Introducción al servicio DHCP

DHCP: Dynamic Host Configuration Protocol

- Servicio de configuración automática de red.
  - Simplifica el proceso de configuración de equipos.
  - Configura a clientes de diferentes SO.
- Se utiliza ampliamente:
  - Entornos domésticos.
  - Entornos empresariales.

Parámetros de red

Los **parámetros de red** que se deben configurar para que un equipo tenga conectividad son:

- Dirección IP y máscara.
- Gateway (Puerta de enlace).
- Servidor DNS.

La configuración se puede llevar a cabo de forma **manual** o **automática**.

La configuración manual también se conoce como **fija** o **estática**

Problemas de la configuración manual

- Hay que configurar cada uno de los equipos manualmente.
- Es posible que se cometan errores:
  - Errores tipográficos.
  - IPs duplicadas.
  - Etc.
- Los parámetros de configuración pueden cambiar con el tiempo. Esto supondría tener que reconfigurar cada equipo.
- A veces los equipos cambian con frecuencia de una subred a otra.
- Aumentan las **tarifas administrativas**.
- Por ello, es conveniente una **configuración centralizada y automatizada**, especialmente en redes medias o grandes.

Protocolo RARP (RFC903)

- Es un método diseñado para que las estaciones de trabajo sin disco encuentren dinámicamente su **dirección IP** a partir de su **dirección MAC**. Es el protocolo "contrario" del ARP (RFC 286), por el que a partir de una IP se obtiene la dirección MAC de un equipo.
- Limitaciones:
  - La dirección MAC tenía que ser configurada en la estación central.
  - Otros parámetros como la **máscara de subred** o **gateway** debían de ser configurados de forma manual.
  - El cliente utiliza como **dirección destino** una dirección **MAC de difusión**:
    - Una petición de este tipo no es enrutada.
    - Es necesario un servidor RARP por cada subred.
- El protocolo **Bootstrap** dejó obsoleto al RARP.

Protocolo BOOTP (RFC 951)

- Es un protocolo de red **UDP** utilizado por los clientes de red para obtener su **dirección IP** automáticamente.
- Permite a las estaciones de trabajo sin disco obtener una **dirección IP**.
- También permite obtener la localización de su **imagen de arranque**.
- Requería el uso de un **disquete** de arranque. Más tarde se integró en la **BIOS** de algunas tarjetas de red y placas para permitir el arranque desde la red.
- **BOOTP** reemplazó a **RARP**, que era un protocolo de la **capa de enlace**.
    - Introdujo la innovación de los **agentes de retrasmisión** : un servidor BOOTP central podía atender a hosts en muchas redes.
- Tiene más funciones, lo que permite obtener más información que la **IP**.

BOOTP: Funcionamiento del protocolo

1. El cliente determina su propia dirección MAC (escrita en una ROM).
2. Un cliente BOOTP envía su dirección en un datagrama UDP al servidor.
    - Si el cliente sabe la dirección del servidor o su dirección IP, debería de utilizarla.
    - En general los clientes no tienen datos de configuración IP completos.
    - Si el cliente no sabe su dirección IP usa **0.0.0.0**.
    - Si el cliente no conoce la IP del servidor usa broadcast **255.255.255.255.
    - El número de puerto es **67/UDP**.

BOOTP: Funcionamiento del protocolo

3. El servidor recibe el datagrama y busca la dirección MAC del cliente en su fichero de configuración, que contiene la dirección IP del cliente.
    - El servidor rellena los campos restantes en el datagrama UDP y lo devuelve al cliente usando el puerto destino **68/UDP**.
4. Cuando se recibe la respuesta el cliente obtiene su IP (permitiendo que responda a peticiones **ARP**) y comenzará su proceso de arranque (**bootstrapping**).

