

---

# Servizo DHCP

## Instalación dun Servidor DHCP en Linux

### Índice

1. Introducción - Comandos de manexo do cliente DHCP.....	2
2. Configuración básica do servizo DHCP en Linux.....	3
2.1. Instalación e configuración básica do servizo.....	3
2.2. Definición de reservas de direccións.....	6
3. Actualizacións dinámicas do servidor DNS.....	7
3.1. Configuración de DDNS no servidor.....	7
3.2. Comprobación das actualizacións.....	11
4. DHCP Failover.....	12
4.1. Como funciona o DHCP failover.....	12
4.2. Configuración do emparellamento entre dous servidores.....	13
4.3. Configuración dun pool en failover.....	15
4.4. Configuración da chave de autenticación.....	15
5. Axentes de reenvío DHCP.....	16

## 1. Introducción - Comandos de manexo do cliente DHCP

Tanto en sistemas Windows como en sistemas GNU/Linux, podemos empregar comandos para comprobar e xestionar a configuración de rede automática no equipo cliente.

### (1) Manexo do cliente DHCP en sistemas Windows

En Windows podemos utilizar o comando "**ipconfig**", cos seguintes parámetros:

- **Comprobación da concesión:** Usaremos **"/all"** para ver cal é o servidor DHCP que adxudicou a configuración ao equipo, así como a data e caducidade da concesión.
- **Liberación da concesión:** Co parámetro **"/release"** comunicaremos ao servidor DHCP a liberación da dirección IP, e o adaptador de rede deixará de ter a súa configuración automática por DHCP.
- **Renovación da concesión:** O parámetro **"/renew"** permite obter ou renovar a configuración automática por DHCP.

### (2) Manexo do cliente DHCP en sistemas GNU/Linux

En Linux, o comando "**dhclient**" permite xestionar o cliente DHCP. As operacións máis relevantes que podemos levar a cabo son:

- **Renovación da concesión:** Simplemente poremos **"dhclient nome\_da\_interface"** para que o equipo adquira de forma automática ou renove a configuración de rede por DHCP. Podemos usar o parámetro **"-v"** para que visualizar os pasos deste proceso.
- **Liberación da concesión:** Co parámetro **"-r"** comunicaremos ao servidor DHCP a liberación da dirección IP, e o adaptador de rede deixará de ter a súa configuración automática por DHCP.

En sistemas Linux, o ficheiro **"/var/lib/dhcp/dhclient.leases"** leva un rexistro do cliente DHCP, así que consultando este ficheiro poderemos obter toda a información das distintas concesións obtidas.

## 2. Configuración básica do servizo DHCP en Linux

Neste apartado veremos a instalación de configuración básica do servidor DHCP do ISC, xa que é o máis utilizado, sobre Debian.

### 2.1. Instalación e configuración básica do servizo

Con **apt-get install isc-dhcp-server** instalamos o servidor DHCP. Podemos observar que trata de iniciarse o servizo DHCP, pero falla. Isto é porque aínda non temos configurado ningún ámbito/rango de IPs para asignar.

Editamos o ficheiro de configuración **/etc/dhcp/dhcpd.conf**. O ficheiro ten moitos exemplos comentados de como realizar distintas configuracións, pero comezaremos configurado opcións como se amosan na imaxe:

```
GNU nano 2.2.6  Ficheiro: /etc/dhcp/dhcpd.conf  Modificado

# attempt to do a DNS update when a lease is confirmed. We defa
# behavior of the version 2 packages ('none', since DHCP v2 did
# have support for DDNS.)
##ddns-update-style none;
ddns-update-style none;

# option definitions common to all supported networks...
## option domain-name "example.org";
## option domain-name-servers ns1.example.org, ns2.example.org;

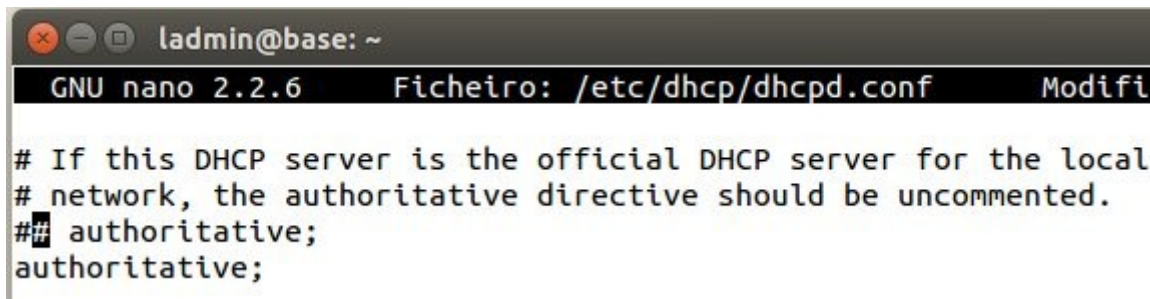
#### Configurado por nós ####
option domain-name "iescalquera.local";
option domain-name-servers 172.16.5.10;
option routers 172.16.5.1;

## default-lease-time 600;
default-lease-time 3600;
max-lease-time 7200;
```

