Unidad 2: Servicio DHCP

Contenido

1. Características 2
2. Ventajas e inconvenientes del uso de servicios de configuración automática de red. 2
3. Componentes 3
4. Asignación 3
   - 4.1. Tipos de asignación 3
   - 4.2. Ámbito 4
   - 4.3. Rango 4
   - 4.4. Exclusiones 5
   - 4.5. Reservas 5
   - 4.6. Tiempo de concesión (lease time) 5
5. Servidores DHCP 6
6. Clientes DHCP 6
7. Tipos de opciones 6
8. Protocolo DHCP 7
9. Funcionamiento 8
   - 9.1. Obtener una concesión 8
   - 9.2. Renovar una concesión 9
   - 9.3. Liberar una concesión 10
   - 9.4. Actualizar parámetros de configuración 11
10. Tipos de mensajes DHCP 11
11. Varios servidores independientes DHCP 11
12. Dar servicio a varias redes 12
    - 12.1. Un servidor DHCP en cada subred 12
    - 12.2. Un servidor centralizado 12
13. Agentes de retransmisión DHCP 12
14. DHCP *Failover Protocol* 13
15. Seguridad 14
16. BOOTP 15

1. Definición.

DHCP es un protocolo de capa de aplicación diseñado para implementar un servicio de configuración automática de red en redes TCP/IP. Su función principal es permitir a los equipos de una red obtener sus parámetros de configuración automáticamente.

2. Ventajas e inconvenientes del uso de servicios de configuración automática de red.

En las redes TCP/IP los administradores de sistema tienen dos opciones a la hora de configurar los equipos:

- Configurar y mantener manualmente la configuración de red de los equipos.
- Usar un servidor DHCP para asignar, configurar y mantener de forma dinámica losdatos de configuración de red de cada equipo.

En el caso de elegir la configuración manual se encontrarán con varias dificultades:

- La configuración de red (dirección IP, mascara de subred, servidores DNS, puerta de enlace…) se define manualmente en cada equipo lo que conlleva un aumento de las tareas de administración de la red.
- Existe la posibilidad de introducir una configuración incorrecta que dé lugar a problemas de comunicación.
- Si un equipo cambia de ubicación y se conecta a una subred diferente será necesario modificar su configuración de red. Esta situación es especialmente importante en redes inalámbricas donde es habitual que los equipos portátiles puedan conectarse en diferentes subredes.
- Si nuestra red crece y en un momento dado es necesario reestructurar la misma, será necesario modificar la configuración de red de todos los equipos.

Sin embargo, al elegir la configuración automática mediante un servicio de red, como DHCP, se obtienen varias ventajas.

- El servidor suministra automáticamente la información de configuración necesaria a los equipos disminuyendo el trabajo a realizar por el administrador.
- Nuevos equipos se pueden conectar a la red sin necesidad de ninguna intervención por parte del administrador.
- Garantiza que los equipos en la red emplean la información de configuración de red correcta y permite cambiar la configuración de varios equipos de forma centralizada.
- Permite reestructurar la red y añadir o modificar servicios de red sin tener que acceder a los equipos, simplemente estableciendo la configuración que se mandará a los equipos de la red.
- Los equipos pueden cambiar de ubicación y conectarse a la red automáticamente.

A pesar de las ventajas y simplicidad de configuración de un servidor DHCP pueden existir reticencias a su uso que no se corresponden con la realidad. Por ejemplo, puede surgir la duda de si los servidores DHCP producen un exceso de tráfico de difusión. Sin embargo, la realidad nos dice que los mensajes de difusión

que se envían son mínimos. En la mayoría de los casos estarán limitados a un paquete de difusión enviado por el cliente para descubrir al servidor DHCP, lo que resulta insignificante en el tráfico total de la red.

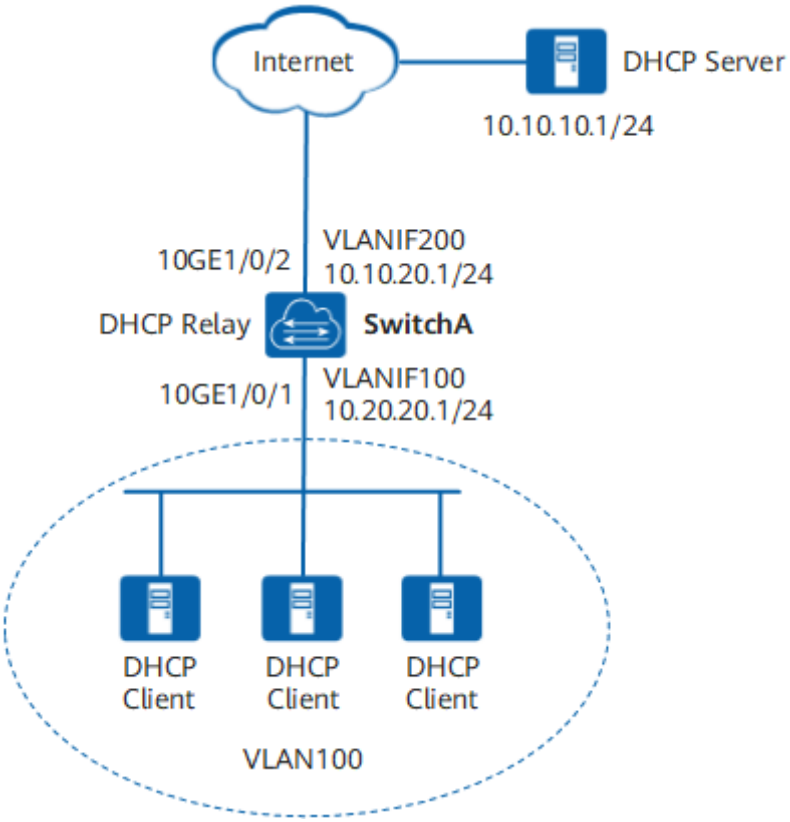
Lo que no resulta recomendable es utilizar DHCP para configurar los servidores que proporcionan servicios de red como servidores de nombres, servidores de correo, etc. Eso es debido a que un fallo en el servidor DHCP podría dejar inutilizados el resto de servicios de la red.

