

## Instalación de DNS en Linux server 24.04

El servidor DNS es el encargado de convertir URL (dominios + servicios) en direcciones IP, por ejemplo, podemos configurarlo con el dominio [victor.com](http://victor.com) e indicarle que cuando alguien escriba en su navegador [www.victor.com](http://www.victor.com), pues convierta esa URL en una dirección IP 192.168.56.1 que es a fin de cuenta la dirección donde estará escuchando un servidor Web en este caso. Este se hace por dos razones, la primera porque a los usuarios le es prácticamente imposible recordar direcciones IP, siendo mucho más amigable los nombres de dominio, la segunda porque a fin de cuenta los ordenadores o servidores se comunican por direcciones IP.

Teniendo un Ubuntu Server instalado y funcionando, los datos del servidor para esta guía serían:

### //Información del sistema base:

- Nombre de host: **ns1**
- FQDN: **ns1.victor.com**
- Dirección IP: **192.168.56.1 (La misma dirección IP que la de DHCP)**

### //Los archivos a editar en esta guía son:

- `/etc/bind/named.conf.options`
- `/etc/default/named`
- `/etc/bind/named.conf.local`
- `/etc/bind/zonas/db.networld.cu` (**archivo inexistente, lo crearemos nosotros**)
- `/etc/bind/zonas/db.10.10.20` (**archivo inexistente, lo crearemos nosotros**)

**Sigue los siguientes pasos sustituyendo el dominio de segundo nivel-”networld” por tu nombre y el dominio superior (TLD) “.cu” por “.es”:**

1- Lo primero que haremos siempre, comprobar actualizaciones:

```
# sudo apt update
# sudo apt upgrade
```

```
usuario@usuario:~$ sudo apt update && sudo apt upgrade
[sudo] password for usuario:
```

2- Nos instalamos el paquete de Bind9 y Nano para editar archivos en caso de que no lo tengamos.

```
# sudo apt install bind9 bind9-utils nano
```

```
usuario@usuario:~$ sudo apt install bind9 bind9-utils nano
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
bind9 ya está en su versión más reciente (1:9.18.28-0ubuntu0.24.04.1).
bind9-utils ya está en su versión más reciente (1:9.18.28-0ubuntu0.24.04.1).
nano ya está en su versión más reciente (7.2-2ubuntu0.1).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
linux-headers-6.8.0-41 linux-headers-6.8.0-41-generic linux-image-6.8.0-41-generic linux-modules-6.8.0-41-generic linux-modules-extra-6.8.0-41-generic
linux-tools-6.8.0-41 linux-tools-6.8.0-41-generic
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 2 no actualizados.
```

3- Comprobamos si Bind9 ya está en funcionamiento, los errores o advertencias son normales (aún no hemos realizado ninguna configuración)

```
# systemctl status bind9
```

```
usuario@usuario:~$ systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-10-30 10:37:42 UTC; 56s ago
     Docs: man:named(8)
  Main PID: 16150 (named)
    Status: "running"
   Tasks: 26 (limit: 9984)
  Memory: 10.3M (peak: 11.9M)
     CPU: 163ms
  CGroup: /system.slice/named.service
          └─16150 /usr/sbin/named -f -u bind

oct 30 10:37:42 usuario named[16150]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
oct 30 10:37:42 usuario named[16150]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
oct 30 10:37:42 usuario named[16150]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
oct 30 10:37:42 usuario named[16150]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
oct 30 10:37:42 usuario named[16150]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
oct 30 10:37:42 usuario named[16150]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
oct 30 10:37:42 usuario named[16150]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
oct 30 10:37:42 usuario named[16150]: network unreachable resolving './NS/IN': 2001:500:1::53#53
oct 30 10:37:52 usuario named[16150]: resolver priming query complete: timed out
oct 30 10:37:52 usuario named[16150]: managed-keys-zone: Unable to fetch DNSKEY set '': timed out
```