BOOTP: Funcionamiento del protocolo

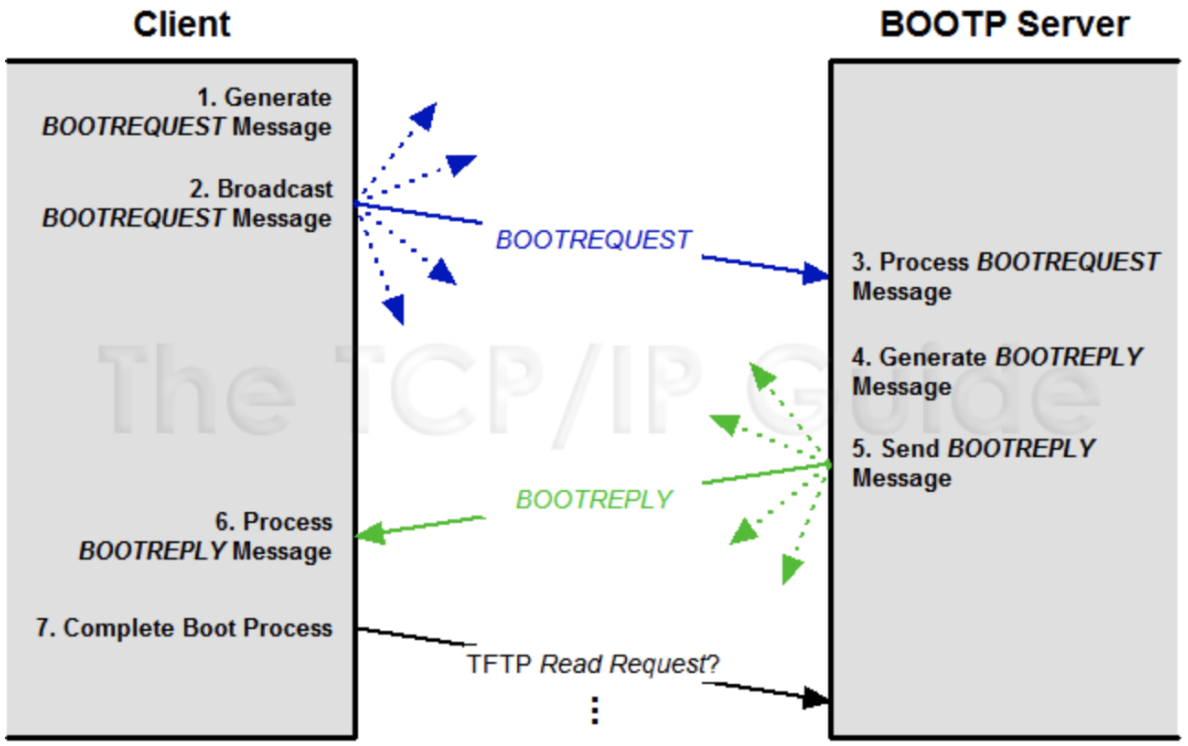


Figure 255: Boot Protocol Operation

The Boot Protocol uses a simple two-step message exchange consisting of a broadcast request and broadcast reply. After the client receives configuration information from the BOOTP server, it completes the bootstrapping process using a protocol such as TFTP.

Fuente: TCP IP Guide

DHCP (RFC 1541)

- DHCP fue desarrollado a partir de 1985 como extensión de BOOTP:
  - **BOOTP** requería **intervención manual** para completar la información de configuración en cada cliente.
  - BOOTP no proporcionaba un **mecanismo de recuperación de las IPs** en desuso.
- Es el estándar IP para simplificar la administración de la configuración IP de los hosts.
- Reduce la complejidad de trabajo **centralizando la administración**.
- Garantiza que los clientes utilizan una **configuración correcta** de los clientes.
- Puede asignar configuraciones en una o varias **subredes**.
- Recupera las direcciones IP en desuso (**más clientes**).

DHCP: Tipos de asignaciones de direcciones IP

1. Elegida dentro de un **rango de direcciones**.
2. **Concreta:**
    - Se utiliza en **equipos especiales** como los servidores.
    - Los equipos son identificados a través de su **dirección MAC**.

DHCP: Técnicas de asignación

1. **Asignación estática**: El servidor reserva una dirección IP en exclusiva para un cliente.
2. **Asignación automática**: El servidor asigna una IP dentro de las que pueda conceder de **forma permanente**.
    - El cliente mantiene esa IP mientras no **renuncie a ella**
    - Funciona bien en redes pequeñas.
    - Se produce un desaprovechamiento de recursos.
3. **Asignación dinámica**:
    - El servidor asigna una IP durante un **intervalo de tiempo limitado** (*lease time*).
    - Si el cliente desea mantener una concesión debe **renovarla**.
    - Si finaliza un tiempo de concesión sin una renovación, el servidor puede entregar la IP a otro cliente.

DHCP: Concesión de direcciones IP

Se utiliza un proceso en 4 pasos, que obtienen su nombre de los tipos de paquetes DHCP:

1. **Descubrimiento DHCP** (DHCP DISCOVER): El cliente trata de encontrar un servidor DHCP en la red y solicita una configuración.
2. **Oferta DHCP** (DHCP OFFER): El servidor hace una oferta de configuración al cliente.
3. **Aceptación DHCP** (DHCP REQUEST): El cliente acepta la oferta del servidor.
4. **Reconocimiento DHCP** (DHCP ACK): El servidor reconoce la solicitud y la confirma.

