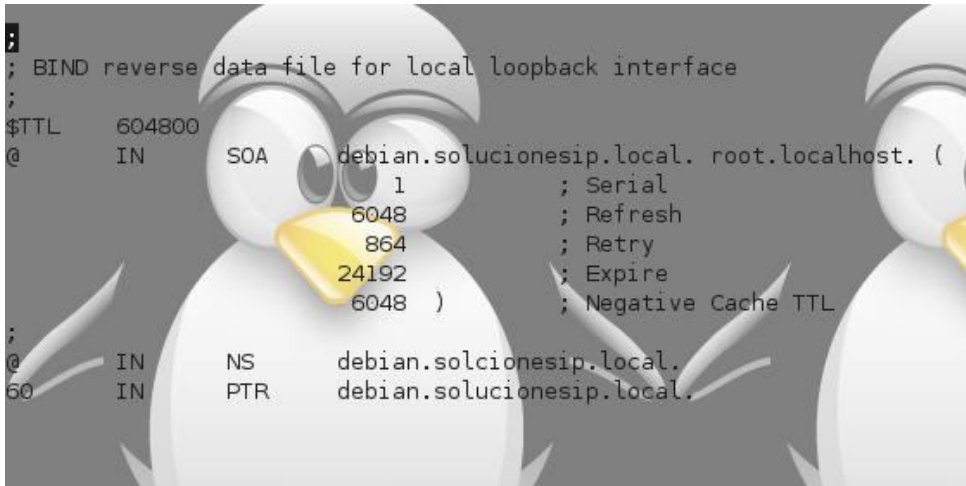


Practica linux

dns

09/06/2013



INDICE

1.-Introduccion

2.-Configuracion de red de los distintos servidores

a)Servidor DNS primario

b)Servidor secundario

3.-Instalacion servicio DNS primario

a)Configuracion DNS primario

4.-Instalacion servicio DNS secundario

a)Configuracion DNS secundario

5.-Comprobacion de errores

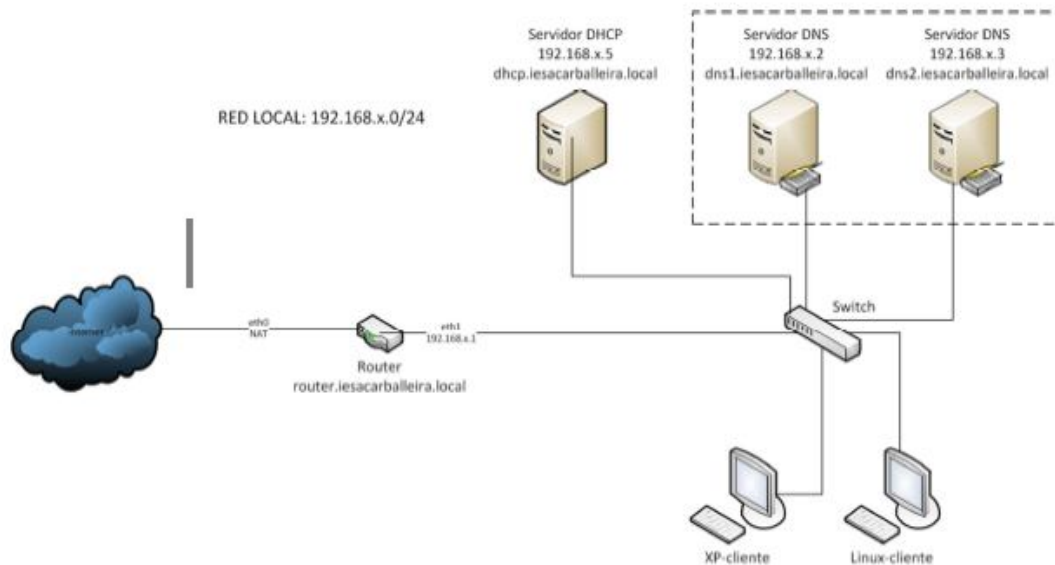
6.-Comprobacion funcionamiento servicio BIND)

7.-Actualizaciones automaticas

a)Comprobacion funcionamiento de las actualizaciones automaticas

LINUX

WINDOWS



1.-INTRODUCCION

Se va a implantar un sistema de servidores y clientes en una red local con varias máquinas virtuales. Para ello vamos a simular el funcionamiento de una red completa de ordenadores. En el programa de virtualización todas las máquinas virtuales han de estar montadas con un interfaz de red interno, esto es, sin acceso al exterior, excepto la máquina que hará las veces de enrutador, que tendrá un interfaz de red en la red interna y otro en NAT para permitir el acceso a Internet.

En la práctica anterior se procedió a la instalación de dos servidores DHCP, uno en Windows y otro en Linux, que no iban a funcionar nunca simultáneamente, con idea de que los clientes pudiesen funcionar indistintamente con uno u otro. Con la misma idea en mente se hizo exactamente lo mismo con la máquina encargada de encaminar a Internet, configurando una en Windows y otra en Linux.

En esta práctica se van a añadir dos servidores de nombres de dominio DNS, tal y como se puede observar en la figura.

El objetivo es doble:

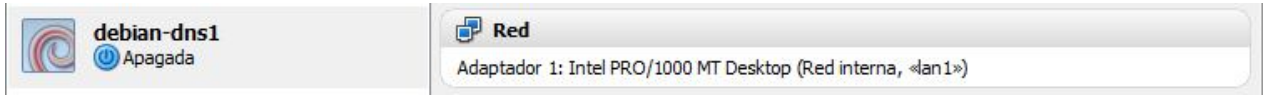
- Que sirvan de traductores de nombres para Internet.
- Que configuren un dominio local para la red interna del usuario.

En el dominio local habrá dos tipos de registros DNS para los equipos de la red interna.