3. Componentes.

El funcionamiento del servicio DHCP está basado en el modelo cliente/servidor y está formado por los siguientes componentes:

- **Servidor DHCP.** Asigna la configuración de red a los clientes.
- **Clientes DHCP.** Realizan peticiones al servidor DHCP y configuran los parámetros TCP/IP con las opciones que recibe del servidor DHCP.
- **Protocolo DHCP.** Conjunto de normas y reglas en base a las cuales "dialogan" los cientes y los servidores DNS.
- **Agentes de retransmisión DHCP.** Escuchan peticiones de clientes DHCP y las retransmiten a servidores DHCP ubicados en otras redes. Se utilizan para centralizar la configuración del servicio DHCP en múltiples redes.

Además, es necesario reseñar que en una red pueden convivir equipos que sean clientes DHCP con otros cuya configuración se haya establecido manualmente.



4. Asignación

A la hora de analizar las asignaciones de direcciones IP que realiza el Servidor DHCP podemos estudiar diferentes conceptos que nos permiten caracterizarlas.

4.1. Tipos de asignación.

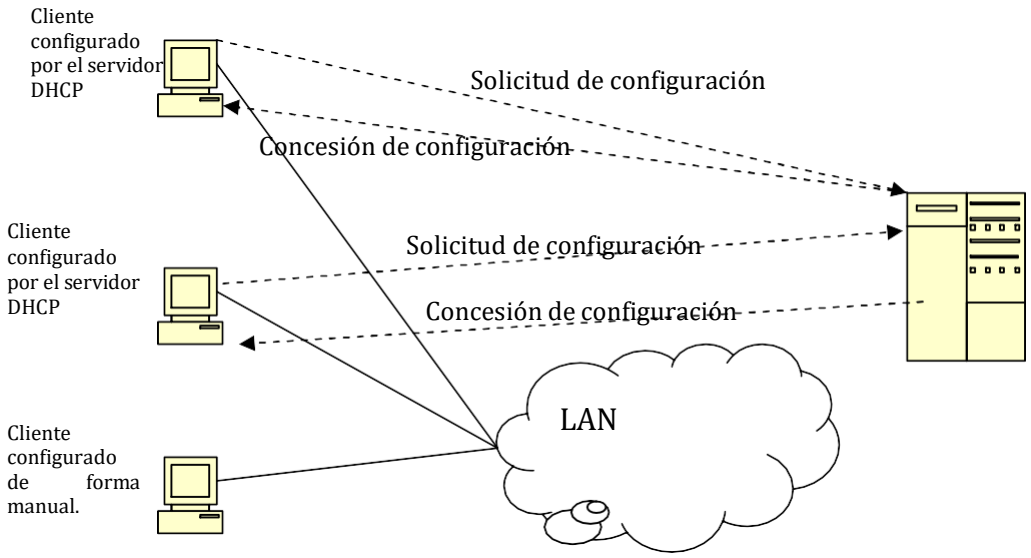
Existen tres tipos de asignaciones a la hora de que un servidor DHCP asigne una configuración a un cliente:

- Asignación manual o estática (Reservas):
  - Asignar direcciones IP concretas a máquinas concretas. A cada dirección física (MAC) le corresponde una dirección IP (preasignada "manualmente" por el administrador.
- Asignación dinámica:
  - El servidor DHCP elige una dirección de un grupo de direcciones disponibles (definidas por el administrador) (rango/ámbito).
  - Realiza una concesión de la dirección IP al cliente durante un plazo limitado (lease time).
- Asignación automática:
  - Asignar direcciones IP de forma permanente a máquinas clientes la primera vez que hacen la solicitud al servidor DHCP y hasta que el cliente las libera.

- La diferencia con la asignación dinámica radica en que en la asignación automática el plazo de concesión es ilimitado.
- Hay que usar este tipo de asignación con precaución porque si un equipo con una asignación sin caducidad es eliminado y no se notifica al servidor DHCP, su dirección IP no se podría reutilizar.

