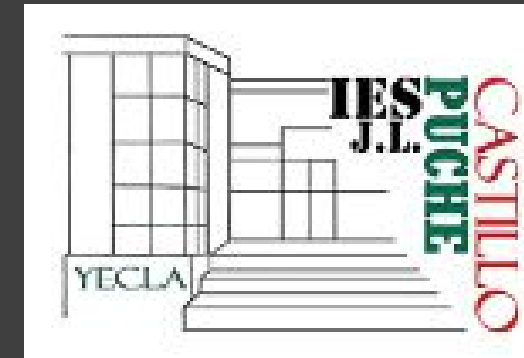


2ºDAW DESPLIEGUE DE APLICACIONES WEB



Unidad 3- Instalación DNS en Ubuntu Server

Profesora:
blanca.palao@murciaeduca.es

Índice

0. Descargar server.

0. Habilitar adaptadores de red.

1. Configuración del servidor.

2. Pruebas de resolución de nombres.

0. Descargar server

- > Descargar ISO y crear máquina Ubuntu servidor nueva.
- > Podemos realizar la práctica y la configuración en el mismo Ubuntu Server dónde tenemos el servicio DHCP ya configurado.
- > Arrancar con una sola tarjeta de red en NAT.

0. Habilitar adaptadores de red

-> Antes de arrancar el servidor, cambiar el adaptador a **NAT** (en el aula) o adaptador puente (en casa) para tener Internet en el server y poder realizar la actualización de los repositorios y la instalación del servicio.

> Arrancamos y nos quedamos con la IP configurada en el adaptador de red enp0s3.

En mi caso:

10.0.2.15

1. Configuración del servidor

Previo a la instalación en Ubuntu, actualizamos repositorios:

> ***sudo su***

> ***apt-get update***

> ***apt-get upgrade***

Si os da error al actualiza, liberad la concesión y volver a solicitar IP

> ***dhclient -r enp0s3 -v***

Instalación **BIND9**: es el servidor de nombres de dominio (DNS) más popular en Internet usado comúnmente en sistemas Unix. Se utiliza cuando un nodo (o host) en Internet contacta a otro mediante el nombre de domino de la máquina y no por su dirección IP.

<https://bind9.readthedocs.io/en/latest/>

1. Configuración del servidor

> apt-get install -y bind9

Carpetas con las que vamos a trabajar (si no las localizas no se ha instalado correctamente el servidor):

Configurar el servidor DNS primario

La configuración de BIND consta de varios archivos que se incluyen desde el archivo de configuración principal, `/etc/bind/named.conf`. Estos nombres de archivos comienzan con named porque ese es el nombre del proceso que BIND ejecuta (abreviatura de “domain name daemon”).

1. Configuración del servidor

1.Configurar el archivo local Comenzaremos configurando el archivo local.

> nano /etc/bind/named.conf.local

Aquí especificaremos nuestras **zonas directas e inversas**. Las zonas DNS designan un alcance específico para administrar y definir registros DNS. Debido a que nuestro dominio será nombre.com -> “blanca.com”, usaremos eso como nuestra zona de directa. Debido a que las direcciones IP privadas de nuestros servidores están en el espacio IP, por ejemplo, 10.0.2.15/24, configuraremos una zona inversa para poder definir búsquedas inversas en ese intervalo.

1. Configuración del servidor

1. Configurar el archivo local

Añada la zona de directa con las siguientes líneas, sustituyendo el nombre de la zona por el dominio que desees:

file será el archivo de la base de datos que vamos a crear y que alojará los dominios vs Ips.

Tipo master = principal.

```
GNU nano 2.9.3 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";
// ZONA DIRECTA

zone "blanca.com" {
    type master;
    file "/etc/bind/db.blanca.com";
};

//ZONA INVERSA

zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.2.0.10";
};
```


1. Configuración del servidor

1. Configurar el archivo local

Suponiendo que nuestra IP de enp0s3 es 10.0.2.15/24, agrega la zona inversa con las siguientes líneas (ten en cuenta que el nombre de nuestra zona inversa comienza con “2.0.10”, que es el octeto inverso de “10.0.2”):

El dominio **in-addr.arpa** es una parte conceptual del espacio de nombres DNS que utiliza direcciones IP para sus zonas inversas:

```
GNU nano 2.9.3 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";
// ZONA DIRECTA

zone "blanca.com" {
    type master;
    file "/etc/bind/db.blanca.com";
};

//ZONA INVERSA

zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.2.0.10";
};
```

