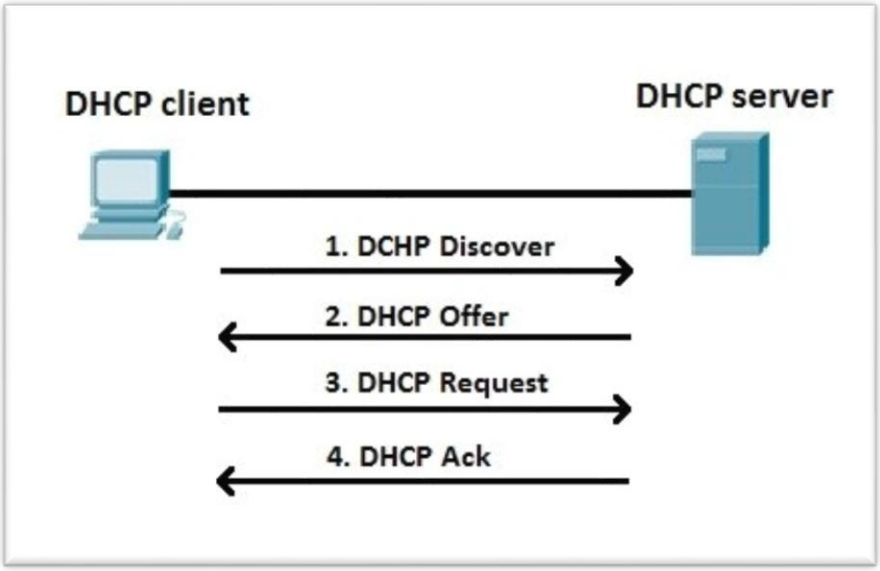
Servidor DHCP (Dynamic Host Configuration Protocol)

Cuando contamos con varios equipos conectados en una red, cada cual debe tener registrada una dirección IP (Internet Protocol) diferente dentro de un rango determinado, para que estos equipos puedan compartir información entre sí, y puedan eventualmente salir a otra red, como por ejemplo hacia internet. Es en este punto donde aparece el término Servidor DHCP (Dynamic Host Configuration Protocol), para hacer una administración centralizada y automática de los parámetros de red.

Sin el DHCP, el administrador de una red, tendría que pasar equipo por equipo registrando la dirección IP asignada a cada cual, junto con otros parámetros de red como la puerta de enlace (gateway), máscara de red, las direcciones de servidores DNS, etc.

El servidor DHCP escucha las peticiones de parámetros de red de los equipos que se encuentran configurados para obtenerlas automáticamente. Así pues un equipo recibe del servidor DHCP la dirección IP, la máscara de red, la puerta de enlace, los servidores DNS y cualquier otro parámetro de red que se requiera. Estos parámetros los entrega el servidor DHCP con un tiempo de vida, conocido tomo “lease-time”, después del cual el cliente DHCP debe solicitar nuevos parámetros al servidor DHCP.



Al servidor DHCP se le pueden poner excepciones dentro del rango de direcciones IP que tiene disponibles para asignar, con el fin de que no las tenga en cuenta, porque pueden estar siendo usadas por ciertas máquinas que necesitan una dirección IP fija o estática. De este modo se evita que el DHCP asigne direcciones ya usadas dentro de la red.

El servidor DHCP permite hacer una administración centralizada de las direcciones IP, evitando conflictos de direcciones IP repetidas, o también permitiendo la distribución de parámetros de red a todos los equipos, que pueden ser modificadas por ejemplo por un cambio de direccionamiento, servidores DNS, rutas estáticas, etc.

Qué es el DHCP

El DHCP es una extensión del protocolo Bootstrap (BOOTP) desarrollado en 1985 para conectar dispositivos como terminales y estaciones de trabajo sin disco duro con un Bootserver, del cual reciben su sistema operativo. El DHCP se desarrolló como solución para redes de gran envergadura y ordenadores portátiles y por ello complementa a BOOTP, entre otras cosas, por su capacidad para asignar automáticamente direcciones de red reutilizables y por la existencia de posibilidades de configuración adicionales.

Tras unas primeras definiciones del protocolo en 1993 en los RFC 1531 y 1541, su especificación definitiva llegó en 1997 con el RFC 2131. La IANA (Internet Assigned Numbers Authority) provee al protocolo de los puertos UDP 67 y 68 (para IPv6, los puertos 546 y 547), también reservados para el protocolo Bootstrap.

La asignación de direcciones con DHCP se basa en un modelo cliente-servidor: el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP que, por su parte, recurre a una base de datos que contiene los parámetros de red asignables. Este servidor, componente de cualquier router ADSL moderno, puede asignar los siguientes parámetros al cliente con ayuda de la información de su base de datos:

- Dirección IP única
- Máscara de subred
- Puerta de enlace estándar
- Servidores DNS
- Configuración proxy por WPAD (Web Proxy Auto-Discovery Protocol)

Así se comunican el cliente DHCP y el servidor DHCP

La asignación automática de direcciones mediante el protocolo de configuración dinámica de host tiene lugar en cuatro pasos consecutivos:

1. El cliente DHCP envía un paquete DHCPDISCOVER a la dirección 255.255.255.255 desde la dirección 0.0.0.0. Con esta denominada difusión amplia o broadcast, el cliente establece contacto con todos los integrantes de la red con el propósito de localizar servidores DHCP

disponibles e informar sobre su petición. Si solo hay un servidor, entonces la configuración es extremadamente sencilla.

2. Todos los servidores DHCP que escuchan peticiones en el puerto 67 responden a la solicitud del cliente con un paquete DHCPOFFER, que contiene una dirección IP libre, la dirección MAC del cliente y la máscara de subred, así como la dirección IP y el ID del servidor.