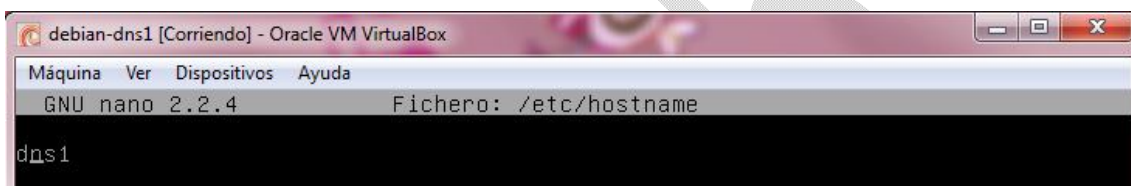
- Unos que se añadirán manualmente en el servidor primario de la zona DNS.
- Otros que serán añadidos de modo automático, función que llevarán a cabo, según sea el caso, bien los propios equipos involucrados, bien el servidor DHCP en nombre de ellos.

2.-Configuracion de red de los distintos servidores

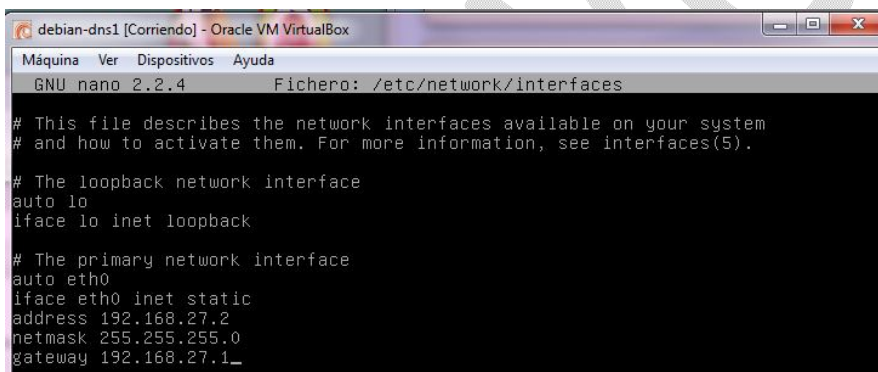
a) Servidor DNS primario (debían-dns1)



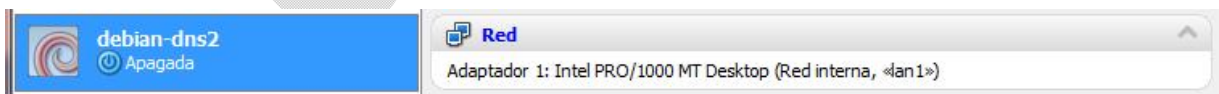
Nombre /etc/hostname



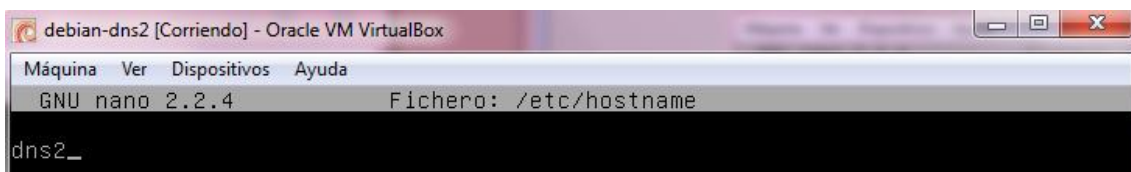
IP 192.168.27.2



b) Servidor DNS secundario (debían-dns2)

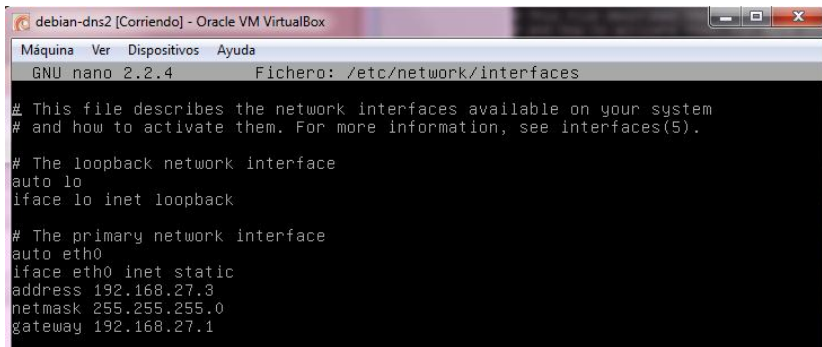


Nombre /etc/hostname



poweb

IP 192.168.27.3



```
debian-dns2 [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
GNU nano 2.2.4 Fichero: /etc/network/interfaces

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

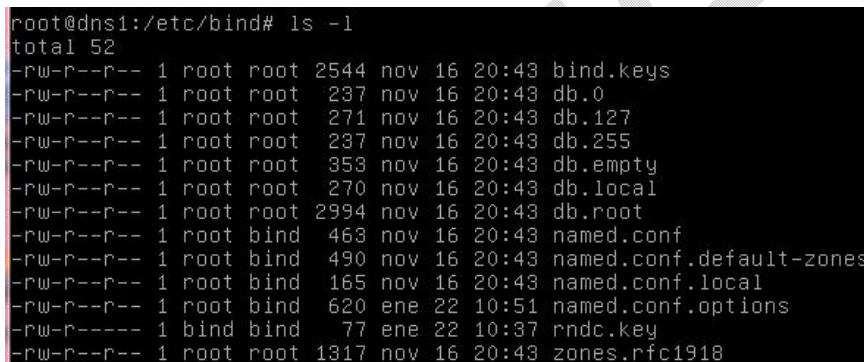
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.27.3
netmask 255.255.255.0
gateway 192.168.27.1
```