Onde haxa ## é que esas opcións eran as que viñan configuradas por defecto e que foron modificadas no ficheiro

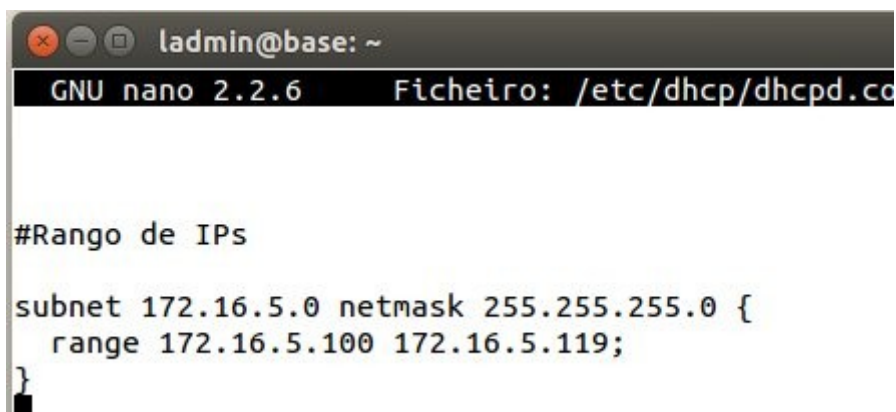
- **option domain-name:** para indicar o nome de dominio que ofrecerá ao cliente.
- **option domain-name-servers:** para indicar as IPs dos servidores DNS.
- **option routers:** para indicar que porta de enlace deben usar os clientes DHCP.
- **default-lease-time:** tempo mínimo que se dá a unha concesión IP (en segundos).

Se este servidor é o oficial para esta LAN debemos indicar que é **authoritative**, deste xeito se o servidor atopa un cliente con configuración DHCP incorrecta enviaralle unha configuración correcta para esta LAN:



```
ladmin@base: ~  
GNU nano 2.2.6    Ficheiro: /etc/dhcp/dhcpd.conf    Modifi  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
## authoritative;  
authoritative;
```

Ao final do ficheiro engadimos o rango de IPs, onde se indica a rede IP, a súa máscara é o rango de IPs a asignar aos clientes. Gardamos o ficheiro:



```
ladmin@base: ~  
GNU nano 2.2.6    Ficheiro: /etc/dhcp/dhcpd.co  
  
#Rango de IPs  
  
subnet 172.16.5.0 netmask 255.255.255.0 {  
    range 172.16.5.100 172.16.5.119;  
}
```

Editamos o ficheiro **/etc/default/isc-dhcp-server** e configuramos o parámetro **INTERFACESv4=""** co nome da interface polo cal se van atender as solicitudes DHCP dos clientes:

```
GNU nano 2.7.4      Ficheiro: /etc/default/isc-dhcp-server      Modificado

# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
INTERFACESv6=""

^G Obter Axuda  ^O Gravar      ^W ¿U-lo?      ^K CortarText  ^J Xustificar  ^C PosicAct
^X Saír         ^R Ler Fich    ^\ Substituír  ^U RepórTexto ^T Ortografía  ^ Ir á liña
```

Xa podemos iniciar o servizo de DHCP con **systemctl start isc-dhcp-server**.