A la hora de establecer la política de asignación de direcciones que empleará el servidor DHCP, se suele emplear una política híbrida en la que se combinan la asignación dinámica para la mayoría de los clientes y la asignación manual para determinados clientes "conocidos" y que necesitan tener siempre la misma dirección IP.

Es necesario recordar también que el servicio DHCP no constituye en sí mismo ningún mecanismo de seguridad. Cualquier usuario que tenga acceso a la red podría configurar manualmente su equipo con una dirección IP válida y tener acceso a los recursos de la red.



4.2. Ámbito.

Se puede definir un ámbito como un agrupamiento administrativo de equipos o clientes de una red que utilizan el servicio DHCP. Dentro del ámbito se reserva un rango de direcciones IP para otorgar a los clientes de dicho ámbito.

Habitualmente el administrador de red creará un ámbito para cada subred y definirá un rango de direcciones IP para otorgar, una máscara de subred, un tiempo de concesión y otros parámetros adicionales como puerta de enlace, servidores DNS, etc…

4.3. Rango.

Es posible definir un rango como un intervalo consecutivo de direcciones IP válidas y disponibles para ser concedidas o asignadas a equipos clientes DHCP de una red determinada.

En un servidor DHCP se pueden configurar tantos ámbitos/rangos como sea necesario para el entorno de red.

4.4. Exclusiones.

Un conjunto de direcciones pueden ser excluidas de un rango para no asignarlas a clientes DHCP.

Normalmente se suelen excluir del rango aquellas direcciones IP que corresponden a equipos que necesitan una dirección IP fija, como servidores, routers o Firewalls, y que se configuran manualmente.

4.5. Reservas.

Consiste en la asignación de una dirección IP fija a un equipo, y se suele utilizar para asignar a servidores o PCs concretos la misma dirección siempre. Es algo similar a configurar manualmente una dirección IP estática, pero de forma automática desde el servidor DHCP.

En este punto es necesario recordar que en una red de área local se identifica al equipo por una dirección física o MAC.

4.6. Tiempo de concesión (lease time)

El plazo del contrato o concesión es el tiempo en que un cliente DHCP mantiene como propios los datos de configuración que le otorgó un servidor.

Cada vez que el cliente arranca, cada cierto tiempo o bien cuando se alcanza el límite de la concesión (lease time) el cliente tiene que solicitar su renovación.

Una vez vencido el plazo del contrato el servidor puede renovar la información del cliente, asignarle otra nueva o extender el plazo de manteniendo la misma información.

Esta característica facilita la restructuración de una red de forma transparente al usuario, que simplemente obtendrá una nueva dirección una vez haya finalizado la concesión de la anterior configuración de red.

A la hora de determinar el tiempo de concesión es necesario analizar las características de la red. Por ejemplo, en los servidores DHCP de Windows el tiempo de concesión por defecto es de ocho días, pero:

- En una red con un gran número de direcciones IP disponibles y donde la configuración de los clientes raramente cambia el administrador podría incrementar el tiempo de concesión para reducir el tráfico derivado de las solicitudes de renovación por parte de los clientes. Por ejemplo, si 30 ordenadores comparten 254 direcciones podría incrementarse el tiempo de concesión a varios meses.
- En una red que tiene un número muy limitado de direcciones IP y donde la configuración de los clientes cambia frecuentemente, o donde los equipos cambian habitualmente de subred, el administrador podría reducir el tiempo de concesión para que las direcciones IP que ya no están siendo usadas puedas estar disponibles para nuevas asignaciones. Por ejemplo, si 220 ordenadores comparten 254 direcciones IP sería adecuado reducir el tiempo de concesión a pocos días.

5. Servidores DHCP.

Los servidores DHCP permiten asignar la configuración de red al resto de máquinas presentes en la red (clientes DHCP) cuando estos arrancan o inician sus interfaces de red. Para realizar esta tarea escuchan las peticiones a través del puerto **67/UDP.**

Permiten configurar de forma automática parámetros como los siguientes.

- **Dirección IP.**
- **Máscara de subred.**
- **Puerta de enlace.**
- **Servidores DNS.**
- **Nombre DNS.**
- **Tiempo máximo de espera de ARP.**
- **Servidores POP3.**
- **Servidor WINS.**
- **Etc.**

Estos parámetros se pueden configurar a distintos niveles. Se pueden establecer a nivel del servidor DHCP, a nivel de ámbito o incluso a nivel de una reserva.

Ejemplos de servidores DHCP son:

- ISC DHCP, utilizado en sistemas Linux/Unix.
- Servidor DHCP de Microsoft.
- Servidores DHCP integrados en routers.

6. Clientes DHCP.

Los clientes realizan peticiones al servidor DHCP y configuran sus parámetros TCP/IP con las opciones que recibe del servidor DHCP. Para esto utilizan el puerto **68/UDP**. Estos clientes DHCP están integrados en Windows, Linux y en otros sistemas operativos.

