Instalación DNS en Linux

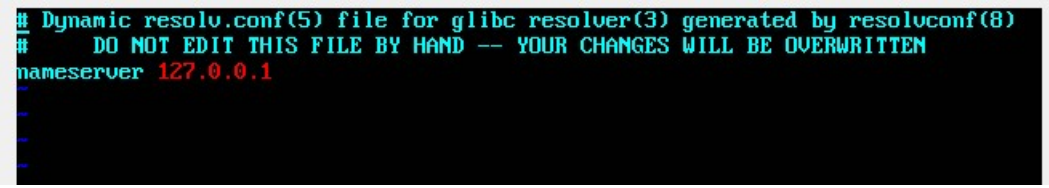
Configuración del cliente DNS en Linux

- El fichero **/etc/nsswitch.conf** especifica la configuración de las bases de datos que necesita el sistema. Este fichero contiene qué información se puede obtener y desde dónde, incluyendo el DNS, Cada línea especifica una base de datos, seguida de ":" y de la fuente desde donde se va a obtener la información. El servicio DNS se identifica con la palabra hosts y como fuentes se especifica "**files**" y "**dns**" , lo que significa que cuando se necesite obtener un nombre de equipo, primero se consultan los ficheros locales (Fichero /etc/hosts) y en segundo lugar se consulta al DNS (en los servidores dns definidos en el fichero /etc/resolv.conf). En definitiva, se determina el orden que usa el resolver para buscar información sobre los nombres de dominio.

/etc/nsswitch.conf

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat
group:          compat
shadow:         compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Fichero /etc/resolv.conf



Es el fichero principal del cliente DNS, guarda las direcciones IP hacia donde se envían las consultas. En este fichero se pueden configurar múltiples opciones de funcionamiento del resolver:

<atributo> <valor1> …. <valorn>

El atributo **nameserver** sirve para identificar los servidores DNS que consultará el resolver en el orden en el que aparecen.

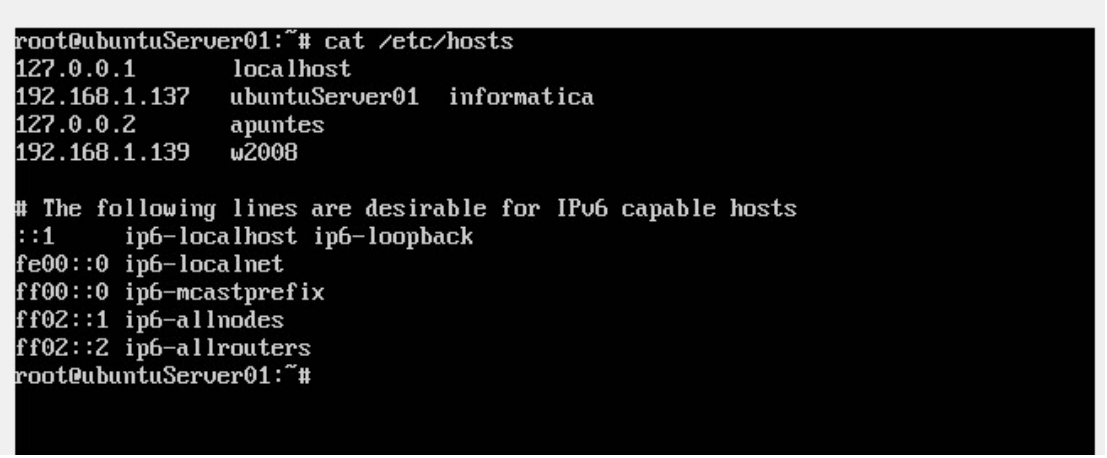
El atributo **domain** especifica el dominio por defecto al que pertenece la máquina, éste será el que se añada a las búsquedas de nombres no cualificados.

El atributo **search** especifica la lista de dominios que se añadirán a los nombres de dominio en las búsquedas de nombres no cualificados.

search y domain son mutuamente excluyentes.

Fichero /etc/hosts

- Contiene una tabla de correspondencias locales entre nombres de equipos y direcciones IP para consultar sin necesidad de enviar peticiones al DNS.



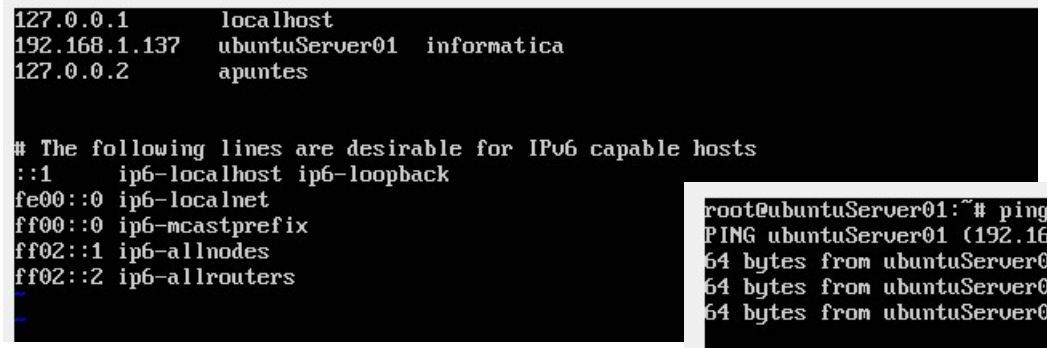
Cambiar nombre de la máquina

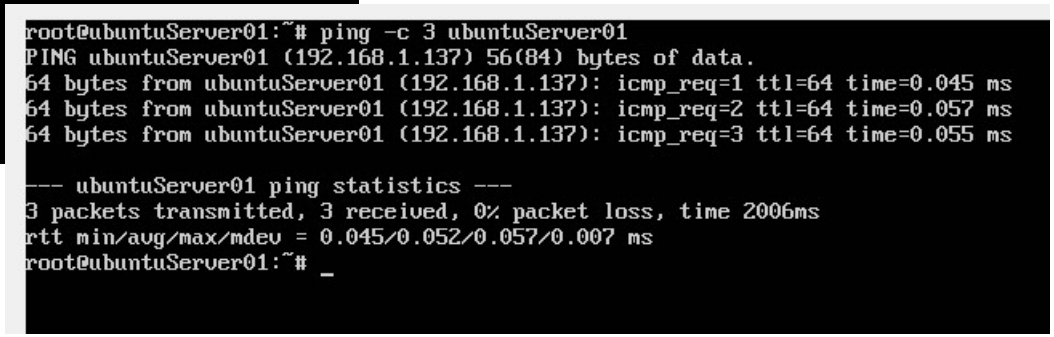
#vi /etc/hostname

Reiniciar y comprobar:

#hostname

Si en el fichero /etc/hosts aparece una entrada para dicha máquina, el ping con el nombre de la máquina funcionará:

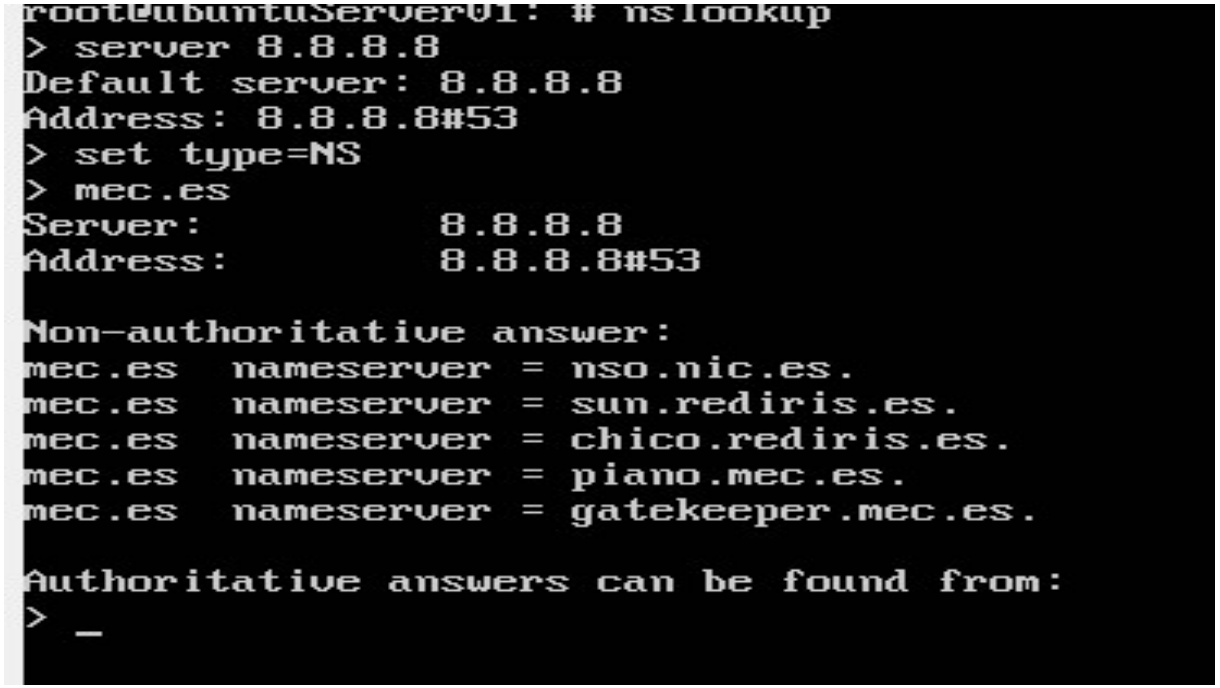




Herramientas de consulta a servidores DNS

- **nslookup** Acceder al comando en modo interactivo. Preguntar al servidor 8.8.8.8.

  Consultar los servidores autorizados (NS) para el dominio mec.es:



Comando host

- **Host**: permite realizar consultas al DNS .
- Obtener la dirección IP de www.mec.es

```
root@ubuntuServer01:~# host www.mec.es
www.mec.es has address 193.147.0.29
root@ubuntuServer01:~#
```

- Obtener el nombre asociado a la IP:

```
root@ubuntuServer01:~# host 8.8.4.4
4.4.8.8.in-addr.arpa domain name pointer google-public-dns-b.google.com.
root@ubuntuServer01:~#
root@ubuntuServer01:~# host 192.168.1.131
131.1.168.192.in-addr.arpa domain name pointer wxp.asir01.net.
root@ubuntuServer01:~#
```

Comando host

- Consulta al servidor 8.8.8.8 por los servidores DNS autorizados para el dominio es:

```
root@ubuntuServer01:~# host -t NS  es 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

es name server ns-ext.nic.cl.
es name server ns1.cesca.es.
es name server sns-pb.isc.org.
es name server ns15.communitydns.net.
es name server a.nic.es.
es name server f.nic.es.
es name server ns3.nic.fr.
root@ubuntuServer01:~#
```

Comando host

- Consulta al servidor DNS 8.8.8.8 por el registro SOA del dominio es:

```
root@ubuntuServer01:~# host -t SOA es 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

es has SOA record ns1.nic.es. hostmaster.nic.es. 2012110400 7200 7200 2592000 36
00
root@ubuntuServer01:~#
```

Comando dig

- Obtener la dirección IP de www.mec.es:

```
root@ubuntuServer01:~# dig www.mec.es

; <<>> DiG 9.8.1-P1 <<>> www.mec.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37475
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;www.mec.es.                    IN      A

;; ANSWER SECTION:
www.mec.es.             85613   IN      A       193.147.0.29

;; AUTHORITY SECTION:
mec.es.                 85613   IN      NS      piano.mec.es.
mec.es.                 85613   IN      NS      gatekeeper.mec.es.
mec.es.                 85613   IN      NS      chico.rediris.es.
mec.es.                 85613   IN      NS      nso.nic.es.
mec.es.                 85613   IN      NS      sun.rediris.es.

;; Query time: 7 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Nov  4 12:17:18 2012
;; MSG SIZE  rcvd: 157

root@ubuntuServer01:~# _
```

Comando dig

- Obtener el nombre asociado a la dirección IP 8.8.4.4:

```
root@ubuntuServer01:~# dig -x 8.8.4.4

; <<>> DiG 9.8.1-P1 <<>> -x 8.8.4.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31299
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;4.4.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
4.4.8.8.in-addr.arpa.   85443   IN      PTR     google-public-dns-b.google.com.

;; AUTHORITY SECTION:
4.8.8.in-addr.arpa.     2642    IN      NS      ns3.google.com.
4.8.8.in-addr.arpa.     2642    IN      NS      ns2.google.com.
4.8.8.in-addr.arpa.     2642    IN      NS      ns4.google.com.
4.8.8.in-addr.arpa.     2642    IN      NS      ns1.google.com.

;; Query time: 8 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Nov  4 12:20:29 2012
;; MSG SIZE  rcvd: 154

root@ubuntuServer01:~#
```

Comando dig

- Consulta al servidor 8.8.8.8 por los servidores DNS autorizados para el dominio es

```
root@ubuntuServer01:~# dig @8.8.8.8 es NS

; <<>> DiG 9.8.1-P1 <<>> @8.8.8.8 es NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44316
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;es.                            IN      NS

;; ANSWER SECTION:
es.                     7456    IN      NS      ns-ext.nic.cl.
es.                     7456    IN      NS      ns1.cesca.es.
es.                     7456    IN      NS      sns-pb.isc.org.
es.                     7456    IN      NS      ns15.communitydns.net.
es.                     7456    IN      NS      a.nic.es.
es.                     7456    IN      NS      f.nic.es.
es.                     7456    IN      NS      ns3.nic.fr.

;; Query time: 63 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Nov  4 12:23:41 2012
;; MSG SIZE  rcvd: 194
```