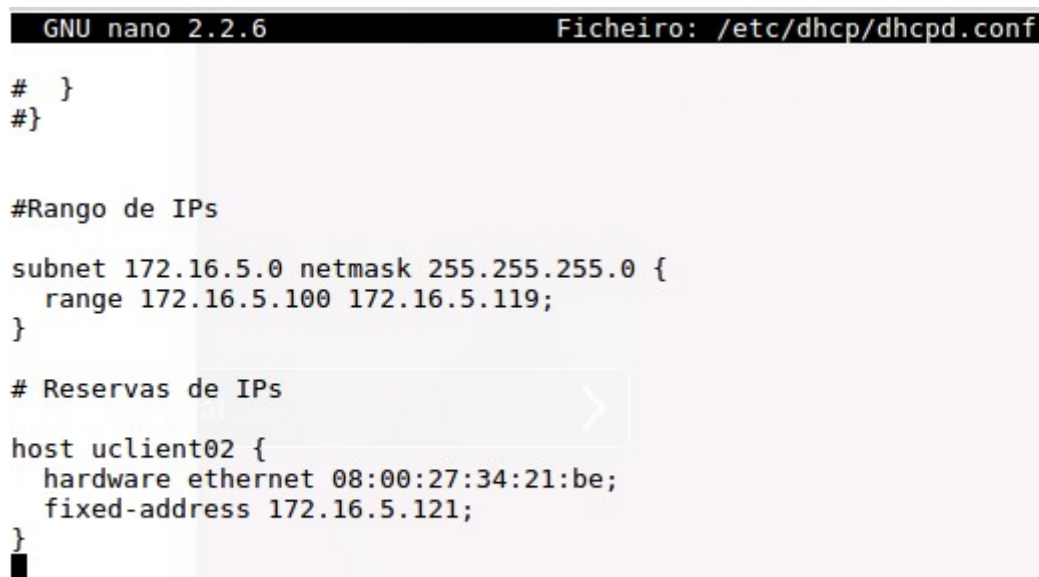
No servidor podemos ver no ficheiro **/var/lib/dhcp/dhcpd.leases** as concesións realizadas.

## 2.2. Definición de reservas de direcciones

Un aspecto interesante é que se coñecemos a MAC dun equipo podemos configurar o servizo DHCP para sempre que ese equipo solicite unha configuración IP lle asigne a mesma IP.

Esa configuración coñécese co nome de reserva de IPs.

Engadimos unha nova entrada **host** ao final do ficheiro **/etc/dhcp/dhcpd.conf** para realizar a reserva:



```
GNU nano 2.2.6                               Ficheiro: /etc/dhcp/dhcpd.conf
# }
#}

#Rango de IPs

subnet 172.16.5.0 netmask 255.255.255.0 {
    range 172.16.5.100 172.16.5.119;
}

# Reservas de IPs

host uclient02 {
    hardware ethernet 08:00:27:34:21:be;
    fixed-address 172.16.5.121;
}
```

Indicamos o nome para a reserva (non ten porque coincidir co nome de equipo), o enderezo MAC do cliente e a IP que se desexa asignar fóra do rango de IPs que se asigna para os equipos que non teñen reserva.

E reiniciamos o servizo DHCP para activar os cambios.

### 3. Actualizacións dinámicas do servidor DNS

Sería interesante que o servidor DHCP actualizase no servidor DNS as concesións que vai ofrecendo, tanto na zona de busca directa **iescalquera.local** como na zona de busca inversa **5.16.172.in-addr.arpa**. Ese proceso coñecese co nome de [DNS dinámico](#) (DDNS).

#### 3.1. Configuración de DDNS no servidor

Comezaremos creando unha chave secreta, e asignaremos esa chave as zonas DNS e ao servizo DHCP:

```
root@dserver00:~# ddns-confgen -a hmac-md5 -z iescalquera.local -r /dev/urandom
# To activate this key, place the following in named.conf, and
# in a separate keyfile on the system or systems from which nsupdate
# will be run:
key "ddns-key.iescalquera.local" {
    algorithm hmac-md5;
    secret "pik94l1nWXcWnzNfN8F3JA==";
};

# Then, in the "zone" definition statement for "iescalquera.local",
# place an "update-policy" statement like this one, adjusted as
# needed for your preferred permissions:
update-policy {
    grant ddns-key.iescalquera.local zonesub ANY;
};

# After the keyfile has been placed, the following command will
# execute nsupdate using this key:
nsupdate -k <keyfile>
```

Para xerar a chave secreta usamos:

**ddns-confgen -a hmac-md5 -z iescalquera.local -r /dev/urandom**

Obtemos unha chave secreta que debemos copiar:

```
root@dserver00:~# ddns-confgen -a hmac-md5 -z ie
# To activate this key, place the following in r
# in a separate keyfile on the system or systems
# will be run:
key "ddns-key.iescalquera.local" {
    algorithm hmac-md5;
    secret "pik94l1nWXcWnzNfN8F3JA==";
};

# Then. in the "zone" definition statement for '
```



