- ¿Cómo asegurar que se dispone de una dirección única en la red?
- Establecimiento manual o automático
- ¿Problemas de compatibilidad por utilizarlo con distintos SO?
- Originalmente en RFC 1531 (y 1532) en el año 1993
- Se actualizó en RFC 2131 y 2132 en el año 1997
- ¿Y en IPv6? RFC 3315
- Hay diversas actualizaciones en otros RFCs

Protocolo BOOTP

- Bootstrap protocol
- RFC 951
- UDP
- UNIX primero pero también Windows
- Integrado en la BIOS de algunas tarjetas de red
- Funcionamiento similar a DHCP por el cual fue sucedido
- ¿Cómo funciona?
  - Un cliente BOOTP envía su dirección MAC en un datagrama UDP sobre el puerto 67 del servidor. El cliente usa como dirección IP (0.0.0.0) y como IP del servidor la dirección (255.255.255.255).
  - El servidor recibe el datagrama y busca la relación entre dirección MAC y dirección IP del cliente. El servidor entrega el nombre de un servidor TFTP y el nombre del archivo de configuración al cliente, además de una IP, usando el puerto UDP 68.
  - Cuando recibe la respuesta, el cliente BOOTP grabará su propia dirección IP (permitiendo peticiones ARP)
    El cliente solicita el archivo de configuración mediante protocolo TFTP

Un poco de historia...

- Microsoft introdujo DHCP en sus Servidores NT con la versión 3.5 de Windows NT a finales de 1994
- El Consejo de Software de Internet (ISC: Internet Software Consortium) publicó distribuciones de DHCP para Unix con la versión 1.0 del ISC DHCP Server el 6 de diciembre de 1997 y una versión (2.0) que se adaptaba mejor el 22 de junio de 1999. Se puede encontrar el software en la web de ISC (Internet Software Consortium)
- Otras implementaciones importantes incluyen:
  - Cisco: añadió un servidor DHCP habilitado en Cisco IOS 12.0 en febrero de 1999
  - Sun: añádió el soporte para DHCP, a su sistema operativo Solaris, en julio de 2001
- ...

Funcionamiento básico DHCP

- Implementado con arquitectura cliente/servidor propia de los protocolos de la pila TCP/IP
- El servidor escucha por el puerto 67 y el cliente por el 68 y utiliza como protocolo de transporte UDP
- El protocolo DHCP permite tres métodos de asignación de direcciones IP que se pueden utilizar de forma simultánea
- La asignación se produce gracias a un intercambio de mensajes entre el cliente y el servidor de manera similar a lo que ocurre con BOOTP

2. Funcionamiento DHCP

¿Cuáles son los 3 métodos de asignación de direcciones?

- **Asignación estática:** Consiste en que el administrador de la red configura el servidor DHCP para que asigne una IP fija a determinados equipos. Esto es posible gracias a que los clientes DHCP cuando hacen una solicitud de IP, se identifican (MAC u opción de identificación de cliente -client identifier-), lo que permite la asignación de una IP específica.
- **Asignación dinámica:** Con este método, el servidor DHCP dispone de uno o varios rangos (pools) de IPs (al menos uno por cada segmento de red por el que se atienden peticiones de clientes), y cuando recibe una solicitud, éste selecciona una del pool adecuado y la asigna con un tiempo de alquiler o concesión (lease time), tiempo que se podrá prorrogar o, en caso contrario, el cliente debe dejar de usar la IP, y comenzar un proceso de nueva solicitud.
- **Asignación automática:** La especificación del DHCP habla de este método, a través del cual el servidor DHCP asigna una IP como en la asignación dinámica, pero de forma permanente. Muchos servidores no implementan este método, tal es el caso del servidor de ISC (es el que utilizaremos) y de Microsoft. En estos casos, este comportamiento puede simularse asignando mucho tiempo de alquiler, que puede llegar hasta 232-2 segundos (> 100 años).

¿Cómo se produce la concesión de dirección?

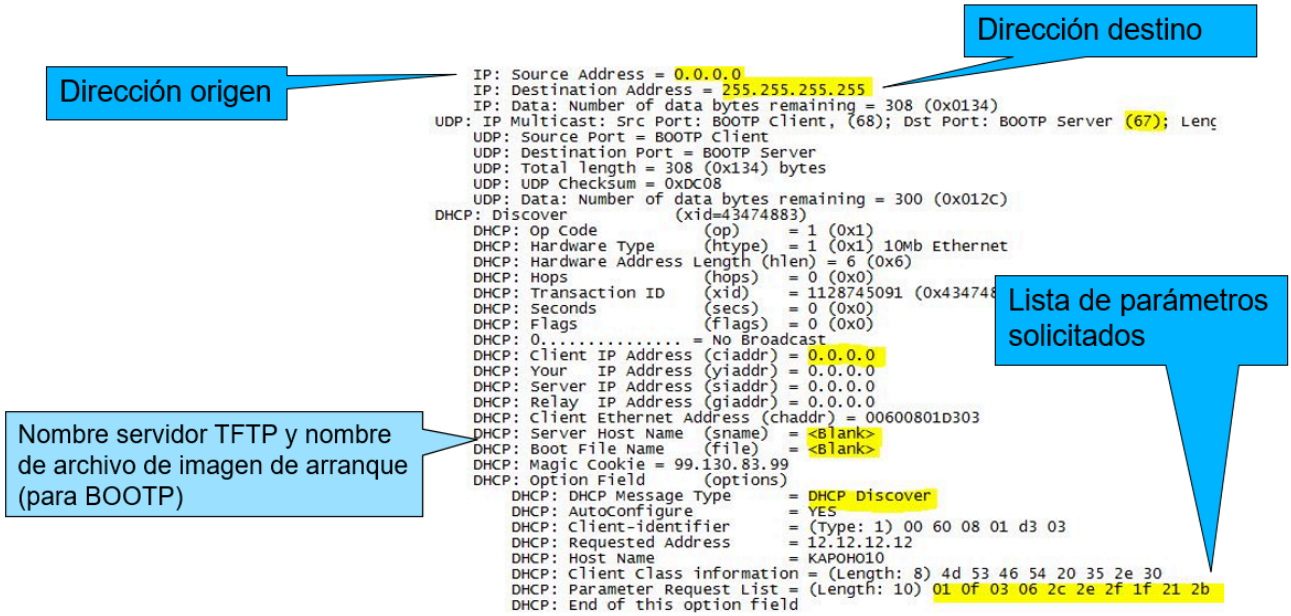
- Cuando el cliente se conecta a la red necesita contactar con un servidor DHCP y conseguir de él una configuración de red. Para ello envía un mensaje de difusión (DISCOVER) que interroga a los potenciales servidores disponibles. Cuando un servidor DHCP recibe este mensaje responde con otro mensaje de difusión (OFFER) con el que se identifica y ofrece una configuración de red

(incluyendo dirección IP) apropiada para el segmento de red en que el cliente se encuentra. En dicho mensaje se incluye la dirección MAC del cliente, lo que le permite reconocerse como destinatario del mensaje.

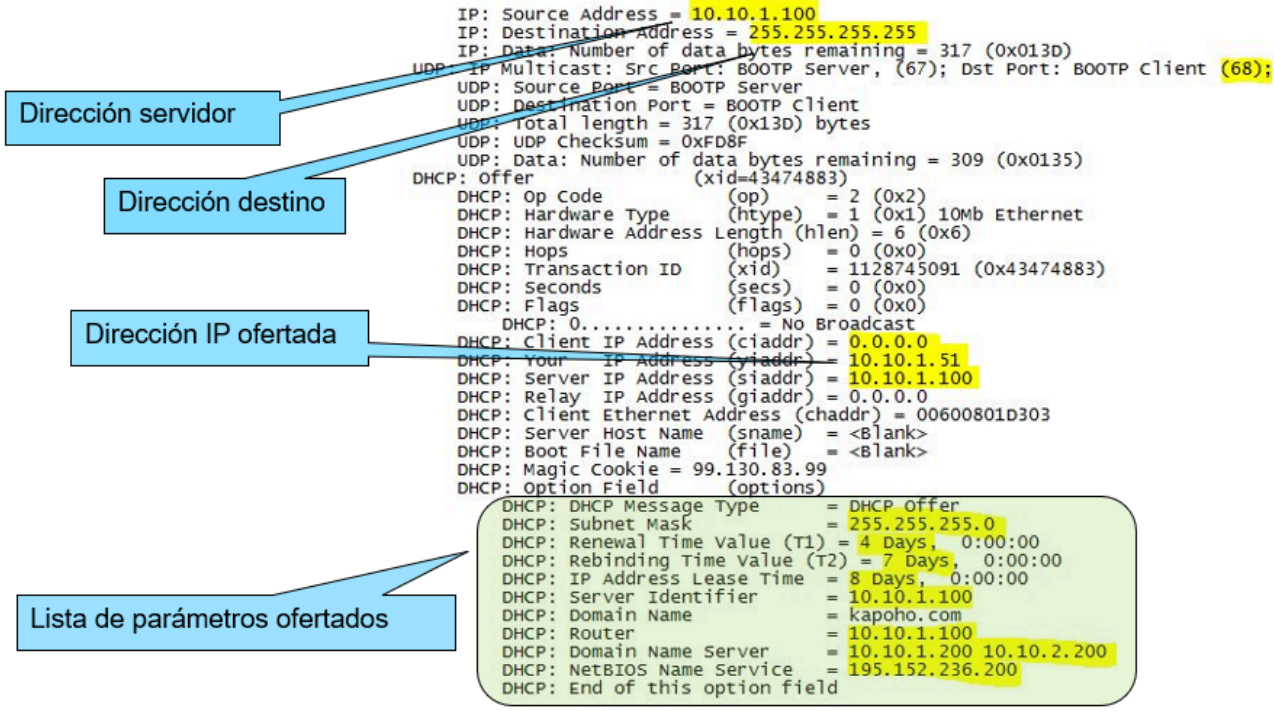
- Una vez la oferta llega al cliente un nuevo mensaje de difusión es enviado por el cliente (REQUEST) donde se solicitan tanto una IP como el conjunto de parámetros de red ofertados por el servidor (se trata de un mensaje necesario que se entiende si se dispone de más de un servidor DHCP que atienda al mismo segmento de red, generalmente se atiende el primero que llega).
- Si el mensaje anterior llega a tiempo al servidor, éste registrará la reserva para el cliente en cuestión, incluyendo el tiempo de concesión o alquiler. Por último se envía un cuarto mensaje de difusión al cliente de aceptación (ACK) que hace que el cliente se configure con los parámetros e IP para su uso.

