Servidor caché DNS

En este modo de funcionamiento, nuestro servidor se comporta como si fuera un auténtico servidor DNS para nuestra red local aunque realmente no sea un servidor DNS propiamente dicho. Cuando recibe una petición de DNS por parte de un cliente de nuestra red, la trasladará a un DNS maestro que puede estar en nuestra red o fuera, almacenará en una memoria caché la respuesta y a la vez la comunicará a quien hizo la petición. Si un segundo cliente vuelve a realizar la misma petición, como nuestro servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet pues cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS. Si nuestro caché DNS almacena la gran mayoría de peticiones que se realizan desde la red local, las respuestas de los clientes se satisfarán prácticamente de forma instantánea proporcionando al usuario una sensación de velocidad en la conexión.

Es un modo de funcionamiento de sencilla configuración ya que prácticamente lo único que hay que configurar son las direcciones IP de un DNS primario y de un DNS secundario.

Por defecto, al instalar el paquete bind está preconfigurado como servidor caché DNS.

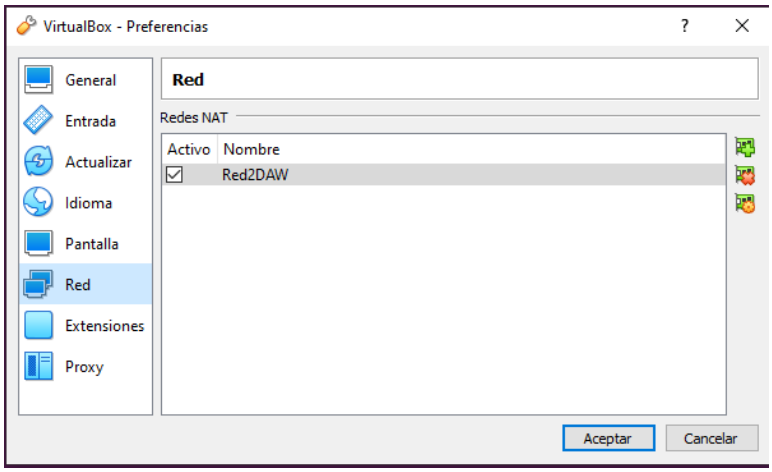


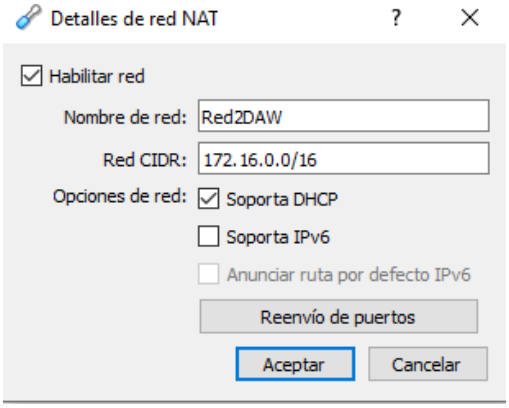
Hay que tener en cuenta que un mismo **servidor DNS** puede desempeñar varias de estas funciones simultáneamente. Por ejemplo, un **servidor DNS** puede ser maestro para una zona, esclavo para otra y actuar como cache.