Creamos con *nano* un ficheiro onde gardala, por exemplo en **/etc/bind/ddns.key**. Observar o nome que lle puxemos á chave (CHAVE-DDNS). Pode ser calquera nome, pero ese nome hai que usalo despois:

```
GNU nano 2.2.6      Ficheiro: /etc/bind/ddns.key

key "CHAVE-DDNS" {
    algorithm hmac-md5;
    secret "pik94l1nWXcWnzNfN8F3JA==";
};
```

Facemos que a ese ficheiro só acceda *root* e o grupo *bind*, poñéndolle permisos 640.

Editamos o ficheiro onde temos definidas as zonas **/etc/bind/named.conf.local**. Incluimos na configuración o ficheiro anterior coa cláusula **include**. En cada zona metemos a entrada **allow-update {key CHAVE-DDNS;;}**

```
GNU nano 2.2.6      Ficheiro: /etc/bind/named.conf.local

include "/etc/bind/ddns.key";

zone "iescalquera.local" {
    type master;
    file "db.iescalquera.local";
    allow-update {key CHAVE-DDNS;;};
};

zone "5.16.172.in-addr.arpa" {
    type master;
    file "db.172.16.5";
    allow-update {key CHAVE-DDNS;;};
};
```



Tócalle agora a quenda ao servizo DHCP. No ficheiro de configuración

**/etc/dhcp/dhcpd.conf** modificamos a entrada **ddns-update-style** de **none** a **interim** para que trate de actualizar as concesións no servizo DNS. Tamén engadir as entradas:

- **ddns-domainname nome de dominio** para indicar o nome do dominio onde realizar as actualizacións.
- **update-static-leases on** para que tamén actualice no servizo DNS as concesións de IP que se fan con reservas.

```
GNU nano 2.2.6      Ficheiro: /etc/dhcp/dhcpd.conf
#
# Sample configuration file for ISC dhcpd for Debian
#
#
# The ddns-updates-style parameter controls whether or n
# attempt to do a DNS update when a lease is confirmed.
# behavior of the version 2 packages ('none', since DHCP
# have support for DDNS.)
##ddns-update-style none;
ddns-update-style interim;
ddns-domainname "iescalquera.local";
update-static-leases on;
```

Na reserva para o equipo uclient02 engadir o nome que se debe rexistrar no servizo DNS coa entrada: **ddns-hostname "uclient02";**

```
GNU nano 2.2.6      Ficheiro: /etc/dhcp/dhcpd.conf
# Reservas de IPs
host uclient02 {
    hardware ethernet 08:00:27:83:66:43;
    fixed-address 172.16.5.121;
    option host-name "uclient02";
    ddns-hostname "uclient02";
}
```

No mesmo ficheiro engadir ao final un **include** do ficheiro da chave e as 2 zonas indicando a IP de quen as xestiona (neste caso o mesmo servidor 127.0.0.1) e a chave secreta a usar para cando o servizo DHCP desexe realizar unha actualización en cada unha das zonas:

```
include "/etc/bind/ddns.key";
```

```
zone iescalquera.local. {  
    primary 172.16.5.10;  
    key CHAVE-DDNS;  
}
```

```
zone 5.16.172.in-addr.arpa. {  
    primary 172.16.5.10;  
    key CHAVE-DDNS;  
}
```

Reiniciamos os servizos DHCP e DNS para aplicar os cambios.

## 3.2. Comprobación das actualizacións

O único que temos que facer para comprobar as actualizacións DDNS é renovar a concesión no cliente. Poderemos comprobar inmediatamente que podemos resolver o nome e a dirección IP do equipo cliente por DNS.