7. Tipos de opciones.

A la hora de establecer los parámetros de configuración que se enviarán a los clientes, podemos establecer parámetros a diferentes niveles:

- **Opciones de servidor:** Se envían a todos los clientes del servidor DHCP.
- **Opciones de ámbito:** Se envían a todos los clientes del ámbito y sobrescriben las opciones de servidor.
- **Opciones de clase:** Se envían a los clientes de acuerdo a la clase de cliente a la que pertenecen.
- **Opciones de equipo:** Se definen para un equipo concreto mediante una reserva. Este tipo de opciones sobrescriben a cualquiera de las demás.

8. Protocolo DHCP.

El protocolo DHCP determina el conjunto de normas y reglas en base a las cuales dialogan los clientes y los servidores DHCP. Como el protocolo DHCP fue desarrollado partiendo del protocolo BOOTP (se explica en apartados posteriores) el formato de un mensaje DHCP está basado en el formato de un mensaje BOOTP.

El formato de un mensaje DHCP es el que se muestra en la Figura 2.2. Tiene una parte fija que aparece en todos los mensajes, aunque no se utilicen todos los campos y una parte variable (options) donde irán las opciones específicas de DHCP:

- **op:** Indica si es solicitud o respuesta.
- **htype:** Tipo de hardware. Por ejemplo Ethernet (1) o redes IEEE 802.
- **Hlen:** Longitud de la dirección hardware.
- **Hops:** Saltos.
- **Xid:**Identificador de la transacción para relacionar peticiones y respuestas.
- **Secs:** Tiempo en segundos desde que el cliente inició el proceso.
- **Flags:** El bit más significativo de este cmapo se utiliza como flag de difusión.
- **Ciaddr:** Dirección IP del cliente.
- **Yiaddr:** Dirección IP que el servidor ofrece al cliente.
- **Siaddr:** Dirección IP del servidor que ofrece la concesión.
- **Giaddr:** Dirección IP del agente de retransisión.
- **Chaddr:** Dirección física del cliente.
- **Sname:** Nombre del servidor DHCP.
- **File:** Nombre del fichero a descargar y arrancar con él.

<table>
<tr><td>Op</td><td>Htype</td><td>Hlen</td><td>Hops</td></tr>
<tr><td colspan="4">Xid</td></tr>
<tr><td colspan="2">Secs</td><td colspan="2">Flags</td></tr>
<tr><td colspan="4">Ciaddr</td></tr>
<tr><td colspan="4">Yiaddr</td></tr>
<tr><td colspan="4">Siaddr</td></tr>
<tr><td colspan="4">Giaddr</td></tr>
<tr><td colspan="4">Cchaddr</td></tr>
<tr><td colspan="4">Snae</td></tr>
<tr><td colspan="4">File</td></tr>
<tr><td colspan="4">options</td></tr>
</table>

Figura 2.2: Formato de los mensajes DHCP

La selección opciones contiene información de configuración envidada entre el cliente y el servidor DHCP. Cada opción tiene un *option code*, que identifica el tipo de opción, un *option lenght*, que identifica el tamaño de los datos y un *option data,* que constituye los datos de la opción.

Cada tipo de mensaje se determina mediante una opción. Por ejemplo, un mensaje **DHCPOFFER** vendría definido por *option code=53*, (tipo de opción para establecer el tipo de mensaje), *option length = 1, option data = 2* (dato que indica el mensaje **DHCPOFFER**). Y así sucesivamente, se irían estableciendo todas las opciones DHCP referidas a ese mensaje.

9. Funcionamiento.

El funcionamiento del servicio DHCP sigue estos pasos:

1) Cuando un cliente DHCP se conecta a la red envía una solicitud en forma de *broadcast* a través de la red.
2) Todos los servidores alcanzados por la solicitud responden al cliente con sus respectivas propuestas.
3) El cliente acepta una de ellas haciéndoselo saber al servidor elegido.
4) El servidor le otorga la información requerida (en este mensaje le otorga un plazo de concesión).
5) Esta información se mantiene asociada al cliente mientras este no desactive su interfaz de red o no expire el plazo del contrato o concesión.
6) Renovaciones:
    a. Cada vez que el cliente arranca, cada cierto tiempo o bien cuando se alcanza el límite de la concesión el cliente tiene que solicitar su renovación.
    b. Una vez vencido el plazo de contrato el servidor puede renovar la información del cliente, asignarle otra nueva o extender el plazo, manteniendo la misma información.

Vamos a estudiar en más detalle las dos situaciones principales del servicio, la que se produce cuando el cliente quiere obtener una concesión y la que produce cuando el cliente quiere renovar su concesión.

9.1. Obtener una concesión.

Partimos de la situación en la que el servidor DHCP está a la escucha de las posibles solicitudes de los clientes. El servidor almacena las posibles direcciones IP a otorgar además del resto de la información.

A la hora de obtener una concesión por parte de un cliente se suceden cuatro etapas, que reciben su nombre de los tipos de paquete DHCP usados en la comunicación:

1) Descubrimiento DHCP (DHCPDISCOVER)

El cliente DHCP difunde por *broadcast* un paquete DHCPDISCOVER para localizar un servidor DHCP.

El mensaje DHCPDISCOVER tiene las siguientes características:

- Puerto destino 67
- Puerto origen 68
- Dirección IP origen: 0.0.0.0
- Dirección IP destino: 255.255.255.255
- Lleva un identificador de transacción.
- Incluye la dirección MAC del cliente.