Ejemplos de mensajes:

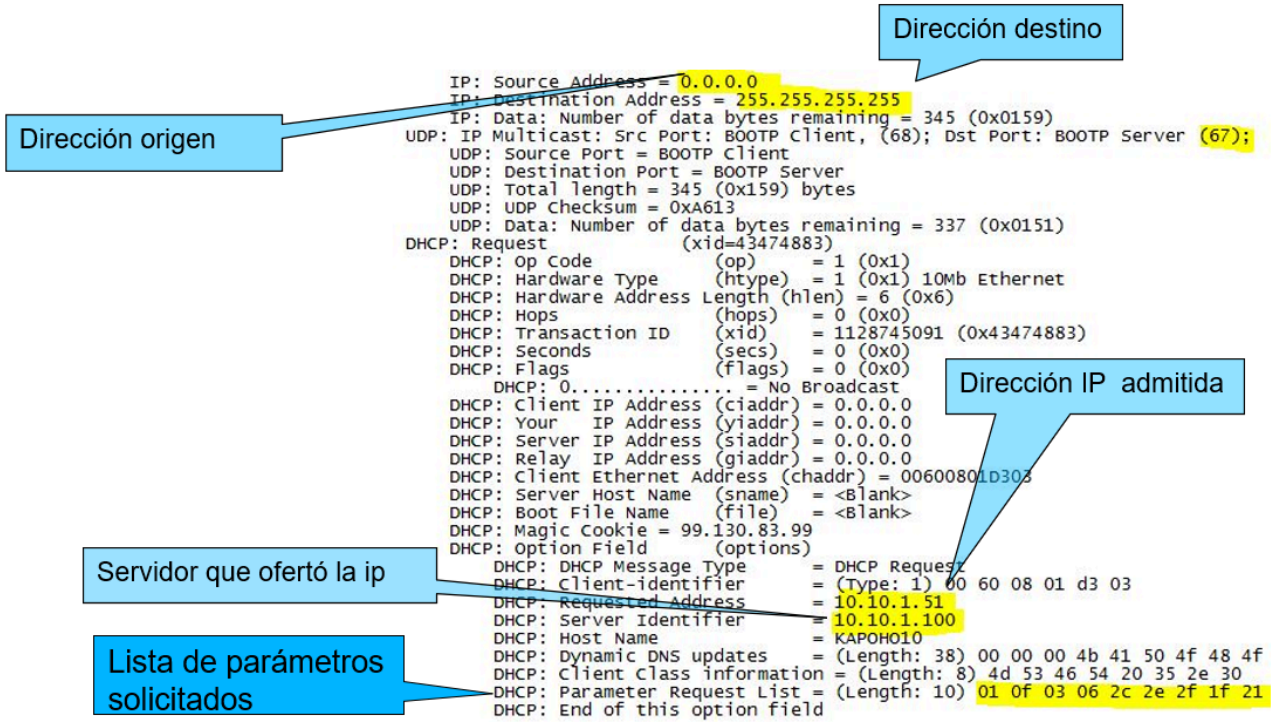
- **Ejemplo de mensaje DHCPDISCOVER:**



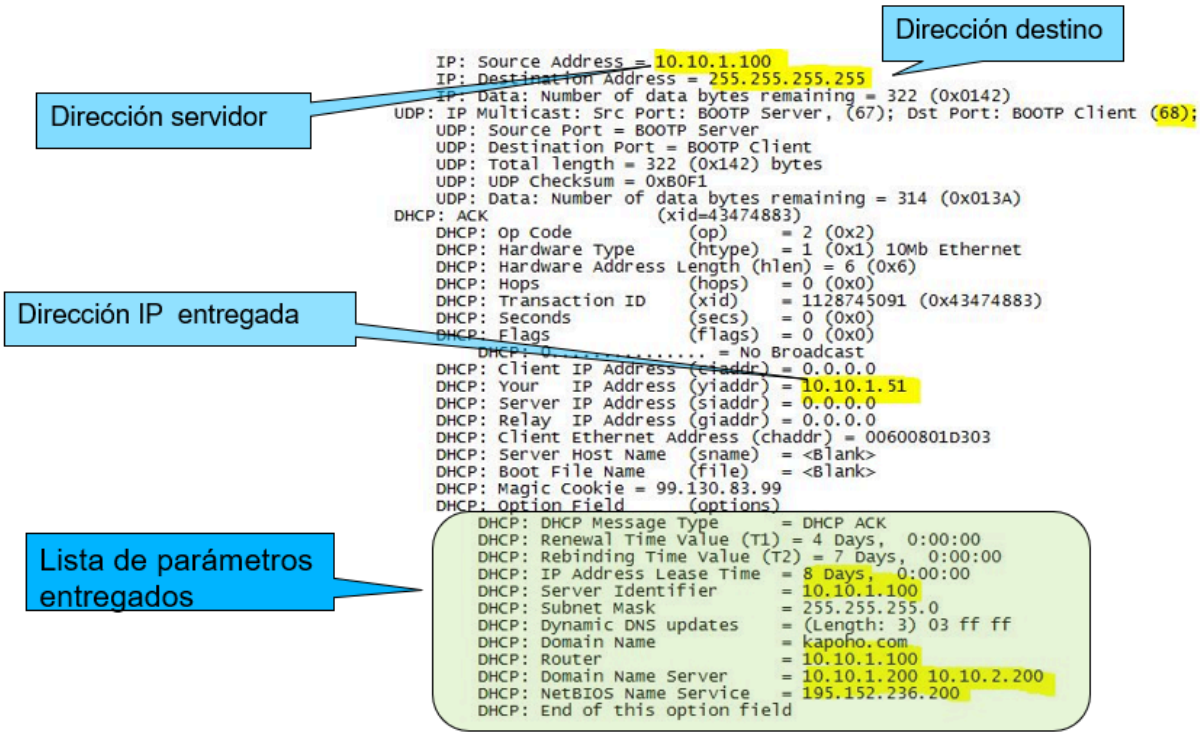
- **Ejemplo de mensaje DHCPOFFER:**



- **Ejemplo de mensaje DHCPREQUEST:**



- **Ejemplo de mensaje DHCPACK:**



3. Práctica 0

Requisitos:

- Haber leído y entendido los puntos anteriores sobre DHCP
- **Durante todo el proceso de la práctica deberán hacerse capturas de imagen de cada uno de los pasos dados así como capturas y almacenaje de los paquetes de wireshark. Algunos de ellos serán solicitados por el profesor una vez concluida la práctica.**

Antes de empezar:

- Sustituye el valor 'XX' por tu número de puesto asignado que venimos utilizando
- Toma nota de todo lo que vayas haciendo, incluyendo errores y soluciones sobre los mismos, así como capturas

Pasos:

1. Puesto que nuestra máquina bookwormXXb dispone de una configuración de red en el adaptador enp0s3 proporcionada por un servidor DHCP debe haber algún cliente ligado a ese servicio corriendo en nuestra máquina. Si utilizas el la aplicación 'lxtask' invocado desde consola como root (y mirando todas las tareas, no solamente las de root) podrás observar, entre los procesos, alguno ligado a DHCP. ¿De qué proceso se trata?
2. Nuestro cliente DHCP puede funcionar de diversas maneras, de hecho hemos matizado la configuración en alguna de nuestras configuraciones de systemd-networkd para evitar el uso del servidor de nombres proporcionado por el servicio DHCP en las prácticas de DNS. Este funcionamiento está ligado a la configuración que tenga.
    1. ¿Dónde está almacenada dicha configuración?
    2. ¿Hay alguna configuración por defecto?
    3. ¿Qué parámetros de la configuración de cliente podríamos modificar?
3. ¿Cómo podemos visualizar los paquetes intercambiados por nuestro cliente DHCP instalado en el servidor y el servidor DHCP del colegio o de casa?
    1. Puedes arrancar Wireshark, capturar paquetes en la interfaz adecuada, filtrar por DHCP para mayor comodidad y provocar el intercambio de mensajes reiniciando los servicios de red. Observa los mensajes intercambiados y extrae conclusiones sobre si son de unidifusión o de difusión tanto en capa de enlace como en capa de red.
    2. ¿Ha cambiado el proceso que se encarga del cliente dhcp?
    3. ¿Cuál es el proceso padre?
    4. Compara los mensajes de ejemplo dados con los tuyos propios y extrae conclusiones en cuanto a semejanzas y diferencias.
4. ¿Qué clientes DHCP tenemos en los equipos clientes LinuxXX y WindowsXX cuando tienen habilitado el adaptador que recibe una configuración de red de manera automática? Repite los apartados 1 y 2 para los sistemas LinuxXX y WindowsXX

NOTA: Recuerda que los registros log del servidor se pueden localizar utilizando `journalctl`. Puedes usar grep para hacer búsquedas concretas de texto y parámetros de tiempo con `--since=` y `--until=` para acotar la búsqueda además de otros muchos que puedes encontrar en la página de ayuda de `journalctl.`

4. Profundizando en el funcionamiento

¿Cómo se presenta un cliente ante el servidor?