Se reiniciamos o servizo DNS ou executamos **rndc freeze** actualizaranse os ficheiros de texto das zonas creadas por nós. Aquí vemos actualizado o ficheiro asociado á zona directa **iescalquera.local** onde vemos que está dado de alta o equipo **uclient02**:

```
root@dserver00:~# rndc freeze
root@dserver00:~# cat /var/cache/bind/db.iescalquera.local
$ORIGIN .
$TTL 86400      ; 1 day
iescalquera.local IN SOA  iescalquera.local. root.iescalquera.l
                        2      ; serial
                        604800  ; refresh (1 week)
                        86400   ; retry (1 day)
                        2419200 ; expire (4 weeks)
                        86400   ; minimum (1 day)
                        )
                        NS      ns.iescalquera.local.
$ORIGIN iescalquera.local.
dserver00      A      172.16.5.10
ns             A      172.16.5.10
uclient01      A      172.16.5.20
$TTL 1800      ; 30 minutes
uclient02      A      172.16.5.121
                TXT    "00c9a67b40484bee0cad4fa3e4432115c7"
```

## 4. DHCP Failover

### 4.1. Como funciona o DHCP failover

Tendo en conta que os clientes buscan o servidor DHCP usando paquetes de broadcast, se implantamos máis de un servidor DHCP na mesma rede sen ningunha configuración especial, non teremos control de que servidor vai atender a petición dun cliente.

Porén, tendo en conta que este servizo é imprescindible para que os equipos teñan conectividade de rede, o seu funcionamento resulta crítico e pode interesarnos en moitos casos configurar varios servidores DHCP para que se repartan o traballo e en caso de caída dalgún deles os outros segan prestando o servizo.

Este mecanismo coñécese como [DHCP failover](#), e imos ver os parámetros básicos para configuralo. Antes de nada hai que ter en conta que esta configuración lévase a cabo establecendo unha relación de *failover* entre dous servidores DHCP, que se asociará a un **pool**, que é un conxunto de direccións dentro dunha subrede definida no servidor DHCP e que pode ter unha configuración particular.

Polo tanto, será necesario definir un *pool* dentro da subrede, aínda que só teñamos un rango de direccións. Distintos *pools* do servidor DHCP poden estar asociados a distintas relacións de emparellamento, polo que pode haber múltiples servidores DHCP redundantes nunha rede.

Será importante para que se estableza o emparellamento que os dous servidores teñan a hora sincronizada e que teñan unha versión similar do servdor DHCP ISC.

Imos ver como facer a configuración de failover para un pool determinado. Teremos que seleccionar un servidor DHCP como primario e outro como secundario.

## 4.2. Configuración do emparellamento entre dous servidores

No servidor DHCP primario engadiremos o seguinte bloque no ficheiro de configuración:

```
failover peer "failover-partner" {  
    primary;  
    address 172.16.5.100;  
    port 519;  
    peer address 172.16.5.101;  
    peer port 520;  
    max-response-delay 60;  
    max-unacked-updates 10;  
    mclt 3600;  
    split 128;  
    load balance max seconds 3;  
}
```

E no servidor DHCP secundario introduciremos o seguinte:

```
failover peer "failover-partner" {  
    secondary;  
    address 172.16.5.101;  
    port 520;  
    peer address 172.16.5.100;  
    peer port 519;  
    max-response-delay 60;  
    max-unacked-updates 10;  
    load balance max seconds 3;  
}
```

Os parámetros establecidos neste bloque que engadimos son:

- **primary** ou **secondary**, para indicar se o servidor é primario ou secundario.
- **address** e **port**, para indicar a dirección IP e porto deste servidor para o emparellamento *failover*.
- **peer address** e **peer port**, para indicar a dirección IP e porto do servidor co que nos emparellamos.
- **max-response-delay**: Indica cantos segundos agardará o servidor por unha mensaxe da parella antes de considerar que non hai conexión con el.
- **max-unacked-updates**: Indica cantas mensaxes BNDUPD pode mandar o servidor remoto antes de recibir unha confirmación (ACK) deste servidor.
- **load balance max seconds**: Serve para indicar a un cliente cantos segundos debe agardar para recibir unha resposta antes de cortar o balanceo de carga entre varios servidores.
- **mclt**: Este parámetro só debe ser definido no servidor primario, non no secundario. Serve para indicar a cantidade de tempo pola que un servidor do emparellamento debe renovar unha concesión se non ten conexión co outro.
- **split**: Este parámetro só debe ser definido no servidor primario, non no secundario. Este valor afecta a como se balancea a carga entre os servidores cando os dous están activos. Canto maior sexa o valor, máis clientes vai a atender o servidor primario fronte ao secundario. O valor de este parámetro vai entre o 0 e o 255 sendo o máis recomendable o 128.

