

BOOTCAMP ESPECIALIDAD GNU/LINUX (2023)

Lab 09 - Servicio DNS

Pedro Antonio Mayorgas Parejo

28 de agosto de 2023

Índice

1	Topología de la red	3
2	Instalación del servicio DNS	3
3	Creando el fichero de configuración de las zonas internas	6
4	Pruebas con el DNS	9

1. Topología de la red

Debido a la definición del ejercicio, se ha definido la siguiente topología, en la cual están los siguientes dispositivos intermedios:

- 2 Switches de Capa 2
- 1 DNS autoritativo .net, con capacidad de conexión NAT
- 2 Clientes, con nombres registrados en el DNS

Esta es la topología de red. Todos los dispositivos tienen la dirección que aparecen o encima o a su izquierda asignada de manera manual.

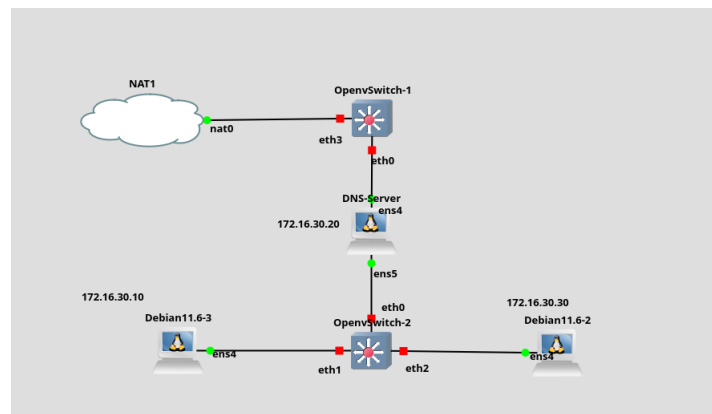


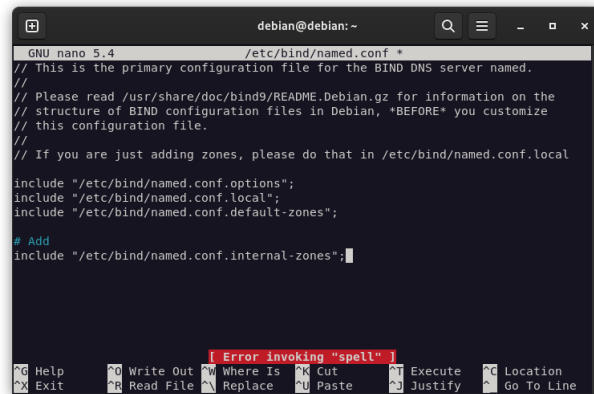
Figura 1: Topología de red.

2. Instalación del servicio DNS

Para la instalación del servicio DNS, tenemos que ejecutar el siguiente comando:

```
1 sudo apt install bind9 bind9utils
2 # FOR DEBUG
3 sudo apt install dnsutils
```

Luego de instalar el servicio DNS, tenemos que configurar el siguiente fichero, para crear una zona y que pueda localizar los ficheros de zona. El fichero en concreto que debemos editar es **/etc/bind/named.conf**. La línea que añadimos, es una ruta que nos permite indicar las zonas internas que queramos crear para nosotros, es un fichero de configuración adicional de las zonas que gestiona bind9.

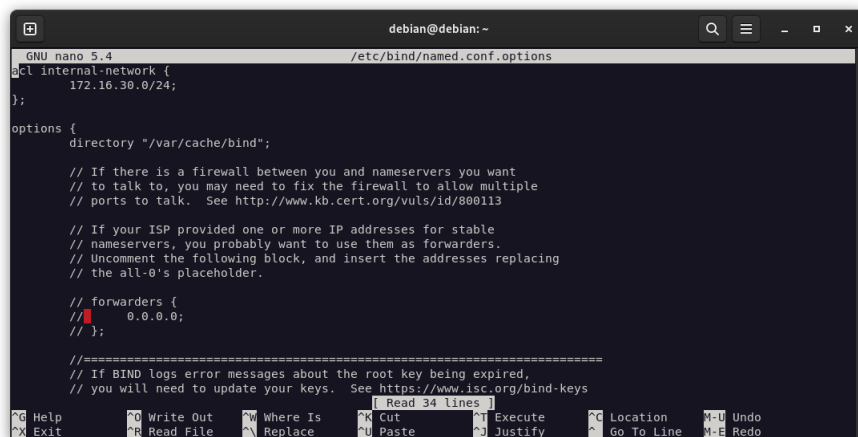


```
GNU nano 5.4 /etc/bind/named.conf *
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
# Add
include "/etc/bind/named.conf.internal-zones";

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Figura 2: Indicando la zona interna.

Ahora editamos otro fichero de configuración interna, para permitir un ACL para la red local para que pueda realizar consultas. El fichero en concreto es `/etc/bind/named.conf.options`.