A partir de este momento, el cliente puede utilizar la configuración concedida.

1. Descubrimiento DHCP (DHCP DISCOVER)

- El cliente difunde un paquete **DHCP DISCOVER** para localizar un servidor DHCP en la red y solicitar una configuración.
    - Cuando inicia **TCP/IP**.
    - Cuando se le negó su concesión al tratar de renovarla.
- Si el cliente no obtiene oferta tras cuatro solicitudes, se autoconfigurará utilizando el protocolo **APIPA**, que lo dotará de conectividad local.
- Periódicamente difundirá un mensaje **DHCP DISCOVER** para tratar de obtener una configuración (cada 5 minutos).

2. Oferta DHCP (DHCP OFFER)

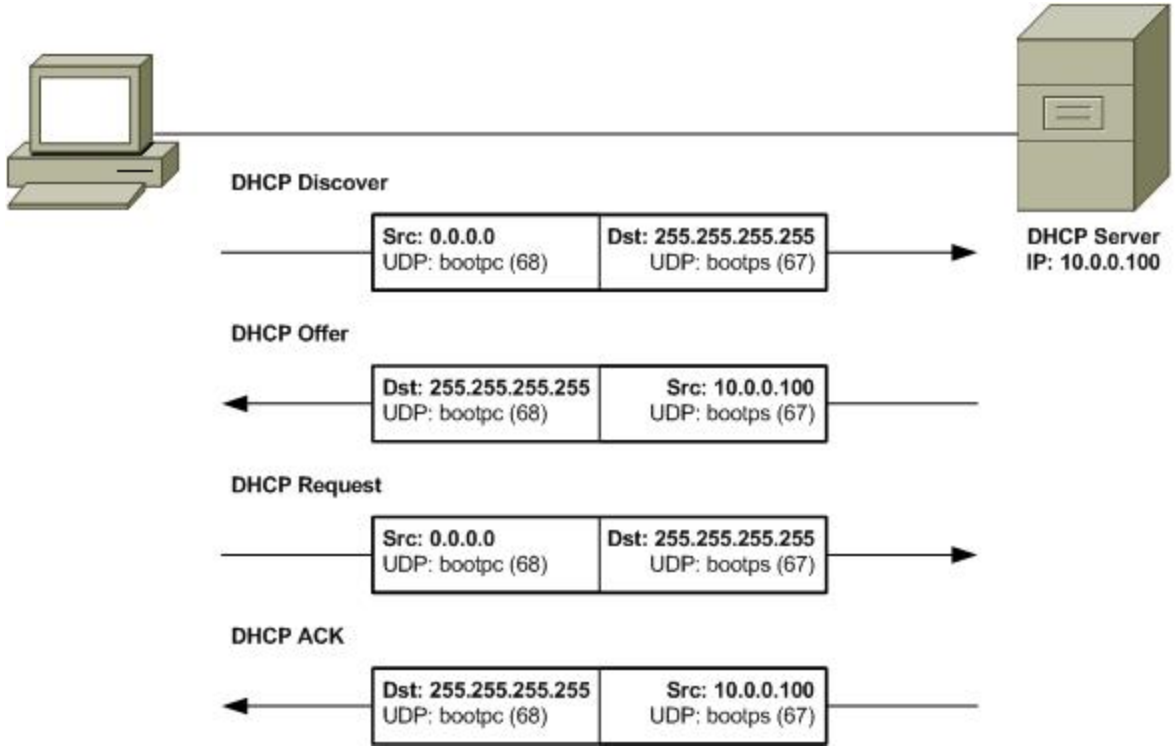
- El servidor difunde un paquete **DHCPOFFER** al cliente con una oferta **IP**.
- El servidor reserva la dirección IP y no se la concederá a ningún otro cliente.
- Es posible que el cliente reciba varias ofertas de varios servidores. Normalmente aceptará la primera.

3. Aceptación DHCP (DHCP REQUEST)

- El cliente difunde un paquete **DHCP REQUEST** para solicitar la configuración ofertada.
    - También se utiliza **DHCP REQUEST** para realizar la **renovación de una concesión**.
- El paquete **DHCP REQUEST** incluye la identificación del servidor cuya oferta el cliente aceptó.
    - Este paquete sirve como notificación de rechazo a otros servidores que hayan realizado una oferta.
    - De esta manera, los servidores pueden retirar su oferta y ofrecer la dirección a otro host.