3.-Instalacion servicio DNS primario

-Instalamos el paquete bind9

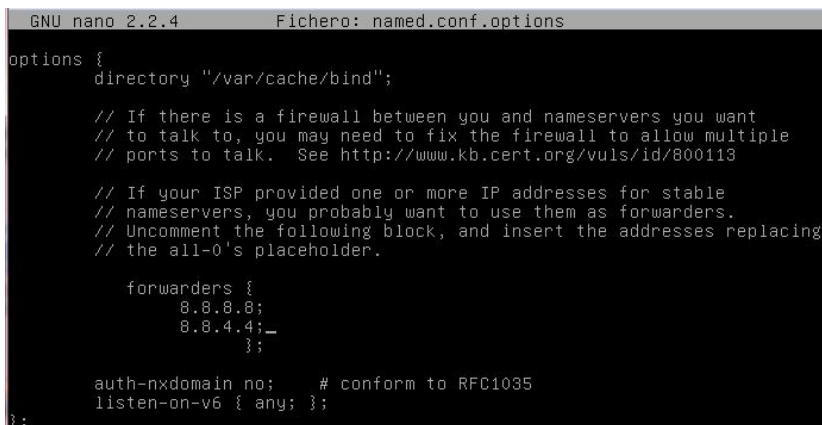
Una vez instalado el servicio DNS se crea una carpeta en “/etc/” llamada “bind” que contiene los archivos de configuración del servicio.



```
root@dns1:/etc/bind# ls -l
total 52
-rw-r--r-- 1 root root 2544 nov 16 20:43 bind.keys
-rw-r--r-- 1 root root 237 nov 16 20:43 db.0
-rw-r--r-- 1 root root 271 nov 16 20:43 db.127
-rw-r--r-- 1 root root 237 nov 16 20:43 db.255
-rw-r--r-- 1 root root 353 nov 16 20:43 db.empty
-rw-r--r-- 1 root root 270 nov 16 20:43 db.local
-rw-r--r-- 1 root root 2994 nov 16 20:43 db.root
-rw-r--r-- 1 root bind 463 nov 16 20:43 named.conf
-rw-r--r-- 1 root bind 490 nov 16 20:43 named.conf.default-zones
-rw-r--r-- 1 root bind 165 nov 16 20:43 named.conf.local
-rw-r--r-- 1 root bind 620 ene 22 10:51 named.conf.options
-rw-r----- 1 bind bind 77 ene 22 10:37 rndc.key
-rw-r--r-- 1 root root 1317 nov 16 20:43 zones.rfc1918
```

-Editamos el archivo “/etc/bind/named.conf.options”.

En este archivo se modifican los reenviadores (DNS a los que recurrirá este servidor si no da resuelto las consultas). Utilizaremos los servidores públicos de google 8.8.8.8 y 8.8.4.4



```
GNU nano 2.2.4 Fichero: named.conf.options

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
        8.8.4.4;_
    };

    auth-nxdomain no; # conform to RFC1035
    listen-on-v6 { any; };
};
```

poweb

-Archivo /etc/resolv.conf.

No es conveniente editarlo directamente ya que existen posibilidades de que la propia maquina en determinados procesos pueda sobrescribirlo alterando así la configuración correcta del servicio.

Mediante la utilidad "resolvconf" podemos hacer que la propia maquina edite el archivo tomando los parámetros configurados en el archivo "/etc/network/interfaces", archivo en el cual añadiremos ciertos parámetros justamente por este motivo.

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.27.2
netmask 255.255.255.0
gateway 192.168.27.1
dns-domain vicente.gomez
dns-nameservers 127.0.0.1
```

Instalamos resolvconf:

```
Configurando resolvconf (1.46) ...
mkdir: se ha creado el directorio «/lib/init/rw/resolvconf»
mkdir: se ha creado el directorio «/lib/init/rw/resolvconf/interface»
```

```
GNU nano 2.2.4 Fichero: /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.0.1
search vicente.gomez
```

-Modificamos /etc/hosts (donde pondremos el nombre de la maquina)

```
GNU nano 2.2.4 Fichero: /etc/hosts
127.0.0.1 localhost
192.168.27.2 dns1.vicente.gomez dns1

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

-Reiniciamos bind

```
root@dns1:/home/vicente# /etc/init.d/bind9 restart
Stopping domain name service...: bind9 waiting for pid 1001 to die.
Starting domain name service...: bind9.
root@dns1:/home/vicente#
```

poweb

-Reiniciamos la red

```
Reconfiguring network interfaces...done.  
root@dns1:/home/vicente# _
```

Prueba del funcionamiento de Bind9 con el comando "dig"

```
root@dns1:/home/vicente# dig www.marca.com_
```

```
; <<> DiG 9.7.3 <<> www.marca.com  
; global options: +cmd  
; Got answer:  
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45182  
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 0  
  
; QUESTION SECTION:  
www.marca.com.                IN      A  
  
; ANSWER SECTION:  
www.marca.com.                5216    IN      A      193.110.128.199
```

```
; AUTHORITY SECTION:  
.                25318   IN      NS      1.root-servers.net.  
.                25318   IN      NS      f.root-servers.net.  
.                25318   IN      NS      m.root-servers.net.  
.                25318   IN      NS      j.root-servers.net.  
.                25318   IN      NS      g.root-servers.net.  
.                25318   IN      NS      h.root-servers.net.  
.                25318   IN      NS      c.root-servers.net.  
.                25318   IN      NS      e.root-servers.net.  
.                25318   IN      NS      d.root-servers.net.  
.                25318   IN      NS      b.root-servers.net.  
.                25318   IN      NS      i.root-servers.net.  
.                25318   IN      NS      a.root-servers.net.  
.                25318   IN      NS      k.root-servers.net.  
  
; Query time: 0 msec  
; SERVER: 127.0.0.1#53(127.0.0.1)  
; WHEN: Sun Jan 22 11:31:07 2012  
; MSG SIZE rcvd: 258
```

a) Configuración DNS primario

Usaremos como dominio "vicente.gomez"

-Editamos /etc/bind/named.conf.local

```
zone "vicente.gomez" {  
    type master;  
    file "/etc/bind/db.vicente.gomez";  
};
```

Hemos creado la zona y la hemos configurado, a continuación crearemos un archivo específico para esa zona que contendrá los registros de algunas las maquinas del dominio, servidores con alguna función específica, el resto de maquinas del dominio (clientes) se registraran a través de las actualizaciones automáticas.

