

# Guía completa para configurar *dnsmasq* con segmentación por departamentos

2/07/2025

Ángel Moreno García  
CodeArts Solutions  
Madrid

## Introducción

Este documento explica cómo instalar, configurar y probar un servidor de red basado en **dnsmasq** que funcione correctamente en una máquina virtual Linux con VirtualBox, usando exclusivamente **red NAT** con la IP **10.0.2.0/24**.

## Objetivos

Se implementa un servidor combinado DHCP + DNS que:

1. Asigna IPs segmentadas por grupos/departamentos
2. Usa reservas fijas por MAC
3. No usa modo bridge (limitación de red NAT)
4. Permite simulación de clientes para pruebas

5.

# Instalación de dnsmasq

Empezaremos con la instalación del servicio dnsmasq, ejecutaremos:

*sudo apt update*

*sudo apt install dnsmasq*

```
angelsrv@srv-base-angel:~$ sudo apt update
sudo apt install dnsmasq -y
Obj:1 http://archive.ubuntu.com/ubuntu plucky InRelease
Des:2 http://security.ubuntu.com/ubuntu plucky-security InRelease [126 kB]
Des:3 http://archive.ubuntu.com/ubuntu plucky-updates InRelease [126 kB]
Des:4 http://archive.ubuntu.com/ubuntu plucky-backports InRelease [126 kB]
Des:5 http://security.ubuntu.com/ubuntu plucky-security/main amd64 Packages [112 kB]
Des:6 http://archive.ubuntu.com/ubuntu plucky-updates/main amd64 Packages [181 kB]
Des:7 http://archive.ubuntu.com/ubuntu plucky-updates/main amd64 Components [30,6 kB]
Des:8 http://security.ubuntu.com/ubuntu plucky-security/main Translation-en [34,3 kB]
Des:9 http://archive.ubuntu.com/ubuntu plucky-updates/restricted amd64 Components [212 B]
Des:10 http://archive.ubuntu.com/ubuntu plucky-updates/universe amd64 Packages [149 kB]
Des:11 http://security.ubuntu.com/ubuntu plucky-security/main amd64 Components [14,7 kB]
Des:12 http://security.ubuntu.com/ubuntu plucky-security/restricted amd64 Packages [67,9 kB]
Des:13 http://security.ubuntu.com/ubuntu plucky-security/restricted Translation-en [16,9 kB]
```

Verificaremos la instalación con:

***dnsmasq --version***

```
angelsrv@srv-base-angel:~$ dnsmasq --version
Dnsmasq version 2.91 Copyright (c) 2000-2025 Simon Kelley
Compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua
TFTP conntrack ipset nftset auth DNSSEC loop-detect inotify dumpfile

This software comes with ABSOLUTELY NO WARRANTY.
Dnsmasq is free software, and you are welcome to redistribute it
under the terms of the GNU General Public License, version 2 or 3.
angelsrv@srv-base-angel:~$
```

## Configuración básica de dnsmasq

Tendremos que configurar la interfaz y el archivo principal para usar solo la red LAN, para ello ejecutaremos y editaremos el archivo con:

***sudo nano /etc/dnsmasq.conf***

### Configura la interfaz y opciones básicas

Escribiremos en la configuración la parte básica de la configuración que vamos a implementar al final del archivo:

```
# Usar solo la interfaz LAN de la VM  
interface=enp0s3  
bind-interfaces  
listen-address=10.0.2.15
```

*enp0s3 es un ejemplo, usa el nombre de la interfaz de red que tengas en tu VM.*

*listen-address debe ser la IP fija que asignamos a la VM dentro de la red NAT (explicado en el siguiente paso).*



```
GNU nano 8.3          /etc/dnsmasq.conf  
  
# Rangos DHCP por grupo  
interface=enp0s3  
bind-interfaces
```

## Configuración de IP estática

Configura una IP fija para tu servidor en la red 10.0.2.0/24, por ejemplo 10.0.2.15:

Edita `/etc/netplan/01-netcfg.yaml` con: `sudo nano /etc/netplan/01-netcfg.yaml` y agrega este contenido:

`network:`

`version: 2`

`ethernets:`

`enp0s8:`

`dhcp4: no`

`addresses: [192.168.1.1/24]`

`gateway4: 192.168.1.254`

`nameservers:`

`addresses: [8.8.8.8, 1.1.1.1]`

Aplica con: `sudo netplan apply`

Verifica con: `ip a show enp0s3`



The screenshot shows a terminal window titled "angelsrv@srv-base-angel: ~". The command "GNU nano 8.3" is displayed at the top. The file "/etc/netplan/01-netcfg.yaml" is open in the editor. The configuration content is as follows:

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 10.0.2.15/24
      gateway4: 10.0.2.2
      nameservers:
        addresses:
          - 8.8.8.8
          - 1.1.1.1
```

## Configuración de rangos DHCP segmentados y reservas

Agrega al final de `/etc/dnsmasq.conf` esta configuración adaptada a tu red `10.0.2.0/24` y las MAC reales:

*# Rangos DHCP segmentados*

```
dhcp-range=set:dev,10.0.2.100,10.0.2.110,12h
```

```
dhcp-range=set:design,10.0.2.120,10.0.2.130,12h
```

```
dhcp-range=set:admin,10.0.2.140,10.0.2.150,12h
```

*# Reservas por MAC y asignación de grupo + IP + nombre host*

```
dhcp-host=08:00:27:24:1e:b8,set=dev,10.0.2.101,dev-pc1
```

```
dhcp-host=08:00:27:c9:fb:c3,set=design,10.0.2.121,design-pc1
```

```
dhcp-host=08:00:27:48:c6:f9,set=admin,10.0.2.141,admin-pc1
```

*# Control de acceso - marcar como conocidos (lista blanca)*

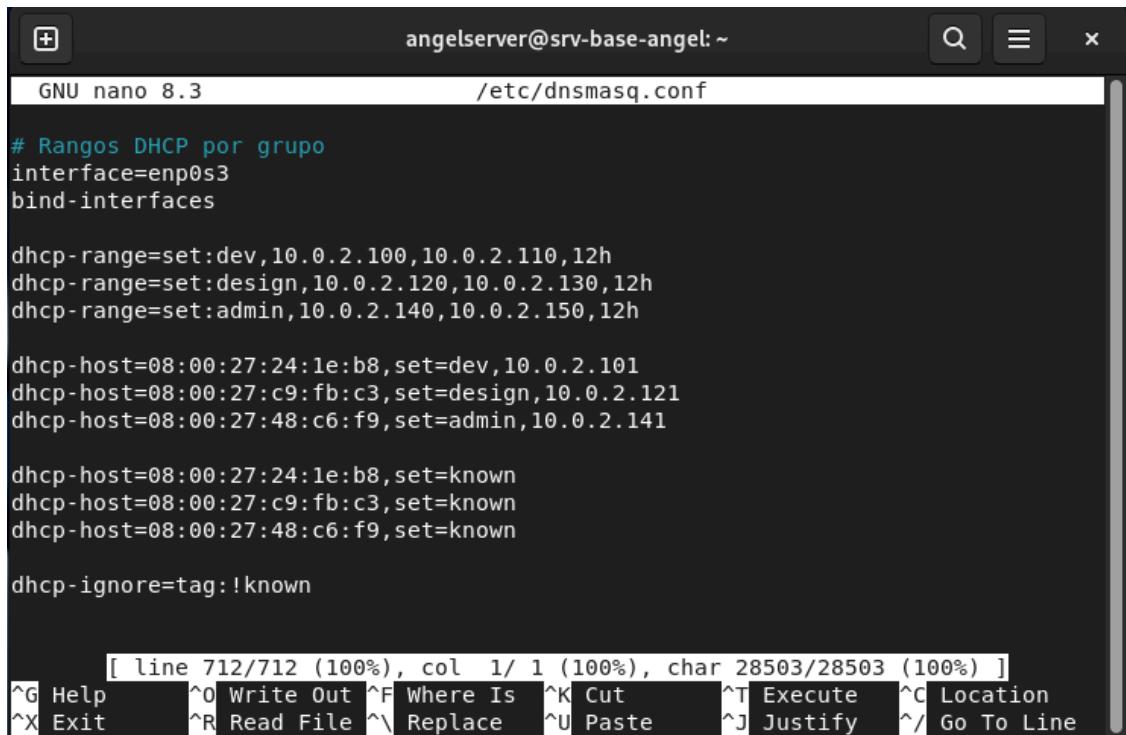
```
dhcp-host=08:00:27:24:1e:b8,set=known
```

```
dhcp-host=08:00:27:c9:fb:c3,set=known
```

```
dhcp-host=08:00:27:48:c6:f9,set=known
```

*# Ignorar peticiones DHCP de dispositivos no conocidos*