Comando dig

- Consulta al servidor 8.8.8.8 por todos los registros de recursos del dominio mec.es : #dig @8.8.8.8 mec.es ANY

```
; <<>> DiG 9.8.1-P1 <<>> @8.8.8.8 mec.es ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24187
;; flags: qr rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;mec.es.                                IN      ANY

;; ANSWER SECTION:
mec.es.                 32968   IN      SOA     gatekeeper.mec.es. root.gatekeep
er.mec.es. 2012072501 10800 3600 604800 10800
mec.es.                 32968   IN      NS      piano.mec.es.
mec.es.                 32968   IN      NS      gatekeeper.mec.es.
mec.es.                 32968   IN      NS      nso.nic.es.
mec.es.                 32968   IN      NS      sun.rediris.es.
mec.es.                 32968   IN      NS      chico.rediris.es.
mec.es.                 32968   IN      TXT     "RFaHqLb3Sd/qgOPYcvShqDj8gdRnDWL
KI3jyfsyNQN9p8XDAlo08ymTA74WSAd0ebbleke/rXaFn1LMKc0L4vw=="
mec.es.                 32968   IN      TXT     "v=spf1 mx ip4:193.147.0.22 ip4:
193.147.0.23 ip4:193.147.0.13 ip4:193.147.0.35  include:outlook.com include:spf.
messaging.microsoft.com -all"
mec.es.                 32968   IN      TXT     "MS=ms50035639"
mec.es.                 32968   IN      MX      100 saturnino.mec.es.
mec.es.                 32968   IN      MX      100 hercules.mec.es.

;; Query time: 55 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Nov  4 12:26:09 2012
;; MSG SIZE  rcvd: 508
```

Instalación bind9

- #apt-get install bind9
- Comprobad que se ha iniciado el servidor (proceso named):

```
root@ubuntu:~# ps aux|grep named
bind      2913  0.0  1.2 161036 12424 ?        Ssl  22:23   0:00 /usr/sbin/name
-u bind
root      2946  0.0  0.0  11904   928 tty1     S+   22:25   0:00 grep --color=au
to named
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~# netstat -nlt
Conexiones activas de Internet (solo servidores)
Proto  Recib Enviad Dirección local          Dirección remota        Estado
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               ESCUCHAR
tcp        0      0 0.0.0.0:80              0.0.0.0:*               ESCUCHAR
tcp        0      0 192.168.1.137:53        0.0.0.0:*               ESCUCHAR
tcp        0      0 127.0.0.1:53            0.0.0.0:*               ESCUCHAR
tcp        0      0 127.0.0.1:953           0.0.0.0:*               ESCUCHAR
tcp6       0      0 :::53                   :::*                    ESCUCHAR
tcp6       0      0 ::1:953                 :::*                    ESCUCHAR
root@ubuntu:~# _
```

Ficheros de configuración : /etc/bind

```
root@ubuntu:/etc/bind# cd /etc/bind
root@ubuntu:/etc/bind# ls -la
total 60
drwxr-sr-x  2 root bind 4096 oct 27 22:23 .
drwxr-xr-x 92 root root 4096 oct 27 22:23 ..
-rw-r--r--  1 root root 2389 oct  9 15:06 bind.keys
-rw-r--r--  1 root root  237 oct  9 15:06 db.0
-rw-r--r--  1 root root  271 oct  9 15:06 db.127
-rw-r--r--  1 root root  237 oct  9 15:06 db.255
-rw-r--r--  1 root root  353 oct  9 15:06 db.empty
-rw-r--r--  1 root root  270 oct  9 15:06 db.local
-rw-r--r--  1 root root 2994 oct  9 15:06 db.root
-rw-r--r--  1 root bind  463 oct  9 15:06 named.conf
-rw-r--r--  1 root bind  490 oct  9 15:06 named.conf.default-zones
-rw-r--r--  1 root bind  165 oct  9 15:06 named.conf.local
-rw-r--r--  1 root bind  890 oct 27 22:23 named.conf.options
-rw-r-----  1 bind bind   77 oct 27 22:23 rndc.key
-rw-r--r--  1 root root 1317 oct  9 15:06 zones.rfc1918
root@ubuntu:/etc/bind#
```

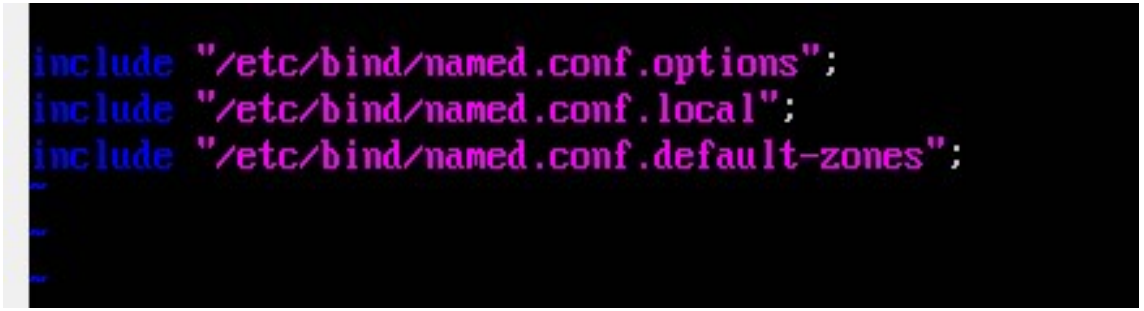
Fichero named.conf

- Es el fichero de configuración principal, almacena la configuración de las diferentes zonas generadas por defecto en la instalación.
- Incluye los ficheros:
  - named.conf.options (opciones generales)
  - named.conf.local (configuración de zonas)
  - named.conf.default-zones (zonas por defecto creadas).

Ficheros de configuración

- **/etc/bind/named.conf.local** – Almacena los nombres de los archivos de zona y de zona inversa y el archivo de configuración de la zona y de la zona inversa.
- **/etc/bind/named.conf.options** – Almacena sentencias para permitir la transferencia de zona (allow-transfer). Esto también puede hacerse en el fichero anterior.

Contenido del fichero **named.conf:**



Ficheros de zonas

- Ficheros que definen los registros de recursos de cada zona.
- Son referenciados desde las declaraciones de zonas en /etc/bind/named.conf.local
- Al instalar el servidor, se crean un conjunto de archivos de zonas por defecto (referenciados en /etc/bind/named.conf.local/default-zones)
  - /etc/bind/db.root (servidores raíz)
  - /etc/bind/db.local (resolución directa del bucle local)
  - /etc/bind/db.127 (resolución inversa del bucle local)
  - /etc/bind/db.0 (resolución directa broadcast)
  - /etc/bind/db.255 (resolución inversa broadcast)

Fichero named.conf.default-zones

```
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

Configuración del servidor como sólo cache

- Hacer copia de seguridad de todos los ficheros de configuración (...conf.options, ...conf.local)
- Si se configura el cliente DNS para que utilice el servidor DNS instalado en la máquina local (127.0.0.1), el servidor resuelve nombres de dominio de Internet. Con el comando nslookup se comprobará.

nslookup www.google.es

Servidor cache

- Por defecto el servidor está configurado como sólo cache (no es autorizado para ninguna zona) y tiene la recursividad activada. Para que el servidor pueda iniciar consultas recursivas tiene que conocer cuáles son los servidores DNS raíz (fichero /etc/bind/db.root)

/etc/bind/db.root