-archivo /etc/bind/db.vicente.gomez

```
GNU nano 2.2.4      Fichero: /etc/bind/db.vicente.gomez
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA    vicente.gomez. root.vicente.gomez. (
        2          ; Serial
        604800     ; Refresh
        86400     ; Retry
        2419200   ; Expire
        604800 )   ; Negative Cache TTL
;
@       IN      NS     dns1.vicente.gomez.
@       IN      NS     dns2.vicente.gomez.
@       IN      A      192.168.27.2
@       IN      A      192.168.27.3
@       IN      AAAA   ::1
dns1    IN      A      192.168.27.2
dns2    IN      A      192.168.27.3
dhcp    IN      A      192.168.27.5
router  IN      A      192.168.27.1
[ 20 líneas leídas ]
^G Ver ayuda  ^O Guardar  ^R Leer Fich ^Y Pág Ant  ^K CortarTxt ^C Pos actual
^X Salir     ^J Justificar ^W Buscar    ^V Pág Sig  ^U PegarTxt  ^T Ortografía
```

```
root@dns1:/home/vicente# ls /etc/bind -l
total 56
-rw-r--r-- 1 root root 2544 nov 16 20:43 bind.keys
-rw-r--r-- 1 root root 237  nov 16 20:43 db.0
-rw-r--r-- 1 root root 271  nov 16 20:43 db.127
-rw-r--r-- 1 root root 237  nov 16 20:43 db.255
-rw-r--r-- 1 root root 353  nov 16 20:43 db.empty
-rw-r--r-- 1 root root 270  nov 16 20:43 db.local
-rw-r--r-- 1 root root 2994 nov 16 20:43 db.root
-rw-r--r-- 1 root bind 427  ene 22 12:18 db.vicente.gomez
-rw-r--r-- 1 root bind 463  nov 16 20:43 named.conf
-rw-r--r-- 1 root bind 490  nov 16 20:43 named.conf.default-zones
-rw-r--r-- 1 root bind 264  ene 22 11:59 named.conf.local
-rw-r--r-- 1 root bind 620  ene 22 10:51 named.conf.options
-rw-r----- 1 bind bind 77   ene 22 10:37 rndc.Key
-rw-r--r-- 1 root root 1317 nov 16 20:43 zones.rfc1918
```

El instructivo TTL (Time To Live) indica la validez (en segundos) de la consulta, tras la cual deberá ejecutarse una actualización. 604800 segundos equivalen a una semana. El número Serial debería incrementarse cada vez que se modifica la zona. El campo Refresh indica el intervalo de tiempo que los DNS secundarios deben refrescar la información del archivo de zona si han habido cambios (10 segundos). Retry indica el intervalo de tiempo que los DNS secundarios deben reintentar actualizar la información si el DNS primario no responde (1 minuto). Expire indica el tiempo que el DNS secundario expira como servidor de nombres de la zona en caso el DNS primario no responda a requerimiento de actualización (4 semanas). Negative Cache TTL indica el TTL en caso de una consulta con respuesta negativa (20 minutos).

Crearemos las zonas de búsqueda inversa de la misma manera:

-Editamos /etc/bind/named.conf.local creando esta vez una zona de búsqueda inversa:

```
zone "27.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.27.168.192";
};
```


poweb

-Editamos el archivo de búsqueda inversa /etc/bind/db.27.168.192 incluyendo todas las maquinas que deseemos.

```
GNU nano 2.2.4 Fichero: /etc/bind/db.27.168.192
:
: BIND reverse data file for local loopback interface
:
:TTL      604800
@        IN      SOA      vicente.gomez. root.vicente.gomez. (
;
;      1          ; Serial
;      604800     ; Refresh
;      86400     ; Retry
;      2419200  ; Expire
;      604800 )   ; Negative Cache TTL
;
@        IN      NS      dns1.vicente.gomez.
@        IN      PTR     dns2.vicente.gomez.
2        IN      PTR     dns1.vicente.gomez.
3        IN      PTR     dns2.vicente.gomez.
1        IN      PTR     router.vicente.gomez.
5        IN      PTR     dhcp.vicente.gomez.

[ 17 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^D Pos actual
^X Salir ^U Justificar ^N Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

-Reiniciamos servicio Bind9

```
root@dns1:/home/vicente# /etc/init.d/bind9 restart
Stopping domain name service...: bind9.
Starting domain name service...: bind9.
```

4.-Instalacion servicio DNS secundario

-Comprobamos el archivo /etc/hosts (que contenga el nombre de este servidor)

```
GNU nano 2.2.4 Fichero: /etc/hosts
127.0.0.1    localhost
192.168.27.3 dns2.vicente.gomez    dns2

# The following lines are desirable for IPv6 capable hosts
::1         ip6-localhost ip6-loopback
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

-Instalación de bind9

```
Añadiendo el usuario del sistema `bind' (UID 103) ...
Añadiendo un nuevo usuario `bind' (UID 103) con grupo `bind' ...
No se crea el directorio personal `/var/cache/bind'.
wrote key file "/etc/bind/rndc.key"
#
Starting domain name service...: bind9.
root@dns2:/home/vicente# _
```

poweb

Instalaremos el paquete "resolvconf" para configurar automáticamente el archivo /etc/resolv.conf (este proceso debemos hacerlo en todas las maquinas), previa configuración del archivo /etc/network/interfaces con los parámetros correspondientes.