```
GNU nano 5.4 /etc/bind/named.conf.options
acl internal-network {
    172.16.30.0/24;
};

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

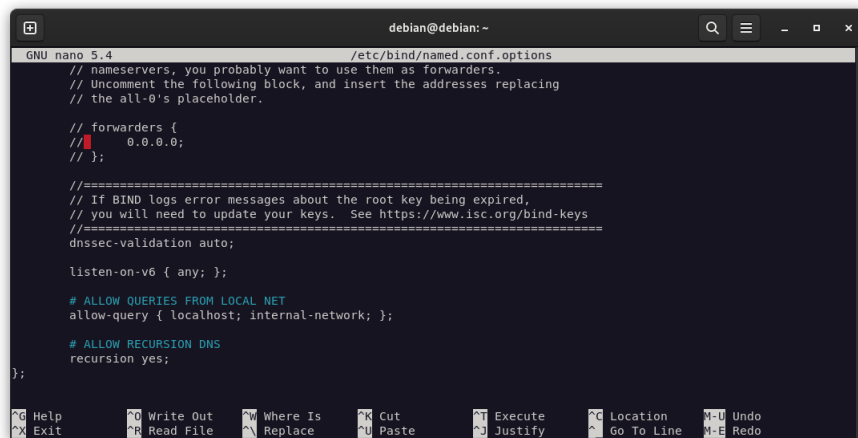
    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // 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
    Read 34 lines
    ^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
    ^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line
    ^M-U Undo
    ^M-E Redo
```

Figura 3: Indicando el ACL para la zona interna.

Luego al final, indicamos las directivas que permiten las consultas al DNS con las ACL y un modo de consulta.



```
GNU nano 5.4 /etc/bind/named.conf.options
// 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; };

# ALLOW QUERIES FROM LOCAL NET
allow-query { localhost; internal-network; };

# ALLOW RECURSION DNS
recursion yes;
};

^G Help      ^O Write Out  ^W Where Is   ^X Cut        ^T Execute    ^G Location   ^+U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^_ Justify    ^_ Go To Line  ^-E Redo
```

Figura 4: Directivas para permitir las consultas.

3. Creando el fichero de configuración de las zonas internas

Ahora debemos crear el fichero de configuración de la zona interna, indicado en `/etc/bind/named.conf`. Dicho fichero tiene dos subficheros, uno de la resolución normal de nombres y otro de la resolución inversa de nombres.

La resolución normal, consiste en que cuando le preguntas a tu DNS quién es pepe.com, este te busca si no tiene esa zona, desde la raíz primero el servidor DNS (root) ., luego el servidor autoritativo .com., luego el servidor DNS .com devuelve la IP de pepe.com.

En la resolución inversa, se apunta a un servidor de autoridad arpa., luego escala la petición a in-addr.arpa, luego va escalando en cada octeo de IPv4 hasta encontrar el DNS que esté en el nodo hoja que se corresponda con la IPv4 completa. En nuestro caso la IPv4 que se escribe como 172.16.30.0/24, se debe escribir al revés y sin la parte del host que se deja sin poner en el fichero de zona de resolución inversa.

Cuando queramos buscar el nombre de dominio de un host, pero solo sabemos su dirección IP, tenemos que ponerla al revés de la siguiente manera, 10.30.16.172.in-addr.arpa, la cual crea una petición de resolución inversa.

Ahora creamos el fichero de la zona interna, la cual quedaría como en la siguiente captura.

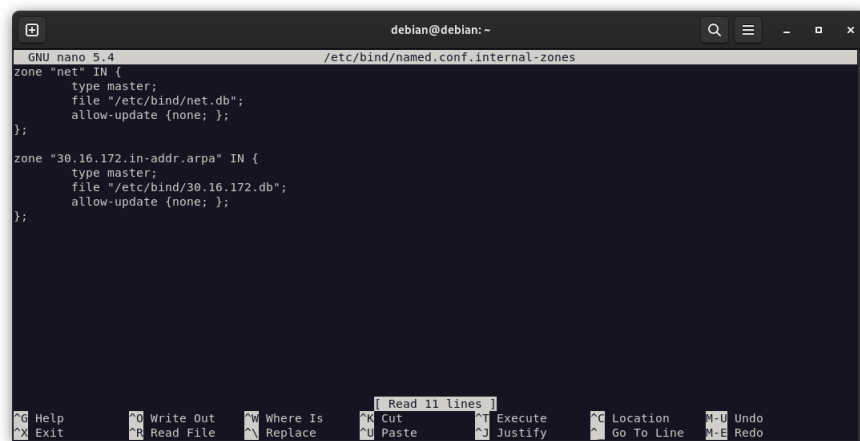


Figura 5: Configuración del fichero de zonas.

En la captura podemos ver, que en cada zona hay un fichero asociado con una ruta absoluta, en dicho fichero, tenemos que generarlo con el de ejemplo que nos trae bind9 para evitar errores tipográficos. Para crear los ficheros hemos utilizado los siguientes comandos:

- 1 `# Fichero DNS normal`
- 2 `sudo cp /etc/bind/db.empty /etc/bind/net.db`
- 3 `# Fichero DNS de Reverse resolution`
- 4 `sudo cp /etc/bind/db.0 /etc/bind/30.16.172.db`

Primero configuramos la zona de resolución normal, esta zona tiene la característica de que aquí se alojan las resoluciones del tipo A, AAAA, NS, MX,...

