Qué es y para qué sirve este protocolo

El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como «**Dynamic Host Configuration Protocol**«, es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados. Este protocolo se encarga de asignar de manera dinámica y automática una dirección IP, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión.

Cuando tenemos un servidor DHCP en funcionamiento, todas las direcciones IP que ha proporcionado a diferentes clientes se guardan en un listado donde se relaciona la IP que se le ha proporcionado (dirección lógica) y la dirección MAC (dirección física de la tarjeta de red). Gracias a este listado, el servidor DHCP se asegura de no proporcionar a dos equipos diferentes la misma dirección IP, lo que ocasiona un caos en la red local. A medida que el servidor va asignando direcciones IP, también tiene en cuenta cuándo pasa un determinado tiempo y caducan, quedando libres para que otro cliente pueda obtener esta misma dirección IP. El servidor DHCP sabrá en todo momento quién ha estado en posesión de una dirección IP, cuánto tiempo ha estado, y cuándo se ha asignado a otro cliente.

El protocolo DHCP incluye varias formas de asignación de direcciones IP, dependiendo de la configuración que realicemos y el escenario, podremos usar una forma de asignación u otra:

- **Manual o estática**: el servidor DHCP nos permitirá configurar un listado de parejas IP-MAC con el objetivo de que siempre se le proporcione a un cliente una determinada dirección IP, y que esta dirección no cambie nunca.
- **Automática**: el servidor DHCP se encarga de proporcionar una dirección IP al cliente que realiza la solicitud, y estará disponible para este cliente hasta que la libere. Existen routers que internamente están configurados para proporcionar direcciones IP

privadas de forma secuencial, sin embargo, hay firmwares que están diseñados para proporcionar una dirección IP específica dentro del rango y que no es secuencial, en base a un algoritmo interno y la dirección MAC que se haya conectado.

- **Dinámica**: este método permite reutilización dinámica de las direcciones IP.

Aunque el protocolo DHCP es muy conocido por proporcionar la dirección IP, máscara de subred y la puerta de enlace, tres parámetros básicos y fundamentales, también es capaz de proporcionar otra información de cara a los clientes, como los siguientes parámetros que son configurables y opcionales:

- Servidor DNS primario y secundario.
- Nombre DNS.
- MTU para la interfaz.
- Servidor y dominio NIS.
- Servidores NTP.
- Servidor de nombre WINS para Windows.
- Otras opciones avanzadas.

Un aspecto muy importante es que, si un sistema Windows no es capaz de obtener una dirección IP a través del cliente DHCP en una red, se inicia un proceso llamado APIPA (Automatic Private Internet Protocol Addressing). Este proceso APIPA que usan los sistemas operativos cuando no se puede obtener una dirección IP por DHCP, este protocolo se encarga de asignar una dirección IP privada de clase B en el rango 169.254.0.0/16 con su correspondiente máscara de subred 255.255.0.0. Este bloque de direccionamiento se conoce como «link-local» para redes IPv4. Aunque los sistemas operativos se autoconfigure esta dirección IP privada, cada 5 minutos volverán a consultar si hay un servidor DHCP en la red para que les proporcione una dirección IP privada de clase A, B o C habitual. Cuando no funciona el servidor DHCP o no lo tenemos configurado, podéis comprobar la dirección IP que se configura automáticamente si consultamos la IP privada que tenemos en nuestro equipo.

Una vez que ya conocemos qué es el protocolo DHCP y sus principales características, vamos a ver su funcionamiento y qué mensajes se intercambian.

Funcionamiento y mensajes de intercambio

La comunicación entre el servidor DHCP y los clientes DHCP que tengamos conectados en la red se realiza a través del protocolo UDP, un protocolo que ya conocemos de otros artículos y que es un protocolo no orientado a conexión. En el caso del servidor DHCP usamos el protocolo UDP puerto 67, en el caso de los clientes usamos el protocolo UDP en el puerto 68. Si tenemos un firewall bloqueando estos puertos, ya sea en el servidor o en el cliente, deberemos revisarlo y añadir una regla de aceptar para origen y/o destino estos puertos, de lo contrario el servicio no funcionará, y no podremos obtener las direcciones IP automáticamente.

Cuando conectamos un equipo por primera vez a la red no tiene direccionamiento IP, por tanto, deberemos «buscar» el servidor DHCP por toda la red, ya que tampoco tenemos información sobre el protocolo ARP en un primer momento. Por este motivo, lo primero que hará el cliente es enviar un **DHCP DISCOVERY** con dirección IP de origen 0.0.0.0 y dirección IP de destino 255.255.255.255 que es la IP de broadcast global. Por supuesto, se envía un datagrama UDP, con puerto de origen el 68 (cliente) y puerto de destino el 67 (servidor). Esta comunicación es de tipo broadcast en la red, e internamente se puede configurar para recibir el OFFER por broadcast o unicast, aunque generalmente es de tipo unicast en el OFFER.

