

Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: “*Careful where you step in*”



> **Img Source:** @Aaron & @Cristian 's GitHub

Index

- **DHCP:** -> readME <-
- **Que és i per a què serveix aquest protocol:** -> readME <-
- **Instal·lació i configuració:** -> readME <-
- **Bibliografia:** -> readME <-

DHCP

El protocol DHCP és un dels més utilitzats pels routers, tant domèstics com també professionals, a més, per defecte qualsevol client cablejat o WiFi està configurat per obtenir una adreça IP per DHCP. Encara que continuament estem utilitzant el DHCP, segurament no coneguem per a què serveix exactament, les seves funcionalitats i també com funciona i quins missatges s'intercanvien entre el servidor i els clients. Avui a RedesZone us explicarem tot el que has de saber sobre el protocol DHCP.

Que és i per a què serveix aquest protocol

El protocol DHCP (Protocol de configuració dinàmica de host) o també conegut com a **Dynamic Host Configuration Protocol**, és un protocol de xarxa que utilitza una arquitectura client-servidor. Per tant, tindrem un o més servidors DHCP i també un o més clients, que s'hauran de comunicar entre ells correctament perquè el servidor DHCP brindi informació als diferents clients connectats.

Aquest protocol s'encarrega d'assignar de manera dinàmica i automàtica una adreça IP, ja sigui una adreça IP privada des del router cap als equips de la xarxa local, o també una IP pública per part d'un operador que utilitzi aquest tipus de protocol per al establiment de la connexió.

Instal·lació i configuració

- apt-get update
- apt-get install isc-dhcp-server
- sudo nano /etc/default/isc-dhcp-server
- sudo nano /etc/default/isc-dhcp-server

```
INTERFACESv4="enp0s8"
```

```
INTERFACESv6=""
```

- sudo nano /etc/dhcp/dhcpd.conf

```
option domain-name "cryptosec.net";
option domain-name-servers 192.168.3.1;
```

```
default-lease-time 60000;
max-lease-time 72000;
```

```
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
```

```
ddns-update-style none;
```

```
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
```

```
authoritative;
```

```
subnet 192.168.3.0 netmask 255.255.255.0 {
    option routers 192.168.3.1;
    option subnet-mask 255.255.255.0;
    range dynamic-bootp 192.168.3.100 192.168.3.200;
    # option domain-nameservers 192.168.3.1;
```

```
#         option domain-name "cryptosec.net";
}
```

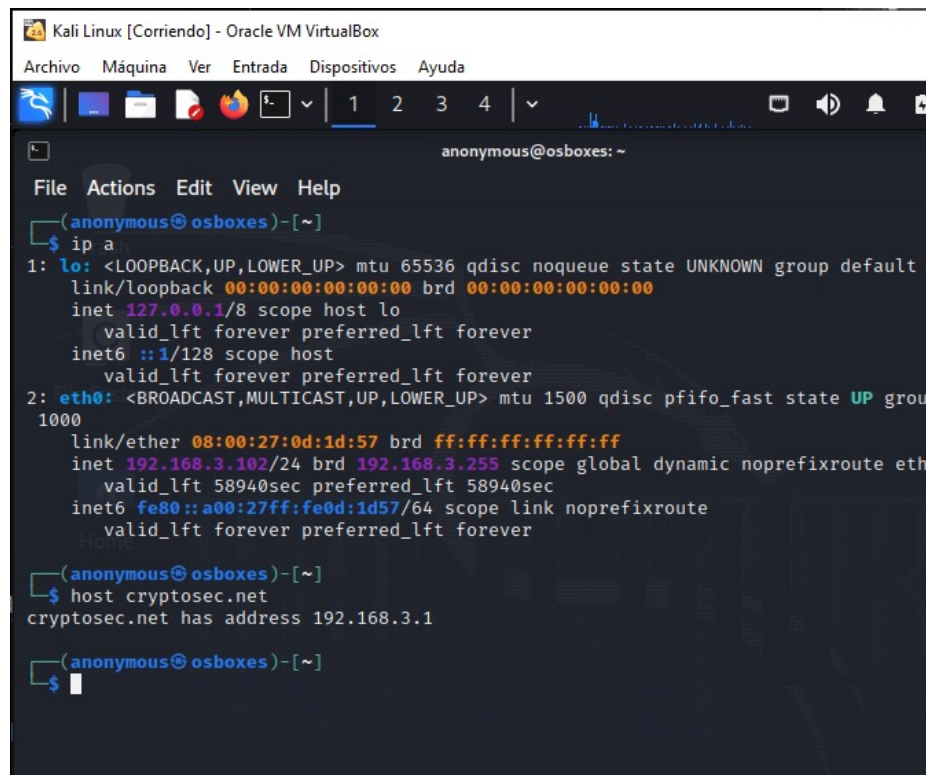
- reiniciar el servidor **DHCP** `sudo systemctl restart isc-dhcp-server`

```
cryptosec@SOACryptosec:/etc/dhcp$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPV4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-05-12 18:44:55 UTC; 6s ago
     Docs: man:dhcpd(8)
    Main PID: 1573 (dhcpd)
      Tasks: 4 (limit: 1066)
    Memory: 4.5M
    CGroup: /system.slice/isc-dhcp-server.service
            └─1573 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcpd

May 12 18:44:55 SOACryptosec dhcpd[1573]: Database file: /var/lib/dhcp/dhcpd.leases
May 12 18:44:55 SOACryptosec dhcpd[1573]: PID file: /run/dhcp-server/dhcpd.pid
May 12 18:44:55 SOACryptosec dhcpd[1573]: Wrote 4 leases to leases file.
May 12 18:44:55 SOACryptosec dhcpd[1573]: Listening on LPF/enp0s8/08:00:27:00:b3:d6/192.168.3.0/24
May 12 18:44:55 SOACryptosec sh[1573]: Listening on LPF/enp0s8/08:00:27:00:b3:d6/192.168.3.0/24
May 12 18:44:55 SOACryptosec sh[1573]: Sending on LPF/enp0s8/08:00:27:00:b3:d6/192.168.3.0/24
May 12 18:44:55 SOACryptosec sh[1573]: Sending on Socket/fallback/fallback-net
May 12 18:44:55 SOACryptosec dhcpd[1573]: Sending on LPF/enp0s8/08:00:27:00:b3:d6/192.168.3.0/24
May 12 18:44:55 SOACryptosec dhcpd[1573]: Sending on Socket/fallback/fallback-net
May 12 18:44:55 SOACryptosec dhcpd[1573]: Server starting service.
cryptosec@SOACryptosec:/etc/dhcp$
```