2) Oferta DHCP (DHCPOFFER)

Los servidores responden a la petición con DHCPOFFER. Donde ofrecen una dirección IP al cliente (basándose en la información que han recibido), máscara de red, tiempo de concesión, etc…

Cada servidor DHCP de respuesta reserva la dirección IP propuesta, para no ofrecerla a toro cliente DHCP antes de que el cliente que realizó la solicitud la acepte.

3) Solicitud DHCP (DHCPREQUEST)

El cliente recibe una o más ofertas de servidores y elige la "mejor". Normalmente la primera.

Difunde (por *broadcast)* un mensaje DHCPREQUEST, poniendo el nombre del servidor elegido en uno de los campos de opciones (ID servidor).

Si el cliente no recibe mensajes DHCPOFFER, expira la petición y reenvía un nuevo mensaje DHCPDISCOVER.

4) Reconocimiento DHCP (DHCPACK) o reconocimiento negativo DHCP (DHCPNACK).

Si el mensaje DHCPREQUEST no contiene su dirección, el servidor considera su oferta rechazada.

Si contiene su dirección, envía un mensaje:

- DHCPACK si la dirección IP aún está disponible.
- DHCPNACK si ya no está disponible o no es válida.

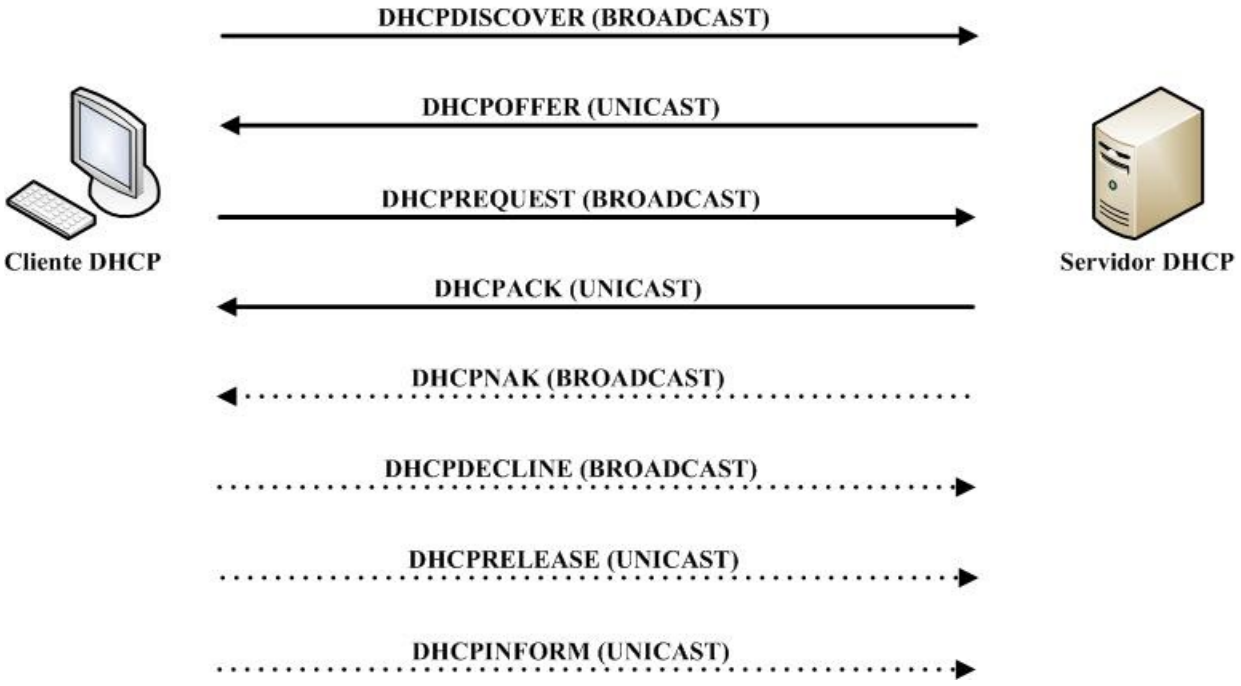
Si el cliente recibe el DHCPACK, puede usar la dirección IP.

- El cliente debe verificar que la dirección IP es válida y no está duplicada.
  - Si la IP es válida, el cliente se inicializa con los datos suministrados por el servidor DHCP.
  - Si encuentra un problema con la dirección asignada, envía un **DHCPDECLINE** al servidor y vuelve al paso 1 (**DHCPDISCOVER**).

Si recibe el DHCPNACK, libera la dirección IP y vuelve al paso 1 (DHCPDISCOVER).

Si el servidor DHCP no está disponible continuamente, se puede llegar a la solución de tener más de un servidor DHCP en la red.

(comando dhclient –v)



¿Qué ocurre si un equipo con una concesión activa cambia de subred?

Si el equipo con una concesión de dirección IP cambia de subred, al ser iniciado mandaría la petición de confirmación al servidor DHCP. Este comprobaría que el mensaje viene de la nueva red por lo que contestaría al equipo indicándole que su dirección IP es inválida. El equipo ante esta respuesta mandaría una petición al servidor DHCP para obtener una nueva concesión válida.

