

configurar DNS

CLIENTE:

ip a -> compruebo que no hay ip configurada

ping 8.8.8.8 -> compruebo que no funciona la conexión a internet

configuracion red > IPv4 > manual: Dirección > 192.168.4.15

Mascara: 255.255.255.0

Puerta Enlace (ip servidor): 192.168.4.250

DNS > servidor > 192.168.4.250

Rutas > direccion > 192.168.4.250

config red avanzada > cableada > ajustes ipv4 >dominios de búsqueda: acgdaw.local

ip a -> comprobar que se ha configurado la ip que hemos puesto (si no funciona reiniciar el cliente)

ip route -> sale la que hemos configurado

resolvestl -> tiene que estar ipDNS y acgdaw.local

SERVIDOR DNS:

sudo nano /etc/netplan/50....

enp0s3: dhcp4: true

enp0s8: dhcp4: false addresses: [192.168.4.250/24]

sudo netplan generate

sudo netplan apply

ip a

CLIENTE:

ping 192.168.4.250

ssh dns@192.168.4.250

ip a

- me apunto las ip que me salen: enp0s3: ip: 10.0.2.15/24

ip route

- me apunto la vía por defecto: 10.0.2.2

sudo nano /etc/netplan/50....

enp0s3: dhcp4: false

addresses: [10.0.2.250/24]

routes: - to: default

via: 10.0.2.2

sudo netplan generate

sudo netplan apply

ip a

ping 8.8.8.8

sudo apt update

sudo apt-get install bind9 bind9-utils

sudo systemctl status bind9

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

```

dns@servidor: /etc/bind
named.conf.options

GNU nano 7.2
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.
    listen-on { any; };
    allow-query { localhost; 192.168.4.0/24; };

    forwarders {
        #10.0.2.2;
        #0.0.0.0;
        8.8.8.8;
    };

    //=====================================================================
    // 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 no;

    recursion yes;
    //listen-on-v6 { none; };
};


```

```

sudo apt install ufw
sudo ufw allow bind9
sudo ufw status
sudo apt remove ufw
sudo apt install netfilter-persistent iptables-persistent
sudo netfilter-persistent save


```

```

sudo nano /etc/netplan/50....
enp0s3: dhcp4: false
    addresses: [10.0.2.250/24]
    routes: - to: default
            via: 10.0.2.2
    nameservers:
        addresses: [10.0.2.250]
        search: [acgdaw.local]


```

```

sudo netplan generate
sudo netplan apply
resovectl
cd /etc/bind
ls
***copia de seguridad del archivo:
sudo cp named.conf.local named.conf.local_fecha


```

```

sudo nano named.conf.local
***añadir debajo del todo:
zone "acgdaw.local" {
    type master;
    file "/etc/bind/zonas/db.acgdaw.local";
};

zone "4.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zonas/db.4.168.192.in-addr.arpa";
};
sudo mkdir zonas
sudo cp db.local zonas/db.acgdaw.local
cd zonas/
sudo nano db.acgdaw.local

```

```

dns@servidor: /etc/bind/zonas
GNU nano 7.2                               db.acgdaw.local *

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.acgdaw.local. root.acgdaw.local. (
                        2           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )     ; Negative Cache TTL
;
@           IN      NS      ns1
ns1          IN      A       192.168.4.250
servidor     IN      A       192.168.4.250
dns          IN      A       192.168.4.15
server        IN      CNAME   servidor

```

```

sudo cp db.acgdaw.local db.4.168.192.in-addr.arpa
sudo nano db.4.168.192.in-addr.arpa

```

```
dns@servidordns:/etc/bind/zonas
GNU nano 7.2          db.4.168.192.in-addr.arpa *

;
; BIND data file for local loopback interface
;
$TTL    604800
@      IN      SOA     ns1.acgdaw.local. root.acgdaw.local. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@      IN      NS      ns1.acgdaw.local.
250   IN      PTR     ns1.acgdaw.local
15    IN      PTR     dns.acgdaw.local.
```

sudo named-checkzone acgdaw.local /etc/bind/zonas/db.acgdaw.local

*****tiene que salir OK

sudo named-checkzone [db.4.168.192.in-addr.arpa](#) /etc/bind/zonas/[db.4.168.192.in-addr.arpa](#)

*****tiene que salir OK

sudo systemctl restart bind9

sudo systemctl status bind9

COMPROBACIONES DESDE CLIENTE OTRO TERMINAL:

nslookup ns1

```
cliente@cliente-VirtualBox:~$ nslookup ns1
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name: ns1.acgdaw.local
Address: 192.168.4.250
```

nslookup ns1.acgdaw.local

```
cliente@cliente-VirtualBox:~$ nslookup ns1.acgdaw.local
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name: ns1.acgdaw.local
Address: 192.168.4.250
```

```
nslookup dns
```

```
cliente@cliente-VirtualBox:~$ nslookup dns
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: dns.acgdaw.local
Address: 192.168.4.15
```

```
ping google.es
```

```
nslookup 192.168.4.250
```

```
cliente@cliente-VirtualBox:~$ nslookup 192.168.4.250
250.4.168.192.in-addr.arpa name = ns1.acgdaw.local.4.168.192.in-addr.arpa.

Authoritative answers can be found from:
```

```
cat /etc/resolv.conf
```

```
cliente@cliente-VirtualBox:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search acgdaw.local
```