4- Permitir de forma sencilla en el Firewall local, el acceso al puerto y protocolo que utiliza Bind9

```
# sudo ufw allow bind9
```

```
usuario@usuario:~$ sudo ufw allow bind9
Rules updated
Rules updated (v6)
```

**//Debe arrojar, Rules Update o Rule added**

5- Configuración mínima de Bind9

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

**//Líneas a modificar, agregar o eliminar (el archivo debe contener lo siguiente)**

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

    listen-on { any; };
    allow-query { localhost; 10.10.20.0/24; };
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    dnssec-validation no;
};
```

```
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    listen-on { any; };
    allow-query { localhost; 192.168.56.0/24; };
    forwarders { 8.8.8.8; 8.8.4.4; };
    dnssec-validation no;

    // 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;
    // };

    //=====
    // 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
    //=====
    //dnssec-validation auto;

    listen-on-v6 { any; };
};
```

- **//listen-on:** define la dirección donde estará escuchando Bind9, si no sabes con exactitud, utiliza la opción any.
- **//allow-query:** define desde que redes o ip es posible realizar consultas, normalmente la misma red a la que pertenece el servidor DNS.
- **//forwarders:** define servidores DNS a los cuales Bind9 reenviará las consultas que él no pueda resolver.
- **//dnssec-validation:** define si se validará un dnssec.

6- Obligar el uso único de IPv4

```
# sudo nano /etc/default/named
```

**//Modificar la línea dejándola así: OPTIONS="-u bind -4"**

```
GNU nano 7.2 /etc/default/named
#
# run resolvconf?
RESOLVCONF=no
# startup options for the server
OPTIONS="-u bind -4"
```

7- Comprobar la configuración de Bind9 y reiniciar el servicio si todo está bien, luego lanzar status para ver si no hay errores.

```
# sudo named-checkconf
```

```
usuario@usuario:~$ sudo named-checkconf
/etc/bind/named.conf.options:26: 'dnssec-validation' redefined near 'dnssec-validation'
```

**//Sirve para chequear la sintaxis de los ficheros de configuración de BIND.**

```
# sudo systemctl restart bind9
```

```
# systemctl status bind9
```

```
usuario@usuario:~$ sudo systemctl restart bind9 && systemctl status bind9
• named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-10-30 11:00:21 UTC; 9ms ago
     Docs: man:named(8)
   Main PID: 17337 (named)
    Status: "running"
     Tasks: 18 (limit: 9984)
  Memory: 7.8M (peak: 8.9M)
     CPU: 111ms
    CGroup: /system.slice/named.service
            └─17337 /usr/sbin/named -f -u bind -4