```

debian@debian:~
GNU nano 5.4 /etc/bind/net.db *
; BIND reverse data file for empty rfc1918 zone

;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL      86400
@         IN      SOA      ns.net. root.ns.net. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        86400 )    ; Negative Cache TTL
;
@         IN      NS       ns.net.

servicel  IN      A        172.16.30.10
ns        IN      A        172.16.30.20
service2  IN      A        172.16.30.30

```

Figura 6: Configuración de la zona .net.

Ahora configuramos la zona de resolución inversa, esta zona es la que tiene todos los PTR.

```

debian@debian:~
GNU nano 5.4 /etc/bind/30.16.172.db
;
; BIND reverse data file for broadcast zone
;
$TTL 604800
@      IN      SOA      ns.net. root.net. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
;
10     IN      PTR      servicel.net
20     IN      PTR      ns.net.
30     IN      PTR      service2.net.

Wrote 15 lines
^X Help      ^O Write Out ^K Where Is  ^N Execute   ^C Location
^Y Exit      ^R Read File ^U Replace   ^J Justify  ^_ Go To Line

```

Figura 7: Configuración de la zona inversa.

Una vez terminada la configuración de las zonas, tenemos que reiniciar el servicio bind9, el cual cuando consultamos el log, para que sepamos que el servicio está funcionando correctamente tenemos que tener las siguientes líneas de que se han cargado tanto nuestra zona, como las zonas que necesita el DNS.

```
1 sudo systemctl restart bind9.service
```

```
debian@debian: ~$ sudo systemctl restart bind9.service
Aug 28 15:46:14 debian named[9175]: automatic empty zone: D.F.IP6.ARPA
Aug 28 15:46:14 debian named[9175]: automatic empty zone: 8.E.F.IP6.ARPA
Aug 28 15:46:14 debian named[9175]: automatic empty zone: 9.E.F.IP6.ARPA
Aug 28 15:46:14 debian named[9175]: automatic empty zone: A.E.F.IP6.ARPA
Aug 28 15:46:14 debian named[9175]: automatic empty zone: B.E.F.IP6.ARPA
Aug 28 15:46:14 debian named[9175]: automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
Aug 28 15:46:14 debian named[9175]: automatic empty zone: EMPTY.AS112.ARPA
Aug 28 15:46:14 debian named[9175]: automatic empty zone: HOME.ARPA
Aug 28 15:46:14 debian named[9175]: configuring command channel from '/etc/bind/rndc.key'
Aug 28 15:46:14 debian named[9175]: command channel listening on 127.0.0.1#953
Aug 28 15:46:14 debian named[9175]: configuring command channel from '/etc/bind/rndc.key'
Aug 28 15:46:14 debian named[9175]: command channel listening on ::1#953
Aug 28 15:46:14 debian named[9175]: managed-keys-zone: loaded serial 2
Aug 28 15:46:14 debian named[9175]: zone localhost/IN: loaded serial 2
Aug 28 15:46:14 debian named[9175]: zone 0.in-addr.arpa/IN: loaded serial 1
Aug 28 15:46:14 debian named[9175]: zone 255.in-addr.arpa/IN: loaded serial 1
Aug 28 15:46:14 debian named[9175]: zone net/IN: loaded serial 2
Aug 28 15:46:14 debian named[9175]: zone 127.in-addr.arpa/IN: loaded serial 1
Aug 28 15:46:14 debian named[9175]: zone 122.168.192.in-addr.arpa/IN: loaded serial 2
Aug 28 15:46:14 debian named[9175]: all zones loaded
Aug 28 15:46:14 debian named[9175]: running
Aug 28 15:46:14 debian named[9175]: managed-keys-zone: Unable to fetch DNSKEY set '': failure
debian@debian: ~$
```

Figura 8: Carga correcta del servicio bind9.

Una vez cargado el servicio DNS correctamente, tenemos que configurar en el fichero de configuración de las interfaces para poder indicar que el DNS es el propio y está en localhost.