Este proceso funcionaría siempre y cuando el enrutador tuviera la capacidad d reenviar los mensajes del protocolo DHCP.

9.2. Renovar una concesión.

El proceso de renovación de concesiones es resultado del valor del período de concesión. Este valor garantiza que DHCP mantiene la información de direcciones IP y que los clientes actualizan o renuevan regularmente sus datos de configuración de direcciones IP.

Los clientes intentan renovar su concesión:

- Cuando se inician (se reinicia la máquina o la interfaz de red) para asegurarse de que pueden usar la dirección IP que tenían anteriormente, y si no es así solicitar otra.
- Antes de que finalice el período de concesión para garantizar que la información de configuración está actualizada. Los clientes DHCP intentan renovar su concesión a intervalos específicos para garantizar que la información de configuración está actualizada.
    - Por defecto un cliente DHCP intenta renovar su concesión a la mitad del plazo de concesión, aunque este parámetro se puede configurar.
    - Si no lo consigue, al finalizar el plazo libera la dirección.
- Renovación manual. La concesión se puede renovar manualmente en el cliente.

Se realizan dos pasos para renovar una concesión:

1) El cliente DHCP difunde un DHCPREQUEST con la opción *Requested IP address* (la dirección previamente asignada).
2) El servidor DHCP correspondiente devuelve DHCPACK o DHCPNACK.

¿Qué ocurre si un equipo se retira de la red?

El servidor DHCP cuando detecte que ha caducado la concesión que tenía ese equipo y no ha recibido ninguna petición de renovación simplemente liberará esa dirección para poder asignarla a próximas peticiones.

¿Qué tiempo de concesión sería el adecuado?

Establecer los tiempos de concesión de las asignaciones dependerá de las características de los equipos que las utilicen. Por ejemplo, si tenemos una red en el aula a la que se conectan los alumnos con portátiles de forma inalámbrica cada día, sería suficiente concesiones de 12 horas, lo que permitiría liberar direcciones al término de cada jornada. Para los equipos de sobremesa del departamento de informática, que no se reponen frecuentemente, una concesión de 30 días podría ser adecuado.

¿Qué ocurre al reiniciar un equipo?

Cuando se reinicia un equipo que ha obtenido la concesión y esta no ha caducado todavía, el equipo cliente mandará un mensaje al servidor DHCP para confirmar si su configuración de red es válida. El servidor DHCP comprueba que la concesión es válida y está activa. Si es así, extiende el tiempo de concesión al valor establecido por defecto. Al recibir el mensaje de confirmación del servidor DHCP el equipo cliente podrá seguir utilizando la red con su configuración de red.

En el caso de que el servidor DHCP no estuviera disponible, el equipo cliente mantendrá activa su configuración hasta que termine el periodo de concesión.

9.3. Liberar una concesión.

El cliente puede devolver la dirección IP al servidor DHCP que se la concedió antes de que finalice el plazo de concesión, mediante DHCPRELEASE. Esta situación se podría dar cuando queremos cambiar el equipo de subred y queremos que la dirección IP que tenía asignada quede liberada inmediatamente.

El cliente manda su dirección IP en el mensaje DHCPRELEASE y no espera una respuesta, deja de utilizar esa dirección IP según termina de enviar el mensaje.

9.4. Actualizar parámetros de configuración.

Finalmente, es conveniente recordar que el servidor DHCP permite **actualizar los parámetros de configuración** de los equipos de la red cada vez que dichos equipos contacten con él. Por ejemplo, si cambia la dirección IP de un servidor DNS en la red, esta se actualizará a los equipos clientes cuando contacten con el servidor, para obtener una concesión, para renovar una concesión o cuando reinicien.

10. Tipos de mensajes DHCP.

A continuación se enumeran los mensajes DHCP utilizados habitualmente.

- DHCPDISCOVER. Mensaje de broadcast de un cliente para detectar los servidores DHCP existentes.
- DHCPOFFER. Mensaje de un servidor hacia un cliente con una oferta de configuración.
- DHCPREQUEST. Mensaje encapsulado en una trama de difusión que va de un cliente a un servidor para:
  - **Aceptar** la oferta de un servidor determinado y rechazar las otras.
  - **Confirmar** la exactitud de la información asignada antes del reinicio del sistema.
  - **Extender** el contrato de una dirección IP determinada.
- DHCPACK. Mensaje del servidor hacia un cliente para enviarle la configuración asignada excluyendo la dirección IP que ya fue aceptada.
- DHCPNACK. Mensaje del servidor al cliente para indicar que la dirección que tiene asignada es incorrecta o que el contrato ha expirado.
- DHCPDECLINE. Mensaje del cliente al servidor indicando que ha encontrado un problema con la dirección IP que le ha sido asignada.
- DHCPRELEASE. Mensaje del cliente al servidor para indicar que renuncia a la dirección otorgada y cancela lo que queda del contrato establecido anteriormente.
- DHCPINFORM. Mensaje del cliente para pedir más información de la que el servidor le ha enviado con DHCPACK.