-/etc/network/interfaces

```
GNU nano 2.2.4 Fichero: /etc/network/interfaces Modificado
# 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 eth0
iface eth0 inet static
address 192.168.27.3
netmask 255.255.255.0
gateway 192.168.27.1
dns-domain vicente.gomez
dns-nameservers 192.168.27.3 192.168.27.2_
```

```
GNU nano 2.2.4 Fichero: /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN

search vicente.gomez
nameserver 192.168.27.2
nameserver 192.168.27.3
```

-Archivo /etc/bind/named.conf.options

Incluiremos otra vez los servidores públicos de Google

```
GNU nano 2.2.4 Fichero: /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
        8.8.4.4;_
    };

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
```

poweb

-Reiniciamos el servicio Bind9

```
Stopping domain name service...: bind9 waiting for pid 944 to die.  
Starting domain name service...: bind9.  
root@dns2:/home/vicente# _
```

-Reiniciamos configuración de red

```
Reconfiguring network interfaces...done.  
root@dns2:/home/vicente# _
```

-Comprobamos el buen funcionamiento del servicio con el comando "dig"

```
; <<>> DiG 9.7.3 <<>> www.marca.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 276  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;www.marca.com.                IN      A  
  
;; ANSWER SECTION:  
www.marca.com.                50      IN      A      193.110.128.199
```

```
;; AUTHORITY SECTION:  
.                20213   IN      NS      k.root-servers.net.  
.                20213   IN      NS      b.root-servers.net.  
.                20213   IN      NS      f.root-servers.net.  
.                20213   IN      NS      c.root-servers.net.  
.                20213   IN      NS      a.root-servers.net.  
.                20213   IN      NS      g.root-servers.net.  
.                20213   IN      NS      l.root-servers.net.  
.                20213   IN      NS      m.root-servers.net.  
.                20213   IN      NS      i.root-servers.net.  
.                20213   IN      NS      d.root-servers.net.  
.                20213   IN      NS      j.root-servers.net.  
.                20213   IN      NS      h.root-servers.net.  
.                20213   IN      NS      e.root-servers.net.  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Sun Jan 22 12:56:10 2012  
;; MSG SIZE rcvd: 258
```

a) Configuración DNS secundario

-Editamos /etc/bind/named.conf.local en el DNS PRIMARIO agregando "allow-transfer" que es la sentencia que permite la transferencia de zona, es decir, el intercambio de información relativa al servicio entre el DNS primario y el secundario(la incluiremos en las dos zonas).

poweb

```
GNU nano 2.2.4 Fichero: /etc/bind/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 "vicente.gomez" {
    type master;
    file "/etc/bind/db.vicente.gomez";
    allow-transfer { 192.168.27.3; };
};

zone "27.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.27.168.192";
    allow-transfer { 192.168.27.3; };
};

[ 20 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

-Editamos /etc/bind/named.conf.local esta vez en el servidor secundario, creamos las zonas (búsqueda directa e inversa) como en el servidor primario, agregamos además "masters" con la correspondiente IP del servidor primario (maestro).

```
GNU nano 2.2.4 Fichero: /etc/bind/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 "vicente.gomez" {
    type slave;
    file "/etc/bind/db.vicente.gomez";
    masters {192.168.27.2; };
};

zone "27.168.192.in-addr.arpa" {
    type slave;
    file "/etc/bind/db.27.168.192";
    masters {192.168.27.2; };
};

[ 22 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

-El usuario de sistema bind en el DNS secundario necesita permisos para modificar archivos en el directorio /etc/bind

Antes

```
drwxr-sr-x 2 root bind 4096 ene 22 12:38 bind
```

poweb

```
root@dns2:/home/vicente# chmod g+ws /etc/bind
root@dns2:/home/vicente# _
```

Después

```
drwxrwsr-x 2 root bind 4096 ene 22 12:38 bind
```

-Reiniciamos el servicio bind9

```
Stopping domain name service...: bind9 waiting for pid 1003 to die.
Starting domain name service...: bind9.
root@dns2:/home/vicente#
```

-Comprobamos que los archivos de configuración del dominio se transfieren

-/etc/bind en el servidor primario

```
root@dns1:/home/vicente# ls /etc/bind -l
total 60
-rw-r--r-- 1 root root 2544 nov 16 20:43 bind.keys
-rw-r--r-- 1 root root 237 nov 16 20:43 db.0
-rw-r--r-- 1 root root 271 nov 16 20:43 db.127
-rw-r--r-- 1 root root 237 nov 16 20:43 db.255
-rw-r--r-- 1 root bind 411 feb 5 11:07 db.27.168.192
-rw-r--r-- 1 root root 353 nov 16 20:43 db.empty
-rw-r--r-- 1 root root 270 nov 16 20:43 db.local
-rw-r--r-- 1 root root 2994 nov 16 20:43 db.root
-rw-r--r-- 1 root bind 460 feb 5 11:06 db.vicente.gomez
-rw-r--r-- 1 root bind 463 nov 16 20:43 named.conf
-rw-r--r-- 1 root bind 490 nov 16 20:43 named.conf.default-zones
-rw-r--r-- 1 root bind 398 feb 4 18:11 named.conf.local
-rw-r--r-- 1 root bind 577 ene 27 17:04 named.conf.options
-rw-r----- 1 bind bind 77 ene 27 16:56 rndc.key
-rw-r--r-- 1 root root 1317 nov 16 20:43 zones.rfc1918
```

```
GNU nano 2.2.4 Fichero: /etc/bind/db.vicente.gomez
$ORIGIN .
$TTL 604800 ; 1 week
vicente.gomez IN SOA vicente.gomez. root.vicente.gomez. (
                2 ; serial
                604800 ; refresh (1 week)
                86400 ; retry (1 day)
                2419200 ; expire (4 weeks)
                604800 ; minimum (1 week)
                )
                NS vicente.gomez.
                A 192.168.27.2
                AAAA ::1
$ORIGIN vicente.gomez.
dhcp A 192.168.27.5
dns2 A 192.168.27.3
router A 192.168.27.1
```