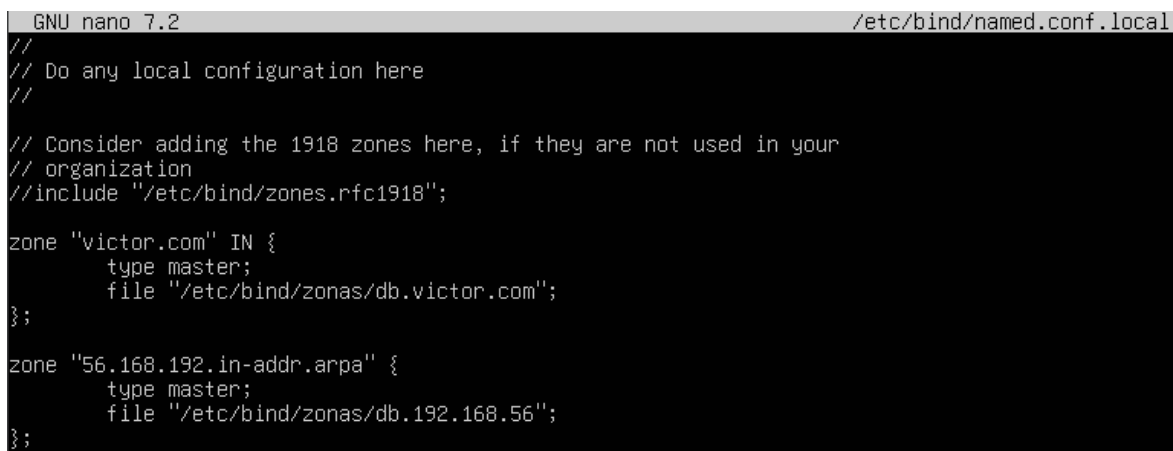
oct 30 11:00:21 usuario named[17337]: configuring command channel from '/etc/bind/rndc.key'
oct 30 11:00:21 usuario named[17337]: command channel listening on 127.0.0.1#953
oct 30 11:00:21 usuario named[17337]: managed-keys-zone: loaded serial 2
oct 30 11:00:21 usuario named[17337]: zone 255.in-addr.arpa/IN: loaded serial 1
oct 30 11:00:21 usuario named[17337]: zone 0.in-addr.arpa/IN: loaded serial 1
oct 30 11:00:21 usuario named[17337]: zone localhost/IN: loaded serial 2
oct 30 11:00:21 usuario named[17337]: zone 127.in-addr.arpa/IN: loaded serial 1
oct 30 11:00:21 usuario named[17337]: all zones loaded
oct 30 11:00:21 usuario named[17337]: running
oct 30 11:00:21 usuario systemd[1]: Started named.service - BIND Domain Name Server.
```

## 8- Agregar las Zonas

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

zone "victor.com" IN {
    type master;
    file "/etc/bind/zonas/db.victor.com";
};

zone "56.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zonas/db.192.168.56";
};
```



```
GNU nano 7.2 /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 "victor.com" IN {
    type master;
    file "/etc/bind/zonas/db.victor.com";
};

zone "56.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zonas/db.192.168.56";
};
```

**//Vas a cambiar el dominio por el que vas a usar al igual que la dirección IP, fíjate que se lee la IP de atrás a adelante obviando el último octeto. Por ejemplo, en el caso la IP es: 10.10.20.13 y está representada en el archivo así: 20.10.10.**

**//La zona networkld.cu es la zona directa de nuestro DNS.**

**//La zona 56.168.192.in-addr.arpa es la zona inversa para nuestros PTR.**

**//Los archivos de zona configurados hay que crearlos porque lógicamente no existen [db.victor.com y db.192.168.56]**

9- Creando el directorio donde guardaremos los archivos de zonas y luego creamos las dos zonas, la directa y la inversa.

```
# sudo mkdir /etc/bind/zonas
```

```
usuario@usuario:~$ sudo mkdir /etc/bind/zonas
```