```
      last update:    Jun 17, 2010
      related version of root zone:   2010061700

formerly NS.INTERNIC.NET

                        3600000  IN  NS    A.ROOT-SERVERS.NET.
.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:BA3E::2:30

FORMERLY NS1.ISI.EDU

                        3600000      NS    B.ROOT-SERVERS.NET.
.ROOT-SERVERS.NET.      3600000      A     192.228.79.201

FORMERLY C.PSI.NET

                        3600000      NS    C.ROOT-SERVERS.NET.
.ROOT-SERVERS.NET.      3600000      A     192.33.4.12

FORMERLY TERP.UMD.EDU

                        3600000      NS    D.ROOT-SERVERS.NET.
.ROOT-SERVERS.NET.      3600000      A     128.8.10.90

FORMERLY NS.NASA.GOV

                        3600000      NS    E.ROOT-SERVERS.NET.
.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
```

Fichero */etc/*resolv.conf

- **Systemd-resolved.service** es el servicio que se encarga de gestionar la resolución de nombres en clientes con **systemd.**
- El fichero /etc/resolv.conf no es más que un link a /run/systemd/resolve/stub-resolv.conf.
- Para realizar cambios en la configuración, no hay que modificar el fichero /etc/resolv.conf. En lugar de eso, hay que modificar su propio fichero de configuración: **/etc/systemd/resolved.conf**
- Para comprobar el estado del servicio, podemos ejecutar el comando **systemd-resolve –status**

Búsquedas DNS

- El orden de las búsquedas DNS vendrá determinado bien por el archivo /etc/host.conf o bien por el archivo /etc/nsswitch.conf (Name Service Switch), según la versión de la librería libc que tenga nuestra máquina. Para asegurarnos, configuraremos ambos archivos para que las búsquedas DNS se hagan primero en el archivo /etc/hosts y después, si no encuentran allí el nombre, pregunten a los servidores que se indiquen en /etc/resolv.conf. El contenido de estos archivos será el siguiente:
- **/etc/host.conf**: determina el orden de las búsquedas DNS. Incluirá la línea:

  order hosts,bind

Búsquedas DNS

- **/etc/nsswitch.conf**: determina el orden de las búsquedas DNS. Incluirá la línea:

  hosts: files dns

- **/etc/hosts**: contiene una lista de direcciones IP y los nombres de las máquinas correspondientes. Este será el primer archivo al que accederá el sistema cuando intente resolver un nombre de dominio. El contenido de /etc/hosts es:
- 127.0.0.1 localhost.localdomain localhost

  192.168.1.137 ubuntuServerxx.asirxx.net

Fichero de configuración de red

Editamos /etc/netplan/01-netcfg.yaml:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
        dhcp6: no
      addresses: [192.168.1.137/24]
      search: [asir01.net]
```

sudo netplan apply

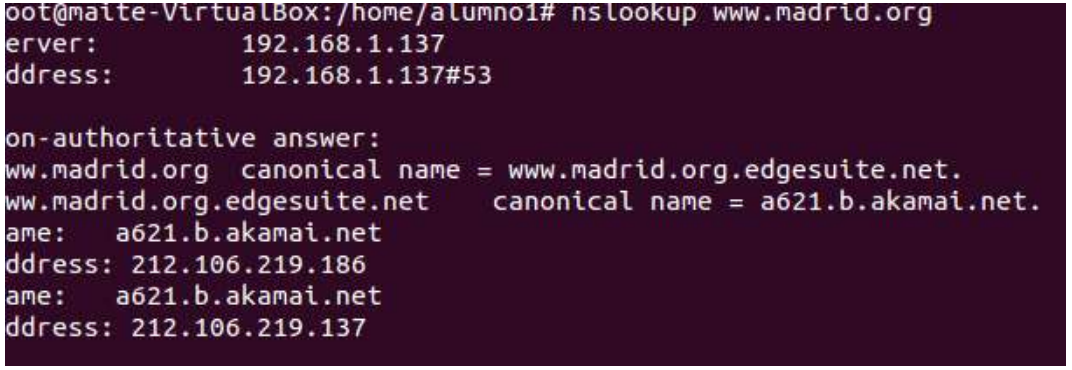
systemctl status systemd-networkd

Desde la M.V. Ubuntu

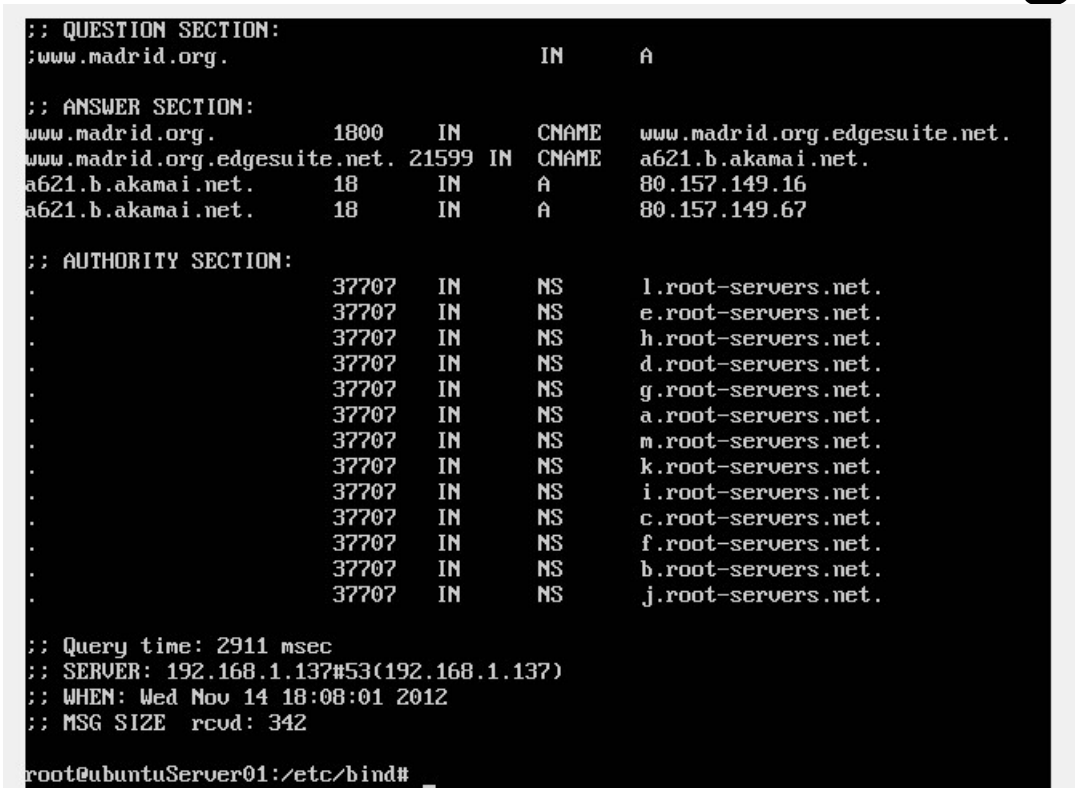
Configurar el resolver para que utilice como servidor DNS el configurado en UbuntuServer y reiniciar el servicio de red.