-/etc/bind en el servidor secundario

```
root@dns2:/home/vicente# ls /etc/bind -l
total 60
-rw-r--r-- 1 root root 2544 nov 16 20:43 bind.keys
-rw-r--r-- 1 root root 237 nov 16 20:43 db.0
-rw-r--r-- 1 root root 271 nov 16 20:43 db.127
-rw-r--r-- 1 root root 237 nov 16 20:43 db.255
-rw-r--r-- 1 bind bind 462 feb 5 11:09 db.27.168.192
-rw-r--r-- 1 root root 353 nov 16 20:43 db.empty
-rw-r--r-- 1 root root 270 nov 16 20:43 db.local
-rw-r--r-- 1 root root 2994 nov 16 20:43 db.root
-rw-r--r-- 1 bind bind 395 feb 5 10:45 db.vicente.gomez
-rw-r--r-- 1 root bind 463 nov 16 20:43 named.conf
-rw-r--r-- 1 root bind 490 nov 16 20:43 named.conf.default-zones
-rw-r--r-- 1 root bind 382 feb 4 19:02 named.conf.local
-rw-r--r-- 1 root bind 588 ene 22 14:16 named.conf.options
-rw-r----- 1 bind bind 77 ene 22 12:38 rndc.key
-rw-r--r-- 1 root root 1317 nov 16 20:43 zones.rfc1918
```

```

GNU nano 2.2.4      Fichero: /etc/bind/db.27.168.192
$ORIGIN .
$TTL 604800      ; 1 week
27.168.192.in-addr.arpa IN SOA  vicente.gomez. root.vicente.gomez. (
                                1          ; serial
                                604800     ; refresh (1 week)
                                86400     ; retry (1 day)
                                2419200   ; expire (4 weeks)
                                604800     ; minimum (1 week)
                                )
                                NS      dns1.vicente.gomez.
                                PTR     dns2.vicente.gomez.
$ORIGIN 27.168.192.in-addr.arpa.
1          PTR     router.vicente.gomez.
2          PTR     dns1.vicente.gomez.
3          PTR     dns2.vicente.gomez.
5          PTR     dhcp.vicente.gomez.

```

5.-COMPROBACION DE ERRORES

A partir de la versión 9 de **BIND** se incluyen dos herramientas software para chequear la sintaxis y semántica de los archivos que describen las zonas y el archivo de configuración principal named.conf. Dichas herramientas son: **named-checkzone** y **named-checkconf**. Y las usamos de la siguiente manera:

sudo named-checkconf

```

root@dns1:/home/vicente# named-checkconf
root@dns1:/home/vicente# _

```

La salida muestra los errores que genera. Si no genera salida, está todo correcto.

sudo named-checkzone vicente.gomez /etc/bind/db.vicente.gomez

```

root@dns1:/home/vicente# named-checkzone vicente.gomez /etc/bind/db.vicente.gomez
zone vicente.gomez/IN: loaded serial 2
OK
root@dns1:/home/vicente# _

```

Este comando genera la siguiente salida si todo está correcto: zone Vicente.gomez/IN:loaded serial 1 OK

sudo named-checkzone 27.168.192.in-addr.arpa /etc/bind/db.27.168.192

```

root@dns1:/home/vicente# named-checkzone 27.168.192.in-addr.arpa /etc/bind/db.27.168.192
zone 27.168.192.in-addr.arpa/IN: loaded serial 1
OK
root@dns1:/home/vicente# _

```

poweb

6.-COMPROBACION DEL SERVICIO BIND9

-nslookup dhcp.vicente.gomez (desde dns1)

```
root@dns1:/home/vicente# nslookup dhcp.vicente.gomez
Server:          192.168.27.2
Address:         192.168.27.2#53

Name:   dhcp.vicente.gomez
Address: 192.168.27.5
```

-dig dhcp.vicente.gomez (desde dns1)

```
; <<>> DiG 9.7.3 <<>> dhcp.vicente.gomez
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38793
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;dhcp.vicente.gomez.          IN      A

;; ANSWER SECTION:
dhcp.vicente.gomez.         604800 IN      A      192.168.27.5

;; AUTHORITY SECTION:
vicente.gomez.             604800 IN      NS     dns2.vicente.gomez.
vicente.gomez.             604800 IN      NS     dns1.vicente.gomez.

;; ADDITIONAL SECTION:
dns1.vicente.gomez.        604800 IN      A      192.168.27.2
dns2.vicente.gomez.        604800 IN      A      192.168.27.3

;; Query time: 1 msec
;; SERVER: 192.168.27.2#53(192.168.27.2)
;; WHEN: Sun Feb  5 11:51:21 2012
;; MSG SIZE rcvd: 122
```

-nslookup 192.168.27.5 (desde dns2)

```
root@dns2:/home/vicente# nslookup 192.168.27.5
Server:          192.168.27.2
Address:         192.168.27.2#53

5.27.168.192.in-addr.arpa    name = dhcp.vicente.gomez.
```

-host 192.168.27.1 (desde dns2)

```
root@dns2:/home/vicente# host 192.168.27.1
1.27.168.192.in-addr.arpa domain name pointer router.vicente.gomez.
```

poweb

-dig router.vicente.gomez (desde dns2)

```
; <<> DiG 9.7.3 <<> router.vicente.gomez
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47478
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
router.vicente.gomez.      IN      A

;; ANSWER SECTION:
router.vicente.gomez.    604800 IN      A      192.168.27.1

;; AUTHORITY SECTION:
vicente.gomez.          604800 IN      NS     dns2.vicente.gomez.
vicente.gomez.          604800 IN      NS     dns1.vicente.gomez.

;; ADDITIONAL SECTION:
dns1.vicente.gomez.     604800 IN      A      192.168.27.2
dns2.vicente.gomez.     604800 IN      A      192.168.27.3

;; Query time: 0 msec
;; SERVER: 192.168.27.2#53(192.168.27.2)
```

7.-ACTUALIZACIONES AUTOMATICAS

Comenzaremos modificando los archivos /etc/bind/name.conf de ambos servidores bind añadiéndole la siguiente línea:

-allow-update {127.0.0.1; 192.168.27.0/24};

```
zone "vicente.gomez" {
    type master;
    file "/etc/bind/db.vicente.gomez";
    allow-transfer { 192.168.27.3; };
    allow-update { 127.0.0.1;
                  192.168.27.0/24; };
};
```

```
zone "27.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.27.168.192";
    allow-transfer { 192.168.27.3; };
    allow-update { 127.0.0.1;
                  192.168.27.0/24; };
};
```

El segundo paso será modificar el archivo /etc/dhcp/dhcp.conf del servidor dhcp para que sea este quien le notifique a los servidores bind los nuevos cambios en los equipos de la red (en el caso de que los propios equipos no lo hagan).

