

Documentación BIND9

BIND es el servidor de nombres de dominio más popular en Internet, que trabaja en todas las plataformas informáticas principales y se caracteriza por su flexibilidad y seguridad.

Domain Name Service (DNS) es el servicio que resuelve los nombres de dominio asociados a una dirección IP para “direccionar” las peticiones a un servidor en específico. Se utiliza cuando un nodo (o host) en Internet contacta a otro mediante el nombre de dominio de la máquina y no por su dirección IP.

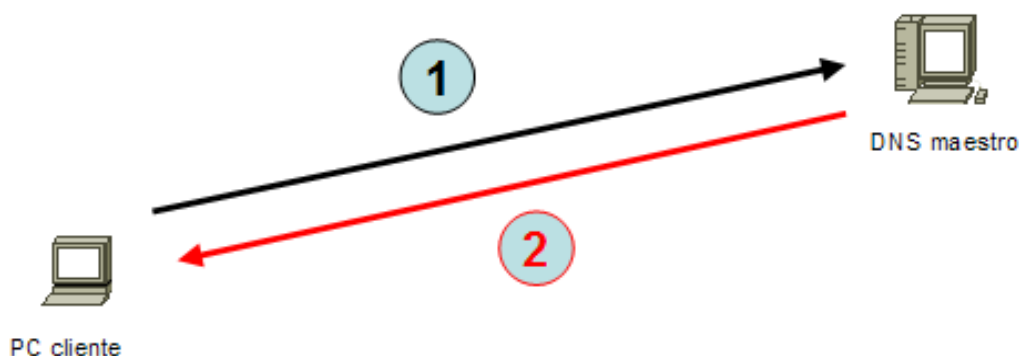
A través de este documento se verán las generalidades del servicio de resolución de nombres, la configuración y mantenimiento de un servicio de nombres con BIND, bajo la plataforma Linux, aunque la mayoría de estos conceptos se pueden aplicar a la cualquier servicio de DNS sobre otras plataformas e acceso a Internet.



1 Tipos de DNS:

1. **Master (Primario):** Aloja los registros autoritarios de una zona, responde las peticiones de resolución de nombres como servidor de **autoridad** y delega copias a los servidores esclavo.

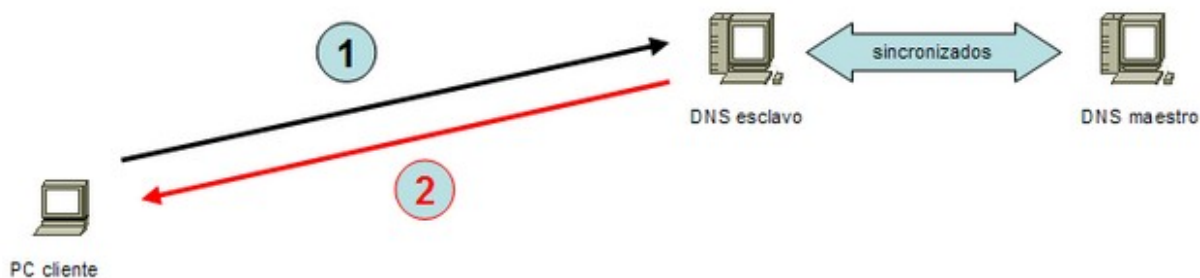
Atenderá **directamente** a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.



1 – Consulta DNS: ¿Cuál es la IP de aula5pc7.ieslapaloma.com?

2 – Respuesta DNS: La IP de aula5pc7.ieslapaloma.com es 192.168.0.107

2. **Slave (Secundario):** Responde a las peticiones de resolución de nombres como servidor de autoridad, pero la información es distribuida por los servidores primarios. Se considera que como medida de seguridad, se requiere al menos uno de estos, preferentemente independiente de la infraestructura del primario (red, energía eléctrica y ubicación geográfica).



Actuará como 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.

- 3. Caché (memòria Cau en Català):** Responde a las peticiones de resolución de nombres pero no es servidor de autoridad, las respuestas las guarda en memoria por un período de tiempo determinado.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet puesto que cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS.