11. Varios servidores independientes DHCP

En una misma red pueden coexistir varios servidores DHCP aunque no sea recomendable. Por ejemplo, se podrían configurar dos servidores DHCP en una red con muchos fallos para una mayor tolerancia a errores.

Cuando se produce esta situación los servidores DHCP no se comunican entre ellos para saber qué direcciones IP debe asignar cada uno. Es responsabilidad de los administradores que sus configuraciones sean independientes y consistentes, de manera que no puedan asignar la misma dirección IP a dos ordenadores distintos. Para ello, basta que los rangos de direcciones IP que puedan proporcionar no tengan direcciones comunes, o si las tienen, que estas sean direcciones reservadas.

Cuando existen varios servidores DHCP independientes trabajando simultáneamente, después de emitir un mensaje DHCPDISCOVER el cliente recibirá varios mensajes ofreciéndole diferentes configuraciones TCP/IP. El cliente

utilizará la primera que reciba e indicará en el mensaje DHCPREQUEST el servidor que ha elegido. Este mensaje se transmitirá a todos los servidores DHCP, con lo que el servidor elegido realiza la concesión y el resto libera las direcciones IP propuestas al cliente.

12. Dar servicio a varias redes.

Para que un servidor DHCP pueda atender a una red física (mismo dominio de difusión) tiene que estar conectado a esa red física. Si se dispone de varias redes interconectadas por routers en las que se quiere configurar el servicio DHCP tenemos dos opciones:

- Configurar un servidor DHCP en cada subred.
- Configurar un servidor DHCP desde una ubicación centralizada a varias subredes.

12.1. Un servidor DHCP en cada subred.

Esta opción supone un aumento del trabajo administrativo y del equipamiento necesario, ya que habrá que ubicar un servidor DHCP en cada subred individual.

12.2. Un servidor centralizado.

Si se quiere mantener un único servidor DHCP centralizado podríamos contemplar varias opciones:

- Conectar el servidor directamente a dichas redes.
- Que los enrutadores que interconectan las redes tengan la capacidad de retransmitir los mensajes del protocolo DHCP entre dichas redes.
- Instalar un agente de retransmisión DHCP en algún equipo y configurarlo para escuchar los mensajes de difusión utilizados por el protocolo DHCP y redirigirlos a un servidor DHCP específico.

¿Qué ocurre si el servidor DHCP recibe peticiones de varias subredes?

Si el servidor está atendiendo a diferentes subredes de la empresa, cuando reciba la petición identificará de qué subred proviene para poder darle una dirección IP válida para esa subred. Si teneos diferentes ámbitos para las distintas subredes, el servidor elegirá una dirección IP sin usar que corresponda con esa subred.

13. Agentes de retransmisión DHCP

Un agente de retransmisión DHC es un equipo o enrutador configurado para escuchar difusiones DHCP procedentes de clientes DHCP y, a continuación, retransmitir dichos mensajes a los servidores DHCP ubicados en distintas redes.

Existen dos tipos de agentes de retransmisión, aquellos que están integrados en routers y aquellos que funcionan en servidores.

Como el proceso de generación de concesiones DHCP se basa en las difusiones, si el servidor DHCP y el cliente están separados por un enrutador que no reenvía las

difusiones DHCP, el proceso de generación de concesiones DHCP no podrá realizarse y el cliente DHCP no recibirá la concesión de dirección IP del servidor DHCP.

Para solventar este problema, el agente de retransmisión DHCP permite que se a cabo el proceso de generación de concesiones entre el cliente DHCP y el servidor DHCP cuando ambos están separados por un enrutador.

El funcionamiento es el siguiente:

1) El cliente DHCP difunde un paquete DHCPDISCOVER.
2) El agente de retransmisión DHCP de la subred del cliente reenvía el mensaje DHCPDISCOVER al servidor DHCP mediante unidifusión.
3) El servidor DHCP emplea la unidifusión para enviar un mensaje DHCPOFFER al agente de retransmisión DHCP.
4) El agente de retransmisión DHCP difunde el paquete DHCPOFFER a la subred del cliente DHCP.
5) El cliente DHCP difunde un paquete DHCPREQUEST.
6) El agente de retransmisión DHCP de la subred del cliente reenvía el mensaje DHCPREQUEST al servidor DHCP mediante unidifusión.
7) El servidor DHCP emplea la unidifusión para enviar un mensaje DHCPACK a la subred del cliente DHCP.

El inconveniente de esta opción radica en que cada subred a la que sea necesario dar servicio DHCP necesitará de un servidor que funcione como agente de retransmisión.

La segunda opción consistirá en utilizar routers que tengan integrado un agente de retransmisión DHCP. Estos routers tendrán que ser adecuadamente configurados para que retransmitan los paquetes DHCP intercambiados entre cliente y servidor.

14. DHCP *Failover Protocol*

Cuando dos servidores DHCP trabajan en la misma red ambos mantienen una base de datos con sus concesiones y el estado de las mismas. Para evitar que una misma dirección IP sea asignada por ambos servidores, una solución consiste en que trabajen con distintos rangos de direcciones. Si ambos servidores quieren trabajar con el mismo rango de direcciones es necesario que puedan sincronizar sus bases de datos de concesiones. El protocolo DHCP *Failover Protocol* permite esta intercomunicación entre **dos servidores DHCP** que dan servicio en la misma red.