Agregaremos las siguientes líneas:

-ddns-updates on;

Activa la actualización automática al DNS.

poweb

ddns-domainname "zonadirecta.com";

Indica el dominio en el que se actualizan los DNS

ddns-rev-domainname "168.192.in-addr.arpa";

Indica la zona inversa que quiero actualizar dinámicamente.

ddns-update-style interim;

Esta línea indica el método de actualización DNS automática

```
allow-unknown-clients;
authoritative;
ddns-updates on;
ddns-update-style interim;
ddns-domainname "vicente.gomez";
ddns-rev-domainname "27.168.192.in-addr.arpa";
send host-name "hostname";

subnet 192.168.27.0 netmask 255.255.255.0 {
```

-Reiniciamos el servicio dhcp

```
Stopping ISC DHCP server: dhcpd.
Starting ISC DHCP server: dhcpd.
root@debian1:~# _
```

Podemos comprobar que las actualizaciones automáticas se están realizando porque en /etc/bind se añaden unos archivos con extensión .jnl que son los que contienen información sobre cualquier modificación que se haga en los equipos del dominio.

```
root@dns1:/home/vicente# ls /etc/bind -l
total 68
-rw-r--r-- 1 root root 2544 nov 16 20:43 bind.keys
-rw-r--r-- 1 root root 237 nov 16 20:43 db.0
-rw-r--r-- 1 root root 271 nov 16 20:43 db.127
-rw-r--r-- 1 root root 237 nov 16 20:43 db.255
-rw-r--r-- 1 root bind 394 feb 5 12:33 db.27.168.192
-rw-r--r-- 1 bind bind 792 feb 5 13:15 db.27.168.192.jnl
-rw-r--r-- 1 root root 353 nov 16 20:43 db.empty
-rw-r--r-- 1 root root 270 nov 16 20:43 db.local
-rw-r--r-- 1 root root 2994 nov 16 20:43 db.root
-rw-r--r-- 1 root bind 450 feb 5 12:34 db.vicente.gomez
-rw-r--r-- 1 bind bind 813 feb 5 13:15 db.vicente.gomez.jnl
-rw-r--r-- 1 root bind 463 nov 16 20:43 named.conf
-rw-r--r-- 1 root bind 490 nov 16 20:43 named.conf.default-zones
-rw-r--r-- 1 root bind 494 feb 5 12:47 named.conf.local
-rw-r--r-- 1 root bind 577 ene 27 17:04 named.conf.options
-rw-r----- 1 bind bind 77 ene 27 16:56 rndc.key
-rw-r--r-- 1 root root 1317 nov 16 20:43 zones.rfc1918
```

a) Comprobación funcionamiento actualizaciones automáticas

LINUX

Modificaremos el nombre de la maquina 'ubuntu-seri' .Pasara de llamarse 'vicente-ubu' a 'clienteubu'

-Registro de 'vicente-ubu' en el archivo /var/lib/dhcp/dhcpd.leases del servidor dhcp

```
lease 192.168.27.51 {
  starts 0 2012/02/05 12:15:20;
  ends 0 2012/02/05 13:15:20;
  tstp 0 2012/02/05 13:15:20;
  cltt 0 2012/02/05 12:15:20;
  binding state active;
  next binding state free;
  hardware ethernet 08:00:27:2d:74:44;
  set ddns-fwd-name = "vicente-ubu.vicente.gomez";
  set ddns-txt = "003e1337f2c4fa017dcd53f5131bdcc8cd";
  set ddns-rev-name = "51.27.168.192.27.168.192.in-addr.arpa";
}

client-hostname "vicente-ubu";
```

-Le cambiamos el nombre por 'clienteubu' y actualiza el registro

```
lease 192.168.27.51 {
  starts 0 2012/02/05 12:29:35;
  ends 0 2012/02/05 13:29:35;
  cltt 0 2012/02/05 12:29:35;
  binding state active;
  next binding state free;
  hardware ethernet 08:00:27:2d:74:44;
  set ddns-fwd-name = "clienteubu.vicente.gomez";
  set ddns-txt = "003e1337f2c4fa017dcd53f5131bdcc8cd";
  set ddns-rev-name = "51.27.168.192.27.168.192.in-addr.arpa";
  client-hostname "clienteubu";
}
```

Esta modificación se manda al servidor bind y actualiza los registros correspondientes:

-dig clienteubu.vicente.gomez

```
; <<> DiG 9.7.3 <<> clienteubu.vicente.gomez
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 1591
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
clienteubu.vicente.gomez.      IN      A

;; ANSWER SECTION:
clienteubu.vicente.gomez. 1800 IN      A      192.168.27.51

;; AUTHORITY SECTION:
vicente.gomez.          604800 IN      NS      dns2.vicente.gomez.
vicente.gomez.          604800 IN      NS      dns1.vicente.gomez.

;; ADDITIONAL SECTION:
dns1.vicente.gomez.     604800 IN      A      192.168.27.2
dns2.vicente.gomez.     604800 IN      A      192.168.27.3

;; Query time: 0 msec
;; SERVER: 192.168.27.2#53(192.168.27.2)
;; WHEN: Sun Feb  5 13:46:51 2012
```

poweb

Como podemos comprobar el servicio funciona correctamente con las nuevas modificaciones