2. Configuración previa del servidor y clientes DNS.

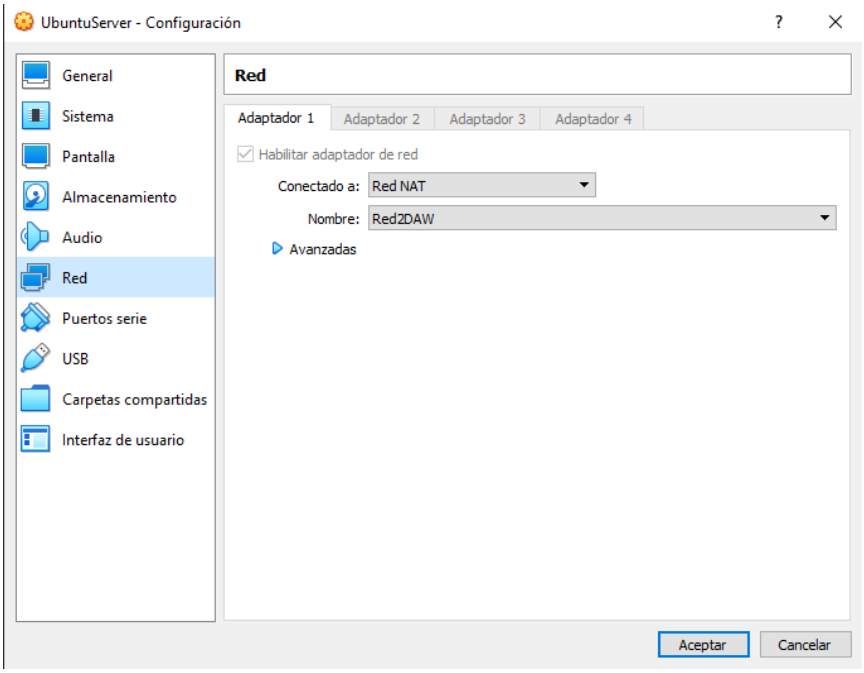
El computador donde se aloje el servidor DNS debería tener una dirección IP estática. Los clientes no es necesario que tengan un IP estática, pero evidentemente, deben tener como dirección del DNS, la IP estática del equipo que sea servidor DNS.

Para la realización de este ejercicio configuraremos una RED NAT en virtualbox. El nombre para la red será **Red2DAW** y será una red **172.16.0.0/16**.





Nuestro servidor dns debe estar conectado a esa red.



Para configurar la dirección de red de nuestro servidor, editaremos el fichero:

/etc/netplan/ 01-network-manager-all.yaml

Completandolo de la siguente manera:

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [172.16.0.5/16]
      gateway4: 172.16.0.1
      nameservers:
        addresses: [172.16.0.5]
```

De esta forma, nuestro servidor dns, tendrá la ip estática 172.16.0.5 / 16. Y el servidor DNS que emplee el servidor será el mismo.

3. Archivos de configuración de Bind

La carpeta **/etc/bind/** contiene una serie de archivos para la configuración de Bind. Los archivos fundamentales son:

- **named.conf**: Contiene la lista de ficheros de configuración, para separar las opciones del servidor de las opciones de las distintas zonas.
- **named.conf.options**: Contiene las opciones que tienen que ver con todo el servidor. Por ejemplo, podría contener información de cuales deben ser los clientes a los que de servicio, servidores a los que permita transferencia de zonas, forwarders...
- **named.conf.local**: Contiene una lista de las zonas de las que el servidor es autoritario, sea como servidor primario o secundario.
- **named.conf.default-zones**: Inclúe una serie de zonas por defecto: Servidores raíz, resolución inversa de la red 127.0.0.0/8, resolución de localhost...
- **ficheros db.**: Normalmente las definiciones de las zonas de las que el servidor es primario se guardan en ficheros que empiezan por *db.*
- **Archivo db.127**: Especificación dirección de retorno.
- **Otros archivos**: db.0, db.255, db.empty, db.local, rndc.conf, rndc.key, zones.rfc1918

Las opciones de configuraión globales normalmente se incluyen en el fichero *named.conf.options* para que tengan valor para todo el servidor. Si se quiere que tengan valor solamente en una zona, se pueden agregar en el fichero de configuración de la zona correspondiente. Algunos ejemplos de las entradas que se pueden incluír son:

- acl: permite crear listas de equipos a los que despues se les permite o deniega ciertas acciones, empleando el nombre de la acl.

acl "redlocal" {192.168.0.0/22;}; //Inclúe todos los equipos de la red 192.168.0.0/22

- allow-query: permite definir que equipos pueden consultar el servidor

  allow-query {any;}; //Permite consultas de todos los equipos
  allow-query {redlocal;};//Permite consultas de todos los equipos en la acl red local .

- forwarders:

  forwarders {8.8.8.8; }; //Define 8.8.8.8 como forwarder al que se le reenviarán todas las preguntas que no son de zonas locales.

3.1 Configuración named.conf.options para este caso práctico

En el archivo named.conf.options, habilitar un forwarder para la resolución de aquellas peticiones que no sea capaz de resolver nuestro servidor DNS