Es importante conocer que el cliente DHCP se presenta ante el servidor incluyendo información identificadora en los mensajes que envía, que puede ser de dos tipos:

- La dirección MAC de su tarjeta de red.
- Una opción denominada 'client identifier', que puede contener texto (con esta opción se independiza de la tarjeta de red).

Si por alguna razón la identificación de cliente de varios clientes fuera la misma el servidor los confundiría

¿Qué ocurre cuando un equipo se reinicia después de haber recibido una concesión de dirección IP por parte de un servidor DHCP?

- Cuando un equipo se reinicia, recupera su última configuración de red e intenta confirmar que puede utilizarla mandando un mensaje al servidor DHCP con todos los parámetros de red (REQUEST). Tras esto, el servidor comprueba si la IP puede utilizarla el cliente (puede haber sido asignada a otro cliente, el cliente puede haber sido movido de segmento de red, etc.), y en caso afirmativo, se lo confirma con un mensaje de aceptación (ACK).
- Existe la posibilidad de que el requerimiento sea rechazado y el cliente tenga que empezar el proceso desde el inicio (descubriendo servidores), como si no hubiese tenido nunca una IP. Éste caso puede ocurrir cuando un equipo se apaga en un segmento de red y se enciende en otro, de modo que el cliente intenta confirmar la configuración que tenía en el antiguo segmento de red y el servidor, al comprobar que está en un segmento distinto, rechaza la propuesta y el cliente comienza de nuevo desde el principio.
- En el caso anterior, si el cliente no recibiera respuesta del servidor, la decisión del cliente es la de configurarse con los antiguos parámetros de red que tenía.

Recordando...

Cuando un cliente se inicia lo hace en un estado denominado INIT. En este caso el cliente y servidor suelen intercambiar los mensajes ya vistos en el apartado anterior:

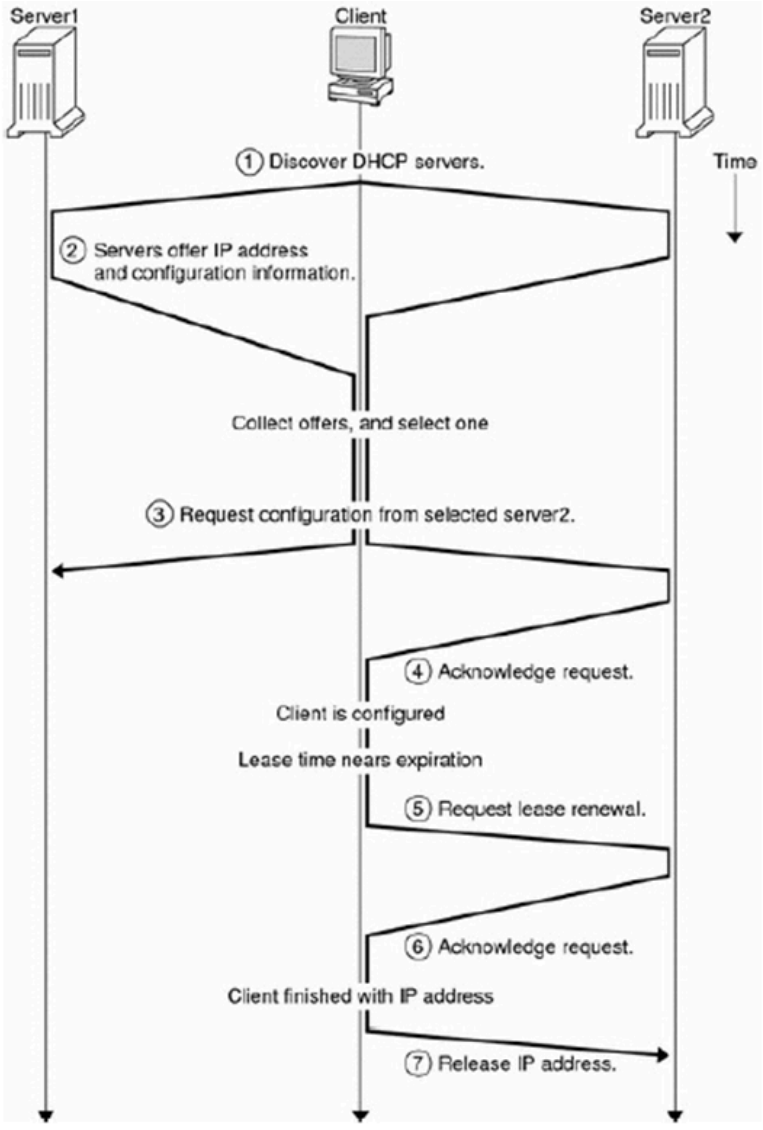
1. Mensaje DHCPDISCOVER: El cliente difunde (broadcast) un mensaje DHCPDISCOVER, y el mensaje se entrega a todos los servidores DHCP en el mismo segmento de red del cliente (este mensaje también es recibido por los agentes de retransmisión del segmento de red del cliente, si existen, y se reenvía a otros servidores DHCP situados en segmentos de red distintos al del cliente).
2. Mensaje DHCPOFFER: Después de que el servidor recibe el mensaje DHCPDISCOVER desde el cliente, encuentra una dirección para asignar al cliente y la pone en un mensaje DHCPOFFER. El servidor también incluye en este mensaje otros parámetros de configuración, según lo definido por el archivo de configuración del servidor. Después de que el servidor ha completado el

mensaje DHCPOFFER, envía el mensaje de vuelta al cliente como difusión (algunas implementaciones del DHCP lo hace en modo unicast en capa de enlace).

3. Mensaje DHCPREQUEST: Después de que el cliente recibe el (los) mensaje(s) DHCPOFFER, envía un mensaje DHCPREQUEST de difusión con los datos de la oferta elegida para que el servidor la confirme. Entre estos datos va la dirección del servidor elegido.
4. Mensaje DHCPACK: Después de recibir el mensaje DHCPREQUEST, el servidor comprueba la dirección y los parámetros de configuración requeridos para asegurar que la dirección todavía está disponible y los parámetros son correctos. Registra la dirección asignada y envía el mensaje DHCPACK para que el cliente se configure definitivamente. El cliente cuando recibe este mensaje y se configura, también registra localmente los valores de la concesión. En el caso de que el servidor hubiera asignado la IP a otro cliente antes de recibir el mensaje DHCPREQUEST del primero, se le envía al cliente el mensaje DHCPNACK, rechazando el requerimiento y el cliente vuelve de esta forma al estado INIT. Este mensaje es de tipo broadcast, pero también, igual que sucede con el mensaje DHCPOFFER, algunas implementaciones del servicio DHCP usan tráfico unicast en capa de enlace.

El diálogo se amplia...

Observa en la siguiente figura cómo se produce el intercambio inicial y las primeras renovaciones:

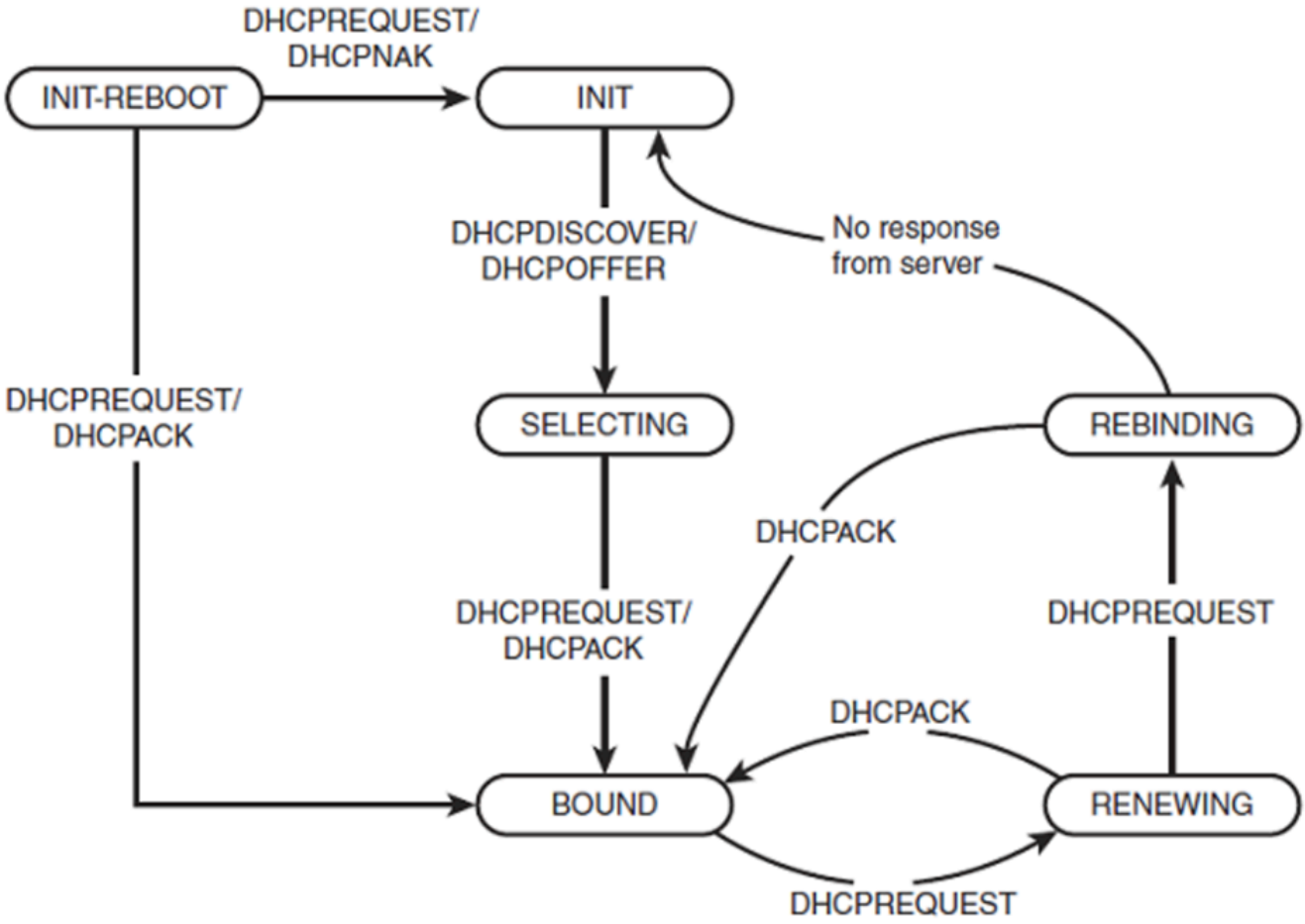


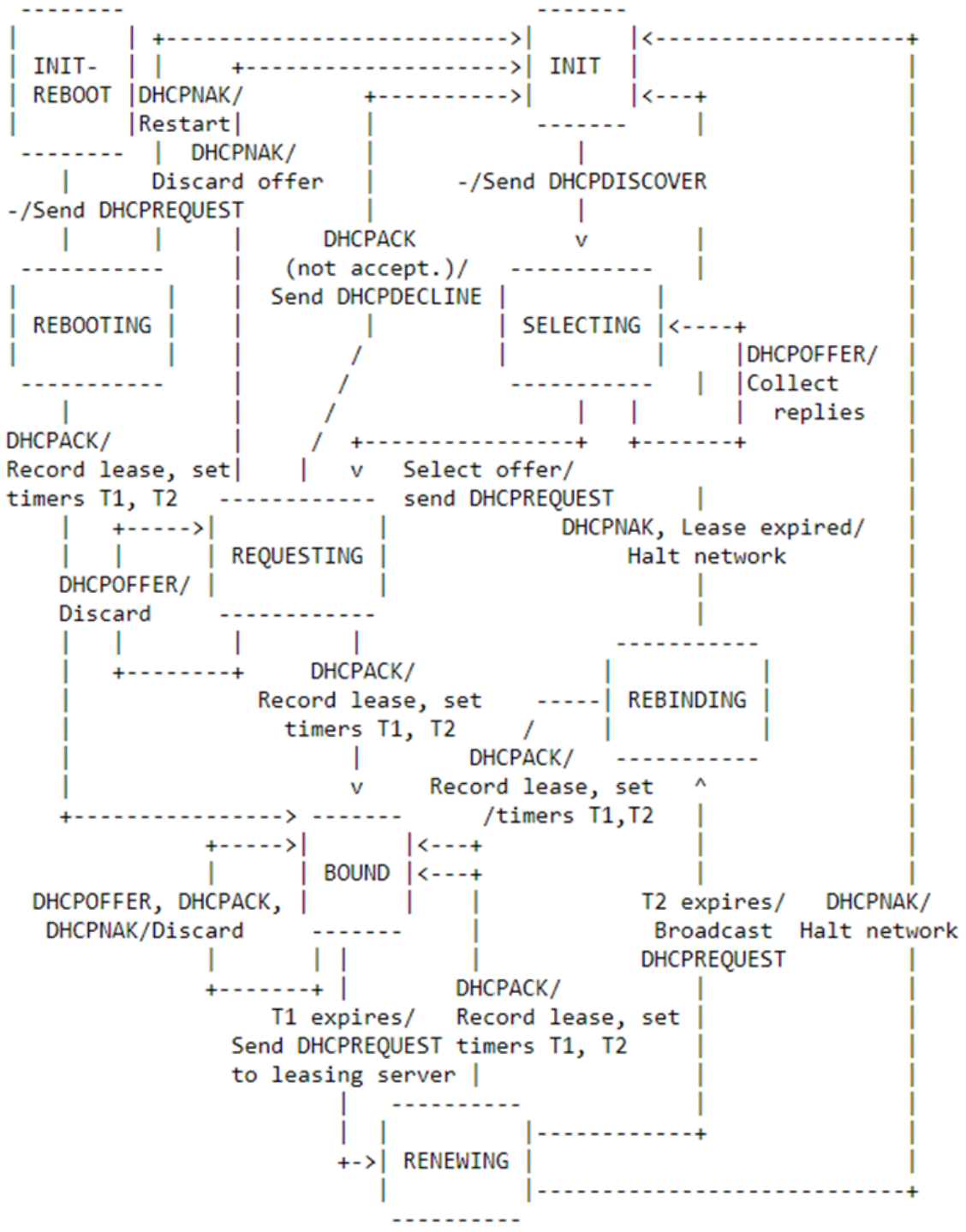
Si un cliente permaneciera en las mismas condiciones y el servidor también se irían produciendo renovaciones de IP una tras otras, sin más que intercambiando mensajes DHCPREQUEST y DHCPACK. Pero no siempre es así, de hecho hay otros mensajes que permiten un diálogo más "profundo" entre cliente y servidor:

- DHCPDECLINE: Mensaje enviado para indicar al servidor que la IP asignada ya está en uso.
- DHCPRELEASE. Mensaje para notificar la liberación de la IP asignada y terminar por tanto el alquiler de la misma.
- DHCPINFORM: Mensaje para consultar los parámetros de configuración local.
- DHCPRENEW: Mensaje para notificar la renovación de la IP asignada durante el tiempo acordado.
- DHCPNAK: Mensaje del servidor para indicar que la dirección asignada no es válida o que el contrato ha finalizado. Debe volver a comenzar el proceso.

Diagrama de estados

La forma concreta en que se producen las operaciones viene determinada por un diagrama de estados que aparece en el RFC 2131 y que se puede ver en las siguientes figuras. La segunda de ellas es la original mostrada en el RFC mencionado:


DHCPREQUEST/
DHCPNAK
INIT-REBOOT
INIT
DHCPDISCOVER/
DHCPOFFER
No response
from server
DHCPREQUEST/
DHCPACK
SELECTING
REBINDING
DHCPACK
DHCPREQUEST/
DHCPACK
DHCPREQUEST
DHCPACK
BOUND
RENEWING
DHCPREQUEST



¿Cómo interpretamos el diagrama de estados cuando se confirma una IP tras un reinicio?

- Cada vez que se reinicia un cliente, éste comprueba si tiene registrada la dirección IP con un contrato de arrendamiento que aún no haya caducado y en caso afirmativo, se pasa al estado INIT-REBOOT e intenta confirmar que su dirección sigue siendo válida con los siguientes mensajes:
  1. Mensaje DHCPREQUEST: El cliente envía la dirección IP para ser confirmada en un mensaje DHCPREQUEST de difusión, el cual es recibido y comprobado por todos los servidores DHCP que están configurados en el segmento de red al que está conectado el cliente. Esta dirección podría no ser válida si el cliente se ha cambiado de segmento de red o si el administrador de la red ha decidido cambiar el direccionamiento del segmento de red, por ejemplo.
  2. Mensaje DHCPACK: Cuando el servidor recibe el mensaje DHCPREQUEST, extrae la dirección solicitada por el cliente y verifica que la dirección es válida y puede utilizarla. Entonces el servidor responde con un mensaje DHCPACK, donde van todos los parámetros de configuración que debe usar el cliente para configurarse. Si el cliente no recibiera respuesta, éste se configurará con la antigua IP siempre que el alquiler no haya expirado.
- Algunos clientes DHCP, como por ejemplo el ISC DHCP Client, cuando se para el servicio al apagar el ordenador, envían un mensaje DHCPRELEASE, por lo que liberan su IP y cuando se reinicia el equipo comienzan en el estado INIT enviando un mensaje DHCPDISCOVER. Este comportamiento no lo tienen los clientes DHCP de Microsoft

¿Cómo interpretamos el diagrama de estados cuando se produce la ampliación de la concesión de la IP?

- El servicio DHCP establece mecanismos para que un cliente pueda extender en el tiempo el contrato de arrendamiento de su IP antes de que éste expire y tenga que dejar de usarla.

- Un cliente DHCP amplía su contrato de arrendamiento mediante el envío de un mensaje unicast al servidor que le concedió la IP, solicitando más tiempo de alquiler. La solicitud de prórroga se envía en un mensaje DHCPREQUEST, y el cliente puede pedir el tiempo que desee. En este punto, el servidor DHCP comprueba que puede renovarla, decide la nueva duración de la extensión de la concesión y envía al cliente en un mensaje DHCPACK unicast el nuevo tiempo de alquiler. El servidor puede no extender el tiempo o incluso ignorar la solicitud.
- Un cliente DHCP se dice que está en el estado de RENEWING cuando comienza el proceso de extensión del contrato de alquiler de su IP, y este proceso lo puede realizar cuantas veces lo necesite.
- Tanto el servidor como el cliente, guardan los nuevos tiempos para un uso posterior. Estos tiempos se dan en segundos y son tres:
  - El tiempo total del alquiler.
  - El tiempo tras el cual se comenzará el proceso de renovación. Se le llama T1. Algunos servidores no suministran este tiempo y el cliente lo establece al 50% del tiempo total de la concesión.
  - El tiempo transcurrido el cual el cliente vuelve a intentar renovar la IP cuando tras el primer intento no ha recibido respuesta del servidor. Se le llama T2 y al igual que con T1, algunos servidores no lo suministran y el cliente lo establece, en este caso, al 87.5% del tiempo total de la concesión.
- Se dice que el cliente entra en el estado de REBINDING cuando estando en el estado de RENEWING, éste no ha recibido respuesta del servidor y han transcurrido T2 segundos desde que comenzó el último contrato de arrendamiento. En este caso, el mensaje DHCPREQUEST es de tipo broadcast y no unicast, con el objetivo de contactar con todos los servidores DHCP y ver si alguno puede renovarle la concesión (podría suceder que el servidor hubiera cambiado de IP).
- La respuesta del servidor en estos casos, también es con un mensaje DHCPACK unicast.

