

1 Configuración TCP/IP

A estas alturas del ciclo, ya sabrás que para que los PCs de una red puedan intercomunicarse entre sí, deben disponer de una **dirección IP** y de una **máscara de subred**. Además, si queremos que disponga de conexión a Internet, es necesario configurar la **dirección IP de la puerta de enlace** y la **dirección IP de dos servidores DNS**.



Ejemplo configuración TCP/IP

Dirección IP	192.168.0.15
Máscara de subred	255.255.255.0
Puerta de enlace	192.168.0.254
DNS preferido	80.58.0.33
DNS alternativo	80.58.32.97

Dentro de una misma red, los PCs deben tener una dirección IP perteneciente al rango de dicha red. Si el rango es desde 192.168.0.0 hasta 192.168.0.255, las IPs de los PCs deberán tener los tres primeros números iguales (192.168.0.X) y el último número podrá cambiar desde 1 hasta 254, porque no se permite la utilización de la primera ni de la última dirección IP del rango ya que quedan reservadas. Cada PC deberá tener una dirección IP diferente. Si dos PCs tienen la misma IP, habrá un conflicto de IP y ninguno de ellos podrá comunicarse hasta que no se resuelva el conflicto cambiando la IP a uno de ellos. Si no sabemos qué IP poner, podemos ver la IP de otro PC de nuestra red en el que funcione correctamente la conexión de Internet y por regla general, cambiar el último valor por otro diferente que no tenga ningún otro PC.

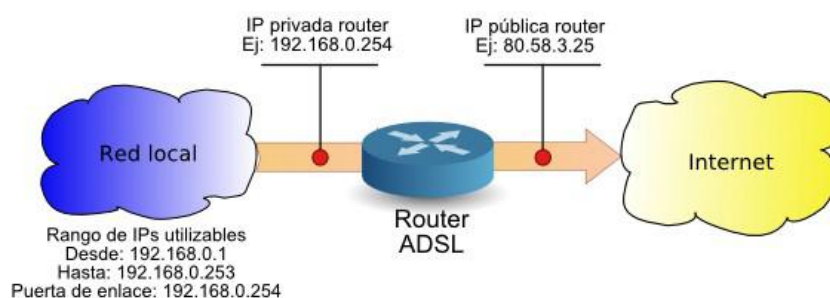
La **Máscara de subred** determina el número de PCs del rango. Casi siempre se suele utilizar la máscara 255.255.255.0 que corresponde a un rango de 256 direcciones IP (suficientes para casi todos los centros educativos) en los que todos los PCs tienen los tres primeros números de la IP iguales y solo cambia el último. Lo normal es que todos los PCs de nuestra red tengan configurada la misma máscara de subred. Si no sabemos cuál es la máscara de subred, podemos verla en otro PC que funcione correctamente la conexión de Internet.

La **Puerta de enlace** deberá ser una IP del rango ya que de lo contrario, nuestro PC no será capaz de comunicarse con ella y no tendrá acceso a Internet. Lo normal es que todos los PCs de nuestra red tengan configurada la misma puerta de enlace. Si no sabemos la IP de nuestra puerta de enlace, podemos verla en otro PC que funcione correctamente la conexión de Internet.

Los **DNS preferido y alternativo** nos los debe proporcionar la compañía que presta el servicio. Telefónica usa el 80.58.0.33 y el 80.58.32.97. Lo normal es que todos los PCs de nuestra red tengan configurados los mismos DNSs. Si no sabemos la IP de los DNS preferido y alternativo, podemos verlos en otro PC que funcione correctamente la conexión de Internet.

2 Direcciones IP públicas y privadas

Las direcciones IP de los PCs de una red local son direcciones privadas ya que los PCs no están directamente conectados a Internet. Solamente el router dispone de conexión directa a Internet y por eso es el único que dispone de una dirección IP pública. Cuando los PCs de una misma red se quieren comunicar unos con otros, lo hacen directamente, pero si quieren comunicarse con Internet, deben hacerlo a través del router. Es equivalente a una



centralita telefónica. Los teléfonos internos de una empresa utilizan números privados (extensiones) y las llamadas al exterior es necesario hacerlas a través de la centralita, que es la única que tiene números de teléfono públicos. Los únicos rangos de direcciones que se pueden utilizar en redes locales son:

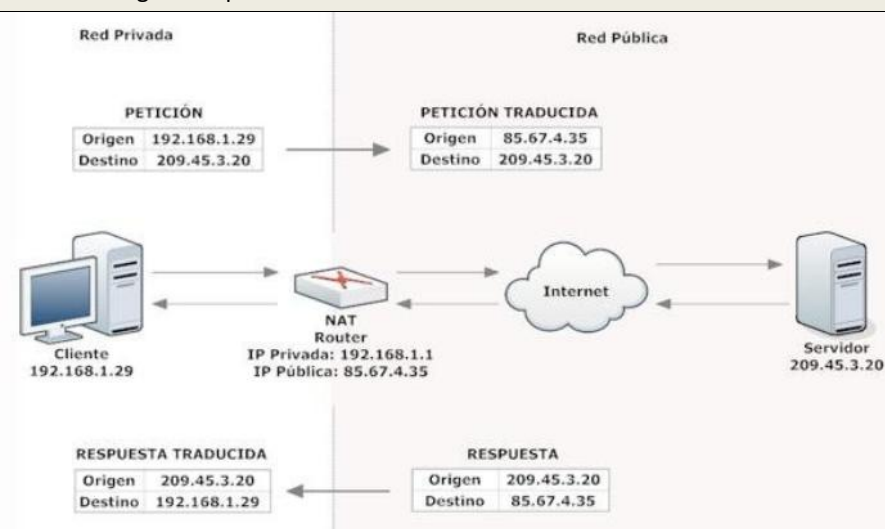
Rangos Redes Locales	
Desde	Hasta
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Estos rangos de direcciones no están asignados a direcciones públicas de Internet, sino que se han reservado para ser utilizados en las redes locales. Si en lugar de configurar nuestra red con estas direcciones utilizamos otro rango, como seguramente sea un rango utilizado por servidores de Internet, no tendremos acceso a dichos servidores.

3 NAT: Traducción de Direcciones de Red

Internet en sus inicios no fue pensado para ser una red tan extensa, por ese motivo se reservaron “sólo” 32 bits para direcciones, pero el hecho es que el número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP se agotaban. Por ello surgió la NAT o Network Address Translation (Traducción de Direcciones de Red). La idea es sencilla, hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Gracias a este “parche”, las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet.

La idea básica que hay detrás de NAT es traducir las IPs privadas de la red en una IP pública para que la red pueda enviar paquetes al exterior; y traducir luego esa IP pública, de nuevo a la IP privada del PC que envió el paquete, para que pueda recibirlo una vez llega la respuesta.

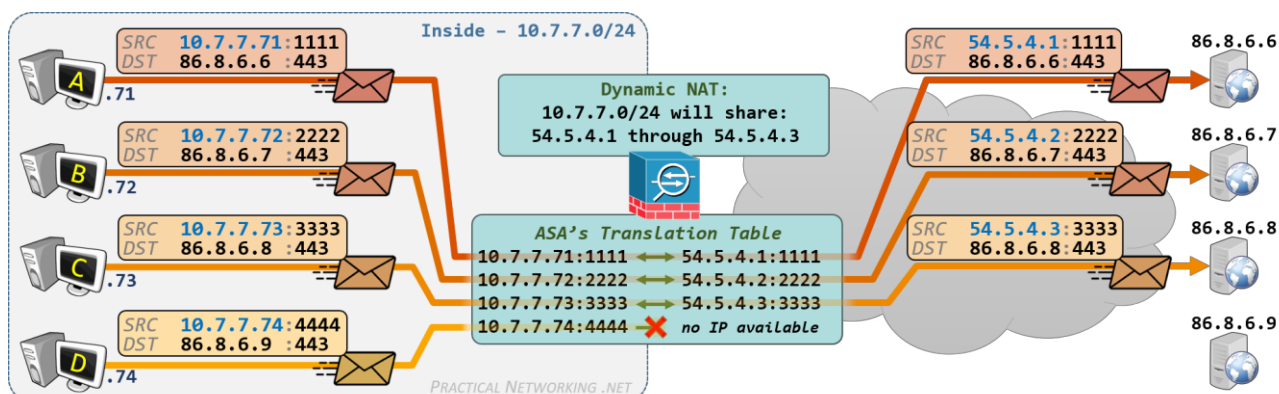


3.1 ¿Cómo funciona?

