

Investigación DHCP

Definición:

El **Protocolo de configuración dinámica de host (DHCP)** es un protocolo de administración de red utilizado en redes de **Protocolo de Internet (IP)** para asignar automáticamente direcciones IP y otros parámetros de comunicación a dispositivos conectados a la red. Funciona bajo una arquitectura cliente-servidor: el servidor DHCP proporciona la configuración y los clientes DHCP (como computadoras, teléfonos, impresoras, etc.) la reciben automáticamente al unirse a la red.

Surgimiento:

La **historia del Protocolo de Configuración Dinámica de Host (DHCP)** comienza con la necesidad de simplificar la asignación de direcciones IP en las redes. En sus inicios, cuando una computadora se conectaba a una red, era necesario asignarle manualmente una dirección IP, junto con otros parámetros como la máscara de subred o la puerta de enlace. Este proceso, además de ser lento y propenso a errores, se volvía difícil de administrar a medida que las redes crecían. Para resolver este problema, en 1985 se desarrolló un protocolo llamado **BOOTP (Bootstrap Protocol)**. BOOTP permitía que ciertos dispositivos, especialmente aquellos sin disco rígido, pudieran obtener automáticamente su configuración de red al encenderse. Si bien representó un gran avance en su momento, BOOTP tenía limitaciones importantes, como la incapacidad de liberar o renovar direcciones IP de forma dinámica. Toda la configuración debía hacerse manualmente en el servidor, lo cual seguía siendo poco práctico en redes con muchos dispositivos.

Para superar estas limitaciones, en 1993 **se introdujo DHCP como una evolución de BOOTP**. El protocolo fue estandarizado inicialmente en el [RFC 1531](#) y más adelante, en 1997, fue actualizado en el [RFC 2131](#), que sigue siendo uno de los documentos principales en la actualidad. La principal ventaja que trajo la **primera versión** de 1993 fue la asignación automática de IPs y sus arrendamientos. La **segunda versión** de 1997 introdujo el modelo DORA, soporte para arrendamientos renovables, y mayor compatibilidad con redes grandes y entornos más complejos. Esta versión es la que aún se utiliza como base estándar.

En la actualidad, DHCP es un componente esencial en prácticamente todas las redes IP, desde las domésticas hasta las empresariales, pasando por redes móviles, ya que permite una gestión más eficiente, rápida y segura de los dispositivos que se conectan a una red.

Usos cómo protocolo:

El protocolo DHCP se utiliza principalmente porque **hace que la administración de redes sea mucho más simple y eficiente**. Sin DHCP, cada dispositivo que se conecta a una red tendría que configurarse manualmente, lo que llevaría mucho tiempo y aumentaría las posibilidades de cometer errores, como asignar dos veces la misma dirección IP a distintos dispositivos. Con DHCP, esa configuración se realiza automáticamente, lo que evita estos errores, reduce los conflictos de direcciones duplicadas y ayuda a usar mejor el rango de direcciones IP disponible. Además, DHCP es fundamental para dispositivos móviles como notebooks, celulares o tablets, ya que les permite conectarse a distintas redes (por ejemplo, de casa, del trabajo o de una cafetería) sin necesidad de que el usuario tenga que ingresar datos técnicos cada vez. Todo se configura automáticamente, de forma rápida y sin complicaciones.

Funcionamiento:

Proceso DORA:

El funcionamiento del protocolo DHCP **se basa en un proceso de cuatro pasos conocido como DORA**, que incluye las fases Discover, Offer, Request y Acknowledge. Todo comienza cuando un dispositivo se conecta a una red y no tiene dirección IP. Entonces envía un mensaje de descubrimiento (Discover) en modo broadcast, buscando un servidor DHCP. Cuando uno o más servidores reciben este mensaje, responden con una oferta (Offer), que incluye una dirección IP disponible y otros datos de configuración como la máscara de subred, la puerta de enlace y los servidores DNS. El dispositivo selecciona una de las ofertas recibidas y responde al servidor con un mensaje de solicitud (Request), confirmando que desea usar la IP ofrecida. Finalmente, el servidor responde con un mensaje de confirmación (Acknowledge), que autoriza al dispositivo a usar esa dirección IP durante un tiempo determinado llamado “arrendamiento”.