```
dhcp-ignore=tag:!known
```



```
GNU nano 8.3          /etc/dnsmasq.conf

# Rangos DHCP por grupo
interface=enp0s3
bind-interfaces

dhcp-range=set:dev,10.0.2.100,10.0.2.110,12h
dhcp-range=set:design,10.0.2.120,10.0.2.130,12h
dhcp-range=set:admin,10.0.2.140,10.0.2.150,12h

dhcp-host=08:00:27:24:1e:b8,set=dev,10.0.2.101
dhcp-host=08:00:27:c9:fb:c3,set=design,10.0.2.121
dhcp-host=08:00:27:48:c6:f9,set=admin,10.0.2.141

dhcp-host=08:00:27:24:1e:b8,set=known
dhcp-host=08:00:27:c9:fb:c3,set=known
dhcp-host=08:00:27:48:c6:f9,set=known

dhcp-ignore=tag:!known

[ line 712/712 (100%), col 1/ 1 (100%), char 28503/28503 (100%) ]
^G Help      ^O Write Out ^F Where Is  ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line
```

## Reglas básicas en iptables

Para permitir tráfico solo desde IPs asignadas:

```
sudo iptables -A INPUT -s 10.0.2.100/28 -j ACCEPT
```

```
sudo iptables -A INPUT -s 10.0.2.120/28 -j ACCEPT
```

```
sudo iptables -A INPUT -s 10.0.2.140/28 -j ACCEPT
```

```
sudo iptables -A INPUT -j DROP
```

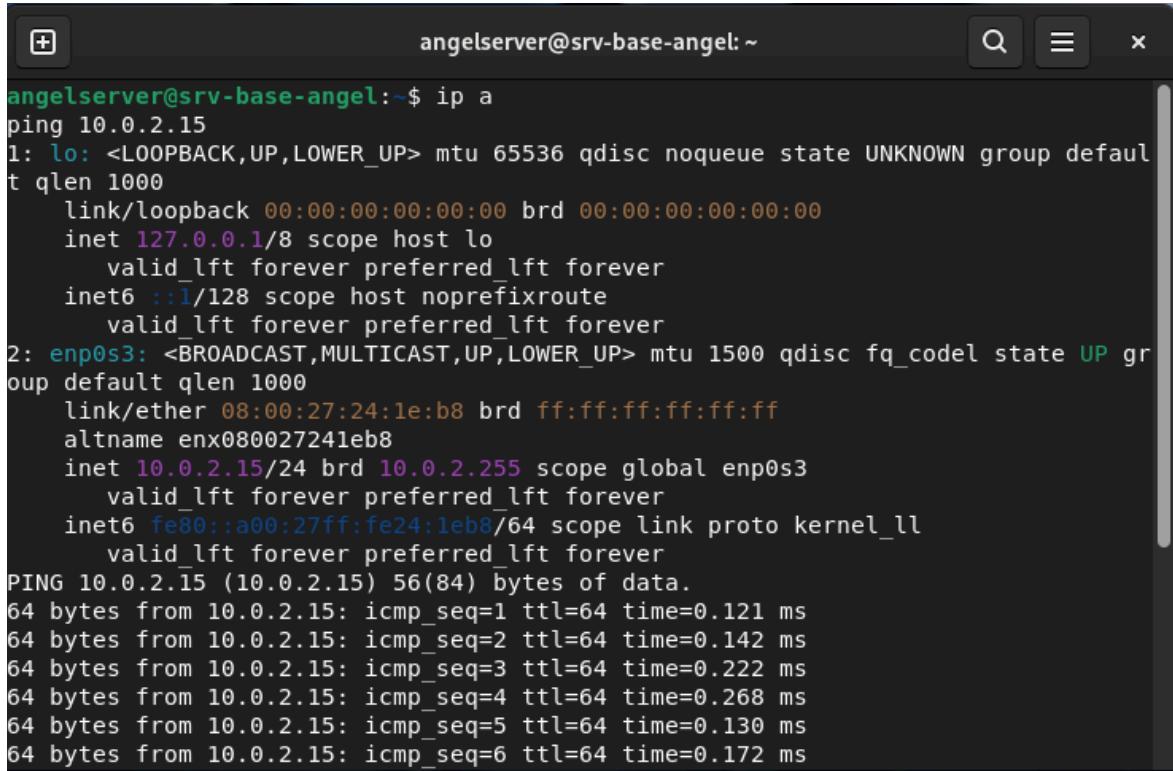
## Simulación y pruebas con clientes Linux

Crearemos **3 máquinas virtuales** clientes para conectarnos a la configuración dnsmasq que hemos creado. Configuraremos cada máquina virtual con adaptador de red **red interna** para que las máquinas puedan verse entre sí y puedan obtener IP por DHCP.

Usaremos los comandos:

**ip a**

**ping 10.0.2.15(en este ejemplo con la ip estática previamente configurada)**



The terminal window shows the command `ip a` being run, displaying the network interfaces and their configurations. It then runs a `ping` command to the IP address 10.0.2.15, showing the response times for six ICMP packets.