En la NAT existen varios tipos de funcionamiento:

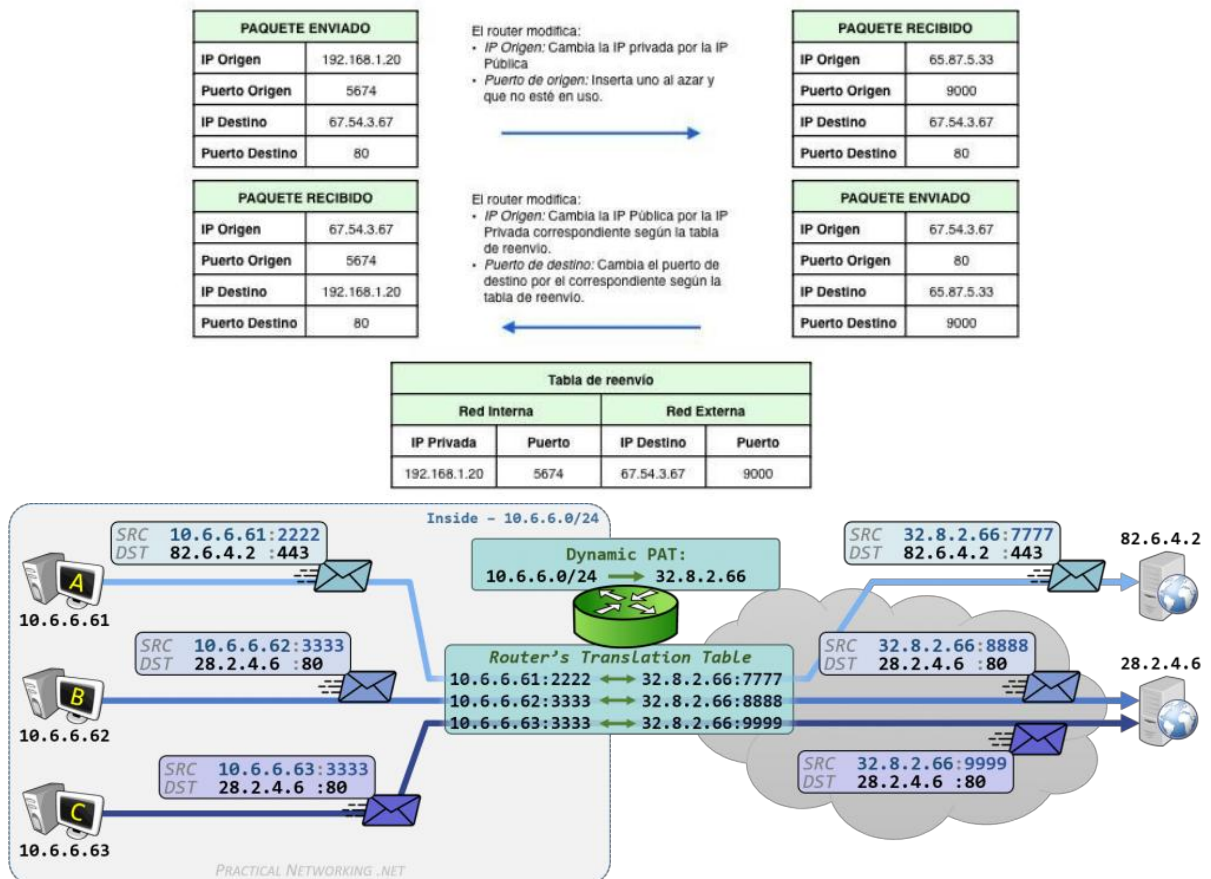
- ✚ **Estática:** Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. (Ver imagen anterior)
- ✚ **Dinámica:** El router tiene asignadas **varias direcciones IP públicas**, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública.

Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando.



- Sobrecarga:** La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos, ya que es el utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. Además del ahorro económico, también se ahorran direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública.

Para poder hacer esto **el router hace uso de los puertos**. En los protocolos TCP y UDP se disponen de 65.536 puertos para establecer conexiones. De modo que cuando una máquina quiere establecer una conexión, el router guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar. Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.



3.2 Ventajas de la NAT

El uso de la NAT tiene varias ventajas:

- La primera y más obvia, el gran ahorro de direcciones IPv4** que supone, recordemos que podemos conectar múltiples máquinas de una red a Internet usando una única dirección IP pública.
- Seguridad.** Las máquinas conectadas a la red mediante NAT no son visibles desde el exterior, por lo que un atacante externo no podría averiguar si una máquina está conectada o no a la red.
- Mantenimiento de la red.** Sólo sería necesario modificar la tabla de reenvío de un router para desviar todo el tráfico hacia otra máquina mientras se llevan a cabo tareas de mantenimiento.

Recordemos que la NAT es solo un parche, no una solución al verdadero problema, por tanto también tiene una serie de desventajas asociadas a su uso:

- Checksums TCP y UDP:** El router tiene que volver a calcular el checksum de cada paquete que modifica. Por lo que se necesita mayor potencia de computación.





No todas las aplicaciones y protocolos son compatibles con NAT. Hay protocolos que introducen el puerto de origen dentro de la zona de datos de un paquete, por lo que el router no lo modifica y la aplicación no funciona correctamente.

4 ¿Qué es el servicio DHCP?

Voy a explicarte en qué consiste este servicio. Todos los nodos de una red deben tener una dirección IP, esta se puede asignar de forma manual o automática. El protocolo DHCP (Dynamic Host Configuration Protocol) o Protocolo de Configuración Dinámica de Host, es un protocolo que permite a los nodos de una red obtener su dirección IP de forma automática.

DHCP es un **protocolo** de tipo **cliente/servidor** en el que un servidor tiene rangos de direcciones IP y las va asignando a los clientes según van estando libres. El servidor sabe en todo momento quien tiene la posesión de una IP mediante la dirección MAC

Al usar este protocolo podrás comprobar las siguientes **ventajas**:





-  No se necesita apuntar la configuración de los equipos.
-  Se protegen las IP de los servidores.
-  No hay conflictos de IP.
-  Se pueden reutilizar las direcciones IP.

5 Configuración de los parámetros de red.

En esta unidad vas a conocer el funcionamiento de un **servicio de configuración automática de los parámetros de conexión en red** y como se instala, configura y prueba el servicio.

En el módulo “**Sistemas Informáticos**” de primer curso del ciclo que estás estudiando se trató la arquitectura TCP/IP y, dentro de ella, el protocolo IP y el sistema de direccionamiento IP usado para asignar direcciones a las interfaces de red de los equipos (ordenadores, routers, impresoras de red y otros). Un ordenador va a tener en cada adaptador o tarjeta de red una configuración de parámetros de red.

Los parámetros de red que principalmente se configuran en un adaptador de red sirven para que:

-  Un ordenador tenga la dirección IP y máscara adecuada para conectarse en red a través del adaptador de red.
-  Se pueda conocer si una dirección IP con la que se conecte está en la misma red que el adaptador.
-  Un ordenador se pueda conectar con otras redes a través de un dispositivo enrutador.
-  Un servidor DNS resuelva los nombres DNS de recursos cuya identificación escribamos en los programas de red mediante un nombre DNS.

La configuración de los parámetros de red de un adaptador de red se puede realizar en cualquier sistema operativo al menos de dos formas: **manual y automática**.



La **configuración manual** también se conoce como **configuración fija o estática**. En esta configuración, el administrador de red se tiene que encargar de escribir en un programa o en un archivo de configuración los valores de los parámetros de configuración. En la **configuración automática**, el administrador simplemente se limita a especificar en los ordenadores que la utilicen, que van a usar esa configuración sin tener que aportar más datos.

5.1 Parámetros de configuración de red.

Para que un adaptador de red tenga conectividad dentro de una red debe tener asignada una **dirección IP** que le identifique y una **máscara de red**. La IP debe pertenecer a la misma red que el resto de equipos de la red. Debes recordar que la máscara junto con la IP permiten determinar si otras direcciones IP con las que se conecte desde el adaptador pertenecen o no a la misma red.