> **Img Source:** @Aaron & @Cristian 's *GitHub*

- Obrir el client *Linux Lite* o el *Debian Minimal 10* i provar-ho: `dhclient -v`. Probar també la connectivitat amb un host a la nostra zona “**cryptosec.net**”



```
Kali Linux [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

anonymous@osboxes: ~
File  Actions  Edit  View  Help

anonymous@osboxes)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
    1000
    link/ether 08:00:27:0d:1d:57 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.102/24 brd 192.168.3.255 scope global dynamic noprefixroute eth
        valid_lft 58940sec preferred_lft 58940sec
    inet6 fe80::a00:27ff:fe0d:1d57/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

anonymous@osboxes)-[~]
$ host cryptosec.net
cryptosec.net has address 192.168.3.1

anonymous@osboxes)-[~]
$
```

> Img Source: @Aaron & @Cristian 's GitHub

```

debian@debian10:~$ sudo dhclient -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:39:90:fd
Sending on   LPF/enp0s3/08:00:27:39:90:fd
Sending on   Socket/fallback
DHCPREQUEST for 192.168.3.100 on enp0s3 to 255.255.255.255
DHCPREQUEST for 192.168.3.100 on enp0s3 to 255.255.255.255
DHCPACK of 192.168.3.100 from 192.168.3.1
bound to 192.168.3.100 -- renewal in 22984 seconds.
debian@debian10:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue stat
    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
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdis
000
    link/ether 08:00:27:39:90:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.100/24 brd 192.168.3.255 scope global d
        valid_lft 50484sec preferred_lft 50484sec
    inet6 fe80::a00:27ff:fe39:90fd/64 scope link
        valid_lft forever preferred_lft forever
debian@debian10:~$ host google.com
google.com has address 142.250.200.78
google.com has IPv6 address 2a00:1450:4003:808::200e
google.com mail is handled by 10 smtp.google.com.
debian@debian10:~$ host cryptosec.net
cryptosec.net has address 192.168.3.1
debian@debian10:~$ _

```

> **Img Source:** @Aaron & @Cristian 's *GitHub*

```
(anonymous@osboxes)-[~]
$ host google.com
google.com has address 142.250.201.78
google.com has IPv6 address 2a00:1450:4003:80e::200e
google.com mail is handled by 10 smtp.google.com.

(anonymous@osboxes)-[~]
$ host cryptosec.net
cryptosec.net has address 192.168.3.1

(anonymous@osboxes)-[~]
$ █
```

> **Img Source:** @Aaron & @Cristian 's *GitHub*

→ [**Tornar a Ciberseguretat**] <←

Bibliografia

- <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/>
- <https://www.fpgenre.es/DHCP/>
- https://www.fpgenre.es/DHCP/descripcion_del_protocolo.html
- <https://docs.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>
- <https://www.webservertalk.com/dhcp-tutorial>
- <https://www.howtoforge.com/tutorial/install-and-configure-isc-dhcp-server-in-debian-9/>
- https://www.fpgenre.es/DHCP/instalacion_del_isc_dhcp.html
- <https://www.linuxsc.net/instalacion-y-configuracion-del-isc-dhcp-server-en-ubuntu/>
- <https://es.linux-console.net/?p=1033>