¿Cómo interpretamos el diagrama cuando se produce la conclusión de la concesión o un cambio de segmento de red que hace que nuestro servidor sea otro?

- Si un cliente no recibe respuesta de un servidor para renovar su concesión antes del vencimiento del contrato de arrendamiento, el cliente debe dejar de usar su dirección IP y volver al estado INIT, cortándose la comunicación por red hasta obtener una nueva IP.
- Cuando un cliente se cambia de segmento de red, al encenderse, se produce el siguiente intercambio de mensajes:
  - Mensaje DHCPREQUEST: Este mensaje se produce en el reinicio del equipo cliente (estado INIT-REBOOT), es broadcast y al llegar al servidor del nuevo segmento, éste comprueba que la IP que se le solicita pertenece a otro segmento, por lo que la rechaza (si está configurado como authoritative)
  - Mensaje DHCPNACK: Con este mensaje, el servidor notifica al cliente que la IP que solicitó no es válida, con lo que el cliente descarta la IP y pasa al estado INIT, comenzando el proceso de cuatro mensajes que ya hemos visto.

¿Qué motivos hacen que un cliente no tenga un dirección IP válida?

- Es nuevo y no ha recibido nunca una IP.
- El tiempo de concesión de la anterior IP ha expirado
- Un servidor DHCP le dice al cliente que su dirección no es válida (con un mensaje DHCPNACK), por ejemplo porque se haya movido de segmento de red.

En estos casos, el cliente pasa al estado INIT porque no tiene una dirección válida

5. Servidor Kea

¿Por qué elegir Kea?

- ISC distribuye dos distribuciones de servidores DHCP completas, de código abierto y basadas en estándares: Kea DHCP e ISC DHCP.
- Kea incluye todas las funciones más solicitadas, es mucho más reciente y está diseñado para un entorno de red más moderno.
- ISC anunció el fin del ciclo de vida del antiguo sistema ISC DHCP en 2022 (sería posible migrar implementaciones de servidores DHCP al servidor Kea).

¿En qué se diferencia el servidor DHCP de Kea del antiguo DHCP de ISC?

- Diseño de componentes modular, extensible con módulos Hooks.
- La distribución Kea incluye demonios independientes para un servidor DHCPv4, un servidor DHCPv6 y un módulo DNS dinámico (DDNS).
- Muchas funciones opcionales se habilitan con módulos Hooks cargados dinámicamente, que solo es necesario ejecutar si se están utilizando (podríamos crear los nuestros en C++)
- Kea utiliza un archivo de configuración JSON que puede modificarse remotamente mediante comandos y recargarse sin detener ni reiniciar el servidor (una operación que podría tardar bastante con DHCP de ISC).
- Kea admite do sbases de datos: MySQL y PostgreSQL, lo que permite que varios servidores Kea compartan los datos con ventajas evidentes:
  - Una base de datos de arrendamiento compartida puede ofrecer una estrategia alternativa para la resiliencia.

  - Una base de datos de reservas de host permite la gestión remota de reservas de host a través de 'Stork' y permite que varios servidores Kea utilicen una base de datos de reservas de host compartida.
  - Una base de datos de configuración permite el uso de algunos elementos de configuración, como subredes, en varios servidores Kea. Esto facilita enormemente la adición de nuevos servidores Kea.
  - Panel gráfico web llamado Stork.
- Kea es multiproceso y, al configurarse para un funcionamiento eficiente , puede ofrecer un rendimiento suficiente para entornos a gran escala con contratos de arrendamiento cortos, que constituyen el escenario más exigente.

¿Código abierto?

- Los demonios principales de Kea son de código abierto y se comparten bajo la licencia MPL2.0.
- Kea se desarrolla abiertamente en el GitLab de ISC.
- Kea funciona en la mayoría de las plataformas Linux y Unix, así como en macOS.
- Se puede compilar desde cero, o utilizar el repositorio de paquetes precompilados para los sistemas operativos más populares, entre ellos Debian.

¿Qué voy a instalar en mi servidor BookWormXXA?

- ¿Qué versión de kea se instalará con nuestra versión de Debian?
- ¿Cómo instalo Kea? ¿Podemos simular su instalación pero no llevarla a cabo?
- ¿Qué paquetes se van a instalar? ¿Alguno sugerido?
- Una vez esté instalado, ¿Va a tener habilitado el arranque automático? Y si es así, ¿Estará arrancado?
- ¿En nombre de qué usuario se arrancará el servicio? ¿Podemos ver el usuario en algún sitio? ¿y el grupo?
- ¿Qué es el formato JSON? ¿Qué formas hay de validar un archivo JSON?
- ¿Cómo puedo hacer una copia de seguridad de las configuraciones del servidor?

6. Práctica 1

Práctica 1 - DHCP

Requisitos previos:

- Servidor BookWormXXA correctamente configurado
- Cliente LINUXXX correctamente configurado. Para ello es necesario arrancar la máquina cliente previamente y modificar la configuración de red para que el adaptador que está en la red interna esté en DHCP en lugar de STATIC.

Instalación y revisión del estado de Kea:

- Instala el servidor de Kea utilizando apt. Observa qué paquetes se van a instalar. Puedes instalar también la documentación.
- Revisa si el servicio está arrancado utilizando el comando adecuado.
- Revisa el archivo de configuración general de Kea: /etc/kea/kea-dhcp4.conf.
- Haz copia de seguridad de ese archivo de configuración original.

Configuración básica del servidor:

1. Sustituye el archivo de configuración (del que has hecho copia de seguridad) por uno con la configuración que se indica a continuación. Parte del archivo que aparece en Sallenet y que lleva formuladas preguntas sobre las que deberás indagar y reflexionar:
    1. Poder escuchar en la interfaz conectada a la red interna
    2. Para que todas las direcciones IP que aparecen pertenezcan a tu red (10.0.128+XX.0/24)
    3. Para que otorgue un rango de direcciones IP entre la 220 y la 239 de las anteriores
    4. Para que se configure un tiempo por defecto de concesión de 90 segundos, un máximo de 180 y un mínimo de 60
2. Valida el formato del archivo en un validador antes de arrancar/recargar el servicio.
3. Inicia el servicio y comprueba que empieza a correr ("active (running)"), sin mensajes de error.
4. Inicia Wireshark en la interfaz interna del servidor bookwormXXA. Activa el filtro "dhcp" para solamente ver la información de DHCP
5. Arrancar la máquina virtual cliente asegurándonos de que en la interfaz interna tenga configurado el cliente DHCP.
6. El intercambio de mensajes debería ser: Discover, Offer, Request y ACK. Transcurridos algo menos de 45 segundos se debería producir la renovación de la concesión con un nuevo mensaje Request y el consiguiente ACK y así sucesivamente cada 40-45 segundos. Observar que los primeros mensajes Request son de difusión, mientras que los siguientes mensajes Request son unicast.
7. Una vez se hayan producido, al menos, dos renovaciones debes detener el servicio DHCP pero se seguirán capturando paquetes con wireshark. Los mensajes del cliente de tipo Request deberían ser como los anteriores hasta que discurra casi el tiempo de agotamiento del otorgamiento de la IP. En ese momento los mensajes deberían ser Request pero de difusión y una vez agotado el tiempo deberían volver a lanzarse mensajes Discover.

8. Volver a arrancar el servidor después de lanzados 2 ó 3 mensajes Discover por parte del cliente. Se repetirá la secuencia de mensajes Discover, Offer, Request y ACK.
9. Consultar el archivo de concesión de direcciones para ver la información referida a las concesiones que el servidor ha hecho. Se encuentra en /var/lib.
10. Hacer backup del archivo de configuración en kea-dhcp4.conf.p1 una vez todo funcione correctamente

Nota importante: Durante todo el proceso de la práctica deberán hacerse capturas de imagen de cada uno de los pasos dados así como capturas y almacenaje de los paquetes de wireshark. Algunos de ellos serán solicitados por el profesor una vez concluida la práctica.

7. Práctica 2

Práctica 2 - DHCP

Requisitos previos:

- Haber completado la práctica 1
- Cliente LINUXXX correctamente configurado. Para ello es necesario arrancar la máquina cliente previamente y modificar la configuración de red para que el adaptador que está en la red interna esté en DHCP en lugar de STATIC.
- Cliente WindowsXX correctamente configurado. Para ello es necesario arrancar la máquina cliente previamente y modificar la configuración de red para que el adaptador que está en la red interna esté en DHCP en lugar de STATIC.

Fundamento teórico

Si queremos otorgar una configuración de red concreta a una máquina con base en características de la máquina necesitamos configurarlo de forma explícita en Kea.

¿Cómo podemos otorgar una dirección IP concreta de un 'Pool' de direcciones a una máquina concreta que se identifique de determinada manera?

