TEMA 3: DHCP

ADMINISTRACIÓN DE SERVICIOS

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

2020/2021

Cristian Martín Fernández

Contenido

- Servidor DHCP
- Instalación
- Convenciones Ubuntu
- Configuración dinámica de DHCP
- Configuración estática de DHCP

Servidor DHCP

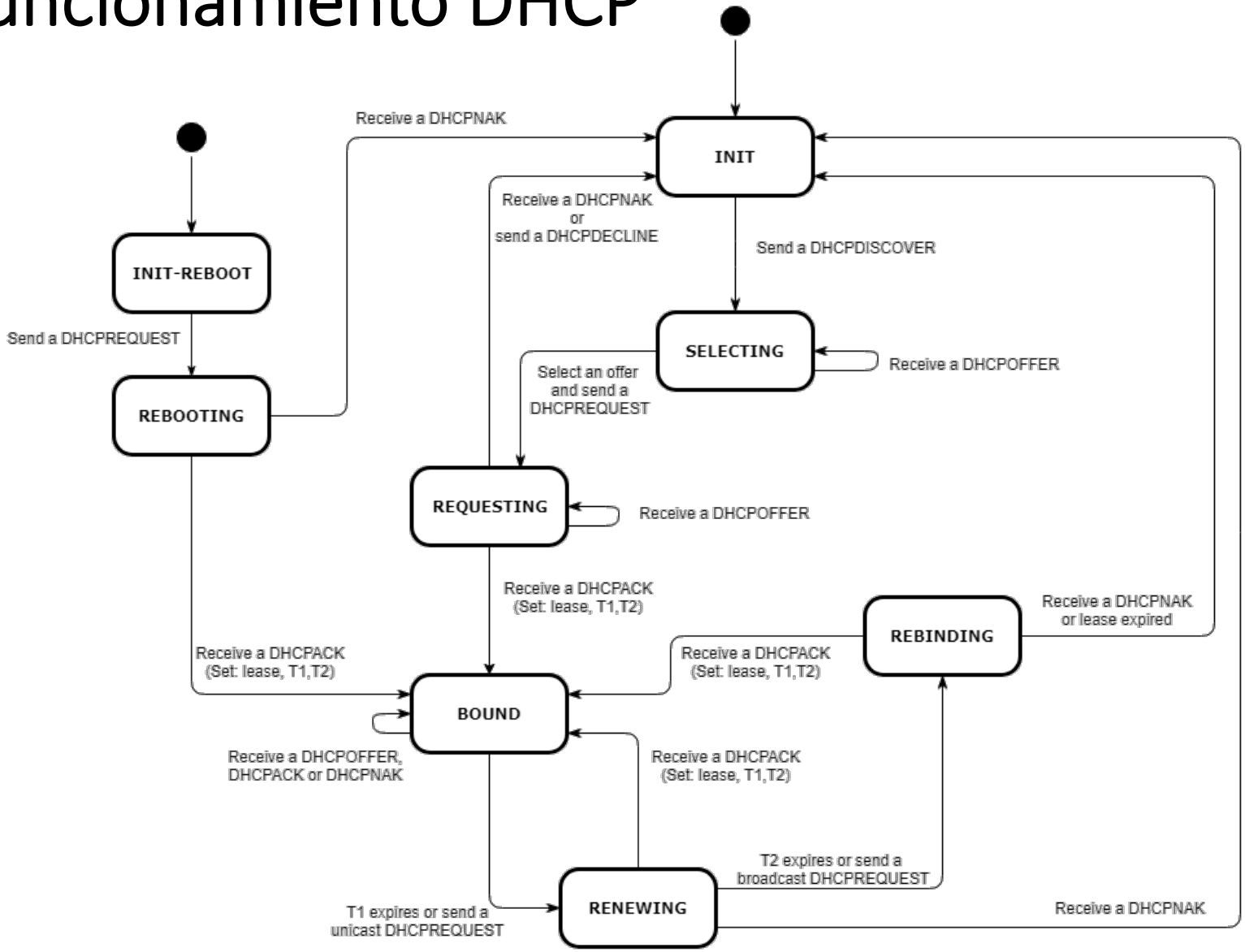
- Servidor DHCP (Dynamic Host Control Protocol) es un protocolo de red que se utiliza para **asignar direcciones IP y proporcionar información de configuración** a dispositivos ordenadores, servidores o dispositivos móviles, para que puedan comunicarse en una red mediante el protocolo IP.