2 Tipos de registros

Para ofrecer suficiente flexibilidad en la configuración, se pueden declarar diversos tipos de registros, que hacen referencia a la función del host. A continuación veremos los más importantes:

- **A (Address):** Es el registro más usado, que define una dirección IP y el nombre asignado al host. Generalmente existen varios en un dominio.
- **MX (Mail eXchanger):** 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. Debe haber al menos uno para un dominio.
- **CNAME (Canonical Name = alias):** Es un alias que se asigna a un host que tiene una dirección IP válida y que responde a diversos nombres. Pueden declararse varios para un host.
- **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.

3 Instalación y configuración

```
# sudo apt-get install bind9
```

```
# cd /etc/bind (Carpeta de configuración)
```

Archivos de configuración:

- /etc/bind/named.conf.local
- /etc/bind/db.local → cp /etc/bind/db.local /etc/bind/*.db
- /etc/bind/db.127 → cp /etc/bind/db.127 /etc/bind/*.db
- /etc/resolv.conf
- /etc/network/interfaces

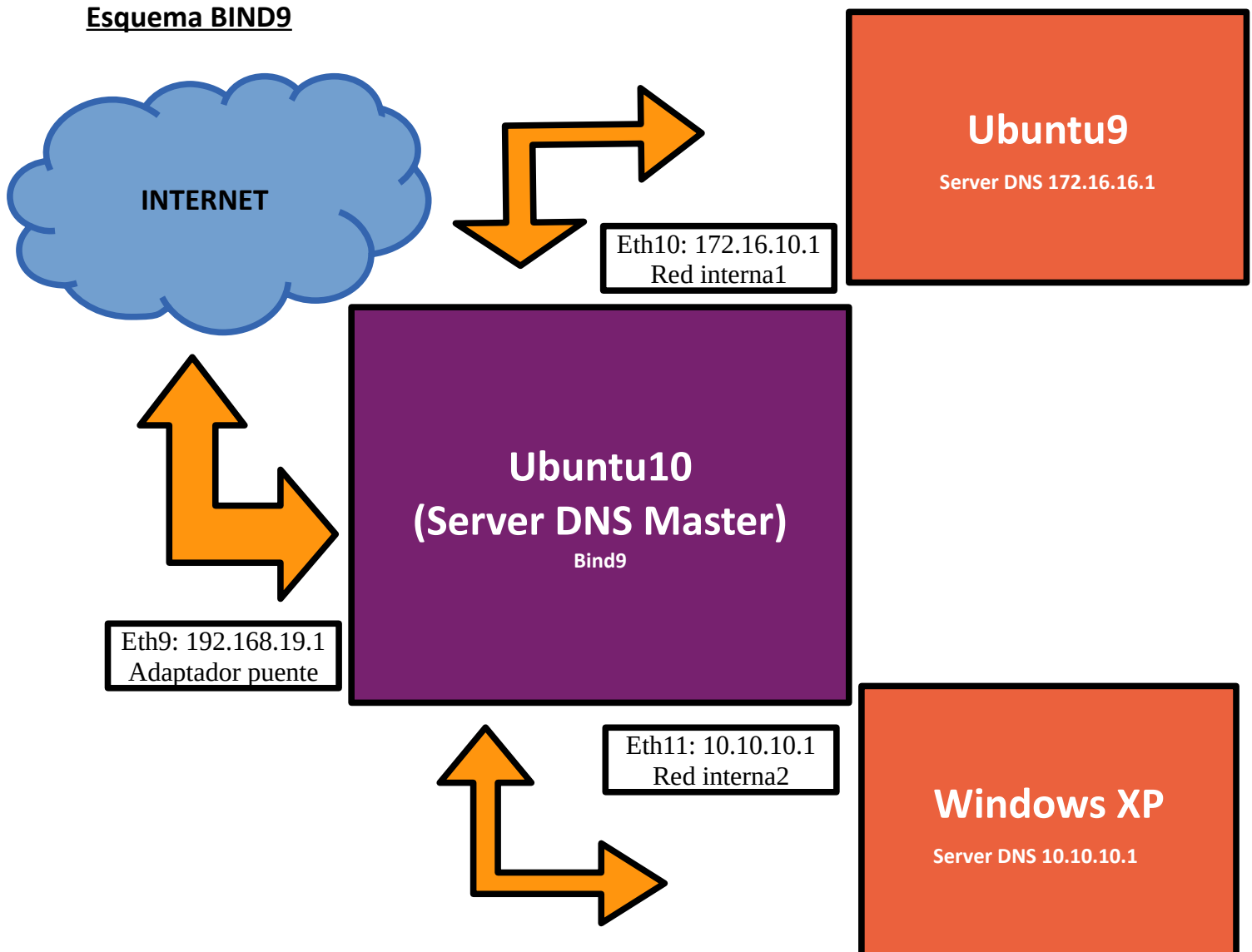
Comandos a utilizar:

- named-checkconf (Verificación de la configuración del Bind9)
- named-checkzone "zona (ejemplo.: 172.16.10.0" /etc/bind/*.db
- /etc/init.d/bind9 restart (Reiniciar el servicio bind9)
- /etc/init.d/networking restart (Reiniciar el servicio networking)
- dig (DNS lookup utility)
 - dig -x
- nslookup
 - nslookup "búsqueda directa"
 - nslookup "búsqueda inversa"
- host: es una sencilla utilidad para realizar búsquedas DNS. Normalmente se usa para convertir nombres en direcciones IP y viceversa.
- Ping (Conectividad)

Esquema VirtualBox

- **Ub10 (Bind9):**
 - Adaptador puente: eth0
 - adaptador interno: intnet1
 - adaptador interno: intnet2
- **Ub9:**
 - adaptador interno: intnet1
- **WXP:**
 - adaptador interno: intnet2

Esquema BIND9



Procedimiento

1. Abrir la máquina de Ubuntu 10.
2. Abrir una terminal con CTRL + ALT + T.
3. Acceder a modo **root**.
4. Introducir gedit **/etc/network/interfaces** e introducir la configuración similar a

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth9
iface eth9 inet static
address 192.168.19.205
gateway 192.168.19.1
netmask 255.255.255.0
network 192.168.19.0
broadcast 192.168.19.255

auto eth10
iface eth10 inet static
address 172.16.10.1
gateway 192.168.19.1
netmask 255.255.255.0
network 172.16.10.0
broadcast 172.16.10.255