```
angels@srv-base-angel:~$ ip a
ping 10.0.2.15
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:24:1e:b8 brd ff:ff:ff:ff:ff:ff
    altname enx080027241eb8
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe24:1eb8/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.121 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.142 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.222 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.268 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.130 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.172 ms
```



```
angelserver@srv-base-angel:~$ ip a
ping 10.0.2.15
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c9:fb:c3 brd ff:ff:ff:ff:ff:ff
    altname enx080027c9fbc3
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86233sec preferred_lft 86233sec
    inet6 fe80::a00:27ff:fec9:fbc3/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.147 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.088 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.085 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.172 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.289 ms
```

```
angelserver@srv-base-angel:~$ ip a
ping 10.0.2.15
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:48:c6:f9 brd ff:ff:ff:ff:ff:ff
    altname enx08002748c6f9
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86346sec preferred_lft 86346sec
    inet6 fe80::a00:27ff:fe48:c6f9/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.061 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.085 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.117 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.080 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.076 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.073 ms
```

## Supervisión de tráfico e identificación

### Captura con tcpdump

Para ver el tráfico DHCP y DNS usaremos:

```
sudo tcpdump -i enp0s3 port 67 or port 53 -w dhcp_dns.pcap
```

*Esto captura tráfico DHCP y DNS para analizarlo con Wireshark o tcpdump.*

```
angelsrv@srv-base-angel:~$ sudo tcpdump -i enp0s3 port 67 or port 53 -n
[sudo] password for angelsrv:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:26:15.630783 IP 0.0.0.68 > 255.255.255.67: BOOTP/DHCP, Request from 08:00:27:24:1e:b8, length 301
11:27:19.170525 IP 0.0.0.68 > 255.255.255.67: BOOTP/DHCP, Request from 08:00:27:24:1e:b8, length 301
11:28:23.019246 IP 0.0.0.68 > 255.255.255.67: BOOTP/DHCP, Request from 08:00:27:24:1e:b8, length 301
11:29:26.545187 IP 0.0.0.68 > 255.255.255.67: BOOTP/DHCP, Request from 08:00:27:24:1e:b8, length 301
11:30:30.375721 IP 0.0.0.68 > 255.255.255.67: BOOTP/DHCP, Request from 08:00:27:24:1e:b8, length 301
11:31:35.187748 IP 0.0.0.68 > 255.255.255.67: BOOTP/DHCP, Request from 08:00:27:24:1e:b8, length 301
11:32:38.479975 IP 0.0.0.68 > 255.255.255.67: BOOTP/DHCP, Request from 08:00:27:24:1e:b8, length 301
```

### Análisis de logs

Para analizar los logs utilizaremos el comando:

```
sudo tail -f /var/log/syslog | grep dnsmasq
```

## Escaneo ARP con arp-scan

Por último, instalaremos y veremos los dispositivos activos y su IP-MAC con:

***sudo apt install arp-scan***

***sudo arp-scan -I enp0s3 10.0.2.0/24***

```
angelserver@srv-base-angel: ~
angelserver@srv-base-angel: $ sudo apt install arp-scan
Installing:
  arp-scan

Installing dependencies:
  libtext-csv-perl  libtext-csv-xs-perl

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 17
  Download size: 736 kB
  Space needed: 2.334 kB / 4.230 MB available

Continue? [S/n] s
Des:1 http://archive.ubuntu.com/ubuntu plucky/universe amd64 libtext-csv-perl al
l 2.06-1 [113 kB]
Des:2 http://archive.ubuntu.com/ubuntu plucky/universe amd64 libtext-csv-xs-perl
  amd64 1.60-1 [131 kB]
Des:3 http://archive.ubuntu.com/ubuntu plucky/universe amd64 arp-scan amd64 1.10
  .0-2build2 [492 kB]
Descargados 736 kB en 3s (284 kB/s)
Seleccionando el paquete libtext-csv-perl previamente no seleccionado.
(Leyendo la base de datos ... 149382 ficheros o directorios instalados actualmen
te.)
Preparando para desempaquetar .../libtext-csv-perl_2.06-1_all.deb ...
```