- Por defecto escucha en el puerto UDP 67. Evolución de BOOTP (la misma IP a la misma MAC).

- DHCP también puede proporcionar propiedades de configuración como: nombre de host, nombre de dominio, servidores de tiempo o de impresión.

- La ventaja de usar DHCP es que los **cambios en la red**, por ejemplo, un cambio en la dirección del servidor DNS, solo necesitan cambiarse en el servidor DHCP, y todos los hosts de la red se reconfigurarán la próxima vez que sus clientes DHCP se actualicen del servidor DHCP.

Funcionamiento DHCP



Servidor DHCP de ISC

- Servidor DHCP de ISC es el más utilizado y disponible en la mayoría de distribuciones de GNU/Linux.

- Lo desarrolla, ISC (Internet Systems Consortium), una empresa sin ánimo de lucro que provee software cumple con los estándares y de calidad, como lo demuestra el servidor BIND.

- Proporciona soporte para BOOT, compatibilidad IPv6, y una implementación de Agent relay.

Instalación Servidor DHCP ISC

- Para instalar un servidor DHCP en Ubuntu:
  - `$ sudo apt install isc-dhcp-server`

- Para consultar su estado (por defecto está en modo error hasta que no se configure):
  - `$ systemctl status isc-dhcp-server`

- Para consultar su log:
  - `$ journalctl –u isc-dhcp-server`

Convenciones Ubuntu

- /etc/dhcp/dhcpd.conf

  Archivo de configuración para el servidor DHCP.
  Muy bien documentado, e incluso proporciona ejemplos para que podamos trabajar con él.

- /var/lib/dhcp/dhcpd.leases

  Este fichero contiene la lista actual de asignaciones DHCP que el servidor ha distribuido.

- /var/log/syslog

  DHCP usa el archivo estándar de registros del sistema para todos sus registros.
  Aquí podemos encontrar cualquier petición realizada desde la red bajo DHCP, además de la respuesta del servidor DHCP.

Configuración DHCP

- Podemos encontrar tres modos de configuración para un servidor de DHCP:

  - **Asignación estática**:
    Se puede forzar a que una dirección IP en concreto se asigne a una dirección MAC y garantizar que cada vez que haga una petición, se le asigne la misma IP.

  - **Asignación dinámica**:
    Las peticiones de host se resuelven con una asignación de dirección IP dentro de un rango de IP válidas por un tiempo determinado. Después que expire este lapso, se revoca la dirección IP y el cliente DHCP tiene que devolverla. Si el cliente aún necesita una dirección IP para efectuar sus operaciones, deberá solicitarla nuevamente.

  - **Asignación automática**:
    Es como una asignación dinámica, pero el servidor DHCP mantiene una tabla de asignaciones de direcciones IP pasadas, de modo que puede asignar preferentemente a un cliente la misma dirección IP que el cliente tenía anteriormente. *El servidor DHCP de ISC no lo implementa*.

Configuración DHCP

- La asignación estática funciona como una configuración de IP estática en un ordenador, pero de forma centralizada en el servidor DHCP.

- El método de asignación dinámica es útil para clientes DHCP que necesitan una dirección IP para una conexión temporal a la red (por ejemplo, en redes wifi grandes). En este caso no se puede asignar una IP única a un usuario ya que cambian continuamente y habrá más usuarios que direcciones IPs.

- La asignación dinámica continua o automática es la más utilizada en routers domésticos con pocos usuarios.

Configuración Servidor DHCP

- Lo primero que tenemos que hacer es configurar el servidor DHCP para indicarle los interfaces para los que debe de escuchar.

- Editamos el fichero `/etc/default/isc-dhcp-server` y añadimos las interfaces de red de nuestra máquina en IPv4. Por ejemplo, la interfaz enp0s3 (para ver las interfaces de red podemos utilizar el comando “ip a”).

```
INTERFACESv4="enp0s3"
```

Configuración Servidor DHCP

- Parámetros de configuración del fichero principal /etc/dhcp/dhcp.conf

default-lease-time 600; # Tiempo de licencia por defecto (en segundos)
max-lease-time 7200; # Tiempo de licencia máximo (en segundos)
min-lease-time 300; # Tiempo de licencia mínimo (en segundos)

- Y más opciones:

authoritative; # servidor DHCP es autoritario en todos los segmentos de la red.
option domain-name-servers 8.8.8.8, 192.168.1.1; # servidores DNS
option domain-name ”aso.local"; # Nombre del dominio
option subnet-mask 255.255.255.0; # Mascara de red
option routers 192.168.50.254; # Router
option broadcast-address 192.168.50.255; # Dirección de broadcast

Configuración dinámica DHCP

- Supongamos que tenemos una red con las siguientes características:

  Cabecera: 10.0.2.0
  Subred: 255.255.255.0
  Puerta de enlace: 10.0.2.2
  DNS 10.0.2.15

- En el archivo de configuración /etc/dhcp/dhcp.conf debemos incluir los parámetros de configuración.