auto eth11
iface eth11 inet static
address 10.10.10.1
gateway 192.168.19.1
netmask 255.255.255.0
network 10.10.10.0
broadcast 10.10.10.255
```

la imagen. Y hacemos un **RESTART**.

5. Abrimos las máquinas Ubuntu 9 (Host) y Windows XP (Host). Y modificamos el **/etc/network/interfaces** (UB9) y de forma estática en Windows XP.

Ubuntu 9

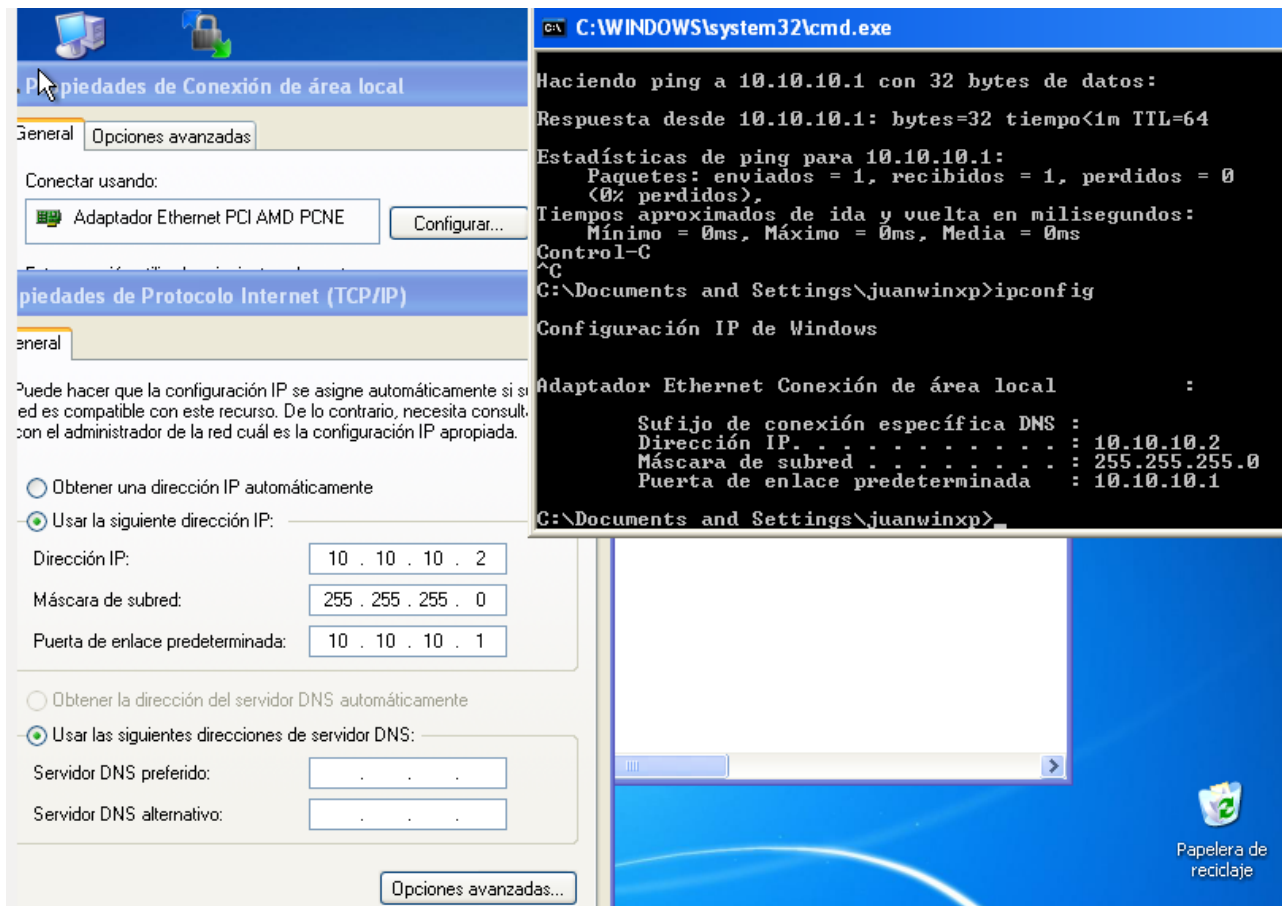
Reiniciamos el servicio. Y probamos su conexión con el Ubuntu 10 (Comando ping) al 172.16.10.1 (Gateway del UB10).

```
GN nano 2.0.9      File: /etc/net
# This file describes the network interface
# and how to activate them. For more d