```
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
angelserver@srv-base-angel: ~
angelserver@srv-base-angel: $ sudo arp-scan --interface=enp0s3 --localnet
Interface: enp0s3, type: EN10MB, MAC: 08:00:27:9a:6c:b0, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.2      52:54:00:12:35:02      (Unknown: locally administered)
10.0.2.3      52:54:00:12:35:03      (Unknown: locally administered)
10.0.2.4      52:54:00:12:35:04      (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.092 seconds (122.37 hosts/sec). 3
  responded
angelserver@srv-base-angel: ~
```

## Conclusión

La configuración de dnsmasq en **VirtualBox** con red **NAT** (10.0.2.0/24) permite gestionar **DHCP** y **DNS** de forma eficiente y segura, incluso con las limitaciones del entorno **NAT**. La guía muestra cómo segmentar la red por grupos, asignar **IPs** fijas por **MAC** y controlar el acceso con listas blancas, garantizando un servicio estable y funcional. Esta configuración es una base sólida para gestionar redes virtualizadas y aprender sobre servicios de red esenciales.

## Informe Técnico de Error: Fallo al iniciar dnsmasq

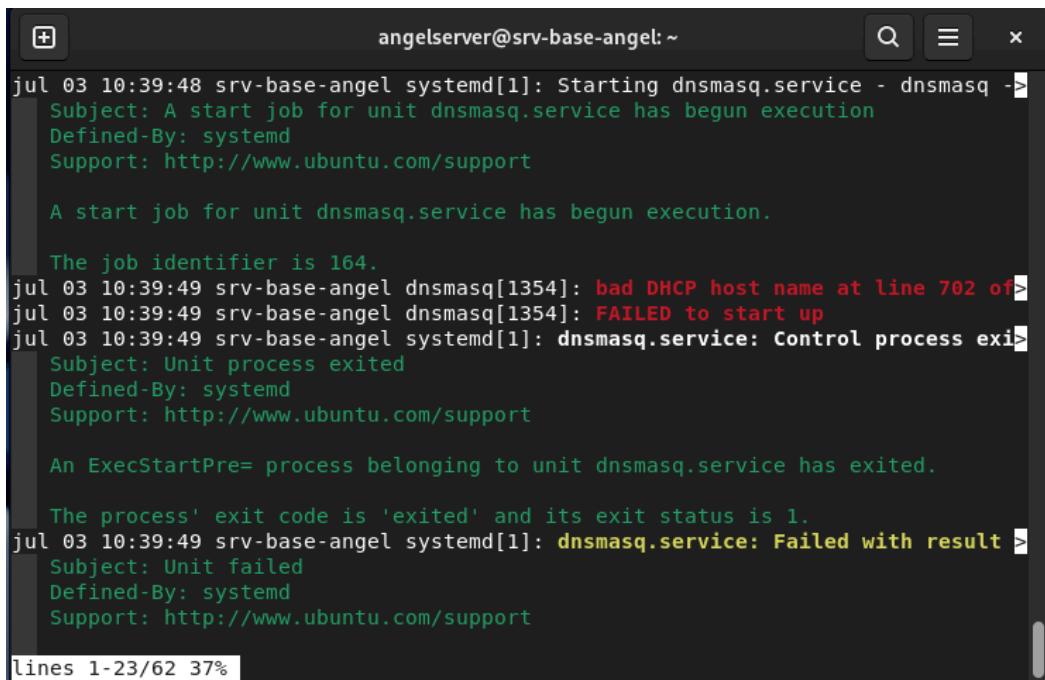
Durante la implementación del servidor DHCP/DNS con dnsmasq, al intentar iniciar el servicio se produce el siguiente error:

*Job for dnsmasq.service failed because the control process exited with error code.*

*See "systemctl status dnsmasq.service" and "journalctl -xeu dnsmasq.service" for details.*

El análisis más detallado muestra:

*dnsmasq: bad DHCP host name at line 702 of /etc/dnsmasq.conf*



The screenshot shows a terminal window with the title 'angelserver@srv-base-angel: ~'. The window displays a log of system events from July 3, 2014, at 10:39:48. It starts with the dnsmasq service being started, followed by an error message indicating a bad DHCP host name at line 702 of /etc/dnsmasq.conf. This leads to the service failing to start up, and finally, the control process exiting with an exit code of 1. The log concludes with the dnsmasq.service failing with result 1. The bottom of the terminal shows the status 'lines 1-23/62 37%'.