Rechazo de Solicitud:

Si el servidor no puede cumplir con la solicitud, envía un mensaje de negación (DHCPNAK). Esto puede suceder, por ejemplo, si la dirección IP solicitada ya ha sido asignada a otro dispositivo. Al recibir este mensaje, el cliente debe reiniciar el proceso desde la fase de descubrimiento para obtener una nueva dirección IP.

Arrendamiento (Lease):

Una vez que se le ha asignado una IP, el dispositivo puede comunicarse normalmente en la red. Sin embargo, la dirección IP tiene un tiempo de arrendamiento limitado (*lease*, en inglés). Esta información es almacenada localmente por el dispositivo, ya sea en memoria o en un archivo del sistema, y se activa un temporizador con la duración indicada por el servidor.

El tiempo de arrendamiento varía según la red y la configuración del servidor DHCP, para redes domésticas suele ser de 24 horas pero en redes empresariales o públicas varía más, entre 1 hora, 7 días o incluso menos de 10 minutos.

Proceso de Renovación:

Para evitar perder la conexión, el cliente intenta renovar la IP antes de que expire el arrendamiento. Este proceso de renovación sigue tres pasos clave definidos por el protocolo:

El primer paso para renovar la dirección IP es a la mitad del tiempo del arrendamiento. El cliente envía un mensaje DHCPREQUEST en modo *unicast* directamente al servidor que le asignó la IP. Si el servidor responde con un DHCPACK, el lease se renueva y el temporizador se reinicia.

Si el servidor no respondió en el paso anterior, el cliente envía un nuevo DHCPREQUEST, esta vez en *broadcast*, con la intención de contactar a cualquier servidor DHCP disponible que pueda renovar el lease.

En caso de no obtener respuesta, el cliente espera a que su tiempo de arrendamiento finalice, entonces pierde su dirección IP y debe reiniciar el proceso DORA desde el principio.

Componentes:

Los componentes principales del sistema DHCP son cuatro:

- ➔ En primer lugar está el **servidor DHCP**, que es el encargado de asignar direcciones IP y otros datos de configuración de red a los dispositivos que se conectan.
- ➔ Luego están los **clientes DHCP**, que pueden ser cualquier dispositivo que se conecte a la red, como computadoras, celulares, tablets o impresoras.
- ➔ También existen los **agentes de retransmisión (relay agents)**, que se usan cuando el servidor DHCP no está en la misma subred que el cliente. Estos agentes se encargan de reenviar los mensajes DHCP entre distintas redes para que la comunicación sea posible.
- ➔ Por último, el sistema cuenta con una **base de datos de arrendamientos**, donde el servidor guarda un registro de qué direcciones IP fueron asignadas, a qué dispositivos y por cuánto tiempo. Esta base de datos permite que el servidor mantenga un control ordenado sobre las direcciones disponibles y evite conflictos en la red.

Instalación:

La instalación de un servidor DHCP varía según el tipo de sistema en el que se utilice. En computadoras con Linux, por ejemplo, se puede instalar fácilmente desde la **terminal**. En sistemas basados en Debian (como Ubuntu), se usa el comando **sudo apt install isc-dhcp-server**, mientras que en sistemas basados en RedHat (como CentOS o Fedora), se utiliza **sudo yum install dhcp**.

En Windows Server, el servicio DHCP se agrega como un "**rol**" desde el **Administrador del Servidor**, una herramienta gráfica que permite instalar y configurar funciones del sistema.

En el caso de los routers domésticos, el servidor DHCP suele venir activado por defecto y se puede configurar desde la interfaz web del router, accediendo a través de un navegador.

Independientemente del sistema, siempre es necesario definir un **rango de direcciones IP** que se pueden asignar a los dispositivos, así como otros parámetros esenciales de red como los **servidores DNS** y la **puerta de enlace predeterminada** (gateway).