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth4
iface eth4 inet static
address 172.16.10.2
gateway 172.16.10.1
netmask 255.255.255.0
network 172.16.10.0
broadcast 172.16.10.255
```

WXP



Reiniciamos el servicio (Habilitando el adaptador de red) y probando su conexión hacia su puerta de enlace.

6. Guardamos la sesión de los hosts Ubuntu 9 y Windows XP.

Configuración BIND9 (Ubuntu10)

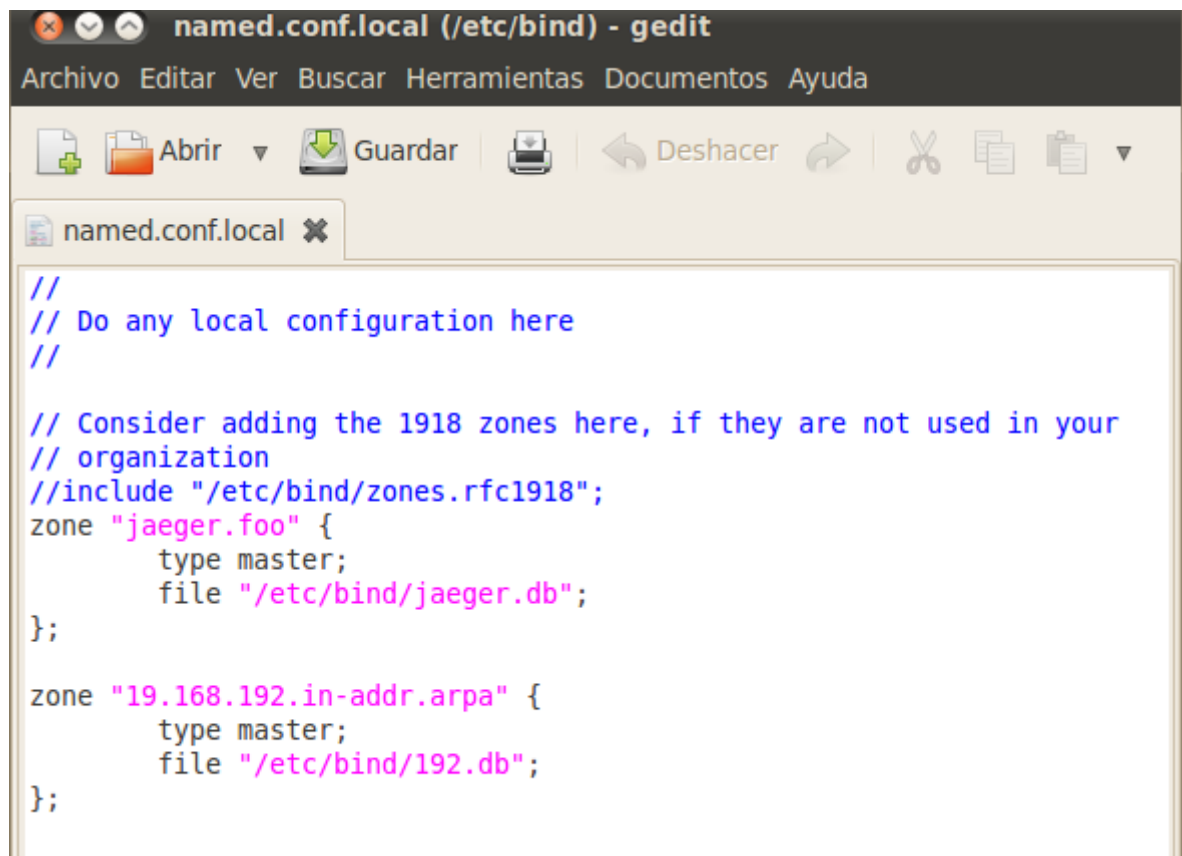
7. Abrimos el Ubuntu 10 y accedimos como #root.

8. Instalamos el servicio BIND9 #apt-get install bind9.

9. Verificamos que el servicio BIND9 está activo #service bind9 status.


10. Entramos en su carpeta “/etc/bind”.

11. Una vez dentro modificamos el archivo **named.conf.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";  
zone "jaeger.foo" {  
    type master;  
    file "/etc/bind/jaeger.db";  
};  
  
zone "19.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/192.db";  
};
```

12. Guardamos los cambios del archivo.
13. Copiamos los archivos “db.local y db.127” añadiéndoles otro nombre según se hayan establecidos en la zona del **named.conf.local**.
14. Abrimos el archivo de búsqueda directa “jaeger.db” y modificamos según la siguiente imagen:

A screenshot of a gedit window titled 'jaeger.db (/etc/bind) - gedit'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Herramientas', 'Documentos', and 'Ayuda'. Below the menu bar is a toolbar with icons for 'Abrir', 'Guardar', 'Deshacer', and other editing functions. The main text area shows the content of 'jaeger.db', which is a BIND data file for 'jaeger.foo'. It starts with a comment '; BIND data file for jaeger.foo' and a '\$TTL 604800'. The main section is an SOA record for 'jaeger.foo.' with a serial of 2, refresh of 604800, retry of 86400, expire of 2419200, and negative cache TTL of 604800. Below the SOA record are several records: an NS record for 'jaeger.foo.', an A record for '@' pointing to '192.168.19.205', an A record for 'dns' pointing to '192.168.19.205', a CNAME record for 'www' pointing to 'jaeger.foo.', and an A record for 'hostpc' pointing to '192.168.19.206'.

```
|;  
; BIND data file for jaeger.foo  
;  
$TTL      604800  
@         IN      SOA      jaeger.foo. root.jaeger.foo. (  
                                2          ; Serial  
                                604800     ; Refresh  
                                86400     ; Retry  
                                2419200    ; Expire  
                                604800 )    ; Negative Cache TTL  
  
@         IN      NS       jaeger.foo.  
@         IN      A        192.168.19.205  
dns       IN      A        192.168.19.205  
www       IN      CNAME    jaeger.foo.  
hostpc    IN      A        192.168.19.206
```