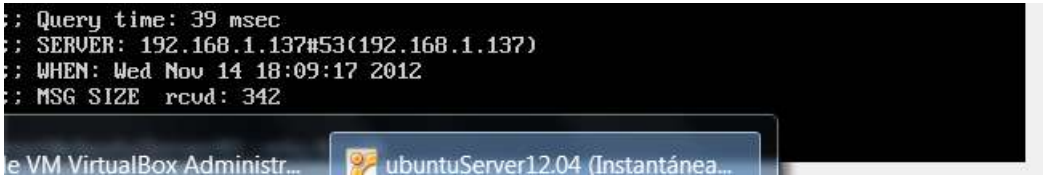
/etc/init.d/networking restart

Hacer una consulta, por ejemplo:



Comando dig





Observad tiempo de Respuesta en consultas Sucesivas.

Reenviador

- Para que el servidor reenvíe consultas a reenviadores (forwaders), descomentar la directiva forwaders del fichero /etc/bind/named.conf.option y reiniciar servidor:

```
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 {
        //      0.0.0.0;
192.168.1.139
         };

        //========================================================================
==
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
==
```

Fichero de logs del sistema

- Verificar que no se han producido errores al arrancar el servidor:
- #vi /var/log/syslog

Configuración del servidor como primario

- El servidor actuará como maestro del dominio asirxx.net.
- No se permitirán actualizaciones automáticas.
- El servidor DNS maestro será el instalado en la máquina UbuntuServer: ubuntuServerxx.asirxx.net (registro NS).
- Los nombres de los equipos serán:

  w2008Serverxx,w7pcxx y ubuntuxx (registros A).

Creando Zonas

- Para ello editamos el fichero : **/etc/bind/named.conf.local** y añadimos las zonas directa e indirecta, por ejemplo:

```
zone “asirxx.net“ {
    type master;
    file “/etc/bind/db.asirxx.net”;
    };
  zone “1.168.192.in-addr.arpa” {
type master;
file “/etc/bind/db.192.168.1”;
};
```

Creando Zonas

- **zone** indica la creación de una nueva zona.
- **type** es el tipo de zona (master o slave)
- **file** indica la ruta donde se encuentra ubicado el fichero que contendrá los registros de la zona.

✓ Es obligatorio acabar todas las líneas con punto y coma ;

✓ La primera zona es la de resolución directa y la segunda es la de resolución inversa. Substituid el nombre de la zona y las IP's por las correspondientes a cada equipo. En la zona de resolución inversa tenemos que poner la IP de nuestra red (por ejemplo, si nuestra red es 192.168.1.0 => tenemos que escribir la IP al revés de esta forma: **1.168.192.in-addr.arpa)**

✓ Después de esto, podemos comprobar si hay algún error en el fichero que acabamos de editar usando el comando:

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

Registro SOA

- Primero definimos el **nombre de la zona** => asirxx.net
- **IN** hace referencia al tipo de protocolo usado (IN = Internet)
- **SOA** es el tipo de registro (Start of Authority), indica el servidor que tiene autoridad en la zona
- **ubuntuServerxx.asirxx.net.** es el nombre que le hemos dado al servidor DNS de esta red
- admin.asirxx.net. Es la dirección de correo electrónica del encargado de mantener la zona.
- Parámetros que están dentro de los paréntesis:
  - ✓ **Numero de Serie:** es el numero de revisión del archivo de zona. Hemos puesto la fecha de la ultima modificación, es importante actualizar ese campo siempre que vayamos a editar el archivo de la zona.
  - ✓ **Tiempo de refresco:** es el tiempo que tarda el servidor secundario en pedirle al servidor Maestro la copia de la zona. El servidor DNS secundario compara el número de serie del registro SOA del archivo de zona del servidor DNS principal y el número de serie de su propio registro SOA. Si son diferentes, el servidor DNS secundario solicitará una transferencia de zona desde el servidor DNS principal. El valor predeterminado es 3.600 (que es 1 hora).
  - ✓ **Tiempo entre reintentos de consulta:** Esto es el tiempo que un servidor secundario espera para recuperar una transferencia de zona fallida. Este tiempo suele ser menor al intervalo de actualización.
  - ✓ **Tiempo de expiración de zona:** es el tiempo antes que un servidor secundario deje de responder a las búsquedas una vez se haya producido un intervalo de actualización de la zona.
  - ✓ **Tiempo Total de Vida:** Tiempo en el que el servidor de nombres mantiene la caché cualquier registro del recurso de este archivo en base de datos.

Registros A, CNAME, MX

- **asirxx.net. IN NS ubuntuServerxx.asirxx.net.**
  Indica servidores con autoridad en la zona.
  NS(Name Server) es el tipo de registro.
- **ubuntuServerxx.asirxx.net. IN A 192.168.1.137**
  Indica el nombre del servidor DNS de la zona.
  Asigna a esa IP el dominio
  ubuntuServerxx.asirxx.net
- Todos los registros de tipo **A** asocian un dominio (que en este caso son ordenadores) a una IP.
- Los registros de tipo **CNAME** asignan un alias por el que también se les conoces a esos dominios.

Configuración del servidor DNS

Se configurarán los siguientes alias:

ns1.asir**xx**.net alias de ubuntuServer**xx**.asir**xx**.net

www.asir**xx**.net alias de ubuntuServer**xx**.asir**xx**.net

ftp.asir**xx**.net alias de w2008Server**xx**.asir**xx**.net

mail.asir**xx**.net alias de ubuntuServer**xx**.asir**xx**.net (actuará como servidor se correo del dominio, registro MX).

El tiempo en cache de las respuestas de la zona será de 3 horas.

Añadiendo Registros de Resolución Directa

- Hay que crear el fichero donde guardaremos los registros: **/etc/bind/db.asirxx.net**

$ttl 38400
asirxx.net. IN SOA ubuntuServer**xx**.asirxx.net. admin.asir**xx**.net. (
2016110601; Número de serie
3600 ; Tiempo de refresco (1 hora)
300 ; Tiempo entre reintentos de consulta (5 min)
17200 ; Tiempo de expiración de zona (2 dias)
10800 ; (TTL) (3 horas))
;
@ IN NS ubuntuServerxx.asir**xx**.net.
ubuntuServerxx.asir**xx**.net IN A 192.168.1.137
ubuntuxx.asir**xx**.net. IN A 192.168.1.133
w2008Server**xx**.asirxx.net. IN A 192.168.1.139
w7pc**xx**.asir**xx**.net. IN A 192.168.1.131
ns1 IN CNAME ubuntuServer**xx**.asir**xx**.net.
www IN CNAME ubuntuServer**xx**.asir**xx**.net.
mail IN CNAME ubuntuServer**xx**.asir**xx**.net.
ftp IN CNAME w2008Server**xx**.asir**xx**.net.
w7 IN CNAME w7pcxx.asir**xx**.net.

- **Nota:** también se puede crear el archivo de zona a partir de **/etc/bind/db.empty**
  cp /etc/bind/db.empty /etc/bind/db.asirxx.net

Configuración de la zona de resolución directa

- 1/ En el fichero **named.conf.local** declarar la zona de resolución directa para el dominio asir**xx**.net:

  zone “asir**xx**.net{

  type master;

  file “/etc/bind/db.asir**xx**.net”; };

2/ Crear el fichero de zona de resolución directa db.asir**xx**.net, añadiendo las directivas y registros de zona necesarios.