- En KEA DHCP, el mecanismo para asignar una dirección IP fija a un *host* específico, incluso si esa IP está contenida dentro de un *Pool* de direcciones, se denomina **"Host Reservation"** (Reserva de Host).
- Estas reservas se configuran dentro de la subred específica en el archivo de configuración `kea-dhcp4.conf` y se identifican mediante un único identificador de cliente: la **dirección MAC** (`hw-address`) o un **identificador de cliente** específico (`client-id`).
- La reserva se define dentro del bloque `reservations` del objeto `subnet4` al que pertenece la máquina:
  - Reserva por Dirección MAC (`hw-address`): Es el método más común en redes IPv4, ya que la dirección MAC es única para cada adaptador de red.

```
{
  "Dhcp4": {
    "subnet4": [
      {
        "subnet": "192.168.1.0/24",
        "pools": [
          {
            "pool": "192.168.1.10 - 192.168.1.100" // El Pool dinámico
          }
        ],
        "reservations": [
          {
            // Reserva para una máquina específica (Identificada por MAC)
            "hw-address": "00:1A:2B:3C:4D:5E", // Dirección MAC del cliente
            "ip-address": "192.168.1.50",       // La IP concreta que quieres asignar
            "hostname": "ServidorWeb"           // (Opcional) Nombre de host
          }
        ]
      }
    ]
  }
}
```

  - Reserva por Client Identifier (`client-id`)
    - Este identificador es el valor enviado por el cliente en la opción **DHCP Option 61** (Client Identifier). Es más común en IPv6 (donde se conoce como DUID), pero se usa en IPv4, especialmente para clientes que no usan su dirección MAC (como algunos sistemas operativos o configuraciones de *netboot*). *El* `client-id` *debe especificarse en formato hexadecimal.*

```
{
  "Dhcp4": {
    "subnet4": [
      // ... configuración de subred anterior
        "reservations": [
          {
            // Reserva para una máquina específica (Identificada por Client ID)
            "client-id": "01:00:1A:2B:3C:4D:5E", // Client ID en formato hexadecimal (Ejemplo: 01 + MAC)
            "ip-address": "192.168.1.60",       // La IP concreta que quieres asignar
            "hostname": "EstacionTrabajo"
          }
        ]
      }
    ]
  }
}
```

- KEA permite que la dirección IP reservada (`ip-address`) **esté contenida dentro de un *pool*** de direcciones dinámicas (como en los ejemplos anteriores). Cuando KEA recibe una solicitud DHCP:
  1. Verifica si el identificador del cliente (MAC o *Client-ID*) coincide con alguna entrada en la sección `reservations`.
  2. Si hay una coincidencia, asigna la **dirección IP reservada** (`192.168.1.50` en el primer ejemplo), independientemente de que esa IP forme parte del rango dinámico del *pool*.

Nota sobre `client-id` y `hw-address`: Solo puedes usar **un tipo de identificador** (`hw-address`, `client-id`, `duid`, etc.) por cada entrada de reserva. No puedes especificar la MAC y el *Client-ID* en la misma reserva.

¿Hay alguna diferencia si la dirección IP no está incluida en un pool de direcciones?

- Si la dirección IP que queremos asignar estáticamente no está incluida dentro de un *pool* de direcciones dinámicas en KEA, **no hay ningún cambio en la sintaxis de la reserva**, pero hay un detalle crucial sobre la **filosofía de configuración** que tenemos que considerar y es que la dirección IP en la reserva debe pertenecer a la **subred** definida en el bloque `subnet4`.
- Puede parecer contradictorio definir un pool de direcciones para otorgar y después otorgar una fuera de ese pool. La razón es que en KEA, las **reservas de *host*** son un mecanismo de **asignación estática** que tiene **prioridad absoluta** sobre la asignación dinámica de *pools*.
  - **Reservas:** Son asignaciones fijas basadas en el identificador del cliente (MAC o *client-id*).
  - **Pools:** Son rangos desde donde KEA distribuye direcciones dinámicas
- Cuando un cliente con una reserva solicita una dirección, KEA primero busca una coincidencia en las reservas. Si la encuentra, asigna esa IP **inmediatamente** y no intenta buscarla en el *pool* dinámico.

La mejor práctica es **mantener las direcciones IP reservadas *fuera* del rango de los pools dinámicos** para evitar cualquier posible conflicto o confusión.

¿Y si se trata de parámetros específicos como por ejemplo el tiempo de concesión?

Para que un cliente reciba una configuración de parámetros específica (como un tiempo de concesión diferente) pero su dirección IP se obtenga **dinámicamente desde un *pool***, hay que utilizar la función de **Clasificación de Clientes (Client Classification)**.

La Clasificación de Clientes nos permite identificar a un *host* o grupo de *hosts* basándonos en criterios (como su MAC o *client-identifier*) y luego aplicarles reglas de configuración únicas, incluyendo diferentes opciones de DHCP o tiempos de concesión, sin necesidad de asignarles una IP estática.

Por ejemplo, si utilizamos la dirección MAC como criterio:

1. **Definir la Clase del Cliente (Client Class):** En el bloque `client-classes` del archivo `kea-dhcp4.conf`, se define una clase personalizada que utiliza una expresión de identificación para reconocer a la máquina. Por ejemplo:

```
{
  "Dhcp4": {
    "client-classes": [
      {
        "name": "lease-especial",
        "test": "option[61].hw-address == '00:1A:2B:3C:4D:5E'" // Identifica por MAC
      }
    ],
    // ...
  }
}

Donde:
```

- `"name": "lease-especial"`: Es el nombre de la clase que se aplicará más adelante.
- `"test": "option[61].hw-address == '00:1A:2B:3C:4D:5E'"`: Esta expresión le indica a KEA que todo paquete DHCP que llegue con la dirección MAC (`hw-address`) especificada (`00:1A:2B:3C:4D:5E`) debe ser clasificado como perteneciente a `"lease-especial"`.
- Si se deseara usar el `client-identifier` (Opción 61) directamente, se puede usar una expresión como: `"test": "option[61].hex == '01:00:1A:2B:3C:4D:5E'"`

2. **Aplicar la Configuración de Concesión:** Dentro de la subred (`subnet4`), se usa el nombre de la clase para anular el parámetro de configuración del servidor que se desea modificar, en este caso, el tiempo de concesión (`valid-lifetime`).

```
{
  "Dhcp4": {
    // ... (client-classes definido arriba)
    "subnet4": [
      {
        "subnet": "192.168.1.0/24",
        "valid-lifetime": 86400, // 24 horas (Configuración por defecto para la subred)
        "pools": [
          {
            "pool": "192.168.1.10 - 192.168.1.100" // Pool dinámico
          }
        ],
        // Aplicación de la configuración especial a la clase
        "client-class-config": {
          "lease-especial": {
            "valid-lifetime": 3600 // 1 hora (Tiempo especial para este cliente)
            // Aquí se puede añadir o anular cualquier otra opción de DHCP, como DNS o Router
          }
        }
      }
    ]
  }
}
```

3. **Funcionamiento:**

- El cliente con la MAC `00:1A:2B:3C:4D:5E` envía una solicitud DHCP.
- KEA lo identifica como perteneciente a la clase `"lease-especial"`.
- KEA le asigna la **siguiente dirección IP disponible** dentro del *pool* dinámico (`192.168.1.10 - 192.168.1.100`).
- La concesión se realiza con el tiempo de vida de **3600 segundos (1 hora)**, anulando la configuración predeterminada de la subred de 24 horas.
- Este enfoque logra el objetivo de darle un tratamiento especial a un cliente (o grupo de clientes) sin necesidad de utilizar reservas de IP estáticas.

Y si el cliente está dentro del bloque 'reservations', ¿también es necesario definir la clase?

- No, si un cliente ya está definido en el bloque `reservations` (reserva de *host*), **no es necesario** definir una clase de cliente (Client Class) separada para aplicarle parámetros específicos como un tiempo de concesión diferente.
- En KEA, la sección `reservations` no solo asigna una dirección IP estática, sino que también permite anular cualquier otra opción DHCP o parámetro de la subred específicamente para ese cliente.
- Simplemente se añade el parámetro `valid-lifetime` (o cualquier otra opción DHCP, como DNS, *routers*, etc.) directamente dentro de la reserva. Esta configuración tendrá prioridad sobre los ajustes generales de la subred.
- Ejemplo: Si queremos que la máquina con la MAC `00:1A:2B:3C:4D:5E` reciba la IP `192.168.1.50` y tenga una concesión de solo 1 hora (3600 segundos), la configuración sería la siguiente:

```
{
  "Dhcp4": {
    "subnet4": [
      {
        "subnet": "192.168.1.0/24",
        "valid-lifetime": 86400, // 24 horas (Configuración por defecto para la subred)
        "pools": [
          {
            "pool": "192.168.1.10 - 192.168.1.100" // Pool dinámico
          }
        ],
        "reservations": [
          {
            "hw-address": "00:1A:2B:3C:4D:5E", // Identificación del cliente
            "ip-address": "192.168.1.50",       // IP Fija (Reserva)
            "valid-lifetime": 3600             // 1 hora (Configuración especial para esta reserva)
            // Puedes añadir cualquier otra opción aquí:
            // "option-data": [ { "name": "domain-name-servers", "data": "8.8.8.8" } ]
          }
        ]
      }
    ]
  }
}
```

En resumen...

KEA utiliza un orden de prioridad claro para la configuración:

1. **Reserva de Host (`reservations`):** Tiene la máxima prioridad. Si un parámetro se define aquí, se aplica.
2. **Clase de Cliente (`client-class-config`):** Si un cliente coincide con una clase, las opciones de esa clase se aplican, anulando las de la subred.
3. **Configuración de Subred (`subnet4`):** Opciones por defecto que se aplican a todos los clientes que obtienen una concesión de forma dinámica en ese segmento de red.

Dado que el cliente está en la reserva, utilizas directamente el nivel de máxima prioridad (Nivel 1). Las Clases de Cliente (Nivel 2) son más útiles para aplicar configuraciones a **grupos** de clientes que obtienen su IP de forma **dinámica**.