```
angelserv@srv-base-angel: ~
[jul 03 10:39:48 srv-base-angel systemd[1]: Starting dnsmasq.service - dnsmasq ->
  Subject: A start job for unit dnsmasq.service has begun execution
  Defined-By: systemd
  Support: http://www.ubuntu.com/support

  A start job for unit dnsmasq.service has begun execution.

  The job identifier is 164.
[jul 03 10:39:49 srv-base-angel dnsmasq[1354]: bad DHCP host name at line 702 of /etc/dnsmasq.conf
[jul 03 10:39:49 srv-base-angel dnsmasq[1354]: FAILED to start up
[jul 03 10:39:49 srv-base-angel systemd[1]: dnsmasq.service: Control process exited
  Subject: Unit process exited
  Defined-By: systemd
  Support: http://www.ubuntu.com/support

  An ExecStartPre= process belonging to unit dnsmasq.service has exited.

  The process' exit code is 'exited' and its exit status is 1.
[jul 03 10:39:49 srv-base-angel systemd[1]: dnsmasq.service: Failed with result >
  Subject: Unit failed
  Defined-By: systemd
  Support: http://www.ubuntu.com/support

lines 1-23/62 37%
```

## Análisis del Problema

El mensaje indica un fallo de sintaxis en una de las líneas que contienen una directiva `dhcp-host`, por un nombre de host considerado inválido por el servicio.

## Hipótesis inicial

Se pensó que el error se debía a un **nombre de host mal escrito** (por ejemplo, incluyendo espacios o caracteres no válidos). Se corrigieron los nombres para cumplir con las reglas DNS.

## Solución Intentada

Se corrigieron los nombres de host como se muestra en el siguiente bloque:

# Rangos DHCP por grupo

*dhcp-range=set:dev,10.0.2.100,10.0.2.110,12h*

*dhcp-range=set:design,10.0.2.120,10.0.2.130,12h*

*dhcp-range=set:admin,10.0.2.140,10.0.2.150,12h*

# Reservas por MAC y asignación de grupo + IP + nombre host

*dhcp-host=08:00:27:24:1e:b8,set=dev,10.0.2.101,dev-pc1*

*dhcp-host=08:00:27:c9:fb:c3,set=design,10.0.2.121,design-pc1*

*dhcp-host=08:00:27:48:c6:f9,set=admin,10.0.2.141,admin-pc1*

# Control de acceso - marcar como conocidos (lista blanca)

*dhcp-host=08:00:27:24:1e:b8,set=known*

*dhcp-host=08:00:27:c9:fb:c3,set=known*

*dhcp-host=08:00:27:48:c6:f9,set=known*

# Rechazar clientes no autorizados (no en lista blanca)

*dhcp-ignore=tag:!known*

## Resultado Obtenido

A pesar de que **todos los nombres de host son válidos**, el servicio **dnsmasq sigue sin iniciar correctamente** y se muestra el siguiente error:

**dnsmasq: bad DHCP host name at line XXX of /etc/dnsmasq.conf**

Incluso **comentando temporalmente las líneas dhcp-host**, el servicio arranca. Esto confirma que la causa está en esas directivas.

## Evidencias

### 1. Error persistente

Por más que se arregle la línea con nombres válidos o se escriba manualmente la línea, el error persiste y no se ejecuta el servicio dnsmasq.

### 2. Captura de líneas que causan error

dhcp-host=08:00:27:24:1e:b8,set=dev,10.0.2.101,dev-pc1

dhcp-host=08:00:27:c9:fb:c3,set=design,10.0.2.121,design-pc1

dhcp-host=08:00:27:48:c6:f9,set=admin,10.0.2.141,admin-pc1

## Conclusión

Aunque se corrigieron los nombres de host para cumplir con el estándar **DNS**, el servicio **dnsmasq sigue sin iniciar debido a que alguna directiva dhcp-host provoca un error que impide levantar el servicio**.

Se procederá a **iniciar una configuración mínima**, y como alternativa, se propondrá configurar las reservas DHCP desde un archivo externo o simplificar las directivas para identificar cuál línea concreta bloquea el arranque.