En esta unidad se hará referencia al direccionamiento **IPv4** aunque para **IPv6**, con sus particularidades, se podrá aplicar lo mismo que para IPv4. En IPv4, una dirección IP es un conjunto de 32 bits que representamos con 4 números decimales separados por puntos. La máscara es también un número de 32 bits cuya primera parte es una secuencia de unos e indica que bits de la IP representan la red a la que pertenece esa IP y cuya segunda parte es una secuencia de ceros que indican que bits de la IP identifican al adaptador de red dentro de la red. La máscara se puede representar, al igual que la IP, con 4 números decimales separados por puntos o con el formato /num, donde num indica cuantos bits sirven para identificar la red a la que pertenece una IP.

Por ejemplo, si un adaptador tiene IP 192.168.1.7 y máscara 255.255.255.0, se puede decir también que el adaptador tiene la IP 192.168.1.7/24 indicando que hay 24 unos en la máscara. Por tanto en esa IP el identificador de red es 192.168.1 y el del adaptador dentro de la red es 7.

Para que un ordenador tenga, a través de un adaptador de red, **conectividad con otras redes** y, en particular, con Internet se debe asignar en el adaptador la **IP de la puerta de enlace** o la IP del dispositivo de red que realiza el encaminamiento hacia otras redes. Lo normal es que esta IP sea la interna del router de conexión a Internet. Para que en los programas de red se puedan usar nombres DNS de equipos en lugar de direcciones IP, se deben asignar las **IP de los servidores DNS**.

La puerta de enlace debe pertenecer a nuestra red. Un servidor DNS puede pertenecer o no a nuestra red. Al final de esta unidad aprenderás a instalar y configurar un servidor DNS.

5.2 Configuración manual de parámetros de red.

Al asignar las direcciones IP de forma manual hay que ser cuidadoso y ordenado. Se debe tener documentada la asignación de IP que se ha hecho en cada ordenador de la red para conocer las IP que ya tenemos utilizadas y las que podemos usar. Todas las direcciones IP de los equipos de una red deben pertenecer a la misma IP de red. Las direcciones IP que se asignen se deben elegir de acuerdo a un criterio de ordenamiento y organización de los ordenadores dentro de la red.

Si se asigna la misma IP a dos ordenadores de una red y ambos están en funcionamiento se produce un **conflicto de IP** lo que provoca que esos dos ordenadores no funcionen correctamente en la red.



En los sistemas Linux Debian/Ubuntu se tiene instalado el software de detección y configuración NetworkManager que incluye una herramienta gráfica para configurar conexiones de red.





5.3 Configuración automática de los parámetros de red.

Establecer la **configuración automática** de los parámetros de red para un adaptador de red es muy sencillo y no se necesita conocer nada acerca de esos parámetros. Sin embargo, para que se pueda establecer la configuración automática se necesita tener en la red algún dispositivo que proporcione el servicio de asignación automática de parámetros de red (**servidor**).

Cuando un ordenador cliente se inicia y está configurado para recibir automáticamente los parámetros de red, realiza un proceso para buscar un servidor en la red que le envíe esos parámetros. Si hay algún servidor, el ordenador cliente recibirá los valores de los parámetros de configuración de red desde el servidor, los asignará y podrá trabajar en red sin ningún problema.

Supongo que ante esta explicación tan simple de una asignación automática de parámetros de red, te surgirán muchas preguntas y dudas sobre el funcionamiento, pero no te preocupes, encontrarás respuestas en los contenidos de esta unidad.

La asignación automática de los parámetros de red presenta varias ventajas frente a la asignación manual:

-  Se puede mover un ordenador entre dos redes que dispongan del servicio de asignación automática sin tener que cambiar su configuración.
-  Es mucho más fácil configurar la red en los ordenadores ya que no hay que recordar los parámetros de configuración necesarios ni hay que escribirlos.
-  Se evitan posibles conflictos de IP en la red, ya que en los servidores se controla que se puedan dar dos IP iguales en la red.
-  Se reduce el trabajo dedicado por los administradores de la red a la configuración de la conexión de red de los equipos.

5.4 Archivo de configuración de parámetros de red.

En los sistemas Linux, si no se dispone de una herramienta gráfica de configuración de los parámetros de red, hay que realizar la configuración editando un archivo de configuración de dichos parámetros. En los sistemas Linux Debian/Ubuntu este archivo es **/etc/network/interfaces**. (Para las nuevas versiones de Ubuntu, ver el documento: "Tema 02 - Actividad 5 - Configurar Red - Ubuntu 18.04")

Si queremos que el adaptador de red de nuestro ordenador reciba los parámetros de red de forma automática, este archivo debe contener lo siguiente:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```


Las dos primeras líneas establecen la configuración de red del adaptador de bucle local. Las dos siguientes son las que establecen la configuración del adaptador "eth0" de conexión a red. En esa configuración, "auto" implica que el adaptador se active en el inicio del sistema e "iface eth0 inet dhcp" significa que el interface o adaptador eth0 tenga una configuración automática de parámetros de red usando el protocolo dhcp.

Si queremos establecer de forma estática la configuración de los parámetros de red del adaptador de red eth0, el archivo debería contener algo como lo siguiente:

```
auto lo
iface lo inet loopback
```

```
auto eth0
iface eth0 inet static
address 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.254
dns-nameservers 8.8.8.8
```

En este caso vemos que la configuración que se establece para eth0 es static, es decir, que se asignan manualmente los parámetros que se escriben a continuación en el propio archivo. En el ejemplo se asigna la IP 192.168.1.1 con la máscara de red 255.255.255.0, la dirección de red es 192.168.1.0, la dirección de broadcast es 192.168.1.255, la dirección IP de la puerta de enlace es 192.168.1.254 y el servidor DNS es 8.8.8.8.

A continuación se indican algunos tutoriales para aprender a configurar los parámetros de red en distintos Sistemas Operativos:

LINUX

Configurar la red en la interfaz gráfica de Ubuntu 16.04 LTS - <https://goo.gl/5cFkSk>

Averiguar la IP en un ordenador con Ubuntu 14.04 LTS - <https://goo.gl/XB7b4d>

Consultar la configuración de la red en Ubuntu con ifconfig - <https://goo.gl/mpcA5a>

Configurar la red en Ubuntu modificando el archivo de configuración - <https://goo.gl/iey48X>

Configurar la red en Ubuntu modificando el archivo de configuración (Posterior a Ubuntu Server 17.04)
<https://xurl.es/tu0qw>

Cambiar nombre interface enp0s3 a eth0 en Ubuntu 16.04.1 - <https://youtu.be/RwgYEWqVxzs>

WINDOWS

Asignar una dirección IP fija en Windows 8.1 - <https://goo.gl/22v8Sd>

Averiguar la IP en un ordenador con Windows 10 - <https://goo.gl/JQBB1U>

Consultar la configuración de la red en Windows con ipconfig - <https://goo.gl/vo7apA>

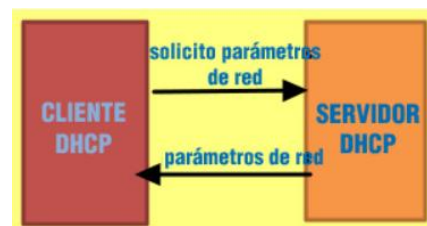
Configurar una dirección IP estática en Windows 10 (VÍDEO) - <https://youtu.be/mBZVp9hGpYw>

6 El protocolo DHCP

El **protocolo DHCP (Dynamic Host Configuration Protocol)**, es un protocolo que corresponde al nivel de aplicación para redes TCP/IP. El objetivo de este protocolo es proporcionar un servicio de red que permita a equipos de una red TCP/IP obtener automáticamente los parámetros de configuración de red.

El funcionamiento de DHCP en la red se basa en un modelo cliente/servidor con uno o varios equipos servidores que proporcionan el servicio y varios equipos clientes que reciben automáticamente los parámetros de configuración de red.

Un cliente DHCP solicita en la red que algún servidor DHCP le proporcione los parámetros de configuración de red. Si hay algún servidor DHCP, el cliente recibirá valores de los parámetros desde el servidor y asignará esos valores para poder empezar a trabajar en red. Un servidor DHCP, aparte de atender a los clientes enviándoles los parámetros, controla cuales son las direcciones IP que ha asignado y cuales están disponibles.