```
GNU nano 5.4 /etc/network/interfaces.d/50-cloud-init
# 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}
auto lo
iface lo inet loopback

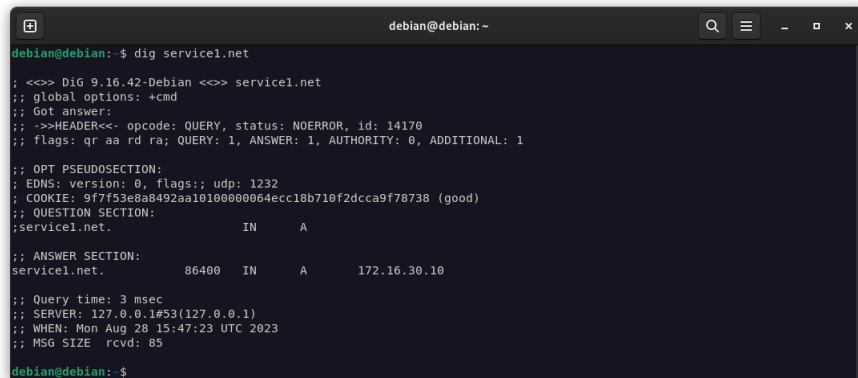
auto ens4
iface ens4 inet dhcp

auto ens5
iface ens5 inet static
address 172.16.30.20
netmask 255.255.255.0
dns-nameservers 127.0.0.1
```

Figura 9: Configuración de interfaces de red.

4. Pruebas con el DNS

Se ha utilizado la herramienta de DIG para realizar las pruebas de la consulta de DNS.



```
debian@debian:~$ dig service1.net

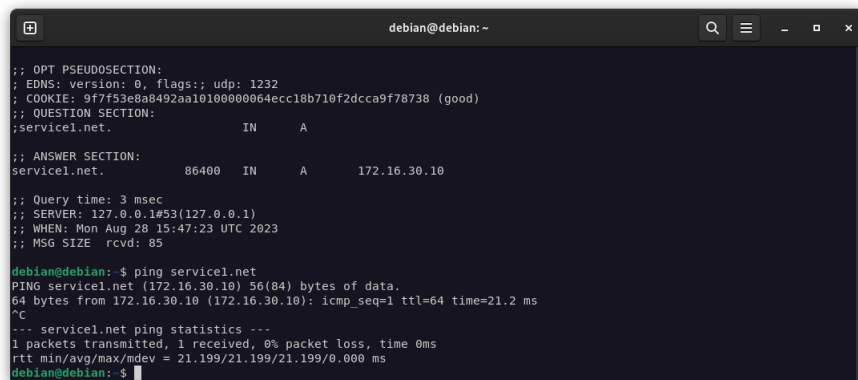
;<>> DiG 9.16.42-Debian <>> service1.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 14170
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1232
; COOKIE: 9f7f53e8a8492aa10100000064ecc18b710f2dcca9f78738 (good)
;; QUESTION SECTION:
;service1.net.                IN      A
;; ANSWER SECTION:
service1.net.                 86400   IN      A      172.16.30.10

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 28 15:47:23 UTC 2023
;; MSG SIZE rcvd: 85

debian@debian:~$
```

Figura 10: Consulta de la IP del service1.net.



```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1232
; COOKIE: 9f7f53e8a8492aa10100000064ecc18b710f2dcca9f78738 (good)
;; QUESTION SECTION:
;service1.net.                IN      A
;; ANSWER SECTION:
service1.net.                 86400   IN      A      172.16.30.10

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 28 15:47:23 UTC 2023
;; MSG SIZE rcvd: 85

debian@debian:~$ ping service1.net
PING service1.net (172.16.30.10) 56(84) bytes of data:
64 bytes from 172.16.30.10 (172.16.30.10): icmp_seq=1 ttl=64 time=21.2 ms
^C
--- service1.net ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 21.199/21.199/21.199/0.000 ms
debian@debian:~$
```

Figura 11: Ping con resolución DNS a service1.net.