### 4.3. Configuración dun pool en failover

Nos dous servidores configuraremos o *pool* da mesma maneira, para que faga uso do emparellamento de *failover*:

```
subnet 172.16.5.0 netmask 255.255.255.0 {  
    pool {  
        failover peer "failover-partner";  
        range 172.16.5.100 172.16.5.119;  
    }  
}
```

### 4.4. Configuración da chave de autenticación

Para securizar a comunicación entre os servidores DHCP, utilizaremos unha capa de programación chamada OMAPI. Esta capa nos permite autenticar a conexión entre os servidores por medio dunha chave privada.

Para configuración unha chave OMAPI, introduciremos a seguinte configuración nos dous servidores emparellados:

```
omapi-port 7911;  
omapi-key omapi_key;  
  
key omapi_key {  
    algorithm hmac-md5;  
    secret Ofakekeyfakekeyfakekey= =;  
}
```

A chave secreta pode ser xerada co comando "[\*dnssec-keygen\*](#)".



## 5. Axentes de reenvío DHCP

As solicitudes de asignación de configuración automática dos parámetros de rede mediante DHCP iníciáanse cando unha máquina arranca. Como xa vimos, o cliente envía unha mensaxe de broadcast, ao que responden o servidor ou servidores da subrede.

O problema é que as mensaxes de broadcast non atravesan os routers, e polo tanto, en cada subrede na que se utilice DHCP debería haber un servidor que escoite as peticións emitidas.

Neste casos, para poder centralizar o servizo nun único servidor para varias redes ou subredes pódense usar axentes DHCP de retransmisión ou reenvío (*DHCP relay agents*).

Un axente DHCP de retransmisión ou reenvío é un dispositivo da rede (en moitos casos, un router) que escoita as solicitudes DHCP que se producen na rede, e as encamiña cara un servidor DHCP que se atopa noutra rede para que este as atenda. O servidor DHCP dará unha resposta que enviará ao axente de reenvío e este á súa vez a trasladará ao cliente que fixo a petición.

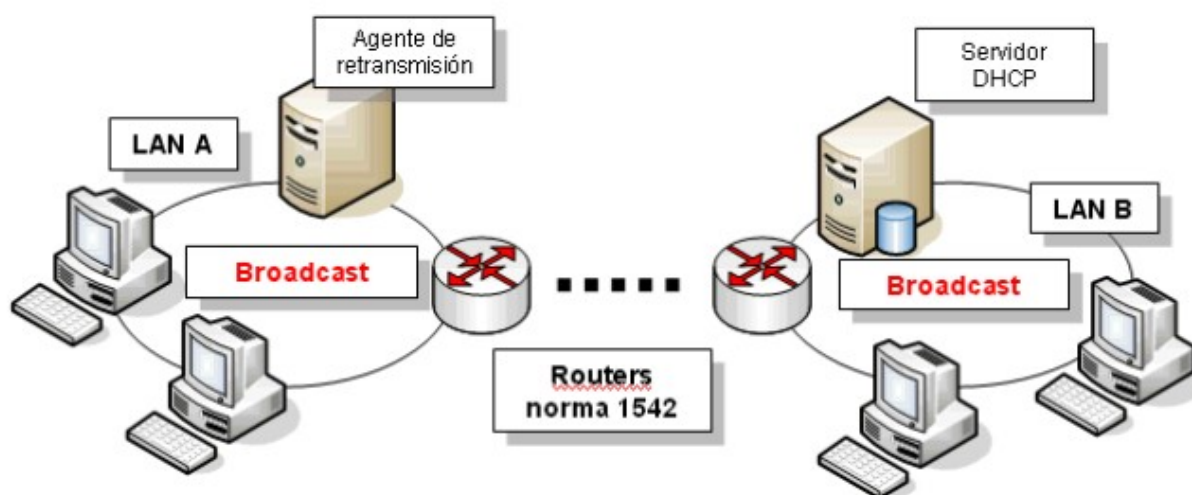


Figura: Funcionamento do axente de retransmisión DHCP

O funcionamento e características dos axentes de retransmisión establécense no RFC 1542.

Para configurar un axente de retransmisión é necesario:

- Activar o axente de retransmisión no dispositivo de encamiñamento.
- Indicar no axente de retransmisión cal é a rede cliente.
- Indicar no axente de retransmisión cal é o servidor DHCP que vai atender as peticións DHCP.

No servidor DHCP centralizado debemos configurar varias subredes ás que se dá servizo indicando as direccións IP que se van a asignar dentro de cada subrede.