4. Reconocimiento DHCP (DHCP ACK)

- El paquete **DHCP ACK** lo difunde un servidor para reconocer y finalizar la concesión de configuración.
- Contiene la información de una concesión válida: dirección IP y otros datos de configuración IP.
- El cliente inicializa su tarjeta de red con los datos facilitados por el servidor.
- Si el servidor envía un reonocimiento negativo **DHCP NAK**, el cliente deberá iniciar de nuevo el proceso de concesión.
    - Esto puede deberse por ejemplo a que la dirección IP ofertada está siendo usada por otro equipo.



Los **servidores DHCP** escuchan peticiones en el puerto **67/UDP**. Los **clientes** escuchan las respuestas de los servidores en el puerto **68/UDP**.

Fuente: Kikobeats - DHCP

Renovación de concesiones DHCP

- El cliente debe renovar su configuración antes de que termine el **intervalo de concesión** (*lease time*).
- En el caso de que no lo consiga, tendrá que iniciar de nuevo una solicitud DHCP.
- El cliente intentará renovar su concesión en cuanto alcanza el **50%** del tiempo de concesión.
- También intentará renovar su concesión cuando se **reinicie**.
- Para renovar, el cliente envía un paquete **DHCP REQUEST** directamente al servidor del que obtuvo la concesión.

Renovación de concesiones DHCP

Si **el servidor está disponible**:

1. **El servidor renueva la concesión**: Envía al cliente un paquete **DHCP ACK** con los parámetros de red actualizados.
2. **El servidor no renueva la concesión**: Envía al cliente un paquete **DHCP NAK**, lo que obliga al cliente a liberar la IP y obtener una válida.

Si **el servidor no está disponible**, el cliente continuará utilizando sus parámetros de configuración actuales.

- Pasado el **87,5%** del tiempo de concesión, el cliente difundirá un **DHCP DISCOVER** y aceptará concesiones de cualquier servidor.

Renovación de concesiones DHCP

Si en un reinicio de un cliente **ningún servidor responde a un DHCP REQUEST**, tratará de conectar con la puerta de enlace predeterminada configurada.

- En el caso de no tener éxito, dejará de utilizar la configuración obtenida.

Si la **concesión caduca**, el cliente deberá dejar de utilizar la configuración e iniciará el proceso de descubrimiento.

La concesión IP se puede **renovar manualmente** en el caso de que la configuración se deba actualizar de inmediato.

Mensajes DHCP

El protocolo establece los mensajes que pueden utilizar servidor y cliente para comunicarse.

1. DHCP DISCOVER
2. DHCP OFFER
3. DHCP REQUEST
4. DHCP ACK
5. DHCP NAK
6. DHCP DECLINE
7. DHCP RELEASE
8. DHCP INFORM

1. DHCP DISCOVER

- Es enviado por un cliente DHCP para solicitar que un servidor le envíe los datos de configuración.
- El mensaje es de **broadcast** por lo que llegará a todos los servidores de la red.

2. DHCP OFFER

- Es enviado por un servidor DHCP en respuesta a un mensaje DHCP DISCOVER.
- El servidor ofrece los parámetros de configuración.
- Antes el servidor comprueba de que la IP que va a ofrecer no está siendo utilizada en la red.
- Si se usa asignación manual, el servidor asigna al cliente la IP que tiene reservada.

3. DHCP REQUEST

- Es un mensaje que envía el cliente como respuesta a un **DHCP OFFER** o para **renovar una concesión**.
- El cliente informa al servidor que **acepta la oferta** y solicita que se le otorgue la configuración.
- Antes de enviar esta respuesta, el cliente comprueba que la **dirección IP** que se le ha ofrecido **no está siendo utilizada en la red**.
- Es un mensaje de difusión que informa a otros posibles servidores de que el cliente ya **acepta una oferta**.
    - Estos servidores pueden entonces liberar la concesión que tienen reservada.

4. DHCP ACK

- Es un mensaje que envía un servidor a un cliente en respuesta de un mensaje **DHCP REQUEST** para confirmar la concesión.
- El servidor informa al cliente de los parámetros de configuración y del tiempo de concesión.
- Cuando el cliente recibe este mensaje establece su configuración de red.

5. DHCP NAK

- Es un mensaje que envía un servidor a un cliente en respuesta de un mensaje **DHCP REQUEST**.
- El servidor **deniega la configuración** solicitada.
- Se puede dar en procesos de renovación, donde la configuración IP solicitada a renovar por el cliente ya está siendo usada o está fuera del ámbito de direcciones asignables por el servidor.
- El cliente debe comenzar el proceso de concesión de configuración.

6. DHCP DECLINE

- Es un mensaje que envía el cliente como contestación a un mensaje **DHCP OFFER**.
- El cliente detecta que la **dirección IP** ofertada ya se encuentra **en uso** en la red.