3. El cliente DHCP escoge un paquete y contacta con el servidor correspondiente con DHCPREQUEST. El resto de servidores también reciben este mensaje de forma que quedan informados de la elección. Con esta notificación, el cliente también solicita al servidor una confirmación de los datos que le ha ofrecido. Esta respuesta también sirve para confirmar parámetros asignados con anterioridad.

4. Para finalizar, el servidor confirma los parámetros TCP/IP y los envía de nuevo al cliente, esta vez con el paquete DHCPACK (DHCP acknowledged o «reconocido»). Este paquete contiene otros datos (sobre servidores DNS, SMTP o POP3). El cliente DHCP guarda localmente los datos que ha recibido y se conecta con la red. Si el servidor no contara con ninguna dirección más que ofrecer o durante el proceso la IP fuera asignada a otro cliente, entonces respondería con DHCPNAK (DHCP not acknowledged o «no reconocido»).

5. La dirección asignada se guarda en la base de datos del servidor junto con la dirección MAC del cliente, con lo cual la configuración se hace permanente, es decir, el dispositivo se conecta a la red siempre con esa dirección que le ha sido asignada automáticamente y que ya no está disponible para ningún otro cliente, lo que significa que los clientes DHCP nuevos no pueden recibir ninguna dirección si ya están todas asignadas, incluso aunque algunas IP ya no se usen activamente. Esto ha llevado a la expansión de las direcciones dinámicas y, en casos especiales, a la asignación manual vía servidor DHCP, que explicamos en los párrafos que siguen.

¿Es seguro el DHCP?

El Dynamic Host Configuration Protocol tiene un punto débil y es su capacidad para ser manipulado fácilmente. Como el cliente hace un llamamiento a discreción a todos los servidores DHCP que podrían responder a su petición, a un atacante le sería relativamente sencillo entrar en la red y hacerse pasar por uno de ellos si tuviera acceso a ella. Este denominado servidor DHCP “Rogue” (corrupto) intenta adelantarse con su respuesta al servidor legítimo y si tiene éxito envía parámetros manipulados o inservibles. Si no envía puerta de enlace, asigna una subred a cada cliente o responde a todas las peticiones con la misma dirección IP, este atacante podría iniciar en la red un ataque de denegación de servicio o Denial of Service.

Más dramático, pero factible, sería el intento de colarse en un router utilizando datos falsos sobre la puerta de enlace y el DNS, de modo que se estaría en posición de copiar o desviar el tráfico de datos. Este ataque man in the middle no tiene el propósito, como el primero, de ocasionar una caída de la red, sino de apropiarse de información sensible como datos bancarios, contraseñas o direcciones postales.

Sea cual sea el tipo de ataque, sus artífices necesitan tener acceso directo a la red para abusar del protocolo DHCP, así que se debe de implementar las medidas de seguridad necesarias que te permitan disfrutar las ventajas de este protocolo de comunicación sin temor a sufrir las consecuencias de una amenaza de este tipo. Para el responsable de una red local es fundamental la protección absoluta ante intentos externos e internos de ataque y la supervisión constante de todos los procesos de red con herramientas como Nagios. En nuestra guía sobre la seguridad WLAN también repasamos las opciones de que dispones para proteger redes inalámbricas.

Usando Cisco

Aunque la configuración del servicio DHCP en router CISCO ya está bien escrito y documentado en muchos sitios por internet, la idea es recogerlo junto con los demás artículos que los alumnos van a ir escribiendo sobre los temas que estamos tocando en el curso.

Como el programa Packet Tracer lo hemos tocado de forma general para la configuración de redes cercanas y poco más, voy a añadir algunas configuraciones más específicas para quien pudiera necesitarlas y para reforzar lo estudiado en clase.

Necesitaremos para probarlo una red como la de la imagen, aunque podría tener solo un ordenador. Una vez conectada vamos a entrar en la configuración del router mediante comandos ya que la configuración de este servicio no es posible realizarla desde el configurador gráfico del router.

En la pestaña de la consola (CLI) se debe entrar en modo privilegiado y luego en modo configuración.

Router> enable

Router# configure terminal

Router(config)#

Una vez llegados hasta aquí nos ponemos manos a la obra. Los pasos a realizar son:

1. Indicamos un rango de ip excluido del pool (conjunto) de direcciones que asignará el servicio dhcp. Se indica la ip inicial y la final del rango a excluir.

Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10

2. Asignamos un nombre al conjunto de direcciones que serán asignadas.

   Router(config)#ip dhcp pool Lan_A

3. Después de ponerle nombre al rango de ip es necesario definir los parámetros de dicho rango.

   Router(dhcp-config)# network 192.168.1.0 255.255.255.0

   Router(dhcp-config)# default-router 192.168.1.1

   Router(dhcp-config)# dns-server 80.58.0.33

4. Con esta configuración el servidor DHCP se encuentra en funcionando a la espera de solicitudes DHCP

No es necesario indicar la interfaz por la cual debe escuchar solicitudes DHCP ya que cuando configuremos la IP y la máscara de red de la interfaz que por defecto no viene configurada estos datos corresponderán a los del pool DHCP y por lo tanto el servicio ya sabrá por donde estar a la escucha.

Verificando la Configuración DHCP

Para poder visualizar la configuración DHCP en nuestro router Cisco, debemos de usar las siguientes instrucciones:

- Muestra los parámetros opcionales importados en la base de datos del servidor DHCP.

  show ip dhcp import

- Muestra los parámetros opcionales importados en la base de datos del servidor DHCP.

  show ip dhcp pool

- Muestra las estadísticas del servidor DHCP, como el número de grupos de direcciones, enlaces y demás.

  show ip dhcp server statistics

En caso de digitar una instrucción equivocada, podemos cancelarla presionando Ctrl + Shift + 6