Si existe un servidor y está funcionando correctamente, le enviará una respuesta llamada **DHCP OFFER**. Este es el datagrama de respuesta del

servidor al cliente ante la petición de obtener parámetros por el protocolo. En este caso la dirección IP de origen será la del propio servidor, que generalmente también actúa de router, la IP de destino será la 255.255.255.255 también, el puerto de origen el 67 y el puerto de destino el 68. En este paquete tendremos la dirección IP privada que se le puede proporcionar y se involucra a la dirección MAC del equipo. Esta comunicación es de tipo unicast generalmente, aunque de forma opcional puede ser broadcast.

Una vez que el cliente recibe el OFFER, le enviará un **DHCP REQUEST** de vuelta. En este caso el cliente selecciona la configuración recibida por el OFFER y una vez más el cliente solicita la IP que indicó el servidor anteriormente. Esta comunicación también es broadcast, porque todavía no tiene una dirección IP privada válida.

Por último, el servidor le enviará un **DHCP ACK** al cliente, diciéndole que lo ha recibido correctamente e incluye toda la información que hayamos configurado en el servidor, como la duración de la conexión, información sobre los servidores DNS y más. Con este último proceso se completan todos los pasos del proceso, el protocolo también esperará un cierto tiempo hasta que el cliente DHCP configure su interfaz correctamente con los parámetros negociados. Una vez que el cliente obtiene la dirección IP, el cliente empezará a recibir información del protocolo ARP con todos los equipos que hay en la red local, con el objetivo de prevenir posibles conflictos de direcciones IP o superposición de grupos de direcciones de servidores DHCP. En caso de encontrar algún problema, el cliente enviará al servidor un mensaje DHCPDECLINE indicando que la dirección ya está en uso.

Una vez que hemos visto cómo funciona el protocolo DHCP, vamos a explicar qué ataques existen y cómo evitarlos.

Donde instalar el DHC

En este caso podemos realizar la instalación de dos formas diferentes. La primera es en un equipo físico y la otra en una máquina virtual. En el caso de optar por la instalación a través de una máquina virtual, si queremos que el servicio DHCP puede proporcionar asignaciones de IP a los equipos que se encuentran en la red física, debemos conectar el adaptador de dicha máquina a un conmutador virtual de Hyper-V, el cual debe ser externo.

Pero en este caso, tendremos que optar por un servicio el cual no dependa en gran parte de un hardware concreto. Esto ocasionará que no funcione bien en la máquina virtual. Puede ser el caso de que requiera que sea procesado por GPU, el cual no está correctamente desarrollado en temas de virtualización en las herramientas más comunes. Por otro lado, cuando se habilita Hyper-V, muchas aplicaciones que son sensibles a la latencia, podrían tener problemas en su ejecución en el host. Esto ocurre porque con la virtualización habilitada, el SO host también se ejecutará sobre un nivel de virtualización que es muy similar a Hyper-V,lo cual se expandirá a todos los sistemas operativos invitados.

Hyper-V también cuenta con diferentes características que varían entre las versiones de Windows 10 u 11 y Server, las cuales es bueno tener en cuenta. Si bien en Windows Server tenemos más opciones, puede darse el caso de que las que hay en Windows 10/11 sean más adecuadas para el sistema, y las cuales será necesario valorar en busca de la mejor opción.

En Windows Server tenemos las funciones:

- Migración de máquinas virtuales de host a host en vivo.
- Réplicas de Hyper-V
- Canales de fibra virtuales.
- Redes SR-IOV
- VHDX compartido

En cuanto a las de Windows 10 y 11:

- Creación rápida y galería de VM
- Red predeterminada (NAT)

Alternativas a los DHCP

En el panorama actual del mundo de las redes, tenemos alternativas para prácticamente todo. El DHCP no es algo que se quede atrás, por lo cual cuenta con sus propias alternativas. A pesar de que se trata de un sistema ampliamente utilizado para asignar las direcciones IP, sí que existen algunas situaciones donde puede ser necesario utilizar otros métodos. Estas son:

- **Configuración manual:** En lugar de utilizar el sistema DHCP, se puede tratar de configurar todos los dispositivos de forma manual, con sus propias direcciones IP estáticas. Esta opción es una de las más seguras, y puede llegar a garantizar que todos estos equipos tengan la misma dirección siempre. Pero lo cierto es que, dependiendo de la amplitud del sistema, resulta algo donde es necesario invertir mucho tiempo, y es muy propensa a tener errores.
- **BOOTP:** El Bootstrap Protocol es un protocolo previo a DHCP. Este se utilizada para establecer configuraciones de dispositivos los cuales no admitían el DHCP. Por lo cual estamos hablando de equipos más antiguos, los cuales en muchos casos se siguen utilizando debido a compatibilidades de software, por ejemplo.
- **DNS Dinámico:** Este sistema permite que los dispositivos de actualicen de forma automática en cuanto a la asignación de las direcciones IP. Esto ocurre a medida que se cambian las direcciones de los propios servidores. Por otro lado, este sistema nos puede ayudar a garantizar que los dispositivos siempre van a tener acceso a recursos que necesitan de la red.
- **Zeroconf:** Se trata de un grupo de protocolos, los cuales permiten que los dispositivos descubran y se conecten de forma automática a otros dispositivos. Esto debe ser en una red local, la cual no tiene necesidad de utilizar un servidor que actúe a modo de nodo central. Este sistema, se utiliza mucho en entornos donde los DHCP no están disponibles, o resultan poco prácticos. Ejemplo de ello, son las redes Ad Hoc, o entornos destinados a pequeñas empresas.