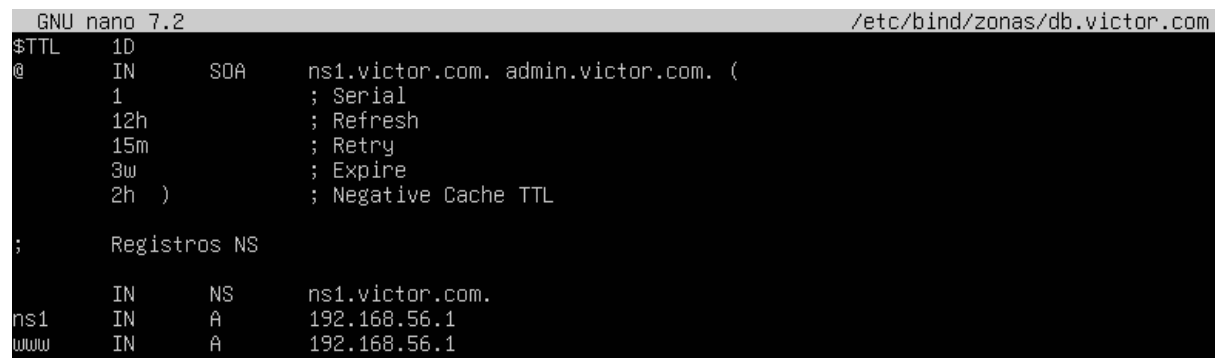
**//Ten en cuenta cambiar los nombres de archivos según el dominio y la IP usada.**

```
# sudo nano /etc/bind/zonas/db.victor.com
```

```
$TTL      1D
@         IN      SOA      ns1.networld.cu. admin.networld.cu. (
        1          ; Serial
       12h        ; Refresh
       15m        ; Retry
        3w        ; Expire
       2h )       ; Negative Cache TTL
```

```
;      Registros NS
```

```
        IN      NS       ns1.networld.cu.
ns1      IN      A        10.10.20.1
www      IN      A        10.10.20.1
```



```
GNU nano 7.2 /etc/bind/zonas/db.victor.com
$TTL      1D
@         IN      SOA      ns1.victor.com. admin.victor.com. (
        1          ; Serial
       12h        ; Refresh
       15m        ; Retry
        3w        ; Expire
       2h )       ; Negative Cache TTL

;      Registros NS

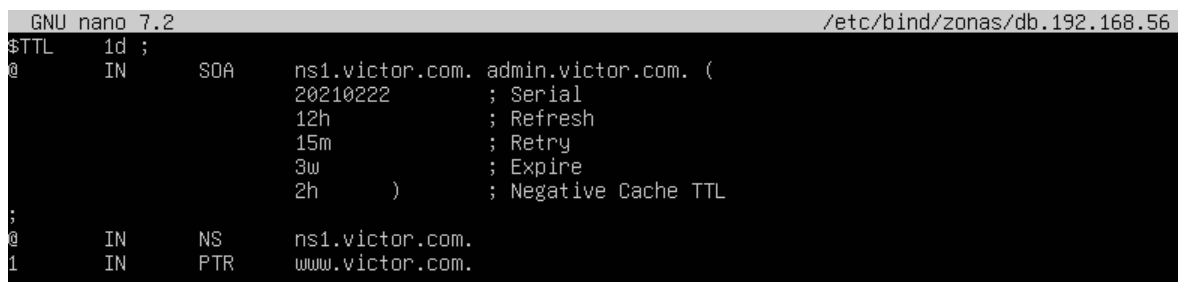
        IN      NS       ns1.victor.com.
ns1      IN      A        192.168.56.1
www      IN      A        192.168.56.1
```

**// La línea etiquetada como ‘serial’ recoge un número que deberá incrementarse manualmente cada vez que editemos este archivo, ya sea para modificar nombres o añadir nuevos.**

**// La línea admin.networld.cu. se trata de la dirección de correo del administrador del servidor DNS sin el @, estos datos al igual que los tiempos de Refresh y demás no se tratan a la ligera, pues son los que dan reputación y confiabilidad a nuestro servidor en el mundo cuando estamos trabajando sobre un servidor DNS autoritativo o real.**

```
# sudo nano /etc/bind/zonas/db.192.168.56
```

```
$TTL      1d ;
@         IN      SOA      ns1.networld.cu. admin.networld.cu. (
                                20210222      ; Serial
                                12h             ; Refresh
                                15m             ; Retry
                                3w              ; Expire
                                2h              ; Negative Cache TTL
                                )
;
@         IN      NS       ns1.networld.cu.
1         IN      PTR      www.networld.cu.
```