Ventajas y desventajas:

Una de las **principales ventajas** de usar DHCP es que automatiza la configuración de red, lo que evita tener que ingresar manualmente la dirección IP y otros datos en cada dispositivo. Esto ahorra mucho tiempo, especialmente en redes grandes con muchos equipos. Además, reduce los errores humanos, como asignar la misma IP a dos dispositivos, y permite utilizar mejor el rango de direcciones IP disponible, ya que las IP se asignan de forma dinámica según la necesidad. También es útil en dispositivos móviles, ya que permite moverse de una red a otra sin tener que cambiar configuraciones.

Sin embargo, DHCP **también tiene algunas desventajas**. Por ejemplo, los dispositivos dependen del servidor DHCP para obtener su dirección IP. Si el servidor no funciona, los dispositivos nuevos no podrán conectarse a la red. También existe el riesgo de que aparezcan servidores DHCP falsos o maliciosos, lo que puede comprometer la seguridad. Otro punto en contra es que el cliente no tiene control sobre la IP que recibe, lo que puede ser un problema en ciertos escenarios donde se necesita una dirección fija. Y finalmente, si la red está mal configurada, pueden surgir errores como asignaciones incorrectas o fallas de comunicación.

Tipos de DHCP:

1. DHCP dinámico: Es el tipo más común. El servidor DHCP asigna automáticamente una dirección IP al cliente por un tiempo determinado (arrendamiento o *lease*). Una vez que vence ese tiempo, el cliente debe renovarla. Si el cliente se desconecta, la IP vuelve a quedar disponible para otro dispositivo. Este tipo es muy usado en redes domésticas y empresariales porque es automático, flexible y no requiere configuración manual.

2. DHCP automático (automatic allocation): En este modo, el servidor asigna una dirección IP al cliente de forma permanente, pero sin intervención del administrador. La diferencia con el dinámico es que, aunque el cliente se desconecte, el servidor recordará su dirección y se la volverá a asignar cuando se reconecte. Es útil cuando se quiere que los dispositivos mantengan siempre la misma IP, pero sin configurar todo manualmente.

3. DHCP manual (asignación fija o estática): Aquí, el administrador de red asocia manualmente una dirección IP específica a un dispositivo, identificándose por su dirección MAC. El servidor DHCP se encarga de asignar siempre esa misma IP a ese equipo. Es común en impresoras, servidores o dispositivos que necesitan una IP fija, pero se quiere seguir usando DHCP para centralizar la gestión.

4. DHCP Relay (agente de retransmisión): Este no es un tipo de asignación, sino una forma de permitir que clientes DHCP en una subred se comuniquen con un servidor DHCP que está en otra subred. El **relay agent** recibe las solicitudes del cliente y las reenvía al servidor, y luego devuelve la respuesta. Esto permite tener un solo servidor DHCP para toda la red, incluso si está dividida en varias subredes.

Documentación técnica:

Droms, R. (1997). *RFC 2131: Dynamic Host Configuration Protocol*. Internet Engineering Task Force (IETF).

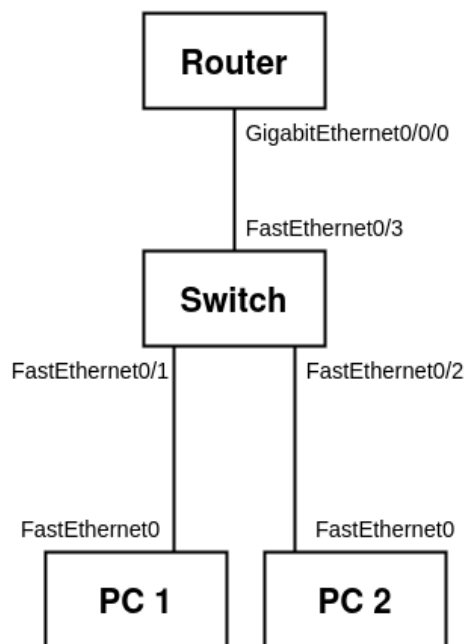
<https://datatracker.ietf.org/doc/html/rfc2131>

Documentación Packet Tracer

Objetivos:

- Asignar una dirección IP a una interfaz.
- Habilitar la interfaz.
- Configurar un pool de direcciones IP dinámicas mediante DHCP.
- Configurar las PCs para que obtengan IP automáticamente.