Windows Server ha incluido esta funcionalidad desde la versión 2008 R2, permitiendo que dos servidores DHCP puedan sincronizar la información de sus concesiones. Un servidor será designado servidor primario DHCP y otro servidor secundario DHCP. Cuando un equipo solicita su configuración IP, por defecto, el servidor primario le responderá. En caso de que este servidor falle será cuando el servidor secundario proporcione la configuración IP al equipo cliente. En esta configuración el servidor secundario, no otorga concesiones y solo recibe actualizaciones del servidor primario. Cuando detecta que no puede comunicarse con el servidor primario será cuando se active como servidor DHCP.

Este protocolo también se puede utilizar para realizar un balanceo de carga, de manera que el trabajo se reparta entre los servidores primario y secundario. En esta configuración ambos servidores contestarían a las peticiones de los clientes, lo que permitirá hacer frente a gran número de peticiones en un corto periodo de tiempo.

Trabajar con dos servidores sincronizados permite una fácil recuperación ante el fallo de alguno de los dos servidores. Si se pierden los datos de un servidor, el otro mantendrá su copia sincronizada con la que poder seguir funcionando con normalidad.

15. Seguridad.

El servidor DHCP puede ser un servicio vital para el funcionamiento de una red TCP/IP, sin embargo, este protocolo no incluye ningún mecanismo de autentificación, lo que produce que sea vulnerable a diferentes tipos de ataques:

- Suplantación del servidor DHCP. Servidores no autorizados podrían proporcionar información falsa a los clientes suplantando al servidor DHCP autorizado (**DHCP spoofing**).
- Denegación de servicio. Una técnica empleada consiste en agotar el rango de direcciones a asignar para así evitar que un cliente pueda obtener una configuración de red. El proceso es el siguiente, un cliente no autorizado solicita una dirección IP al servidor DHCP y una vez concedida, cambia su dirección MAC para pedir una nueva dirección IP, y así sucesivamente hasta agotar el rango de direcciones disponibles.
- "Hombre en medio". Un servidor no autorizado puede responder a un cliente que busca un servidor DHCP y otorgarle una dirección IP válida, pero darle como puerta de enlace su propia dirección IP. De esta forma, el cliente manda los paquetes al atacante, que después de procesarlos los reenvía al router para que el cliente no se dé cuenta del ataque. Esta tipo de ataque tiene más posibilidades de éxito cuando el servidor DHCP está alejado de los clientes.
- Clientes no autorizados podrían acceder a los recursos configurando manualmente su interfaz de red.
- Clientes no autorizados podrían realizar ataques para intentar congestionar al servidor DHCP.

En las redes de área local se pueden configurar los *switches* para protegerse de estos ataques mediante DHCP *snooping).* Tras activar esta función en el *switch* se declara de confianza el puerto por el que genera respuestas el servidor DHCP autorizado, siento todos los demás puertos no fiables. Si llegaran mensajes de otros servidores DHCP por cualquier otro puerto estos serían rechazados. De esta forma se pueden resolver los problemas de "hombre en medio" y DHCP *spoofing*.

También es interesante acceder a los ficheros de *logs* de los servidores DHCP para auditar posibles peticiones no autorizadas.

16. BOOTP

El protocolo BOOTP (Boot Strap Protocol) constituye un primer intento de configuración automática de red. Este protocolo de la capa de aplicación funciona sobre UDP y se puede considerar como un precedente de DHCP. Al igual que este, está basado en el modelo cliente/servidor.

Podemos afirmar que BOOTP se basa en un protocolo estático de configuración fundamentado en una **tabla estática establecida de antemano,** y en donde las asociaciones direcciones físicas-direcciones IP se establecen previamente y **manualmente** por el administrador.

Este protocolo es obsoleto, y ya no se usa en la actualidad.

17. PXE

Preboot eXecution Environment (PXE) (Entorno de ejecución de prearranque), es un entorno para arrancar e instalar el sistema operativo en computadoras a través de una red, de manera independiente de los dispositivos de almacenamiento de datos disponibles (como discos duros) o de los sistemas operativos instalados.

El protocolo PXE consiste en una combinación de los protocolos DHCP y TFTP con pequeñas modificaciones en ambos. DHCP es utilizado para localizar el servidor de arranque apropiado, con TFTP se descarga el programa inicial de bootstrap y archivos adicionales.

Para iniciar una sesión de arranque con PXE el firmware envía un paquete de tipo DHCPDISCOVER extendido con algunas opciones específicas de PXE al puerto 67/UDP (puerto estándar del servicio DHCP). Estas opciones indican que el firmware es capaz de manejar PXE, pero serán ignoradas por los servidores DHCP estándar. Es entonces donde entra en juego el servidor de arranque PXE, quien será el que ofrezca a los clientes los datos necesarios para la descarga de la imagen de arranque.

Para conocer más acerca de este protocolo puedes consultar el siguiente enlace.