Fichero de zona db.asir**xx**.net

```
;
;Fichero db.asir01.net
;
$TTL    1D
asir01.net.     IN      SOA     asir01.net.   administrador.asir01.net. (
                                1          ; Serial
                           604800          ; Refresh
                            86400          ; Retry
                          2419200          ; Expire
                            10800 )        ; Negative Cache TTL (3 horas)
; @ equivaldría al nombre de la zona
;Servidores DNS del dominio
        IN      NS      ubuntuServer01.asir01.net.
          ; El blanco al principio equivale al valor del registeo anterior
;Hosts
ubuntuServer01  IN  A  192.168.1.137
ubuntu01                IN  A  192.168.1.133
w2008Server01   IN  A  192.168.1.139
wxp01.asir01.net.               IN  A  192.168.1.13
;Como no termina en punto no se autocompleta
;Alias
ns1     IN      CNAME   ubuntuServer01
www     IN      CNAME   ubuntuServer01
ftp     IN      CNAME   w2008Server01
mail    IN      CNAME   ubuntu01

; servidores de correo
@       IN      MX      10      ubuntu01
```

Fichero de zona db.asir**xx**.net

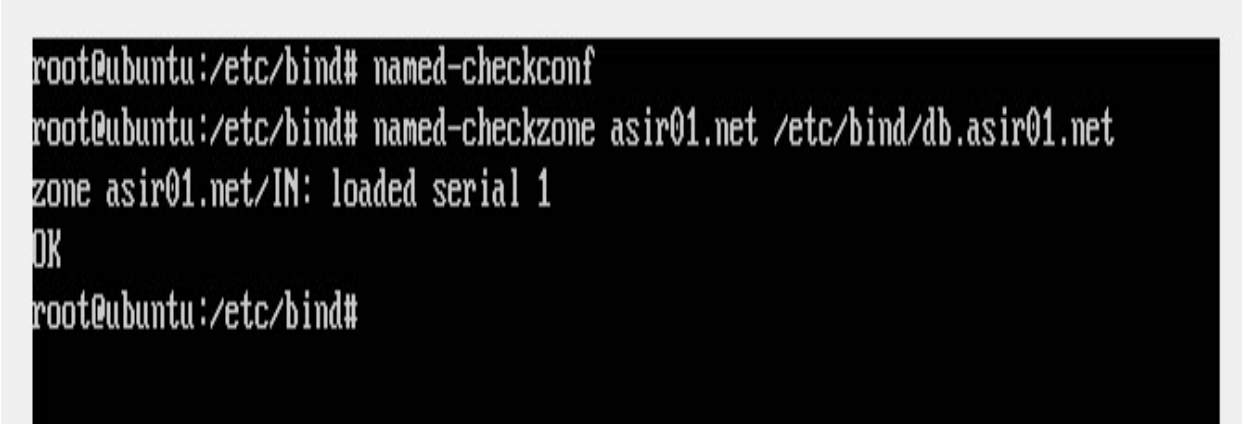
```
$TTL    86400
@       IN SOA ubuntuServer.asir253.net. admin.asir253.net (
                  1; serial
              21600; refresh
               3600; retry
             604800; expire
              86400);TTL

@       IN      NS      ubuntuServer.asir253.net.
ubuntuServer    IN      A       192.168.1.17
windowsxp       IN      A       192.168.1.133
w2008server     IN      A       192.168.1.139
xp              IN      CNAME   windowsxp
ns              IN      CNAME   w2008server
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"db.asir253.net" [Sólo lectura] 15L, 348C                    1,1           Todo
```

Sintaxis

- @ equivale al nombre de la zona definido en named.conf.local
- El ‘.’ tiene el significado:
  - A todos los nombres de dominio que se escriben sin el punto (nombres no cualificados) se les añade el nombre de la zona.
  - Cuando se escribe un nombre de dominio completo, debe terminar con punto.
- Si el primer campo de una línea de RR se deja en blanco toma el valor de la línea del RR anterior.

Chequeo de la sintaxis de los ficheros de configuración y zona

- #named-checkconf Comprueba el fichero de configuración principal.
- # named-checkzone Comprueba el fichero de zonas.



Comprobaciones

- **Reiniciar** el servidor DNS:
  #/etc/init.d/bind9 restart
  # service bind9 stop/start
- Consultar el fichero de logs del sistema
  #tail /var/log/syslog

```
root@ubuntu:/etc/bind# named-checkconf
root@ubuntu:/etc/bind# named-checkzone asir01.net /etc/bind/db.asir01.net
zone asir01.net/IN: loaded serial 1
OK
root@ubuntu:/etc/bind# /etc/init.d/bind9 restart
 * Stopping domain name service... bind9
waiting for pid 1998 to die
                                                                    [ OK ]
 * Starting domain name service... bind9                           [ OK ]
root@ubuntu:/etc/bind# service bind9 restart
 * Stopping domain name service... bind9
waiting for pid 2480 to die
                                                                    [ OK ]
 * Starting domain name service... bind9                           [ OK ]
root@ubuntu:/etc/bind# tail /var/log/syslog
Oct 28 13:03:05 ubuntu named[2523]: command channel listening on 127.0.0.1#953
Oct 28 13:03:05 ubuntu named[2523]: command channel listening on ::1#953
Oct 28 13:03:05 ubuntu named[2523]: zone 0.in-addr.arpa/IN: loaded serial 1
Oct 28 13:03:05 ubuntu named[2523]: zone 127.in-addr.arpa/IN: loaded serial 1
Oct 28 13:03:05 ubuntu named[2523]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct 28 13:03:05 ubuntu named[2523]: zone localhost/IN: loaded serial 2
Oct 28 13:03:05 ubuntu named[2523]: zone asir01.net/IN: loaded serial 1
Oct 28 13:03:05 ubuntu named[2523]: managed-keys-zone ./IN: loaded serial 2
Oct 28 13:03:05 ubuntu named[2523]: running
Oct 28 13:03:05 ubuntu named[2523]: zone asir01.net/IN: sending notifies (serial
 1)
root@ubuntu:/etc/bind# _
```

Probando la configuración del archivo de zona

 # named-checkconf /etc/bind/named.conf.local

- **Probando la configuración del Servidor**

  También podemos probar si el servidor DNS carga con éxito el archivo que contiene los registros usando el comando:

 # named-checkzone asirxx.net /etc/bind/db.asirxx.net

- Para reiniciar el servidor

#/etc/init.d/bind9 restart

Configurando los clientes DNS

- Antes de añadir los registros de resolución inversa vamos a probar si nuestro servidor DNS funciona. Para eso tenemos que editar los siguientes ficheros:
- **/etc/host.conf**:
  # The "order" line is only used by old versions of the C library.
  order hosts,bind
  multi on

- **Editamos /etc/netplan/01-netcfg.yaml:**
- Configuración de la tarjeta de red
  dns-nameservers 192.168.1.137 # El DNS local
  dns-search asirxxx.net
- **/etc/resolv.conf** Este fichero contendrá al principio, después de reiniciar, **search asirxx.net** y **nameserver 192.168.1.137** que es la IP del servidor DNS.