1. Configuración del servidor

1.Configurar el archivo local Renombramos el fichero inverso que hay y que se llama **db.127.** > cp db.127 [nombre de vuestro fichero zona directa]

```
root@blanca:/etc/bind# ls
bind.keys  db.255      db.root      named.conf.local  zones.rfc1918
db.0       db.empty    named.conf    named.conf.options
db.127     db.local    named.conf.default-zones  rndc.key
root@blanca:/etc/bind# more db.127
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      localhost. root.localhost. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       localhost.
1.0.0     IN      PTR      localhost.
root@blanca:/etc/bind#
```

```
root@blanca:/etc/bind# ls
bind.keys  db.255      db.root      named.conf.local  zones.rfc1918
db.0       db.empty    named.conf    named.conf.options
db.127     db.local    named.conf.default-zones  rndc.key
root@blanca:/etc/bind# _
```

Renombrar para que se llame con el nombre del fichero configurado en la zona inversa. En mi caso: **db.2.0.10**

1. Configuración del servidor

1.Configurar el archivo local Renombramos el fichero directo que hay y que se llama **db.local**:

```
root@dns:/etc/bind# ls
bind.keys  db.2.0.10  db.empty  named.conf  named.conf.opt
db.0       db.255     db.local  named.conf.default-zones  rndc.key
db.127     db.blanca.com  db.root  named.conf.local  zones.rfc1918
```

```
db.127     db.blanca.com  db.root  named.conf.local
root@dns:/etc/bind# cp db.local db.blanca.com
```

> **cp db.local** [nombre de vuestro fichero zona directa]

1. Configuración del servidor

1.Configurar el archivo local Ahora actualizamos el fichero de zona directa para indicar nuestro nombre de dominio:

> *nano db.blanca.com*

- Nombre del servidor autoritario (SOA).
- Email admin.
- @, hace referencia al nombre de la zona, en mi caso blanca.com.
- Línea para el servidor de nombre NS.
- La máquina A del servidor.
- El DNS está en la misma máquina.

```
root@dns:/etc/bind# more db.blanca.com
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA     blanca.com. root.blanca.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS      blanca.com.
@         IN      A       192.168.30.2
servidordns IN      A       192.168.30.2
cliente1   IN      A       192.168.30.6
cliente2   IN      A       192.168.30.7
root@dns:/etc/bind# more db.2.0.10
```

1. Configuración del servidor

1. Configurar el archivo local Editamos el fichero de zona directa:

> *nano db.2.0.10*

- Nombre del servidor autoritario (SOA).
- Email admin.
- @, hace referencia al nombre de la zona, en mi caso blanca.com.
- La IP de la máquina que estamos configurando en cada PTR.

```
root@dns:/etc/bind# more db.2.0.10
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      blanca.com. root.blanca.com. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       blanca.com.
192.168.30.2 IN      PTR    blanca.com.
192.168.30.2 IN      PTR    servidor dns.blanca.com.
192.168.30.6 IN      PTR    cliente1.blanca.com.
192.168.30.7 IN      PTR    cliente2.blanca.com.
blanca.com. IN      A       192.168.30.2
root@dns:/etc/bind# _
```

1. Configuración del servidor

1. Configurar el archivo local En las imágenes se exponen ejemplos.

En este supuesto práctico:

- El Server de Ubuntu tiene la IP:
192.168.30.2
- El cliente de Ubuntu 22,04:
192.168.30.6
- El cliente de Windows 10:
192.168.30.7

```
root@dns:/etc/bind# more db.blanca.com
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA     blanca.com. root.blanca.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS      blanca.com.
@         IN      A       192.168.30.2
servidordns IN      A       192.168.30.2
cliente1   IN      A       192.168.30.6
cliente2   IN      A       192.168.30.7
root@dns:/etc/bind# more db.2.0.10
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA     blanca.com. root.blanca.com. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS      blanca.com.
192.168.30.2 IN      PTR   blanca.com.
192.168.30.2 IN      PTR   servidordns.blanca.com.
192.168.30.6 IN      PTR   cliente1.blanca.com.
192.168.30.7 IN      PTR   cliente2.blanca.com.
blanca.com. IN      A       192.168.30.2
root@dns:/etc/bind#
```

1. Configuración del servidor

1.Configurar el archivo local Ahora testeamos si están bien configurados ambos con (cambiar por vuestro dominio y nombre del file):

> *named-checkzone blanca.com /etc/bind/db.blanca.com*

> *named-checkzone blanca.com /etc/bind/db.2.0.10*

```
root@dns:/etc/bind# named-checkzone blanca.com /etc/bind/db.2.0.10
zone blanca.com/IN: loaded serial 1
OK
root@dns:/etc/bind# named-checkzone blanca.com /etc/bind/db.blanca.com
zone blanca.com/IN: loaded serial 2
OK
root@dns:/etc/bind# _
```