```
forwarders {
        //Dns publico de google
        8.8.8.8;
        8.8.4.4 ;
};
```

3.2 Dominio a crear

El ejemplo de dominio que se va a crear puede ser **daw.local**.

Para ello vamos a **abrir el archivo named.conf.local** para crear la zona de nuestro dominio, y añadiremos el siguiente contenido al fichero para definir la zona de nuestro dominio daw.local.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
// include "/etc/bind/zones.rfc1918";
```

```
//Definición de la zona de resolución directa. El nombre del dominio es daw.local
//El archivo de definición de la zona es /etc/bind/db.daw.local
zone "daw.local"{
        type master;
        file "/etc/bind/db.daw.local";
};

//Definición de la zona de resolución inversa. 0.16.172
//El archivo de definición de la zona es /etc/bind/ri.172.16.0
zone "0.16.172.in-addr.arpa" {
        type master;
        file "/etc/bind/ri.172.16.0";
};
```

db.daw.local será el fichero que contenga la definición de nuestra zona.

Nota: Se puede realizar una verificación de los ficheros de configuración y de zona por posibles fallos mediante los comandos "**named-checkconf**" y "**named-checkzone**" respectivamente.

Estos comandos suelen ejecutarse con la siguiente sintaxis:

- named-checkconf [-p] {filename}

Comprueba la sintaxis pero no la semántica de un fichero de configuración **named**. El fichero se analiza y comprueba errores de sintaxis, junto con todos los archivos incluidos en él. Si no se especifica ningún fichero, por defecto se comprueba /etc/named.conf.

- p → imprime la salida del fichero si no fueron detectados errores.

- filename → El nombre del archivo de configuración que desea comprobar.

- named-checkzone {zonename} {filename}

- named-checkzone → comprueba la sintaxis y la integridad de un archivo de zona. Realiza las mismas comprobaciones que named hace al cargar una zona. Esto hace que sea útil para comprobar los archivos de zona antes de configurarlos en un servidor de nombres.

- zonename → El nombre de dominio de la zona que se comprueba.

- filename → El nombre del archivo de zona que define la zona a comprobar.

3.3 Fichero de configuración de la zona.

Será el fichero db.daw.local. Este fichero no existe, pero podemos crearlo a partir del fichero /etc/bind/db.local, para luego modificarlo. Para ello podemos hacer una copia del mismo y a continuación modificarlo. O tambien podemos crearlo desde cero.

```
cp /etc/bind/db.local /etc/bind/db.daw.local
```

En este fichero vamos a definir algunas de las características del la zona dns así como de los equipos del dominio.

