Protocolo de configuración dinámica de host (DHCP)

Autores: Pineda y Schaab

- ¿Qué es?

  Es un protocolo de red tipo cliente/servidor.

- ¿Para qué sirve?

  Sirve para que un servidor DHCP asigne una dirección IP y otros parámetros de configuración de red a cada dispositivo en esta, con tal de que puedan comunicarse con otros dispositivos a través de sus respectivas IP.

- ¿Cómo se usa?

  El servidor posee una lista de direcciones IP dinámicas y las asigna a los clientes mientras estos quedan libres, y sabe en todo momento quién usó las IP's, cuánto tiempo y a quién se la asignó luego.

- ¿Cómo y por qué se originó?

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.

proporcionar otra información de cara a los clientes, como los siguientes parámetros que son configurables y opcionales:

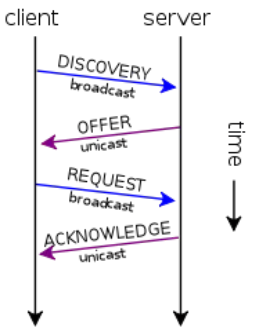
Servidor DNS primario y secundario.
Nombre DNS.
MTU para la interfaz.
Servidor y dominio NIS.
Servidores NTP.
Servidor de nombre WINS para Windows.

APIP

Teniendo en cuenta que la definición de protocolo es “Conjunto de reglas que rigen el funcionamiento de un sistema”, podemos entender que DHCP es un protocolo de red del tipo que relaciona al cliente con el servidor. Es un protocolo que se encarga de asignar una IP a cada dispositivo dentro de una red, además de otros parámetros de configuración de red. Aquel que comprende el protocolo puede supervisar y distribuir desde un mismo punto las direcciones IP, y de forma automática, reasignar nuevas IPs si se diera el caso de que un dispositivo se conecte desde un lugar distinto en la red.
DHCP nace debido a que se utilizaba el protocolo RARP (Reverse Address Resolution Protocol), pero este era un protocolo de la capa de enlace de datos que hacía que fuese muy tedioso de utilizar en múltiples plataformas de servidores, entonces se reemplazó por BOOTP, siendo este uno de los primeros métodos para asignar direcciones IP de forma dinámica. A su vez, BOOTP, que requería intervención manual para completar la información de configuración de cada cliente y no se pueden recuperar las direcciones IP en desuso, fue extendido con DHCP, que si entregaba una gran variedad de parámetros de configuración extra a los clientes IP y además tenía la capacidad de asignar muchas más IPs en las redes actuales, que cada vez eran más grandes. Finalmente en 2003 se documentó DHCPv6 y luego se complementó con otros RFC y se amplió aún más para proporcionar información a los clientes sobre la configuración automática de direcciones sin estado. Siendo los RFC documentación extensa sobre el funcionamiento de Internet y redes, englobando protocolos, procedimientos, entre otros.

El protocolo DHCP tiene tres formas de asignación de direcciones IP: **asignación manual o estática** (le asigna una dirección IP a una máquina determinada, se suele utilizar cuando se quiere controlar la asignación de direcciones IP de cada cliente y quienes se conectan)(Asigna una dirección IP en base a una dirección MAC manualmente, permitiendo controlar el flujo de clientes, quién puede y no puede conectarse), **asignación automática** (Le asigna una dirección IP a una máquina cliente la primera vez que esta realiza una solicitud al servidor DHCP y hasta que el cliente la libera, se suele utilizar cuando el número de clientes no varía demasiado) y **asignación dinámica** (es el único método que permite la reutilización dinámica de las direcciones IP. El administrador asigna un rango de direcciones y todos los dispositivos que se conecten pueden pedirle al servidor una dirección cuando su tarjeta de red se inicializa).

El funcionamiento del protocolo DHCP consta de cuatro procesos principales, **Discovery**, **Offer**, **Request** y **Acknowledge**. La comunicación entre servidor y cliente suele darse a través de, del lado servidor, el protocolo UDP puerto 67, y del lado cliente, se utiliza también UDP pero en el puerto 68. En la **primera instancia**, **Discovery**, el cliente no cuenta con una dirección IP asignada, por lo que va a intentar encontrar una, enviando un mensaje a la red. Para ello envía una dirección IP de origen 0.0.0.0, junto a una dirección IP de destino 255.255.255.255, esta es la IP de broadcast global, dentro de un datagrama a la vez que otros d



atos a completar por el servidor. Un datagrama es un conjunto de información hecha por el protocolo UDP. contiene IP de origen y destino, a la vez que otros datos relevantes para los protocolos que la utilizan. De existir y encontrar, dentro de la misma red, un servidor funcional, le enviará una respuesta al cliente, llamada **Offer**. Esta respuesta, en forma de datagrama y de tipo unicast, contiene una IP de origen propio del servidor, y de destino la IP es 255.255.255.255, con los respectivos puertos 67 y 68, sin sumarle otro tipo de información más que la dirección IP que el servidor

puede otorgar junto a la dirección MAC a asociar. Cuando el cliente recibe la respuesta, envía un **Request**. Vuelve a enviar de forma broadcast la solicitud de IP que el servidor le ofreció junto a la configuración ofrecida. Como situación final, el servidor envía un **Acknowledge**, confirmando que recibió correctamente la información que se configuró, duración de la conexión, información de los servidores DNS, servidor NTP, entre otros datos. Una vez el servidor termine de configurarse correctamente dada la nueva información, el cliente comenzará a recibir información del protocolo ARP, junto a los otros equipos que pertenecen a la red local. Esto evita conflictos entre direcciones IP o superposición de grupos de direcciones en los servidores. En caso de error, el servidor genera un mensaje de Decline indicando que la dirección IP ya está en uso.

El sistema no es perfecto y cuenta con una falla importante en cuanto a seguridad. Los servidores DHCP no cuentan con autenticación por parte del servidor, lo cual termina por permitir que en una red con un DHCP legítimo, surja otro servidor DHCP malicioso. Si ocurriera esto, como el cliente tiende a mandar el mensaje a todas las direcciones de la red, si la que contesta primero a su Discovery es la maliciosa, esta podría proveerle datos que, más adelante, podría aprovechar. Con este tipo de ataque, llamado “Rogue DHCP Server”, el atacante podría cortar la conexión a Internet de los usuarios que estuvieran en su red, a la vez que podría reenviarle a los dispositivos involucrados resultados maliciosos ya que él controlaría el DNS y por lo tanto el flujo de datos. La forma de evitar que surjan, o por lo menos que no afecten, los servidores Rogue es implementando la tecnología de los switches, DHCP Snooping, que bloquea los DHCP Offer y DHCP Acknowledge de los puertos donde no esté permitido. Otro ataque más común es aquel en el que se envían demasiadas solicitudes de IP al servidor, consiguiendo que este colapse debido al flujo excesivo de datos y por lo tanto genera que toda la red caiga al no poder otorgar más direccionamientos en la red.

Implementación:
Configurar servidor, cambiar parámetros. Explicar el proceso.
permiten levantar un servidor DHCP por cada subred que nosotros hayamos configurado

https://www.youtube.com/watch?v=fUK6d3s1Im4

https://www.youtube.com/watch?v=cwSKZReA0gQ

https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/

https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host

https://datatracker.ietf.org/doc/html/rfc2132

https://www.ionos.es/digitalguide/servidores/know-how/unicast/

https://es.wikipedia.org/wiki/Protocolo_de_datagramas_de_usuario
https://www.ugr.es/~fernanla/Untitled.pdf