También se modifican los archivos de zona, que ahora incluirá las maquinas asignadas por dhcp

```
GNU nano 2.2.4 Fichero: /etc/bind/db.vicente.gomez
$ORIGIN .
$TTL 604800 ; 1 week
vicente.gomez IN SOA vicente.gomez. root.vicente.gomez. (
    6 ; serial
    10 ; refresh (10 seconds)
    60 ; retry (1 minute)
    2419200 ; expire (4 weeks)
    604800 ; minimum (1 week)
)
    NS dns1.vicente.gomez.
    NS dns2.vicente.gomez.
    A 192.168.27.2
    A 192.168.27.3
    AAAA ::1
$ORIGIN vicente.gomez.
$TTL 1800 ; 30 minutes
clienteubu A 192.168.27.51
TXT "003e1337f2c4fa017dcd53f5131bdcc8cd"
$TTL 604800 ; 1 week
dhcp A 192.168.27.5
dns1 A 192.168.27.2
dns2 A 192.168.27.3
router A 192.168.27.1
```

WINDOWS

Modificaremos el nombre 'xp' por 'clientexp'. A continuación se muestran los registros originales de 'xp' en el archivo /var/lib/dhcp/dhcpd.leases en el servidor dhcp:

-antes de modificar ('xp')

```
lease 192.168.27.50 {
  starts 0 2012/02/05 12:51:40;
  ends 0 2012/02/05 13:51:40;
  cltt 0 2012/02/05 12:51:40;
  binding state active;
  next binding state free;
  hardware ethernet 08:00:27:70:55:41;
  uid "\001\010\000'pUA";
  set ddns-rev-name = "50.27.168.192.27.168.192.in-addr.arpa";
  set ddns-client-fqdn = "xp.vicente.gomez";
  client-hostname "xp";
}
```

-despues de modificar el nombre ('clientexp')

```
lease 192.168.27.50 {
  starts 0 2012/02/05 13:00:12;
  ends 0 2012/02/05 14:00:12;
  cltt 0 2012/02/05 13:00:12;
  binding state active;
  next binding state free;
  hardware ethernet 08:00:27:70:55:41;
  uid "\001\010\000'pUA";
  set ddns-rev-name = "50.27.168.192.27.168.192.in-addr.arpa";
  set ddns-client-fqdn = "clientexp.vicente.gomez";
  client-hostname "clientexp";
}
```

poweb

-dig clientexp.vicente.gomez

```
; <<>> DiG 9.7.3 <<>> clientexp.vicente.gomez
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58818
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

; QUESTION SECTION:
clientexp.vicente.gomez.      IN      A

; ANSWER SECTION:
clientexp.vicente.gomez. 1200    IN      A      192.168.27.50

; AUTHORITY SECTION:
vicente.gomez.          604800  IN      NS      dns1.vicente.gomez.
vicente.gomez.          604800  IN      NS      dns2.vicente.gomez.

; ADDITIONAL SECTION:
dns1.vicente.gomez.     604800  IN      A      192.168.27.2
dns2.vicente.gomez.     604800  IN      A      192.168.27.3

; Query time: 1 msec
; SERVER: 192.168.27.2#53(192.168.27.2)
; WHEN: Sun Feb  5 14:03:24 2012
--More--
```

-Archivos de zona en el servidor bind, tanto directa como inversa

```
GNU nano 2.2.4      Fichero: /etc/bind/db.vicente.gomez
$ORIGIN .
$TTL 604800      ; 1 week
vicente.gomez   IN SOA  vicente.gomez. root.vicente.gomez. (
                    9      ; serial
                    10     ; refresh (10 seconds)
                    60     ; retry (1 minute)
                    2419200 ; expire (4 weeks)
                    604800 ; minimum (1 week)
                )
                NS      dns1.vicente.gomez.
                NS      dns2.vicente.gomez.
                A      192.168.27.2
                A      192.168.27.3
                AAAA   ::1
$ORIGIN vicente.gomez.
$TTL 1800      ; 30 minutes
clienteubu     A      192.168.27.51
               TXT     "003e1337f2c4fa017dcd53f5131bdcc8cd"
$TTL 1200      ; 20 minutes
clientexp      A      192.168.27.50
$TTL 604800    ; 1 week
dhcp           A      192.168.27.5
dns1           A      192.168.27.2
dns2           A      192.168.27.3
router        A      192.168.27.1
```

```
GNU nano 2.2.4      Fichero: /etc/bind/db.27.168.192
$ORIGIN .
$TTL 604800          ; 1 week
27.168.192.in-addr.arpa IN SOA  vicente.gomez. root.vicente.gomez. (
                               8          ; serial
                               10         ; refresh (10 seconds)
                               60         ; retry (1 minute)
                               2419200   ; expire (4 weeks)
                               604800    ; minimum (1 week)
                               )
                               NS        dns1.vicente.gomez.
                               NS        dns2.vicente.gomez.
$ORIGIN 27.168.192.in-addr.arpa.
1 PTR router.vicente.gomez.
$ORIGIN 27.168.192.27.168.192.in-addr.arpa.
$TTL 1800           ; 30 minutes
50 PTR clientexp.vicente.gomez.
51 PTR clienteubu.vicente.gomez.
$ORIGIN 27.168.192.in-addr.arpa.
1 PTR router.vicente.gomez.
$ORIGIN 27.168.192.27.168.192.in-addr.arpa.
$TTL 1800           ; 30 minutes
50 PTR clientexp.vicente.gomez.
51 PTR clienteubu.vicente.gomez.
$ORIGIN 27.168.192.in-addr.arpa.
$TTL 604800         ; 1 week
2 PTR dns1.vicente.gomez.
3 PTR dns2.vicente.gomez.
5 PTR dhcp.vicente.gomez.
$TTL 1200           ; 20 minutes
50 PTR clientexp.vicente.gomez.
```