- @ representa el nombre del dominio. En nuestro caso daw.local
- A (Address). Es el registro más usado, que define una dirección IPv4 y el nombre asignado al host. Generalmente existen varios en un dominio.
- AAAA. El registro que contiene la dirección IPv6 de un dominio (a diferencia de los registros A, que enumeran la dirección IPv4).
- MX. La abreviatura MX significa mail exchange (intercambio de correo electrónico). Mediante el registro MX, y según el DNS, el cliente averigua en qué dominio se encuentra el servidor de correo electrónico adecuado. Se usa para identificar servidores de correo, se pueden definir dos o más servidores de correo para un dominio, siendo que el orden implica su prioridad. Se indica con un numero despues de MX la prioridad que tendra en el caso de existir varios servidores de correo. Numero más bajo, mayor prioridad.
- CNAME (Canonical Name). Es un alias que se asigna a un host que tiene una dirección IP valida y que responde a diversos nombres. Pueden declararse varios para un host. Reenvía un dominio o subdominio a otro dominio, NO proporciona una dirección IP
- NS (Name Server). Define los servidores de nombre principales de un dominio. Debe haber al menos uno y pueden declararse varios para un dominio.
- SOA (Start Of Authority). Este es el primer registro de la zona y sólo puede haber uno en cada archivo de la zona y sólo está presente si el servidor es autoritario del dominio. Especifica el servidor DNS primario del dominio, la cuenta de correo del administrador y tiempo de refresco de los servidores secundarios.
- 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 de la zona DNS inversa.

```
;Definición de la resolucion directa
$TTL  86400
@       IN      SOA     serverdns.daw.local. admin.daw.local. (
                        2022011500      ; Serial
                          604800        ; Refresh
                           86400 ; Retry
                          2419200       ; Expire
                          3600)  ; Negative Cache TTL
;
@               IN      NS      serverdns.
serverdns       IN      A       172.16.0.5
servidor1       IN      A       172.16.0.90
pc1             IN      A       172.16.0.150
pc2             IN      A       172.16.0.151
pc3             IN      A       172.16.0.152
pc4             IN      A       172.16.0.153
www             IN      CNAME   servidor1
ftp             IN      CNAME   servidor1
@               IN      MX   0  mail.
mail            IN      A       172.16.0.100
```

- TTL especifica el tiempo máximo que otros servidores DNS y aplicaciones deben mantener en caché ese registro. Si el valor es 0, entonces no se mantiene ningún caché.
- Serial: es un identificador del archivo, puede tener un valor arbitrario pero se recomienda que tenga la fecha con una estructura AAAA-MM-DD y un consecutivo de versión.
- Refresco: número de segundos que un servidor de nombres secundario debe esperar para comprobar de nuevo los valores de un registro.
- Reintentos: número de segundos que un servidor de nombres secundario debe esperar después de un intento fallido de recuperación de datos del servidor primario.
- Expiración: número de segundos máximo que los servidores de nombre secundarios retendrán los valores antes de expirarlos.
- TTL Negative Cache: es la cantidad de tiempo que los clientes deben almacenar en caché los resultados negativos. Si un servidor DNS busca un registro y falta, a menudo "almacenará en caché negativamente" el hecho de que falta este registro, y no intentará buscarlo nuevamente por un tiempo.

3.4 Fichero de resolución inversa

Para que nuestro servidor DNS sea capaz de llevar a cabo la resolución inversa, debemos añadir en el fichero named.conf.local la definición de la zona de resolución inversa.

```
//Definición de la zona de resolución inversa. 0.16.172
//El archivo de definición de la zona es /etc/bind/ri.172.16.0
zone "0.16.172.in-addr.arpa" {
        type master;
        file "/etc/bind/ri.172.16.0";
};
```

Del mismo modo, se debe configurar el archivo ri.172.16.0, que contendrá las resoluciones inversas de nuestra zona

```
;Resolucion inversa
$TTL  86400
@       IN      SOA     serverdns.daw.local. admin.daw.local. (
                        2015101500          ; Serial
                         604800   ; Refresh
                          86400   ; Retry
                        2419200  ; Expire
                         3600 )    ; Negative Cache TTL
;
@       IN      NS      serverdns.daw.local.
100     IN      PTR     serverdns.
90      IN      PTR     servidor1.
150     IN      PTR     pc1.
151     IN      PTR     pc2.
152     IN      PTR     pc3.
153     IN      PTR     pc4.
@       IN      PTR     mail.
```

De esta forma, quedaría definido nuestro fichero con la configuración para la resolución inversa.

3.5 Probar el funcionamiento

Mediante los comandos host, nslookup o dig, probamos el funcionamiento de nuestro servidor DNS. Solicitaremos la resolución directa e inversa al servidor, observando si el resultado es el esperado.

Ejemplos:

- host <nombre de host> host pc3.daw.local ; host ftp.daw.local
- nslookup <nombre de host> nslookup servidor1.daw.local
- host <dir IP>
- nslookup <dir IP>