Un servidor DHCP envía, o puede enviar, varios parámetros de red que permitan a los clientes trabajar en red y utilizar todos los servicios disponibles. En explicaciones posteriores, centraremos las cuestiones sobre el funcionamiento DHCP en la asignación de la IP, aunque realmente se asignan más parámetros.

6.1 Tipos de asignaciones en DHCP

Ya sabemos que un cliente DHCP recibe desde un servidor los parámetros de configuración de red y entre ellos la IP. El servidor, por tanto, es quien asigna IP a los clientes DHCP. Pero, ¿cómo decide el servidor la IP que asigna a un cliente? ¿Durante cuánto tiempo asigna una IP a cada cliente? Estas cuestiones se responden en función del tipo de asignación utilizado en el servidor DHCP.

El **tipo de asignación DHCP** es el mecanismo por el cual un servidor DHCP decide la IP que tiene que entregar a un cliente y durante cuánto tiempo concede una licencia o autorización al cliente para que use esa IP.

La IP que asigna un servidor DHCP a un cliente puede ser elegida dentro de un conjunto posible de direcciones IP, o puede ser obligatoriamente una IP concreta. Cuando un cliente DHCP recibe de un servidor una IP para que la utilice, se dice que recibe una **concesión**. La concesión puede asignarse por tiempo limitado o por tiempo ilimitado. El protocolo DHCP establece la posibilidad de utilizar en los servidores DHCP tres técnicas de asignación DHCP:

- ✚ **Asignación estática o manual:** Mediante esta técnica se reserva una IP en exclusiva para un cliente. Un cliente recibe siempre la misma IP. El servidor asocia la IP con una identificación del cliente, que normalmente es la **dirección física del adaptador de red (MAC)**. Siempre que un ordenador cliente solicita al servidor una IP, enviará un identificador y este identificador permitirá al servidor concederle la IP asociada con ese identificador.

- ✚ **Asignación automática:** Mediante esta técnica el servidor DHCP asigna a cualquier cliente DHCP que lo solicite una dirección IP (dentro de todas las que tenga disponibles para conceder) **de forma permanente**. El cliente DHCP va a mantener esa dirección IP mientras no renuncie a ella, es decir, mientras no envíe un mensaje al servidor indicando esa renuncia. La asignación automática tiene como principal problema que si un equipo cliente ha recibido una IP por ese mecanismo, la IP que ha recibido no va a poder ser usada por ningún otro cliente aunque el primero estuviera apagado, incluso por mucho tiempo.

- ✚ **Asignación dinámica:** Mediante esta técnica se asigna a cada cliente DHCP una IP **durante un intervalo de tiempo limitado**. Durante ese tiempo, el servidor DHCP no va a conceder la IP asignada a ningún otro cliente. Para que un cliente pueda mantener una IP previamente concedida, debe renovar la concesión con el servidor antes de que termine el tiempo de concesión. Si termina un tiempo de concesión sin haber hecho la renovación (por ejemplo cuando un ordenador se apaga por tiempo mayor), la IP correspondiente va a poder ser entregada a otro cliente DHCP.



7 Funcionamiento de DHCP

En este apartado vamos a ver todo lo que ocurre cuando un cliente DHCP solicita que se le asigne desde un servidor una IP de forma automática.

Las conexiones DHCP se desarrollan sobre el protocolo de transporte UDP, es decir, los mensajes DHCP que se intercambian un cliente y un servidor son transportados en la red por el protocolo UDP. Un **servidor DHCP usa el puerto UDP 67** mientras que un **cliente DHCP usa el puerto UDP 68**.

Básicamente, el proceso de configuración automática de IP en un cliente DHCP se desarrolla en cuatro pasos:

- ✚ La **solicitud**: el cliente DHCP envía un mensaje de difusión a todos los equipos de la red, en el que solicita que algún servidor DHCP le envíe los parámetros de configuración de red y, fundamentalmente, una IP. En este mensaje, el cliente envía su dirección MAC para que pueda responderle cualquier servidor DHCP que reciba la solicitud.

- ✚ La **Propuesta**: cualquier servidor DHCP de la red que haya recibido la solicitud, envía un mensaje al cliente en el que propone una IP dentro de un rango de IP disponibles para asignar y una máscara. Un servidor DHCP, antes de enviar la propuesta, comprueba si la IP que va a proponer ya se está usando en la red. Para ello envía un mensaje ARP para que le responda algún ordenador que pudiera tener esa IP. Si la IP estuviera ya utilizada, el servidor buscará otra IP para asignar.
- ✚ La **aceptación**: comienza cuando un cliente DHCP ha recibido la propuesta de una IP desde un servidor. Al recibir la propuesta, el cliente comprueba si la IP está siendo usada por algún ordenador de la red, al igual que hizo el servidor. Si la IP no está siendo usada, el cliente envía un mensaje de difusión a toda la red indicando que acepta la propuesta. En el mensaje de difusión indica cual es la IP que acepta y el servidor desde el que se envió la propuesta aceptada. Si el cliente DHCP recibe a continuación otros mensajes de propuesta desde otros servidores, no responde a esos mensajes. El mensaje de aceptación de IP sirve para que todos los servidores DHCP de la red conozcan que el cliente ya ha aceptado una propuesta hecha desde un determinado servidor.
- ✚ La **Confirmación**. el servidor cuya propuesta ha sido aceptada, recibe el mensaje de aceptación y envía al cliente DHCP un mensaje de confirmación que incluye la IP que se asigna, la máscara, otros parámetros de red y otras opciones de configuración. Desde este momento, el cliente dispone de un tiempo de licencia o de concesión para usar la IP. Cuando el cliente ha utilizado la mitad del tiempo de concesión, inicia un proceso de renovación en el que solicita al servidor que le había asignado la IP que le renueve la licencia, es decir, que le conceda seguir usando la IP por el tiempo de concesión.

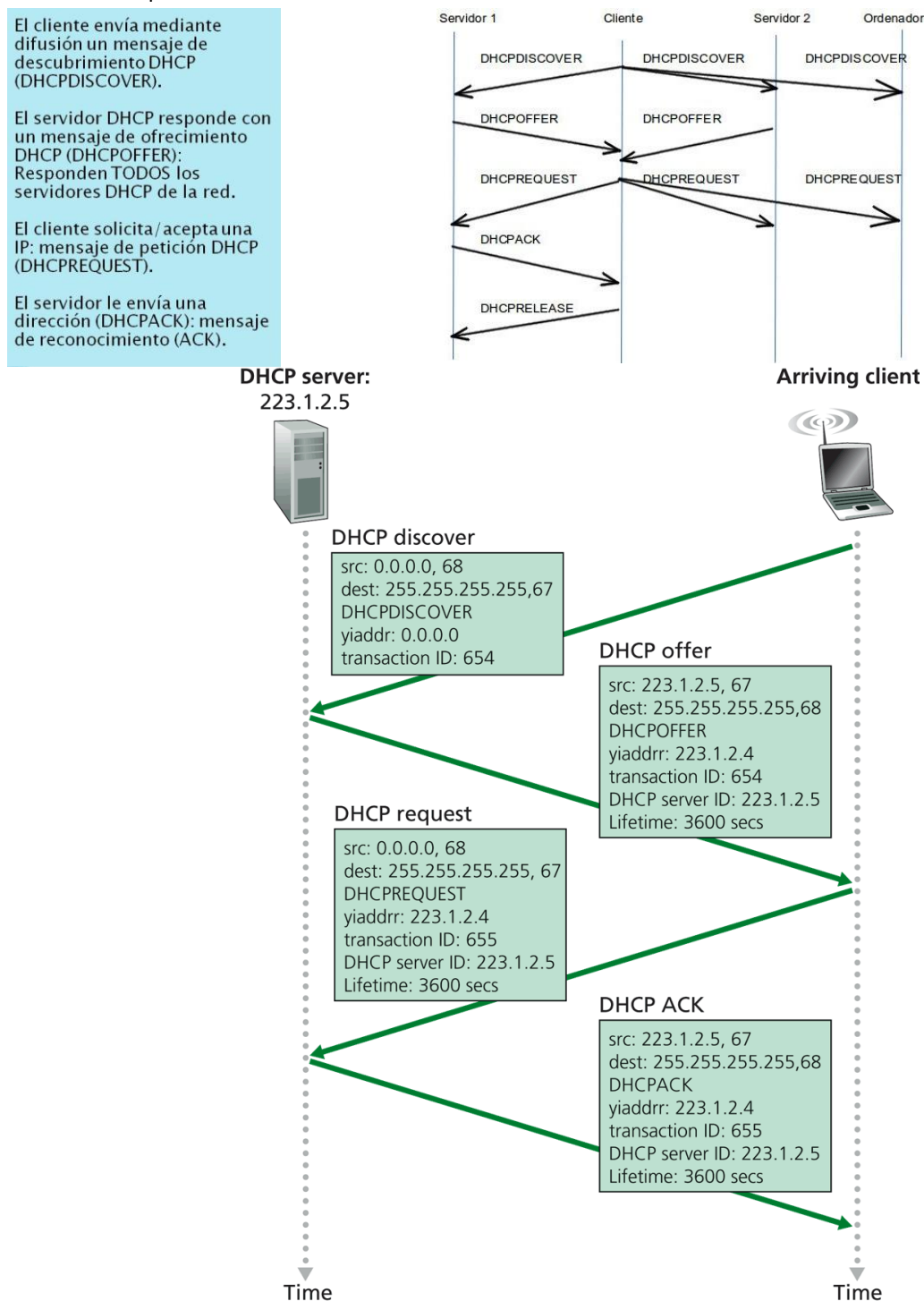
7.1 Mensajes DHCP.