1. Configuración del servidor

1. Configurar el archivo local Reseteamos el servicio DNS:

> *systemctl restart bind9*

```
root@dns:/etc/bind# systemctl restart bind9
root@dns:/etc/bind# _
```

Pasamos a comprobar que el adaptador enp0s3 tenga correctamente la IP con la que hemos trabajado:

> *networkctl status*

Con este comando vemos un resumen de los dispositivos de red y su estado de conexión ->

```
root@dns:/etc/bind# networkctl status
• State: routable
  Address: 10.0.2.15 on enp0s3
           fe80::a00:27ff:fe53:4661 on enp0s3
  Gateway: 10.0.2.2 on enp0s3
    DNS: 212.230.135.2
         212.230.135.1
Search Domains: home
root@dns:/etc/bind#
```


1. Configuración del servidor

1. Configurar el archivo local Consultar estado servicio DNS:

>*service bind9 status*

```
root@dns:/home/blanca# service bind9 status
• bind9.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
  Active: active (running) since Sun 2021-11-21 18:30:24 UTC; 23min ago
    Docs: man:named(8)
  Main PID: 801 (named)
    Tasks: 4 (limit: 2315)
   CGroup: /system.slice/bind9.service
           └─801 /usr/sbin/named -f -u bind

nov 21 18:53:25 dns named[801]: network unreachable resolving 'ntp.ubuntu.com/A/IN': 2001:500:1::
nov 21 18:53:25 dns named[801]: network unreachable resolving 'ntp.ubuntu.com/A/IN': 2001:500:2::
nov 21 18:53:25 dns named[801]: network unreachable resolving 'ntp.ubuntu.com/A/IN': 2001:500:84:
nov 21 18:53:26 dns named[801]: network unreachable resolving 'ntp.ubuntu.com/AAAA/IN': 2001:500:
nov 21 18:53:26 dns named[801]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
nov 21 18:53:28 dns named[801]: network unreachable resolving 'ntp.ubuntu.com/A/IN': 2001:500:2d:
nov 21 18:53:29 dns named[801]: network unreachable resolving 'ntp.ubuntu.com/AAAA/IN': 2001:500:
nov 21 18:53:29 dns named[801]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
nov 21 18:53:29 dns named[801]: resolver priming query complete
nov 21 18:53:32 dns named[801]: network unreachable resolving 'ntp.ubuntu.com/A/IN': 2001:500:2f:
lines 1-19/19 (END)
```

1. Configuración del servidor

1. Configurar el archivo local

Vamos al fichero de configuración de red /etc/netplan/01-netcfg.yaml y:

- Lo modificamos para poner el adaptador enp0s3 con la IP actual. En el caso de la red interna que estamos siguiendo: 192.168.30.2

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [10.0.2.15/24]
      gateway4: 10.0.2.15
      nameservers:
        addresses: [10.0.2.15,8.8.8.8]

root@dns:/etc/netplan# netplan apply
root@dns:/etc/netplan# _
```

1. Configuración del servidor

1. Configurar el archivo local

Revisad que los siguientes ficheros de configuración tenga la IP del servidor de DNS bien puesta:

`/run/systemd/resolve/resolv.conf`

`/etc/resolv.conf`

Reiniciamos la máquina para que coja los últimos cambios > *reboot*

```
GNU nano 2.9.3 /run/systemd/resolve/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs must 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 10.0.2.15
nameserver 8.8.8.8
```

```
GNU nano 2.9.3 /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# 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 "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must 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 10.0.2.15
options eds0
```

1. Configuración del servidor

1.Configurar el archivo local Ahora ejecutamos el comando

>nslookup

Para que nos resuelva el DNS local configurado y nos contesta que es el localhost.

```
root@dns:/home/blanca# nslookup blanca.com
Server:          10.0.2.15
Address:         10.0.2.15#53

Name:   blanca.com
Address: 10.0.2.15

root@dns:/home/blanca# _
```

Si os da error al realizar la instrucción nslookup, probad a tirar y levantar el adaptador de red:

1. Configuración del servidor

1.Configurar el archivo local Hacemos ping a las máquinas por IP y por nombre de dominio:

```
root@dns:/home/blanca# ping cliente1.blanca.com
PING cliente1.blanca.com (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=1 ttl=64 time=0.009 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=4 ttl=64 time=0.026 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=5 ttl=64 time=0.026 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=6 ttl=64 time=0.027 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=7 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=8 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=9 ttl=64 time=0.027 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=10 ttl=64 time=0.025 ms
^C
--- cliente1.blanca.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9215ms
rtt min/avg/max/mdev = 0.009/0.024/0.027/0.005 ms
root@dns:/home/blanca#
```