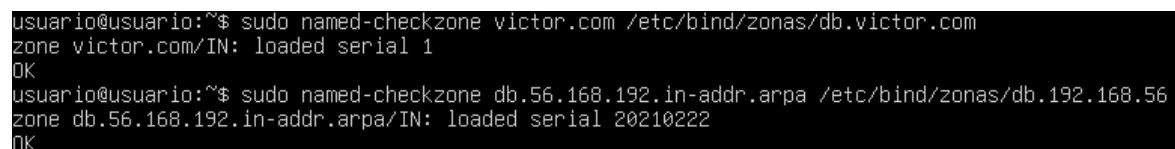


```
GNU nano 7.2 /etc/bind/zonas/db.192.168.56
$TTL      1d ;
@         IN      SOA      ns1.victor.com. admin.victor.com. (
                                20210222      ; Serial
                                12h             ; Refresh
                                15m             ; Retry
                                3w              ; Expire
                                2h              ; Negative Cache TTL
                                )
;
@         IN      NS       ns1.victor.com.
1         IN      PTR      www.victor.com.
```

**//Es importante en estos dos archivos que acabamos de crear respetar los signos, cualquier error conlleva que el servidor no arranque.**

10- Comprobar los archivos de zona que acabamos de crear para ver si todo está bien.

```
# sudo named-checkzone victor.com /etc/bind/zonas/db.victor.com
# sudo named-checkzone db.56.168.192.in-addr.arpa
/etc/bind/zonas/db.192.168.56
```



```
usuario@usuario:~$ sudo named-checkzone victor.com /etc/bind/zonas/db.victor.com
zone victor.com/IN: loaded serial 1
OK
usuario@usuario:~$ sudo named-checkzone db.56.168.192.in-addr.arpa /etc/bind/zonas/db.192.168.56
zone db.56.168.192.in-addr.arpa/IN: loaded serial 20210222
OK
```

**//Debemos obtener un OK en cada comprobación**

## 11- Reiniciamos nuevamente

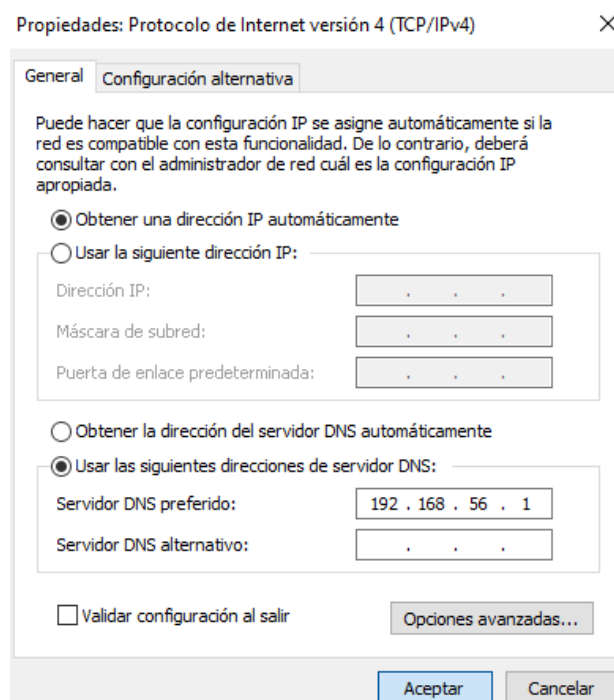
# sudo systemctl restart bind9

```
usuario@usuario:~$ sudo systemctl start bind9 && systemctl status bind9
• named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-10-30 11:30:29 UTC; 10min ago
     Docs: man:named(8)
   Main PID: 18630 (named)
    Status: "running"
     Tasks: 18 (limit: 9984)
  Memory: 7.6M (peak: 8.8M)
     CPU: 85ms
    CGroup: /system.slice/named.service
           └─18630 /usr/sbin/named -f -u bind -4

oct 30 11:30:29 usuario named[18630]: managed-keys-zone: loaded serial 3
oct 30 11:30:29 usuario named[18630]: zone 0.in-addr.arpa/IN: loaded serial 1
oct 30 11:30:29 usuario named[18630]: zone 255.in-addr.arpa/IN: loaded serial 1
oct 30 11:30:29 usuario named[18630]: zone localhost/IN: loaded serial 2
oct 30 11:30:29 usuario named[18630]: zone 127.in-addr.arpa/IN: loaded serial 1
oct 30 11:30:29 usuario named[18630]: zone victor.com/IN: loaded serial 1
oct 30 11:30:29 usuario named[18630]: zone 56.168.192.in-addr.arpa/IN: loaded serial 20210222
oct 30 11:30:29 usuario named[18630]: all zones loaded
oct 30 11:30:29 usuario named[18630]: running
oct 30 11:30:29 usuario systemd[1]: Started named.service - BIND Domain Name Server.
```