Forwarders

- Si por ejemplo, queremos acceder a Google.com. Como no tenemos ese registro en nuestra base de datos, el servidor DNS que tengamos configurado deberá pasarle la consulta de resolución de nombre a otro servidor DNS. Esos servidores DNS son también conocidos como Forwarders y en Bind se configuran de la siguiente manera:

#/etc/bind/named.conf.options

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

forwarders {
8.8.8.8;
8.8.4.4;
};

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

- Esos son los servidores públicos de Google. Cuando nuestro servidor local no encuentre un dominio se lo preguntara al servidor DNS de Google.

Aplicando los cambios y probando la resolución directa

- Reiniciamos la configuración de la Tarjeta de Red :

#/etc/init.d/networking restart

- Y probamos la resolución directa haciendo ping por ejemplo a :

#ping w7pcxx.asirxx.net :

- Vemos que funciona y que hace ping al ordenador que nosotros hemos definido en el archivo de registros de zona.

- Otros comandos que podemos probar son:

#host linux

#nslookup

#dig asirxx.net

Añadiendo Registros de Resolución Inversa

- Ahora creamos la base de datos de la **resolución inversa**, con ella, a partir de una IP podemos saber el nombre de host. Es un registro de tipo **PTR**(Pointer-Puntero).

- Creamos una zona inversa en el fichero de zona del servidor, “1.168.192.in-addr.arpa”. En la declaración de la zona inversa incluimos el fichero db.192.168.1 . Ahora hay que crearlo:

vi db.192.168.1

- O copiar uno de los ficheros de resolución inversa que viene con el servidor :

cp db.127 db.192.168.1

Configuración de la zona de resolución inversa

- En el fichero de configuración named.conf.local declarar la zona de resolución inversa para la red 10.12.0.0/16 (en los ejemplos :192.168.1.0/24):

```
zone “1.168.192.in-addr.arpa”{
   type master;
   file “etc/bind/db.192.168.1”;
};
```

Archivo de Resolución Inversa

```
; Archivo de Resolucion Inversa
$TTL 604800
1.168.192.in-addr.arpa. IN SOA ubuntuServerxx.asirxx.net.  admin.
    .asirxx.net. (
    2012111201 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
    ;
    1.168.192.in-addr.arpa. IN NS ubuntuServerxx.asirxx.net.
    137.1.168.192.in-addr.arpa. IN PTR ubuntuServerxx.asirxx.net.
    133.1.168.192.in-addr.arpa. IN PTR ubuntuxx.asirxx.net.
    139.1.168.192.in-addr.arpa. IN PTR w2008Serverxx.asirxx.net.
    131                         IN PTR w7pcxx.asirxx.net.
```

Fichero de zona: db.1.168.192

```
$TTL    86400
@       IN SOA ubuntuServer.asir253.net. admin.asir253.net. (
                1; serial
            21600; refresh
             3600; retry
           604800; expire
            86400);TTL

                IN      NS      ubuntuServer.asir253.net.
17.1.168.192.in-addr.arpa.              IN      PTR     ubuntuServer
133             IN      PTR     windowsxp
139             IN      PTR     w2008server
```

Fichero de zona: db.192.168.1

```
$TTL    86400
1.168.192.in-addr.arpa.         IN SOA ubuntuServer.asir253.net. admin.asir253.ne
t. (
                  1; serial
              21600; refresh
               3600; retry
             604800; expire
              86400);TTL

1.168.192.in-addr.arpa.          IN      NS      ubuntuServer.asir253.net.
17.1.168.192.in-addr.arpa.                IN      PTR     ubuntuServer
133             IN      PTR     windowsxp
139             IN      PTR     w2008server
```

Sintaxis

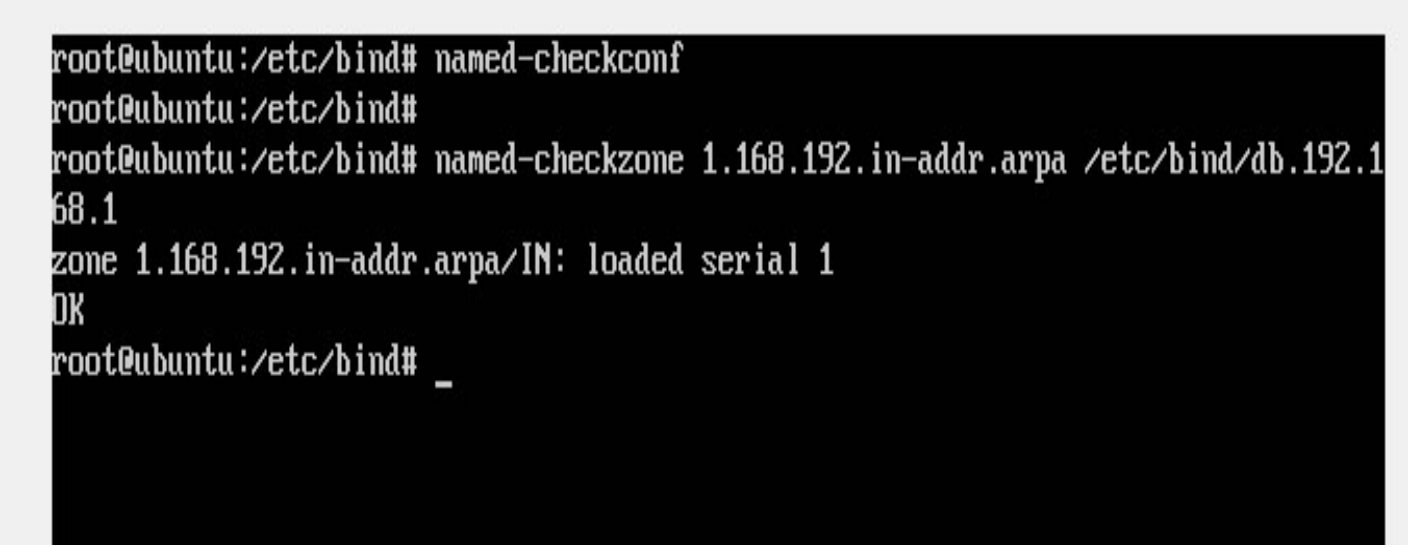
#named-checkconf

- Y luego comprobamos si carga la zona correctamente:

#named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192.168.1

- **Probando la Resolucion Inversa**

  #host 192.168.1.133

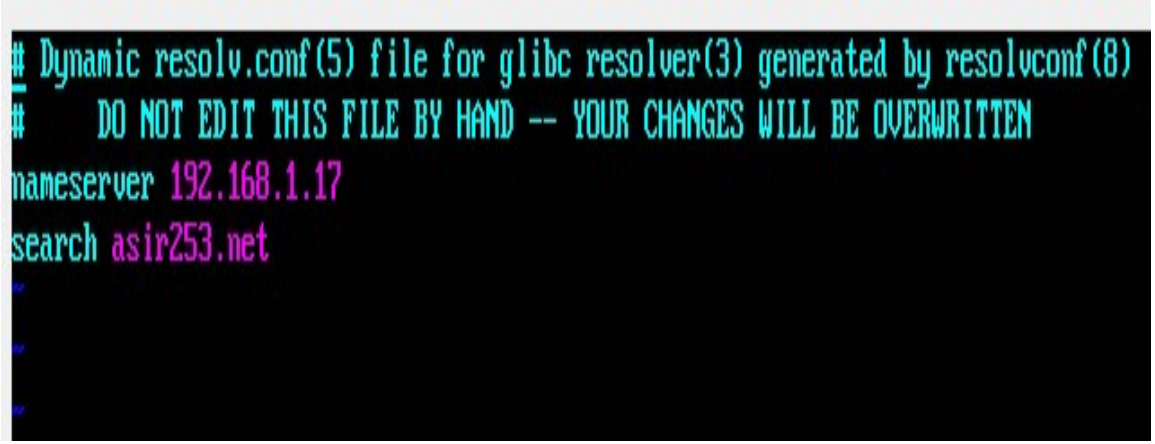


Reinicio y comprobación

```
root@ubuntu:/etc/bind# service bind9 restart
 * Stopping domain name service... bind9
waiting for pid 2652 to die
                                                                    [ OK ]
 * Starting domain name service... bind9                           [ OK ]
root@ubuntu:/etc/bind#
root@ubuntu:/etc/bind# nslookup 192.168.1.133
Server:         127.0.0.1
Address:        127.0.0.1#53

133.1.168.192.in-addr.arpa      name = ubuntu01.asir01.net.

root@ubuntu:/etc/bind# nslookup 192.168.1.13
Server:         127.0.0.1
Address:        127.0.0.1#53

13.1.168.192.in-addr.arpa       name = wxp01.asir01.net.

root@ubuntu:/etc/bind# _
```

Comprobación

- Reiniciar el servicio de red
- /etc/init.d/networking stop/start
- Vi /etc/resolv.conf



Resolviendo …

```
alumno@ubuntuServer:/etc/bind$ nslookup xp
Server:         192.168.1.17
Address:        192.168.1.17#53

xp.asir253.net  canonical name = windowsxp.asir253.net.
Name:   windowsxp.asir253.net
Address: 192.168.1.133

alumno@ubuntuServer:/etc/bind$ host xp
xp.asir253.net is an alias for windowsxp.asir253.net.
windowsxp.asir253.net has address 192.168.1.133
alumno@ubuntuServer:/etc/bind$
alumno@ubuntuServer:/etc/bind$ _
```

```
alumno@ubuntuServer:/etc/bind$ nslookup
> ubuntuserver
Server:         192.168.1.17
Address:        192.168.1.17#53

Name:   ubuntuServer.asir253.net
Address: 192.168.1.17
> xp
Server:         192.168.1.17
Address:        192.168.1.17#53

xp.asir253.net  canonical name = windowsxp.asir253.net.
Name:   windowsxp.asir253.net
Address: 192.168.1.133
>
```

Resolución inversa

```
alumno@ubuntuServer:/etc/bind$ dig -x 192.168.1.133

; <<>> DiG 9.9.5-3ubuntu0.5-Ubuntu <<>> -x 192.168.1.133
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33966
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;133.1.168.192.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
133.1.168.192.in-addr.arpa. 86400 IN    PTR     windowsxp.1.168.192.in-addr.arpa
.

;; AUTHORITY SECTION:
1.168.192.in-addr.arpa. 86400   IN      NS      ubuntuServer.asir253.net.

;; ADDITIONAL SECTION:
ubuntuServer.asir253.net. 86400 IN      A       192.168.1.17

;; Query time: 4 msec
;; SERVER: 192.168.1.17#53(192.168.1.17)
;; WHEN: Wed Nov 04 18:21:47 CET 2015
;; MSG SIZE  rcvd: 133
```

Comando host. Modo interactivo

```
alumno@ubuntuServer:/etc/bind$ host -t SOA asir253.net
asir253.net has SOA record ubuntuServer.asir253.net. admin.asir253.net.asir253.n
et. 1 21600 3600 604800 86400
alumno@ubuntuServer:/etc/bind$ host -t NS asir253.net
asir253.net name server ubuntuServer.asir253.net.
alumno@ubuntuServer:/etc/bind$ host -t A asir253.net
asir253.net has no A record
alumno@ubuntuServer:/etc/bind$ host -t A ns
ns.asir253.net is an alias for w2008server.asir253.net.
w2008server.asir253.net has address 192.168.1.139
alumno@ubuntuServer:/etc/bind$ host -t PTR 192.168.1.133
133.1.168.192.in-addr.arpa domain name pointer windowsxp.1.168.192.in-addr.arpa.
alumno@ubuntuServer:/etc/bind$
```

Comando host

```
root@ubuntuServer01:~# host -t SOA asir01.net 192.168.1.137
Using domain server:
Name: 192.168.1.137
Address: 192.168.1.137#53
Aliases:

asir01.net has SOA record asir01.net. admin.asir01.net. 1 604800 86400 2419200 1
0800
root@ubuntuServer01:~# host -t A www 192.168.1.137
Using domain server:
Name: 192.168.1.137
Address: 192.168.1.137#53
Aliases:

www.asir01.net is an alias for ubuntu01.asir01.net.
ubuntu01.asir01.net has address 192.168.1.133
root@ubuntuServer01:~# host -t A mail 192.168.1.137
Using domain server:
Name: 192.168.1.137
Address: 192.168.1.137#53
Aliases:

mail.asir01.net is an alias for wxp01.asir01.net.
wxp01.asir01.net has address 192.168.1.131
root@ubuntuServer01:~# _
```

Configuración de los equipos de la red virtual

- Cambiar el DNS a la dirección de la MV del UbuntuServer

```
root@maite-VirtualBox:/home/alumno1# dig  mail.asir01.net

; <<>> DiG 9.8.1-P1 <<>> mail.asir01.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9429
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;mail.asir01.net.               IN      A

;; ANSWER SECTION:
mail.asir01.net.        86400   IN      CNAME   ubuntu01.asir01.net.
ubuntu01.asir01.net.    86400   IN      A       192.168.1.133

;; AUTHORITY SECTION:
asir01.net.             86400   IN      NS      ubuntuServer01.asir01.net.

;; ADDITIONAL SECTION:
ubuntuServer01.asir01.net. 86400 IN     A       192.168.1.137

;; Query time: 3 msec
;; SERVER: 192.168.1.137#53(192.168.1.137)
```

Bibliografía

- http://juananpc.com/instalacion-y-configuracion-de-un-servidor-dns-en-ubuntu-server-16-04/
- https://moss.sh/es/configuracion-problematica-systemd-resolved/
- http://manpages.ubuntu.com/manpages/bionic/es/man5/nsswitch.conf.5.html
- http://www.taringa.net/posts/linux/6545540/Instalar-un-DNS-con-Bind-9-paso-a-paso.html
- http://wiki.elhacker.net/redes/administracion-de-redes-gnu-linux/instalacion-de-un-servidor-dns-en-gnu-linux-en-modo-consola
- http://www.dominios-internet.com/dns/