El protocolo DHCP establece cuales son los mensajes que se pueden enviar entre clientes y servidores DHCP y cuál es el formato y significado de esos mensajes. Estos mensajes DHCP son:

- ✚ **DHCP_DISCOVER**: Es enviado por un cliente DHCP para solicitar que algún servidor DHCP de la red le envíe los parámetros de configuración de red. El mensaje es de broadcast o difusión por lo que llegará a todos los posibles servidores DHCP de la red.
- ✚ **DHCP_OFFER**: Es enviado por un servidor DHCP en respuesta a un mensaje DHCP_DISCOVER de un cliente. El servidor ofrece en el mensaje una concesión de una IP junto con valores para los parámetros solicitados por el cliente. Antes de enviar un DHCP_OFFER, el servidor hace una comprobación de que la IP que va a ofrecer no está siendo usada en la red. Si se usa asignación manual o, estática, en el servidor, éste asigna al cliente la IP que tiene reservada para el cliente.
- ✚ **DHCP_REQUEST**: Es un mensaje que se envía desde un cliente en respuesta a un mensaje DHCP_OFFER recibido desde un servidor o bien cada vez que el cliente tiene que renovar una concesión. Mediante este mensaje, el cliente indica al servidor que acepta la oferta hecha por el servidor y solicita que le otorgue una concesión de la IP. Antes de enviar esta respuesta, el cliente comprueba si la IP que se le ha ofrecido está siendo usada ya en la red. Este mensaje es de difusión, lo que sirve para que otros posibles servidores de la red conozcan que el cliente ya ha aceptado una oferta. Si el cliente recibe otras ofertas desde otros servidores no envía respuestas a ellas.
- ✚ **DHCP_ACKnowledge**: Es un mensaje que envía un servidor a un cliente en respuesta a un mensaje DHCP_REQUEST. En este mensaje, el servidor indica al cliente que le asigna la IP solicitada durante un tiempo de concesión establecido. En este mensaje se incluyen valores para el resto de parámetros de configuración. Cuando el cliente recibe este mensaje establece los parámetros de configuración de red con los valores entregados desde el servidor.
- ✚ **DHCP_NAK**: Es un mensaje que se podría enviar desde un servidor a un cliente en respuesta a un mensaje DHCP_REQUEST para indicarle que no puede entregarle la IP que ha solicitado en ese mensaje. No es muy normal el envío de este mensaje. Podría darse en procesos de renovación de concesiones cuando la IP que está solicitando renovar el cliente se ha reservado o está fuera del ámbito de direcciones asignables por el servidor.

- ✚ **DHCP_DECLINE:** Es un mensaje que enviará el cliente DHCP en sustitución de un mensaje DHCP_REQUEST cuando detecta que la IP que se le ha ofrecido ya está siendo usada en la red.
- ✚ **DHCP_RELEASE:** Es un mensaje que envía el cliente DHCP al servidor para indicarle que da por terminada la concesión. Este mensaje no tiene que enviarle un cliente de forma obligatoria cuando desea cancelar una concesión. Si el servidor recibe este mensaje, considera liberada la IP sobre la que el cliente tenía la concesión.
- ✚ **DHCP_INFORM:** Es un mensaje que puede enviarle el cliente DHCP al servidor para solicitarle parámetros adicionales de configuración de red (no recibidos con anterioridad o recibidos y solicitando una actualización).

En las siguientes imágenes se muestra el esquema de intercambio de mensajes DHCP en un proceso de configuración automática de parámetros de red.



7.2 Parámetros asignados por DHCP.

¿Conoces todos los parámetros de configuración de red que se pueden asignar mediante DHCP a un cliente? ¿Sabes cuáles de esos parámetros se asignan de forma obligatoria y cuáles de forma opcional?

Un cliente DHCP puede recibir de un servidor varios **parámetros** de configuración de red. Algunos de esos parámetros son asignados siempre desde el servidor por lo que se consideran **obligatorios**. El resto de parámetros deben ser solicitados por el cliente y pueden ser asignados opcionalmente por el servidor y se consideran **opcionales**.

Parámetros obligatorios:

- ✚ Dirección IP del cliente.
- ✚ Máscara de subred del cliente.
- ✚ Tiempo de concesión o duración de la licencia (lease time).
- ✚ Tiempo de renovación de la licencia (renewal time).
- ✚ Tiempo de reconexión (rebinding time).



Si un cliente agota el tiempo de concesión sin renovar dicha concesión, el servidor considera liberada la IP que ha concedido al cliente.

Un cliente DHCP realiza un proceso de renovación de una concesión para poder seguir usando una IP concedida anteriormente durante un nuevo tiempo de concesión. De forma general, los servidores DHCP asignan un tiempo de renovación igual a la mitad del tiempo de concesión. Un proceso de renovación se inicia con un mensaje DHCP-REQUEST. El tiempo de reconexión especifica que transcurrido ese tiempo sobre una concesión, si no se ha realizado una renovación, habrá que solicitar una IP mediante una nueva conexión DHCP. En esa conexión se podrá recibir la concesión de la IP anterior siempre que no se haya agotado el tiempo de concesión.

Los parámetros opcionales, se definen dentro de las opciones del protocolo DHCP en el RFC 2132. De todos ellos, algunos destacables que se le pueden entregar a los clientes son:

- ✚ Dirección IP de la puerta de enlace.
- ✚ Servidores DNS.
- ✚ Nombre de dominio DNS.
- ✚ Dirección de broadcast en la red.
- ✚ Servidores SMTP (de transferencia de correo).
- ✚ Nombre del servidor WINS.
- ✚ MTU o longitud máxima de la unidad de transferencia para el adaptador de red.
- ✚ Tiempo máximo de espera de respuesta para el protocolo ARP.

8 Como configurar el servidor DHCP.

Ahora llega lo más importante ¿Cómo configuras los servidores? A continuación verás como configurarlo en Ubuntu Server.

Como futuro técnico es conveniente que sepas, que también se puede configurar un router como servidor DHCP. Puede ser incluso que por defecto esté configurado como tal.



8.1 Instalación y administración del servicio DHCP - Linux.

ISC desarrolla de forma oficial software libre DHCP para sistemas Linux. En concreto, desarrolla tres paquetes de software:

- ✚ Software servidor DHCP.
- ✚ Software cliente DHCP.
- ✚ Software agente relay DHCP o agente de Retransmisión de DHCP.

Desde ahora tendrás en cuenta que en este curso haremos principalmente referencia a servicios instalados sobre las distribuciones Ubuntu de Linux. Lo que se indique como válido para Ubuntu, en general, lo será también para distribuciones Debian. Otras distribuciones como CentOS, Fedora, RedHat o como OpenSuse presentan sus particularidades..