Implementación:



Primero **instalamos packet tracer** en nuestro pendrive booteable con Linux y una vez instalado, **armamos la red**: con 1 router, 1 switch y 2 PCs.

Luego, **conectamos los dispositivos**. Para realizar las conexiones de la red, utilizamos **cables de cobre**, que son los más comunes en este tipo de configuraciones (representados por líneas negras continuas). El router se conectó al switch mediante el puerto GigabitEthernet0/0/0 del router hacia el puerto FastEthernet0/3 del switch. Luego, conectamos las PCs al switch utilizando los puertos FastEthernet0/1 y FastEthernet0/2 del switch, que van respectivamente a los puertos FastEthernet0 de cada computadora.

Una vez conectados, **configuramos el router entrando a la interfaz CLI** (IOS command line interface). Con este código se configura un router Cisco para que funcione como servidor DHCP en una red local. Primero se le asigna una dirección IP a la interfaz del router y se la habilita para que pueda comunicarse con otros dispositivos. Luego se establece un rango de direcciones IP que serán asignadas automáticamente a las PCs mediante el protocolo DHCP. También se configura la puerta de enlace predeterminada y un servidor DNS. Finalmente, en cada PC se selecciona la opción de obtener IP por DHCP para que reciban la configuración de red automáticamente y puedan conectarse al router y entre ellas.

Código implementado:

Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.	Entramos a la configuración global del router para modificar sus ajustes
Router(config)#interface gigabitethernet0/0/0 Router(config-if)#ip address 192.168.10.1 255.255.255.0	Entramos a configurar una interfaz específica (<i>gigabitethernet0/0/0</i>). Le asignamos la IP <i>192.168.10.1</i> con máscara <i>255.255.255.0</i> cuyo rango es de <i>192.168.10.1</i> a <i>192.168.10.254</i> .
Router(config-if)#no shutdown	El comando no shutdown activa la interfaz.
Router(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up exit	El sistema nos indica que se activó la interfaz que acabamos de configurar. Y volvemos a la configuración global del router.
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10	Reservamos el rango de IPs del <i>192.168.10.1</i> al <i>192.168.10.10</i> , para que el DHCP no las asigne automáticamente . Sin esto, el DHCP podría asignar estas IPs a una PC, y se generaría un conflicto de direcciones IP .
Router(config)#ip dhcp pool LAN Router(dhcp-config)#network 192.168.10.0 255.255.255.0 Router(dhcp-config)#default-router 192.168.10.1	Creamos un grupo de configuración DHCP llamado “ LAN ”, y el router va a usar esto para entregar IPs automáticamente a las PCs.
Router(dhcp-config)#dns-server 8.8.8.8	El router les dice a las PCs que usen el DNS de Google (<i>8.8.8.8</i>) para resolver nombres de dominio.
Router(dhcp-config)#exit Router(config)#end	Salimos de la configuración del router.

Finalmente en cada PC, ingresas a la pestaña **Desktop**, luego a **IP Configuration**, y ahí seleccionas la opción **DHCP**. Al hacer esto, la PC le solicita automáticamente al router una dirección IP y otros datos de red (como la máscara de subred, la puerta de enlace y el DNS). Si el router está correctamente configurado como servidor DHCP, la PC recibirá toda esta información sin necesidad de ingresarla manualmente, quedando conectada a la red automáticamente.

Bibliografía

<https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>

https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

<https://www.portnox.com/cybersecurity-101/dhcp-protocol/>

<https://www.techtarget.com/searchnetworking/definition/DHCP>