## 12- Comprobar funcionamiento desde otro PC.

- A) En la máquina de Windows cliente, indica que el DNS es la máquina que hemos configurado:





```

Adaptador de Ethernet Ethernet:


  Sufijo DNS específico para la conexión. . . : example.org
  Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
  Dirección física. . . . . : 08-00-27-42-77-0A
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Vínculo: dirección IPv6 local. . . : fe80::89ac:248:b464:f973%5(Preferido)
  Dirección IPv4. . . . . : 192.168.56.101(Preferido)
  Máscara de subred . . . . . : 255.255.255.0
  Concesión obtenida. . . . . : lunes, 4 de noviembre de 2024 13:02:31
  La concesión expira . . . . . : lunes, 4 de noviembre de 2024 13:40:10
  Puerta de enlace predeterminada . . . . . : 192.168.56.1
  Servidor DHCP . . . . . : 192.168.56.1
  IAID DHCPv6 . . . . . : 101187623
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-2E-70-5D-91-08-00-27-42-77-0A
  Servidores DNS. . . . . : 192.168.56.1
  NetBIOS sobre TCP/IP. . . . . : habilitado
  
```

También hay que comprobar que el servidor DHCP de Ubuntu este configurado de manera estática. Y ejecutar el comando “sudo netplan apply” para sincronizar los cambios.

```

GNU nano 7.2 /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses: [192.168.56.1/24]
      dhcp4: true
      dhcp-identifier: mac
#
#
version: 2
  
```

ping [www.victor.com](http://www.victor.com)

 Símbolo del sistema

```

C:\Users\cliente>ping www.victor.com

Haciendo ping a www.victor.com [192.168.56.1] con 32 bytes de datos:
Respuesta desde 192.168.56.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.56.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.56.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.56.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.56.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
  
```

- B) Otra opción, podría ser configurar el servidor DHCP para que nos dé los DNS primarios por defecto. Investiga como se configura el servidor DHCP en Ubuntu para que te asigne por defecto el DNS de tu servidor. Comprueba que funciona en la máquina de Ubuntu cliente.

Puedes configurarlo desde el archivo de “/etc/dhcp/dhcpd.conf” escribiendo la siguiente línea de código “option domain-name-servers 192.168.56.1” desde la configuración de reserva o la configuración normal de rango de DHCP.

```
host UCVictor {
    hardware ethernet 08:00:27:80:00:3b;
    fixed-address 192.168.56.33;
    option domain-name-servers 192.168.56.1;
}
```

```
#DHCP para la red interna
subnet 192.168.56.0 netmask 255.255.255.0 {
    range 192.168.56.100 192.168.56.200;
    option subnet-mask 255.255.255.0;
    option routers 192.168.56.1;
    option broadcast-address 192.168.56.255;
    option domain-name-servers 192.168.56.1;
}
```

```
usuario@UCVictor:~$ ping www.victor.com -c4
PING www.victor.com (192.168.56.1) 56(84) bytes of data.
64 bytes from www.victor.com (192.168.56.1): icmp_seq=1 ttl=64 time=0.772 ms
64 bytes from www.victor.com (192.168.56.1): icmp_seq=2 ttl=64 time=0.870 ms
64 bytes from www.victor.com (192.168.56.1): icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from www.victor.com (192.168.56.1): icmp_seq=4 ttl=64 time=0.710 ms

--- www.victor.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0.710/0.914/1.304/0.232 ms
```