Vamos a comenzar viendo un listado de paquetes que contienen la cadena dhcp en el nombre:

```
#apt-cache search -names-only dhcp
```

```
alumno-VirtualBox alumno # apt-cache search --names-only dhcp
maas-dhcp - MAAS DHCP server
neutron-dhcp-agent - Neutron is a virtual network service for Openstack - DHCP agent
strongswan-plugin-dhcp - strongSwan plugin for forwarding DHCP request to a server
isc-dhcp-client - Cliente de DHCP del ISC
isc-dhcp-client-dbg - Cliente ISC DHCP (símbolos de depuración)
isc-dhcp-common - Archivos comunes que utilizan todos los paquetes isc-dhcp*
isc-dhcp-dev - API para el acceso y la modificación del estado del servidor y el cliente de DHCP
isc-dhcp-relay-dbg - Demonio de retransmisión DHCP (símbolos de depuración)
isc-dhcp-server - Servidor ISC DHCP para asignación automática de direcciones IP
isc-dhcp-server-dbg - Servidor ISC DHCP para asignación automática de direcciones IP (depuración)
udhcp - Contiene la implementación del cliente busybox DHCP
dhcp-probe - network DHCP or BOOTP server discover
dhcpd-dbus - Dbus bindings for dhcpd
dhcpd-gtk - GTK+ frontend for dhcpd and wpa supplicant
dhcpd5 - DHCPv4, IPv6RA and DHCPv6 client with IPv4LL support
```

Antes de instalar el dhcp server, comprobaremos que no está instalado.

```
#dpkg -l "*dhcp*"
```

```
alumno-VirtualBox alumno # dpkg -l "*dhcp*"
Deseado=Desconocido/Instalar/Eliminar/Purgar/Retener
| Estado=No/Instalado/Config-files/Desempaquetado/Medio-conf/Medio-inst/espera-disparo/pendiente-disparo
|/ Err?=(ninguno)/Requiere-reinst (Estado,Err: mayúsc.=malo)
||/ Nombre Versión Arquitectura Descripción
+++-----+-----+-----+-----+
un dhcp-client <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcp3-client <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcp3-common <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcpd <ninguna> <ninguna> (no hay ninguna descripción disponible)
ii isc-dhcp-client 4.2.4-7ubuntu12 i386 ISC DHCP client
ii isc-dhcp-common 4.2.4-7ubuntu12 i386 common files used by all the isc-dhcp* packages
un udhcp <ninguna> <ninguna> (no hay ninguna descripción disponible)
```

Vemos que solo está instalado el cliente (isc-dhcp-client), por lo que procederemos a instalar el paquete dhcp server (isc-dhcp-server o dhcp3-server depende de la versión de Ubuntu que tengamos):

```
#apt-get install isc-dhcp-server
```

```
alumno@alumno-VirtualBox ~ $ sudo apt-get install isc-dhcp-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  isc-dhcp-client isc-dhcp-common
Paquetes sugeridos:
  apparmor isc-dhcp-server-ldap
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-server
Se actualizarán los siguientes paquetes:
  isc-dhcp-client isc-dhcp-common
2 actualizados, 1 se instalarán, 0 para eliminar y 760 no actualizados.
Necesito descargar 2.066 kB de archivos.
Se utilizarán 2.279 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Mostramos nuevamente la lista de paquetes instalados para comprobar que ya aparece el dhcp-server:

```
#dpkg -l "*dhcp*"
```

```
alumno@alumno-VirtualBox ~ $ dpkg -l "*dhcp*"
Deseado=Desconocido/Instalar/Eliminar/Purgar/Retener
| Estado=No/Instalado/Config-files/Desempaquetado/Medio-conf/Medio-inst/espera-disparo/pendiente-disparo
|/ Err?=(ninguno)/Requiere-reinst (Estado,Err: mayúsc.=malo)
||/ Nombre Versión Arquitectura Descripción
+++-----+-----+-----+-----+
un dhcp <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcp-client <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcp3-client <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcp3-common <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcp3-server <ninguna> <ninguna> (no hay ninguna descripción disponible)
un dhcpd <ninguna> <ninguna> (no hay ninguna descripción disponible)
ii isc-dhcp-client 4.2.4-7ubuntu12.1 i386 ISC DHCP client
ii isc-dhcp-common 4.2.4-7ubuntu12.1 i386 common files used by all the isc-dhcp* packages
ii isc-dhcp-server 4.2.4-7ubuntu12.1 i386 ISC DHCP server for automatic IP address assignment
un isc-dhcp-server-ldap <ninguna> <ninguna> (no hay ninguna descripción disponible)
un udhcp <ninguna> <ninguna> (no hay ninguna descripción disponible)
```

Podemos ver información detallada del paquete instalado:

```
#dpkg -s isc-dhcp-server
```

```
alumno@alumno-VirtualBox ~ $ dpkg -s isc-dhcp-server
Package: isc-dhcp-server
Status: install ok installed
Priority: optional
Section: net
Installed-Size: 2224
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: i386
Source: isc-dhcp
Version: 4.2.4-7ubuntu12.13
Replaces: dhcp3-server
Provides: dhcp3-server
Depends: debconf (>= 0.5) | debconf-2.0, sysv-rc (>= 2.88dsf-24) | file-
2.8.2), isc-dhcp-common (= 4.2.4-7ubuntu12.13), lsb-base, adduser
Suggests: isc-dhcp-server-ldap, apparmor
```

También podemos usar las aplicaciones gráficas de instalación/desinstalación de software para facilitarnos el proceso de instalación. Estas aplicaciones son muy fáciles de usar y nos permiten instalar la mayoría del software disponible.

8.2 Inicio y parada del servicio DHCP.

Cuando hemos instalado el servicio DHCP, como se ha descrito anteriormente, el servicio queda preparado para iniciarse siempre durante el inicio del sistema. Pero, si queremos detener o iniciar el servicio en un momento dado, ¿qué tenemos que hacer? ¿Por qué puede ser necesario detener y reiniciar el servicio?

El **estado del servicio** puede ser en **ejecución** (running) o **parado** (stopped). Se puede consultar el estado con la opción **status** de la orden service:

La gestión del estado de un servicio normalmente incluye las opciones start, stop, status, restart y reload. Estas son las más usuales, pero cada servicio puede definir las que crea oportunas. Estos son ejemplos de gestión del estado del servicio DHCP:

- ✚ Se puede **arrancar el servicio** con la opción start del comando service:
- ✚ Se puede **detener el servicio** con la opción stop de la orden service:
- ✚ Se puede **iniciar de nuevo el servicio** (recargar) con la opción reload o restart del comando service:
- ✚ Para saber las opciones posibles de un servicio se puede hacer el truco:

```
usuario@usuario-VirtualBox ~ $ sudo service isc-dhcp-server patapum
Usage: /etc/init.d/isc-dhcp-server {start|stop|restart|force-reload|status}
```

Comprobar que el servidor DHCP está en funcionamiento es un proceso muy sencillo, basta comprobar que el servicio está encendido. Esto no quiere decir, en ningún caso, que el servicio esté funcionando correctamente. Quizás el servidor está encendido pero no está correctamente configurado. De hecho, la configuración es la parte realmente importante de la administración de un servicio, y también del servicio DHCP.



Aparte de comprobar el estado del servicio (con la opción **status**), el administrador puede asegurarse de que el demonio del servicio está en ejecución buscando su PID (Process Identifier o indicador de proceso). Otra actividad a hacer es monitorizar el registro de actividades del servicio (los logs). Todo el tráfico DHCP es tráfico de red TCP/IP; por lo tanto también se puede observar el estado de los puertos y analizar el tráfico que se produce.

Todo proceso en el sistema tiene un identificador de proceso. El PID de los servicios usualmente se guardan en el sistema de archivos (en el **directorio /var/run**) en forma de archivo que contiene un valor numérico (en texto) correspondiente al PID del proceso



Con el servicio en marcha siempre se puede observar el PID del servidor con algunas de las siguientes opciones:

```
usuario@usuario-VirtualBox /var/run $ ps -A | grep dhcp
1462 ?        00:00:00 dhcpcd

usuario@usuario-VirtualBox /var/run $ service isc-dhcp-server status
isc-dhcp-server start/running, process 1462

usuario@usuario-VirtualBox /var/run $ ls -l /var/run/dhcp-server/dhcpd.pid
-rw-r--r-- 1 dhcpcd dhcpcd 5 sep 30 13:46 /var/run/dhcp-server/dhcpd.pid
usuario@usuario-VirtualBox /var/run $ cat /var/run/dhcp-server/dhcpd.pid
1462
```

Todos los servicios del sistema normalmente se monitorizan anotando en ficheros de texto un registro de todas las acciones que realizan, son los archivos conocidos como **archivos de log**. Tanto se puede utilizar un archivo genérico por el sistema como un archivo independiente para un servicio determinado. El servidor DHCP utiliza el archivo de monitorización estándar **/var/log/syslog**. En este archivo se registra cada vez que el servicio se pone en marcha y se detiene, entre otras cosas.

#cat /var/log/syslog | grep dhcp

```
Sep 30 14:03:24 usuario-VirtualBox dhcpd: DHCPDISCOVER from 08:00:27:fb:81:96 via eth0
Sep 30 14:03:24 usuario-VirtualBox dhcpd: ICMP Echo reply while lease 172.16.0.100 valid.
Sep 30 14:03:24 usuario-VirtualBox dhcpd: Abandoning IP address 172.16.0.100: pinged before offer
Sep 30 14:03:42 usuario-VirtualBox dhcpd: DHCPDISCOVER from 08:00:27:fb:81:96 via eth0
Sep 30 14:03:43 usuario-VirtualBox dhcpd: ns1.example.org: temporary name server failure
Sep 30 14:03:43 usuario-VirtualBox dhcpd: ns2.example.org: temporary name server failure
Sep 30 14:03:43 usuario-VirtualBox dhcpd: DHCPOFFER on 172.16.0.101 to 08:00:27:fb:81:96 (usuario-VirtualBox) via eth0
Sep 30 14:03:43 usuario-VirtualBox dhcpd: DHCPREQUEST for 172.16.0.101 (172.16.0.100) from 08:00:27:fb:81:96 (usuario-VirtualBox) via eth0
Sep 30 14:03:43 usuario-VirtualBox dhcpd: DHCPACK on 172.16.0.101 to 08:00:27:fb:81:96 (usuario-VirtualBox) via eth0
Sep 30 14:05:51 usuario-VirtualBox dhcpd: receive_packet failed on eth0: Network is down
```

El servicio DHCP guarda la información de **registro de las concesiones** que efectúa, en un fichero de **leases**. Esto le permite seguir la pista de las direcciones IP que ha concedido y mantener la consistencia entre varios arranques del mismo servidor. Se puede observar este archivo en **/var/lib/dhcp/dhcpd.leases**:

```
usuario@usuario-VirtualBox ~ $ cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.2.4

lease 172.16.0.100 {
    starts 3 2015/09/30 11:49:38;
    ends 3 2015/09/30 11:59:38;
    tstp 3 2015/09/30 11:59:38;
    cltt 3 2015/09/30 11:49:38;
    binding state free;
    hardware ethernet 08:00:27:fb:81:96;
}
server-uid "\000\001\000\001\035\236\210\010\000\373\201\226";

lease 172.16.0.100 {
    starts 3 2015/09/30 12:03:24;
    ends 3 2015/09/30 12:03:24;
    cltt 3 2015/09/30 12:03:24;
    binding state abandoned;
    next binding state free;
    rewind binding state free;
    client-hostname "usuario-VirtualBox";
}
```

Las tareas principales para configurar un servidor DHCP son las siguientes:

- ✚ Instalar el software del servidor DHCP.
- ✚ Activar / desactivar el servicio DHCP.
- ✚ Observar / hacer la lista de la configuración actual del servidor DHCP.
- ✚ Modificar la configuración del servidor DHCP.
- ✚ Monitorizar los *logs* del servicio DHCP y los archivos de registro de las concesiones (*leases*).

8.3 Archivos relacionados con la configuración y administración de DHCP

Tras haber instalado en Linux el servidor DHCP, en el sistema de archivos se han creado varios **archivos relacionados con la administración y configuración del servicio**. Es necesario que conozcas donde se encuentran esos archivos, cual es su nombre, que función tienen y como se pueden modificar o interpretar. En este apartado vamos a ver la información relativa al sistema Linux Ubuntu.

Los archivos y directorios más importantes relacionados con el servicio DHCP en Ubuntu son:

- ✚ **Directorio /etc/dhcp:** Contiene archivos de configuración relacionados con el servicio DHCP. El principal de los archivos es **dhcpd.conf**.
- ✚ **Archivo /etc/dhcp/dhcpd.conf** es el archivo de configuración del servidor. En el siguiente apartado describiremos cual es la sintaxis de este archivo.
- ✚ **Archivo /etc/dhcp/dhclient.conf** es un archivo de configuración del cliente DHCP. Se encuentra en cualquier ordenador con Ubuntu que tenga el cliente DHCP instalado. Su contenido indica cómo se comporta el cliente cuando solicita el servicio DHCP. Por ejemplo, en el archivo se indican cuales son los parámetros de red que solicita el cliente a los servidores DHCP.

- ✚ **Archivo `/etc/default/isc-dhcp-server`** establece los interfaces de red por los que el servidor DHCP atiende o escucha a los clientes.
- ✚ **Archivo `/var/lib/dhcp/dhcpd.leases`** contiene información actualizada sobre las concesiones que ha otorgado el servidor a los clientes. Dentro de este archivo hay una entrada por cada concesión que se ha dado y en la que se indica la IP que se ha concedido al cliente, la dirección física del cliente, cuanto tiempo de concesión se ha utilizado, etc.
- ✚ **Archivo `/usr/sbin/dhcpd`** es el archivo ejecutable correspondiente al servicio. Es un demonio que se encarga de escuchar las solicitudes de los clientes DHCP y controlar la entrega correcta de parámetros de red a los clientes.
- ✚ **Archivo `/var/log/syslog`** es un archivo de texto donde se registran los inicios y paradas de los servicios (registro de logs de servicios). Cuando se produzcan fallos al iniciar y detener el servicio DHCP debemos consultar la información que nos da este archivo sobre el fallo producido para intentar solucionarlo.

8.4 El archivo de configuración del servicio DHCP.

Cuando se inicia el servidor DHCP en Linux, se ejecuta el demonio correspondiente al servicio cuyo nombre es `dhcpd`. El archivo **`dhcpd.conf`** es un archivo de texto que es leído y establece la configuración correspondiente al servidor DHCP.

Siempre que hagamos modificaciones en este archivo, debemos reiniciar el servicio DHCP para que trabaje con la nueva configuración.



Si se producen fallos al iniciar el servicio DHCP, se guarda información sobre el fallo en el archivo registro de logs de servicio. En ese archivo se indica el tipo de fallo y la parte del archivo de configuración que ha producido el fallo.

El archivo consta de una secuencia de **sentencias** o directivas de dos tipos:

- ✚ **Parámetros.**
- ✚ **Declaraciones.**

Los **parámetros** permiten establecer una opción de configuración del servicio. En los parámetros se puede asignar un valor o un conjunto de valores, que determinan una condición de funcionamiento del servidor o el valor de parámetro que se entrega a los clientes. Se usan principalmente dos sintaxis para asignar valores a los parámetros:

- ✚ `Nombre_parámetro;`
- ✚ `Nombre de parámetro valores;`

La primera sintaxis significa que está activado el parámetro. La segunda sintaxis permite asignar uno o varios valores a los parámetros. **Si se asignan varios valores, estos se separan con espacios.**

Dentro de las declaraciones se pueden incluir parámetros e incluso otras declaraciones. Las declaraciones tienen la sintaxis