15. Abrimos el archivo de búsqueda inversa “192.db” y modificamos según la siguiente imagen:

A screenshot of a gedit window titled '192.db (/etc/bind) - gedit'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Herramientas', 'Documentos', and 'Ayuda'. Below the menu bar is a toolbar with icons for 'Abrir', 'Guardar', 'Deshacer', and other editing functions. The main text area shows the content of '192.db', which is a BIND reverse data file for 'jaeger.foo'. It starts with a comment '; BIND reverse data file for jaeger.foo' and a '\$TTL 604800'. The main section is an SOA record for 'ns.jaeger.foo.' with a serial of 1, refresh of 604800, retry of 86400, expire of 2419200, and negative cache TTL of 604800. Below the SOA record are several PTR records: an NS record for 'jaeger.foo.', a PTR record for '205' pointing to 'jaeger.foo.', a PTR record for '205' pointing to 'dns.jaeger.foo.', a PTR record for '205' pointing to 'www.jaeger.foo.', and a PTR record for '206' pointing to 'hostpc.jaeger.foo.'.

```
|;  
; BIND reverse data file for jaeger.foo  
;  
$TTL      604800  
@         IN      SOA      ns.jaeger.foo. root.jaeger.foo. (  
                                1          ; Serial  
                                604800     ; Refresh  
                                86400     ; Retry  
                                2419200    ; Expire  
                                604800 )    ; Negative Cache TTL  
  
@         IN      NS       jaeger.foo.  
205       IN      PTR      jaeger.foo.  
205       IN      PTR      dns.jaeger.foo.  
205       IN      PTR      www.jaeger.foo.  
206       IN      PTR      hostpc.jaeger.foo.
```

16. Comprobamos que la configuración del BIND9 esté correcto.

- *(named-checkconf)*

17. Comprobamos que las zonas estén correctas:

- *(named-checkzone jaeger.foo /etc/bind/jaeger.db)*
- *(named-checkzone 19.168.192.in-addr.arpa /etc/bind/192.db)*

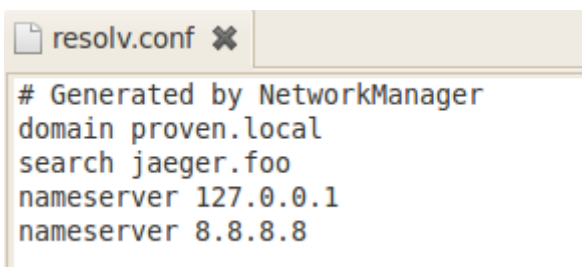
```
root@aarondns:/etc/bind# named-checkzone 19.168.192.in-addr.arpa 192.db
zone 19.168.192.in-addr.arpa/IN: loaded serial 1
OK
root@aarondns:/etc/bind#
```

18. Reiniciamos el servicio con **service bind9 restart** o **/etc/init.d/bind9 restart**

Asignación resolv.conf

Las máquinas del Ubuntu10 y Ubuntu9 revisan su archivo `/etc/resolv.conf` para poder resolver y poder realizar peticiones a sus servidores DNS establecidos en cierto archivo. Para ello se han de añadir.

Ub10



```
# Generated by NetworkManager
domain proven.local
search jaeger.foo
nameserver 127.0.0.1
nameserver 8.8.8.8
```

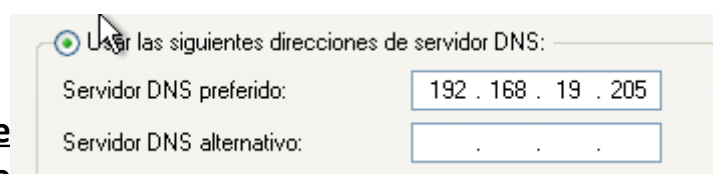
Ub9

`resolv.conf` → `nameserver 176.16.10.1`

`search jaeger.foo`

Windows XP

Verificación de resolución de nombres



Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: 192 . 168 . 19 . 205

Servidor DNS alternativo: . . .

Verificamos a que las máquinas virtuales, cuando intenten pedir una solicitud sobre la resolución de un nombre de dominio, el Ubuntu10 se la conceda.