Ataques que existen al DHCP

El protocolo DHCP no utiliza ningún tipo de autenticación, por este motivo es muy vulnerable a ataques y existen diferentes tipos de ataques que vamos a poder realizar.

Un ataque muy común es configurar un servidor DHCP no autorizado para proporcionar información «falsa» o «maliciosa» a los clientes. Cuando conectamos un servidor DHCP ilegítimo en una red local que ya tiene un

servidor DHCP legítimo, los clientes obtendrán la dirección IP, DNS y demás información al primero que responda. Por este motivo, un usuario malintencionado podría levantar un «**Rogue DHCP Server**» en la red, para hacerse con el control de las direcciones de varios clientes. Cuando un ciberdelincuente instala un Rogue DHCP, lo hace por varios motivos:

- **Realizar un ataque de denegación de servicio a la red**: si el cliente o los clientes obtienen este direccionamiento, puede «cortar» la conexión a Internet. De esta forma, los clientes no tendrán acceso a Internet ni tampoco a la red local.
- **Ataque Man in the Middle**: al tener el control total sobre el direccionamiento y los servidores DNS, ni siquiera es necesario hacer un ataque ARP Spoofing porque tendremos el control total de toda la red, y podremos reenviar a los clientes a webs maliciosas modificando los servidores DNS de nuestro propio servidor DHCP que acabamos de instalar. Un servidor DHCP ilegítimo puede proporcionar información falsa de servidores DNS a los diferentes clientes. Por supuesto, no solamente accederán a las webs maliciosas, sino que también podrá espiar fácilmente las conexiones porque nosotros seremos el gateway.

Para mitigar este ataque, se debe garantizar que no haya ningún Rogue DHCP en nuestra red local, y ahí entra en juego el «DHCP Snooping» que incorporan los switches. Esta tecnología permite bloquear los mensajes DHCP Offer y DHCP Ack de los puertos donde no esté permitido, es decir, donde no esté el servidor legítimo. De esta forma, aunque al servidor DHCP falso le lleguen los mensajes, nunca podrá contestar y los clientes de la red local permanecerán a salvo. En el siguiente esquema se puede ver cómo funciona el DHCP Snooping:

Otro ataque muy común a los servidores DHCP, debido a que no tenemos ningún tipo de mecanismo de autenticación de los clientes, es el de realizar decenas de peticiones de direcciones IP, con el objetivo de agotar el almacenamiento de direcciones IP del servidor, al presentar nuevos identificadores de cliente cada vez que se realiza una petición. Esto haría que el servidor «colapse» y no pueda proporcionar más direccionamiento. Existen algunos mecanismos de mitigación, sobre todo a nivel de operadores de Internet que hacen uso de DHCP, como la RFC3046 usando etiquetas la cual se usa como un token de autorización, también tenemos la RFC3118 que es para autenticar los mensajes pero que no se ha usado ampliamente. Con el lanzamiento del protocolo 802.1X para autenticar a los clientes cableados, se dejó en un segundo plano estos RFC.

Sea cual sea el ataque, quién lo ocasione debe tener acceso a la red para que este pueda abusar de este protocolo. Por eso es recomendable tomar ciertas medidas de seguridad que nos permita llevarlo a cabo con garantías. De cara a la red local lo más importante es tener bien configurado el DHCP Snooping para evitar los Rogue DHCP, de esta forma, estaremos protegidos.

Qué es DHCP estático o «Static DHCP»

La funcionalidad de DHCP estático o también conocido como «Static DHCP» o «Static Mapping», es la posibilidad de configurar de manera específica un determinado cliente, basado en su dirección MAC o en su «Client identifier». Gracias a esta función, podremos fijar unos parámetros específicos para este cliente en concreto, como, por ejemplo, la misma dirección IP privada siempre para que nunca cambie. Otras opciones que podemos configurar es

el nombre de host, configurar los servidores DNS y WINS, el nombre de dominio, los servidores NTP, TFTP, LDAP y otra información que también pueden proporcionar los servidores DHCP.

El funcionamiento del Static DHCP es muy sencillo, debemos poner la MAC o client identifier en la correspondiente sección, a continuación, configuraremos una dirección IP específica y el resto de parámetros que nosotros queramos que tenga el cliente. A continuación, podéis ver todas las opciones de configuración disponibles en un sistema operativo pfSense.