```
debian@debian:~$ dig service2.net

;<<> DiG 9.16.42-Debian <<> service2.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56101
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b3f0c1984652e3f20100000064ecc22b689803f8a616fff4 (good)
;; QUESTION SECTION:
;service2.net.                IN      A

;; ANSWER SECTION:
service2.net.                86400   IN      A      172.16.30.30

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 28 15:50:03 UTC 2023
;; MSG SIZE rcvd: 85

debian@debian:~$ ping service2.net
```

Figura 12: Consulta de la IP del service2.net.

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37077
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c6da4ecd8bd8ce50100000064ecc0253f85612133a36893 (good)
;; QUESTION SECTION:
;service2.net.                IN      A

;; ANSWER SECTION:
service2.net.                86400   IN      A      172.16.30.30

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 28 16:15:33 UTC 2023
;; MSG SIZE rcvd: 85

debian@debian:~$ ping service2.net
PING service2.net (172.16.30.30) 56(84) bytes of data:
64 bytes from service2.net (172.16.30.30): icmp_seq=1 ttl=64 time=8.79 ms
64 bytes from service2.net (172.16.30.30): icmp_seq=2 ttl=64 time=7.58 ms
64 bytes from service2.net (172.16.30.30): icmp_seq=3 ttl=64 time=5.30 ms
^C
--- service2.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.304/7.224/8.786/1.444 ms
debian@debian:~$
```

Figura 13: Ping con resolución DNS a service2.net.

En el siguiente hacemos una consulta especial de DNS, donde indicamos que queremos saber quienes son los servidores DNS con el campo NS.

```
debian@debian:~$ dig NS net.

;<<>> Dig 9.16.42-Debian <<>> NS net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20107
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 46b8be27af06a7520100000064ecc23ec8c6c6c521465593 (good)
;; QUESTION SECTION:
;net.                                IN      NS
;; ANSWER SECTION:
net.                                86400   IN      NS      ns.net.
;; ADDITIONAL SECTION:
ns.net.                             86400   IN      A        172.16.30.20
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 28 15:50:22 UTC 2023
;; MSG SIZE rcvd: 93
debian@debian:~$
```

Figura 14: Conociendo los servidores de nombres de autoridad en .net.

En la siguiente captura, hemos creado una consulta especial para obtener el registro PTR, para que el DNS nos devuelva el nombre completo de una dirección IP.

```
debian@debian:~$ dig PTR 30.30.16.172.in-addr.arpa.

;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 28 15:58:09 UTC 2023
;; MSG SIZE rcvd: 129
debian@debian:~$ dig PTR 30.30.16.172.in-addr.arpa.

;<<>> Dig 9.16.42-Debian <<>> PTR 30.30.16.172.in-addr.arpa.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41547
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 53650041a14706730100000064ecc417863ba0b67d0e7ddf (good)
;; QUESTION SECTION:
;30.30.16.172.in-addr.arpa.        IN      PTR
;; ANSWER SECTION:
30.30.16.172.in-addr.arpa. 604800 IN      PTR      service2.net.
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 28 15:58:15 UTC 2023
;; MSG SIZE rcvd: 108
debian@debian:~$
```

Figura 15: Obteniendo el registro PTR de la ip 172.16.30.30 que nos devuelve el nombre servicio2.net.

Luego por último el comando dig permite la consulta sin tener que poner in-addr.arpa pasándole el parámetro -X para que te haga el nombre de resolución inversa.

```
debian@debian: ~  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Mon Aug 28 15:58:09 UTC 2023  
;; MSG SIZE rcvd: 129  
  
debian@debian:~$ dig PTR 30.30.16.172.in-addr.arpa.  
  
;<<>> DiG 9.16.42-Debian <<>> PTR 30.30.16.172.in-addr.arpa.  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 41547  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: 53650041a14706730100000064ecc417863ba0b67d0e7ddf (good)  
;; QUESTION SECTION:  
;30.30.16.172.in-addr.arpa. IN PTR  
  
;; ANSWER SECTION:  
30.30.16.172.in-addr.arpa. 604800 IN PTR service2.net.  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Mon Aug 28 15:58:15 UTC 2023  
;; MSG SIZE rcvd: 108  
debian@debian:~$
```

Figura 16: Resolución inversa de 172.16.30.10.