```
Declaración {
    [parámetros]
    [declaraciones]
}
```

8.4.1 Declaraciones

Vamos a ver los **tipos de declaraciones** que se pueden establecer en el archivo de configuración **`dhcpd.conf`** del servidor DHCP en los sistemas Linux y que nos van a permitir declarar la red en la que trabaja el servidor y el conjunto de direcciones IP que concede el servidor en la red.

Las declaraciones que podemos utilizar son:

- ✚ **Subnet.** `subnet subnet-number netmask netmask {[parameters] [Declarations]}`
Permite definir opciones para una subred concreta. Es la sentencia más usual en las definiciones de configuración del servidor DHCP.
Dentro de esa declaración es obligatorio especificar al menos un conjunto de direcciones que otorga el servidor en la red. A este conjunto de direcciones se le denomina rango.

-  **Host.** host hostname {[parameters] [Declarations]}
- Proporciona un ámbito de definición para un equipo concreto. Las opciones que se definen dentro de una sentencia host afectan únicamente al equipo indicado. Se requiere una sentencia host para poder hacer asignaciones dinámicas fijas (asignar siempre la misma IP basándose en la MAC).
-  **Shared-network:** shared-network name {[parameters] [Declarations] }
- Permite agrupar varias subredes (subnet) en una misma declaración.
Se utiliza cuando una misma red física se compone de varias subredes lógicas.
-  **Group.** group {[parameters] [Declarations]}
- Se utiliza para agrupar declaraciones de manera que las opciones definidas afecten al grupo de elementos que contiene. Estos pueden ser shared-networks, Subnet, hosts y hasta otros grupos.
-  **Range:** range [dynamic-bootp] low-address [high-address];
- Indica el intervalo de direcciones dinámicas disponibles para asignar. El servidor DHCP extrae las direcciones dinámicas de este intervalo de direcciones.

Ejemplo de sintaxis:

```
subnet IP_red netmask mascara_de_red {  
    range IP_menor IP_mayor;  
    [parámetros]  
}
```

Es adecuado hacer reservas para ordenadores de la red que vayan a ser servidores dentro de la red. En una declaración host se da un nombre a la declaración que corresponderá al nombre del equipo para el que se hace la reserva y se indica la dirección física o MAC del equipo y la IP que se le va a asignar. La sintaxis de esta declaración es:

```
host nombre {  
    [parámetros]  
    hardware ethertnet direccion_MAC;  
    fixed-address dirección_IP;  
}
```

Las declaraciones **shared-network** y **group** permiten simplificar el archivo de configuración agrupando en una declaración varias declaraciones. Los parámetros que se asignen dentro de una declaración shared-network o group funcionarán como parámetros globales para todas las declaraciones que se hagan dentro.

La declaración **shared-network** nos permite describir una red que está dividida en varias subredes. Por tanto, dentro de una declaración shared-network tendremos varias declaraciones subnet. El uso de shared-network es problemático ya que no asegura que unos equipos reciban o no IP dentro de una subred concreta. Los parámetros que se establezcan dentro de la declaración shared-network configurarán todas las subredes de la shared network. La sintaxis es:

```
shared-network nombre {  
    [parámetros y declaraciones]  
    Declaración subnet de primera subred  
    [otras declaraciones subnet]  
}
```



La declaración **group** permite incluir varias declaraciones host y se usa para aplicar los mismos parámetros a todas las declaraciones que se realicen dentro de ella. Se pueden usar varias declaraciones group en el archivo de configuración. La sintaxis de una declaración group es:

```
group nombre {  
    [parámetros y declaraciones host]  
}
```

8.4.2 Parámetros

Al iniciar la unidad hablábamos de que un servidor de asignación automática de parámetros de configuración red asignaba IP a los clientes y otros muchos parámetros como puerta de enlace, nombre del dominio DNS, servidores DNS etc. Ahora aprenderemos a establecer en los sistemas Linux los parámetros de red que se entregarán a los clientes así como opciones de configuración del funcionamiento del servidor DHCP.

Recordemos que en el archivo **dhcpd.conf** hay dos tipos de sentencias o directivas: parámetros y declaraciones. Los parámetros permiten establecer los “parámetros” de red que asigna el servidor DHCP a los clientes y opciones de funcionamiento del servicio. Un mismo parámetro se puede declarar en varias partes del archivo de configuración, pudiéndole asignar distintos valores. Dependiendo de donde se declara un parámetro podemos hablar de:

-  **Parámetros Globales:** Se declaran fuera de las sentencias de declaración y afectan a todos los clientes del servicio.
-  **Parámetros Locales:** Se declaran dentro de una sentencia de declaración y afectan sólo a los clientes definidos en esa declaración. Si a un parámetro local se le ha asignado un valor de forma global, en el ámbito local prevalece el valor asignado de forma local.

Todos los parámetros que se declaren con **option** son parámetros que el servidor puede entregar a los clientes. En la siguiente tabla se describe la sintaxis de los principales parámetros que podemos encontrar en un archivo de configuración. En la sintaxis, se representan en cursiva, los valores que se asignan a cada parámetro.

Sintaxis.	Descripción.
authoritative;	Implica que el servidor es autoritativo en la red. El servidor reasignará IP a los clientes que detecte mal configurados. La sentencia opuesta a ésta es " not authoritative ".
default-lease-time <i>segundos;</i>	Tiempo de concesión que se otorgará a los clientes por defecto, es decir, cuando éstos no hayan solicitado otro.
max-lease-time <i>segundos;</i>	El máximo tiempo de concesión que se puede otorgar a los clientes.
min-lease-time <i>segundos;</i>	El mínimo tiempo de concesión que se puede otorgar a los clientes.
range <i>ip_menor ip_mayor;</i>	Un rango o conjunto de IP que otorgará el servidor a los clientes. Dará IP comprendidas entre la IP menor y la IP mayor, ambas incluidas. Este parámetro debe estar incluido dentro de una declaración subnet .
hardware <i>tipo dirección_física;</i>	Permite indicar cuál es la dirección física de un cliente DHCP. En tipo se indica el tipo de adaptador de red del cliente (normalmente ethernet).
fixed-address <i>IP;</i>	Permite indicar cuál es la IP que se reserva para un cliente concreto. Este parámetro se debe incluir en una declaración host y está asociado al parámetro fixed-address .
option subnet-mask <i>máscara</i>	Indica la máscara de red que usarán los clientes.
option broadcast-address <i>dirección;</i>	Indica cual es la dirección IP de broadcast que usarán los clientes.
option routers <i>IP;</i>	Indica cual es la dirección IP de la puerta de enlace que se entregará a los clientes.
option domain-name <i>"nom_dominio";</i>	Indica cual es el nombre de dominio que usará el cliente como dominio de pertenencia.
option domain-name-servers <i>servidores;</i>	Indica cuales son los servidores DNS que deben usar los clientes. Generalmente se indican las IP de éstos y se separan con coma.

Ejemplo de configuración del DHCP básica:

```
# Opciones globales del servidor DHCP (usuales)
ddns-update-style none;

# Definición de la red a la que se ofrece el servicio DHCP
subnet 192.168.0.0 netmask 255.255.255.0 {
    # Opciones genéricas para todos los equipos de la red
```

```
option routers 192.168.0.1;
option subnet-mask 255.255.255.0;
option domain-name "iessidon.org";
option domain-name-servers 192.168.1.1;
# Definición del intervalo de IPs dinámicas a usar
# Y los tiempos de las concesiones
range 192.168.0.128 192.168.0.254;
default-lease-time 21600;
max-lease-time 43200;

# Opciones de equipos individuales
# El servidor imp obtiene siempre una dirección fija basada en MAC
host imp {
    hardware ethernet 12: 34: 56: 78: AB: CD;
    fixed-address 207.175.42.254;
}
}
```

Ejemplo de configuración del DHCP avanzada

```
ddns-update-style interim;

subnet 192.168.1.0 netmask 255.255.255.0 {
    #---default gateway

    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    option nis-domain "domain.org";
    option domain-name "domain.org";
    option domain-name-servers 192.168.1.1;
    default-lease-time 21600;
    max-lease-time 43200;

    # We want the nameserver to appear at a fixed address
    host ns {
        hardware ethernet 12: 34: 56: 78: AB: CD;
        fixed-address 207.175.42.254;
        default-lease-time 43200;
        max-lease-time 86400;
    }
}
```

Ejemplo de configuración del DHCP avanzada II

```
subnet 10.0.0.0 netmask 255.255.255.0 {
    option routers 10.0.0.254;

    group {
        filename "osProfesores";
        next-server ncd-booter;
        host ncd2 {hardware ethernet 0:c0:c3:88:2d:81; }
        host ncd3 {hardware ethernet 0:c0:c3:00:14:11; }
    }
    # Unknown clientes get this pool.
    pool {
        option domain-name-servers sidon.com;
        max-lease-time 300;
    }
}
```

```
        range 10.0.0.200 10.0.0.253;
        allow unknown-clientes;
    }

    # Known clientes get this pool.
    pool {
        option domain-name-servers ns1.example.com, ns2.example.com;
        max-lease-time 28800;
        range 10.0.0.5 10.0.0.199;
        deny unknown-clientes;
    }
}
```