7. DHCP RELEASE

- Es un mensaje que envía el cliente DHCP al servidor para **dar por finalizada la concesión**.
- No es un mensaje obligatorio, pero de ser enviado, el servidor considerará liberada la dirección IP y podrá ofertarla.
- Los clientes pueden enviar este comando, por ejemplo, cuando se van a apagar.

8. DHCP INFORM

Es un mensaje que puede enviarle el cliente DHCP al servidor para solicitar parámetros opcionales de configuración o una actualización.

Parámetros asignados por DHCP

- Un cliente DHCP puede recibir de un servidor varios parámetros de red.
- Algunos de estos parámetros se consideran obligatorios.

Parámetros obligatorios:

- IP, máscara de subred, tiempo de concesión (lease time), tiempo de renovación (renewal time), tiempo de reconexión (rebinding time).

Algunos parámetros opcionales:

- Dirección IP del router por defecto, servidores DNS, nombre de dominio DNS, dirección de broadcast de la red, servidores SMTP, servidores NTP...

Agentes de reenvío (Agent Relay)

- Hasta ahora sería necesario que hubiera un servidor DHCP en cada red en la que haya clientes.
- Si hay varias subredes, es necesario utilizar un **agente de reenvío**.
- Los *agent relay* escuchan en una subred las peticiones de los clientes y las mandan al servidor, que se encuentra en otra red.
- Una vez el servidor conteste, el agente de reenvío remitirá la respuesta al cliente.
- De esta manera no es preciso contar con un servidor por subred.
- Generalmente el agente de reenvío estará implementado en un **router**, aunque también podría estar en un PC con varias tarjetas de red.

Configuración del agente de reenvío

Es necesario:

- Activar el **agent relay** en el dispositivo de encaminamiento.
- Indicar al agente cuál es la red cliente.
- Indocar al agente cuál es el servidor DHCP que va a otorgar concesiones.

DHCP Failover Protocol

- Es un método para permitir la comunicación entre dos servidores DHCP.
- Permite redundancia y balanceo de carga.
    - El servidor DHCP es un recurso crítico en la red.

Seguridad en DHCP

1. DHCP Spoofing
2. DHCP Starvation Attack
3. Rogue DHCP attack

DHCP Spoofing

- DHCP es un protocolo que simplifica la configuración de la red a los administradores.
- No utiliza ninguna forma de autenticación.
- Utiliza mensajes de tipo broadcast, por lo que cualquier equipo conectado puede recibirlos.
- Un atacante podría enviar una configuración maliciosa a un cliente.
    - Podría suplantar al servidor y enviar una oferta maliciosa.
    - Por ejemplo, podría enviar como parámetro de gateway la IP de su equipo, y así realizar un ataque **Man in the Middle**.
    - También podría dar lugar a un ataque de **DOS**.

DHCP Starvation Attack

- El atacante envía múltiples **DHCP REQUEST** con diferentes direcciones **MAC** falsificada (Mac Spoofing) en un breve periodo de tiempo.
- De esta forma puede acabar con el **pool** o grupo de direcciones asignables del servidor.
- El servidor no responderá a las solicitudes de los clientes legítimos porque no puede otorgarles una configuración.
- Este ataque prepara el escenario para que el atacante se haga pasar por el servidor **DHCP** y envíe mensajes falsificados para engañar a los clientes.

Rogue DHCP attack

- Tras realizar el ataque de **Starvation**, el atacante puede configurar su propio servidor DHCP falso.
- Así puede escuchar peticiones y responder con configuraciones maliciosas.
- Por lo general, intentará establecerse a sí mismo como el **servidor DNS** y como la **puerta de enlace** predeterminada para los clientes.

Redes domésticas

- En las redes domésticas LAN o WLAN, los routers asumen la función del servidor DHCP.
- Todos los dispositivos pueden convertirse en un servidor DHCP.
- El atacante puede conectar un portátil a una red WLAN y así controlar la asignación de direcciones.

DHCP Snooping

- Protege de actividades maliciosas y de fuentes de error:
    - Si se instala un nuevo router en la red, éste puede tener configurado un servidor DHCP y asignar direcciones inválidas.
    - En una empresa se puede dar si los empleados conectan sus dispositivos a la red sin conocimiento del administrador.
- El DHCP snooping es una función de seguridad de segundo nivel del modelo OSI.
- La función está integrada en el conmutador o switch, el cual conecta a los clientes con los servidores DHCP.
- Se trata de un protocolo que primero verifica toda la información DHCP que pasa a través del conmutador.
- Solo los paquetes aprobados que provengan de servidores de confianza se envían a los clientes.