```
pipe 4
root@dns:/home/blanca# ping servidorDNS.blanca.com
PING servidorDNS.blanca.com (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=1 ttl=64 time=0.048 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 10.0.2.15 (10.0.2.15): icmp_seq=3 ttl=64 time=0.025 ms
^C
--- servidorDNS.blanca.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.025/0.033/0.048/0.010 ms
root@dns:/home/blanca#
```

1. Configuración del servidor

1.Configurar el archivo local Si probáis a llamar a una máquina que no está en el DNS incluida:

```
root@dns:/home/blanca# ping cliente3.blanca.com
ping: cliente3.blanca.com: Name or service not known
root@dns:/home/blanca# _
```

```
root@dns:/home/blanca# ping 10.0.2.16
PING 10.0.2.16 (10.0.2.16) 56(84) bytes of data.
From 10.0.2.15 icmp_seq=1 Destination Host Unreachable
From 10.0.2.15 icmp_seq=2 Destination Host Unreachable
From 10.0.2.15 icmp_seq=3 Destination Host Unreachable
From 10.0.2.15 icmp_seq=4 Destination Host Unreachable
^C
--- 10.0.2.16 ping statistics ---
5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 4017ms
pipe 4
root@dns:/home/blanca#
```

1. Configuración del servidor

2. Configurar el archivo `options` `named.conf.options`

Contiene una serie de directivas para establecer opciones de configuración global para el servidor. Vamos a ver unas pocas de las muchísimas que hay.

Permite definir un conjunto de opciones de configuración. Estas opciones sólo se pueden definir dentro de `options`. La directiva `options` sólo puede aparecer una vez en el archivo.

Dentro de `options` se pueden usar, entre otras, las siguientes directivas:

-> **Forwarders:** especifica los servidores de reenvío a los que se enviarán las consultas que no se puedan resolver localmente.

1. Configuración del servidor

2. Configurar el archivo `options` `named.conf.options`

- > **Directory**: indica el directorio donde el servidor almacena archivos temporales, como por ejemplo, los que constituyen la caché DNS.
- > **Allow-query**: indica mediante direcciones IP de equipos o de red los ordenadores a los que les está permitido hacer consultas al servidor.
- > **Blackhole**: permite indicar direcciones IP de equipos a los que no se les va a responder a las consultas DNS que realicen.

1. Configuración del servidor

2. Configurar el archivo `options` `named.conf.options`

Forwarders: vamos a configurar los DNS a los que se les deberá pasar la consulta de resolución de nombre a otro servidor DNS cuando el local no pueda resolver. Esos servidores DNS son también conocidos como Forwarders y en Bind se configuran en la siguiente ruta:

`/etc/bind/named.conf.options`

```
GNU nano 2.9.3 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 {
    //     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;

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

1. Configuración del servidor

2. Configurar el archivo `options` `named.conf.options`

Editamos para incluir los servidores públicos de Google. Cuando nuestro servidor local no encuentre un dominio se lo preguntara al servidor DNS de Google:

```
GNU nano 2.9.3                                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; };

    //=====
    // 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;

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

2. Pruebas de resolución de nombres.

Levantamos un cliente y probamos:

Ubuntu server solo DNS [Corriendo] - Oracle VM VirtualBox

```
root@dns:/etc/bind# more db.blanca.com
;
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA      blanca.com. root.blanca.com. (
        2          ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )    ; Negative Cache TTL
;
@      IN      NS       blanca.com.
@      IN      A        192.168.30.2
servidordns IN A        192.168.30.2
cliente1  IN A        192.168.30.6
cliente2  IN A        192.168.30.7
root@dns:/etc/bind# more db.2.0.10
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@      IN      SOA      blanca.com. root.blanca.com. (
        1          ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )    ; Negative Cache TTL
;
@      IN      NS       blanca.com.
192.168.30.2 IN PTR     blanca.com.
192.168.30.2 IN PTR     servidordns.blanca.com.
192.168.30.6 IN PTR     cliente1.blanca.com.
192.168.30.7 IN PTR     cliente2.blanca.com.
blanca.com. IN A        192.168.30.2
root@dns:/etc/bind# _
```

windows10 [Corriendo] - Oracle VM VirtualBox

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Papelera de
rec
Símbolo del sistema - nslookup
Microsoft Windows [Versión 10.0.19043.928]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Blanca>nslookup
30.168.192.in-addr.arpa
    primary name server = blanca.com
    responsible mail addr = root.blanca.com
    serial = 1
    refresh = 604800 (7 days)
    retry = 86400 (1 day)
    expire = 2419200 (28 days)
    default TTL = 604800 (7 days)
Servidor predeterminado: UnKnown
Address: 192.168.30.2

> set q=a
> cliente1.blanca.com
Servidor: UnKnown
Address: 192.168.30.2

Nombre: cliente1.blanca.com
Address: 192.168.30.6

> _
```