¿Cómo podrías definir una clase para que incluyera a un conjunto de clientes y a estos otorgarles unos parámetros determinados diferentes de los definidos de forma global en la subred?

- Reflexiona sobre ello -

Pasos de la práctica:

1. Con la misma configuración de la práctica anterior: Modificar el archivo de configuración (recuerda haber hecho copia de seguridad previamente) para conseguir que:
   - Se otorgue a la máquina WindowsXX (usando su dirección MAC como información de identificación) la dirección IP 10.0.128+XX.50.
   - Tiempo máximo de alquiler de direcciones de 60 segundos.
   - Tiempo por defecto de alquiler de direcciones de 30 segundos.
2. Revisa los logs del servidor y recoge evidencias (registros) sobre el funcionamiento del servidor: concesión de direcciones, renovación, identificación del cliente, etc.
3. Realiza una captura, usando Wireshark, en que se vea el identificador de cliente enviado por el cliente.

NOTA: Durante todo el proceso de la práctica deberán hacerse capturas de imagen de cada uno de los pasos dados así como capturas y almacenaje de los paquetes de Wireshark. Algunos de ellos serán solicitados por el profesor una vez concluida la práctica.

8. Práctica 3

Requisitos previos:

- Haber completado las prácticas 1 y 2
- Cliente LINUXXX correctamente configurado. Para ello es necesario arrancar la máquina cliente previamente y modificar la configuración de red para que el adaptador que está en la red interna esté en DHCP en lugar de STATIC.
- Cliente WindowsXX correctamente configurado. Para ello es necesario arrancar la máquina cliente previamente y modificar la configuración de red para que el adaptador que está en la red interna esté en DHCP en lugar de STATIC.

Fundamento teórico:

Recordando...

Lo que hemos visto hasta ahora nos permite concluir que el servidor DHCP Kea aplica los parámetros de configuración siguiendo un orden de **especificidad creciente**, lo que significa que la configuración más detallada o específica tiene **prioridad** sobre la configuración más general.

El orden general de aplicación (de menor a mayor prioridad) es:

1. **Configuración Global:** Estos son los ajustes que se aplican a **todos** los servicios DHCP (generalmente en el nivel superior del archivo de configuración JSON).
2. **Configuración a Nivel de Interfaz:** Si se especifican ajustes para interfaces de red concretas, anulan la configuración global para esas interfaces.
3. **Configuración a Nivel de Subred (`subnet`):** Los parámetros definidos dentro de una subred específica (por ejemplo, `subnet4` o `subnet6`) anulan la configuración global y de interfaz para esa subred. Aquí se definen los *pools* de direcciones, *routers*, servidores DNS, etc.
4. **Configuración de Clases de Host (`host-classes`) y Opciones de Subred:** Dentro de una subred, las configuraciones específicas aplicadas a las clases de host (grupos de clientes con características similares) tienen mayor prioridad.
5. **Reservas de Host Específicas (`reservations`):** Esta es la configuración con la **máxima prioridad**. Una reserva de dirección IP basada en la dirección MAC del cliente (o DUID para DHCPv6) anulará cualquier otra configuración para ese host particular.

¿Qué parámetros son exclusivos de alguno de los ámbitos anteriores?

Pese a que muchos parámetros son comunes y se pueden usar en cualquiera de los ámbitos anteriores, algunos están diseñados para ser utilizados exclusivamente en ámbitos de configuración específicos debido a su naturaleza.

- Nivel Global: Afectan el funcionamiento de todo el servicio DHCP (v4 o v6) y generalmente se encuentran en la sección superior del archivo de configuración JSON.
  - `interfaces`: Especifica las interfaces de red que Kea debe escuchar. Es fundamental para el arranque del servicio.
  - `dhcp-ddns`: Parámetros de configuración relacionados con la actualización dinámica de DNS (DDNS).

- `control-socket`: Configuración para el socket que utiliza el Agente de Control de Kea para la gestión remota.
- `loggers`: Define cómo se gestionan los mensajes de registro (*logs*) de todo el servidor Kea.
- `lease-database`: Configura la base de datos (por ejemplo, Cassandra, MySQL, PostgreSQL o *memfile*) utilizada para almacenar todas las concesiones de DHCP.

- Nivel de subred (IPv4 o IPv6): Definen cómo se asignan las direcciones y opciones dentro de un rango de red específico.
  - `pools`: La lista de **rangos de direcciones IP** disponibles que Kea puede asignar a los clientes dentro de esa subred. Este es el parámetro más distintivo del nivel de subred.
  - `interface`: **(Exclusivo a veces)** Permite especificar qué interfaz o interfaces de red están directamente conectadas a esta subred particular, limitando el ámbito de escucha para esa subred.
  - `client-classes`: Permite definir y asignar políticas a **clases de clientes** específicas dentro de esa subred (por ejemplo, reservar un rango para clientes conocidos o aplicar restricciones a clientes desconocidos).
  - `option-data`: Si bien las opciones DHCP se pueden configurar globalmente, si se configuran aquí, **solo se envían a los clientes de esta subred**.
- Nivel de reserva de Host (reservations): Estos parámetros se utilizan para asignar una configuración fija a un único cliente, identificándolo por su hardware de red o por su identificador único.
  - `ip-address`: La **dirección IP fija** que se reservará para este host específico.
  - `hw-address`: (DHCPv4) La **dirección MAC** que identifica de forma única al cliente al que se le aplicará la reserva.
  - `duid`: (DHCPv6) El **Identificador Único de DHCP** (DUID) que identifica al cliente IPv6.
  - `client-id`: (DHCPv4) El identificador de cliente que se puede usar en lugar de la dirección MAC para la reserva.
  - `hostname`: El nombre de host que se enviará al cliente o se utilizará para DDNS, específico para este host.

La exclusividad principal en las reservas es el uso de identificadores de cliente (`hw-address`, `duid`, `client-id`) para vincular la configuración a un único dispositivo.

¿Cómo puede Kea distinguir entre clientes conocidos y desconocidos para poder aplicar configuraciones diferentes?

Kea DHCP proporciona mecanismos robustos para distinguir entre clientes conocidos y desconocidos, lo que permite aplicar configuraciones de red, políticas de seguridad y opciones de DHCP diferentes.

Como vimos en la práctica anterior existen las **Reservas de Host** y **Clases de Cliente**. Pues bien, estas son las dos formas en que KEA puede distinguir clientes:

Reservas de host:

1. Reservas de Host (Clientes Conocidos). La forma más directa y de **máxima prioridad** para identificar un cliente como "conocido" es crear una **reserva de host**.
    1. Una reserva vincula una configuración específica (como una IP fija y ciertas opciones) a un identificador de hardware único, lo que garantiza que Kea siempre reconocerá y tratará a ese cliente de una manera predefinida.
    2. Los parámetros clave son:
        1. **Identificadores Únicos:** La reserva se basa en identificadores de hardware:
            1. **DHCPv4:** Se usa principalmente la dirección **MAC** (`hw-address`).
            2. **DHCPv6:** Se usa el **DUID** (`duid`) o la dirección MAC.
        2. **IP Fija:** Aunque no es estrictamente necesario, el uso más común es asignar una dirección IP estática (`ip-address`) a ese cliente.
        3. **Prioridad:** La configuración de una reserva **anula** cualquier otra configuración de subred o global para ese cliente.
2. Cualquier cliente que **NO** tenga una reserva explícita se considera **desconocido** y se le asigna una dirección del *pool* general de la subred, recibiendo la configuración predeterminada de esa subred.

Clases de Cliente (`Client Classes`)

Las clases de cliente permiten agrupar clientes basándose en criterios dinámicos que Kea evalúa durante el proceso de solicitud DHCP (DISCOVER). Puedes definir reglas para clasificar a los clientes y luego aplicarles políticas específicas.

1. Distinción por Clase: La clave es crear dos clases: una para los clientes conocidos y otra para los desconocidos.
2. Definición de la Clase:
    1. "Conocida": Se utiliza una clase para identificar clientes que tienen un atributo particular que podemos definir. Como criterio común se puede utilizar la propiedad `$known` que Kea establece internamente, o basar la clasificación en el **identificador de cliente** que envían:
    2. "Desconocida" (`UNSPECIFIED`): Kea tiene una clase interna implícita (`UNSPECIFIED` o a veces `UNKNOWN`) para los clientes que **no coinciden** con ninguna de las clases definidas.
3. Aplicación de la configuración: En la definición de la subred, se pueden configurar opciones **diferentes** basadas en la clase a la que pertenece el cliente:
    - **Clientes Conocidos (Clase definida):** Se les asignan opciones como un tiempo de concesión muy largo (`max-lease-time`) o un servidor DNS específico.
    - **Clientes Desconocidos (No coinciden con ninguna clase):** Reciben la configuración general de la subred, que podría tener un tiempo de concesión corto y ser restringidos a un *pool* de direcciones pequeño..

```
"client-classes": [
    {
        "name": "Clientes_Reservados",
        "test": "member('Clientes_Reservados')"
        /* Esta clase se usa si el cliente ya está en el sistema de reservas */
    },
    {
        "name": "Mis_Servidores",
        "test": "substring(option[60].hex, 0, 4) == '4d6163'"
        /* Ejemplo: basar la clasificación en una opción específica enviada por el cliente (vendor-class-
identifier) */
    }
]
```

Pasos de la práctica:

1. Modificar el archivo de configuración de la Práctica 2 (recuerda haber hecho copia de seguridad previamente) para conseguir que:
    - Se otorgue a la máquina LinuxXX (por ser cliente conocido) una dirección del pool 10.0.128+XX.150 a 10.0.128+XX.159
        - Tiempo máximo de alquiler de direcciones de 90 segundos
        - Tiempo por defecto de alquiler de direcciones de 45 segundos
    - Se otorgue a la máquina WindowsXX (por ser cliente desconocido) una dirección del pool 10.0.128+XX.160 a 10.0.128+XX.169. Cuidado, porque habrá que quitar la dirección reservada de la práctica anterior.
        - Tiempo máximo de alquiler de direcciones de 40 segundos
        - Tiempo por defecto de alquiler de direcciones de 20 segundos
2. Revisa los logs del servidor y recoge evidencias (registros) sobre el funcionamiento del servidor: concesión de direcciones, renovación, identificación del cliente y tiempo de concesión
3. Recoge evidencias en que se muestre el tiempo por el que se ha concedido la IP a cada uno de los clientes

NOTA: Durante todo el proceso de la práctica deberán hacerse capturas de imagen de cada uno de los pasos dados así como capturas y almacenaje de los paquetes de wireshark. Algunos de ellos serán solicitados por el profesor una vez concluida la práctica. Para poder realizar esta práctica es necesario haber realizado las prácticas 1 y 2

9. Práctica 4

Requisitos previos:

- Haber completado, al menos, la práctica 1
- Cliente LINUXXX correctamente configurado. Para ello es necesario arrancar la máquina cliente previamente y modificar la configuración de red para que el adaptador que está en la red interna esté en DHCP en lugar de STATIC.
- Cliente WindowsXX correctamente configurado. Para ello es necesario arrancar la máquina cliente previamente y modificar la configuración de red para que el adaptador que está en la red interna esté en DHCP en lugar de STATIC.
- Una tercera máquina cliente que podrá ser cualquiera de las que tienes instaladas para otros módulos.
- Haz copia de seguridad de la configuración del servidor antes de modificarla

Fundamento teórico:

Uno de la formas en que un servidor puede atender a diferentes subredes es disponiendo de diferentes interfaces por los que aceptar peticiones, cada una de ellas para diferentes subredes. Evidentemente se requerirá disponer de algún interfaz de red adicional así como de la configuración adecuada para dicha subred.

Pasos de la práctica:

1. Crear un nuevo interfaz en el servidor que se configurará utilizando systemd-networkd: Interfaz en red interna pero con otro nombre para distinguirla de la primera, por ejemplo acabándola en 2.
2. Subred a incluir: 10.0.192+XX.00/24. La IP del servidor A que incluirá esta subred es la .1. El servidor B no tienen IP de esta subred.
3. Modificar el archivo de configuración de alguna de las prácticas anteriores (recuerda haber hecho copia de seguridad previamente) para conseguir que se el servidor escuche en ambas interfaces internas, para que otorgue direcciones de la nueva subred, para que otorgue un rango de direcciones entre la 220 y la 239 de las anteriores y para que se configure un tiempo por defecto de concesión de 100 segundos, un máximo de 200 y un mínimo de 50
4. Comprobación de que el servidor DNS está correctamente configurado en todos los clientes (recuerda que, inicialmente, debe ser el 10.0.128+XX.2) y comprobación sobre qué nombres se pueden resolver desde el nuevo cliente. Reflexiona las razones por las que ocurre. Haz pruebas también preguntando directamente al servidor DNS instalado en BookwormXXA.
5. Sin alterar las configuraciones de red de ningún servidor, habilita una configuración en el servidor DHCP y los servidores DNS para que los clientes de ambas subredes puedan disponer de resolución de nombres de todas las zonas tratadas durante el curso (excepto las del examen), así como cualquier otro nombre de Internet.

NOTA: Durante todo el proceso de la práctica deberán hacerse capturas de imagen de cada uno de los pasos dados así como capturas y almacenaje de los paquetes de wireshark. Algunos de ellos serán solicitados por el profesor una vez concluida la práctica. Para poder realizar esta práctica es necesario haber realizado, al menos, la práctica 1

10. Solicitud parámetros red

¿Cómo puede un cliente DHCP solicitar valor para determinados parámetros cuando intenta descubrir servidores DHCP?

El cliente DHCP gestionado por **systemd-networkd** solicita opciones DHCP concretas al servidor DHCP mediante el parámetro `SendOption` en su archivo de configuración `.network`.

Por ejemplo, para que el cliente solicite un tiempo de concesión (`lease time`) específico, se debe modificar o crear un archivo de configuración para la interfaz de red, típicamente ubicado en `/etc/systemd/network/`.

```
[Match]
Name=eth0  ; Cambia 'eth0' al nombre de tu interfaz

[Network]
DHCP=ipv4

[DHCPv4]
# Especifica el tiempo de concesión deseado.
# La opción DHCP 51 (Lease Time) se solicita en segundos.
SendOption=51:<tiempo_en_segundos>
```

Es importante entender que el cliente **solicita** este tiempo, pero la **decisión final** sobre el tiempo de concesión recae en el **servidor DHCP**:

- El servidor **Kea** leerá la solicitud del cliente.
- Si el tiempo solicitado está dentro de los límites configurados en el servidor (tiempos mínimo y máximo), el servidor podría conceder ese tiempo.
- Si el tiempo solicitado está fuera del rango permitido o el servidor ignora la opción, el servidor **otorgará su propio tiempo de concesión predeterminado** (definido por el parámetro `default-lease-time` o `max-lease-time` de Kea).

11. Actualización DNS

¿Cómo es posible cuando se otorga una dirección IP a un host el DNS pueda resolver el nombre por dicha dirección IP?

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones:

- Por defecto en Windows
- Hay que explicitarlo en Linux

¿Cómo se puede habilitar y configurar en Kea y Bind9?

Configuración para que el servidor tenga permitido enviar las peticiones

- Es necesario habilitar la opción de actualizaciones dinámicas de forma global (`"enable-updates": true`)
- Si no se configura globalmente es necesario habilitar en la subred en envío de actualizaciones automáticas (`"ddns-send-updates"`)

Configuración para que el servidor puede hacer el envío efectivo

Se hace a través de un complemento específico, que se llama D2. Para ello:

- Debe tener instalado el paquete de configuración DDNS (kea-dhcp-ddns-server)
- Editar adecuadamente el archivo de configuración (`kea-dhcp-ddns.conf`) en sus diferentes aspectos:
  - ¿Qué IP, puerto y modo de control?
  - ¿Sobre qué dominios y a qué servidores DNS y con qué clave se van a enviar las peticiones?
  - ¿Cómo configuramos las claves que se van a usar?

Configuración del servidor DNS para que acepte las peticiones:

- La clave rndc-key u otra que usemos ha de coincidir con la del servidor DHCP
- Debemos ser explícitos permitiendo en la zona directa e inversa las actualizaciones con "`allow-update`"

12. Relay

¿Qué ocurre cuando en una red o en un segmento de red no hay servidor DHCP?

Como sabemos, el protocolo DHCP funciona principalmente con mensajes de **difusión (broadcast)** en su fase inicial (*DHCP Discover* y *DHCP Request*).

- Los mensajes de difusión están **limitados** al segmento de red local o subred (dominio de difusión), ya que los rúteres están diseñados para no reenviarlos a otras redes por defecto.
- En redes grandes con múltiples subredes separadas por rúteres tener un servidor DHCP en cada subred sería ineficiente.

El **DHCP Relay Agent** (que puede ser un rúter, un conmutador de capa3, un firewall, incluso un servidor dedicado) resuelve este problema.

¿Cómo Funciona el DHCP Relay Agent?

El Agente de Retransmisión DHCP actúa como un **intermediario** o un "puente" entre el cliente DHCP y el servidor DHCP.

1. Recepción del Broadcast (Cliente → Relay Agent)
    1. El **cliente DHCP** arranca y envía un mensaje de difusión (*DHCP Discover*) en su subred para encontrar un servidor.
    2. El **DHCP Relay Agent** recibe este mensaje de difusión en una de sus interfaces.
2. Conversión y Reenvío (Relay Agent → Servidor)
    1. El Relay Agent encapsula el mensaje de difusión original dentro de un nuevo paquete y lo reenvía como un mensaje de **unidifusión (unicast)** a la dirección IP del **servidor DHCP** (dirección que debe haber sido configurada previamente en el agente).
    2. **Importante:** El Relay Agent añade su **propia dirección IP de interfaz** (la *Gateway IP* o campo `giaddr` del paquete DHCP) en el mensaje. Esto le indica al servidor DHCP **a qué subred pertenece el cliente** que hizo la solicitud. (si el valor de este campo es 0.0.0.0 el servidor sabe que el mensaje le está llegando directamente desde el cliente.
3. Asignación y Oferta (Servidor → Relay Agent)
    1. El **servidor DHCP** examina el campo `giaddr` para determinar de qué subred proviene la solicitud.
    2. Utiliza esa información para seleccionar un **pool de direcciones IP** adecuado para esa subred.
    3. El servidor envía el mensaje de oferta (*DHCP Offer*) y posteriormente el mensaje de confirmación (*DHCP ACK*) como paquetes de **unidifusión** de vuelta a la dirección IP del **Relay Agent** (no al cliente).
4. Entrega al Cliente (Relay Agent → Cliente)
    1. El **Relay Agent** recibe el mensaje del servidor y lo reenvía al **cliente DHCP** en la subred original, en un formato que sería original, haciendo que el cliente vea el proceso como algo transparente.
    2. Este proceso se repite para los mensajes de *DHCP Request* y *DHCP ACK*, completando el proceso de asignación de la dirección IP.

```
Bootp flags: 0x0000 (Unicast)
    0... .... .... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 192.168.1.98
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 192.168.1.69
  Client MAC address: GigaByteTech_e8:6b:ed (00:24:1d:e8:6b:ed)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
> Option: (53) DHCP Message Type (Request)
```