- Aquí necesitamos añadir una declaración de subred que proporciona toda la información sobre nuestra subred junto con el rango de direcciones IP que el servidor DHCP puede utilizar.

Configuración dinámica DHCP

- Supongamos que el rango de direcciones IP que vamos a distribuir es 10.0.2.50 a 10.0.2.99 entonces tendremos la siguiente configuración en el fichero principal de DHCP:

```
subnet 10.0.2.0 netmask 255.255.255.0 {
  range 10.0.2.50 10.0.2.99;
  option routers 10.0.2.2;
}
```

NMAP

- Podemos instalar el comando `nmap` que es popularmente conocido para en ciberseguridad para descubrir hosts y puertos. Pero además, proporciona un cliente DHCP.
  - $ sudo apt install nmap

- Para utilizar nmap y descubrir los puertos abiertos del sistema es tan sencillo como ejecutar:
  - `$ nmap localhost`
  - `$ nmap  8.8.8.0-24`

- Pero también puede ser utilizado para descubrir hosts en nuestra red y ver quién está conectado a nuestra Wifi ☺:
  - `$ nmap -sP 192.168.1.0/24`

NMAP

- También permite conocer las versiones de los servicios:
  - `$ nmap -sV localhost`
- Escanear títulos de HTTP en los hosts:
  - `$ nmap --script=http-title localhost`
- Escanear los 20 puertos más conocidos:
  - `$ nmap --top-ports 20 localhost`

NMAP

- Descubrir el sistema operativo de un host:
  - `$ nmap -A -T4 192.168.1.33`

- Y encontrar vulnerabilidades:
  - `$ nmap -Pn --script vuln localhost`

- A lo que íbamos ☺ Desde el cliente nmap se puede ejecutar de la siguiente forma un cliente DHCP para comprobar si el servidor devuelve una dirección IP.
  - `$ sudo nmap --script broadcast-dhcp-discover -e <interfaz de red>`

Cliente DHCP

- Se instala también un cliente DHCP que se puede utilizar para renovar la IP de nuestro servidor DHCP, por ejemplo, en la interfaz de red enp0s3:
  - `$ sudo dhclient enp0s3 -v`

Ámbito de la declaración de DHCP

- El servidor DHCP determina los parámetros y opciones que deben usarse para una petición DHCP según el ámbito al que se asocia dicho cliente.

- Existe el **ámbito global** cuyas opciones y/o parámetros se aplican a todos los clientes, pero también existen ámbitos más específicos creados con las declaraciones, y si aplica, se activarán las configuraciones de menor nivel:
  - shared-network
  - subnet
  - pool
  - host
  - group

Red compartida

- Todas las subredes que comparten la misma red física deben especificarse dentro de una declaración `shared-network`:

```
shared-network aso-compartida {
  option domain-name      "aso.uma.es";
  option routers 192.168.1.254;

  subnet 192.168.1.0 netmask 255.255.255.0 {
     parameters for subnet
     range 192.168.1.1 192.168.1.31;
  }
  subnet 192.168.1.32 netmask 255.255.255.0 {
    # declaramos este rango para que lo controle el servidor pero no ofrecemos IPs
  }
```

Configuración pool

- La declaración de pool se puede utilizar para especificar un grupo de direcciones que se tratarán de forma diferente a otro grupo de direcciones, incluso en el mismo segmento de red o subred. Este se define dentro de una subnet o un shared-network.

```
subnet 10.0.0.0 netmask 255.255.255.0 {
    option routers 10.0.0.254;

    # Clientes no conocidos
    pool {
        max-lease-time 300;
        range 10.0.0.200 10.0.0.253;
        allow unknown-clients;
    }

    # Clientes conocidos
    pool {
        max-lease-time 28800;
        range 10.0.0.5 10.0.0.199;
        deny unknown-clients;
    } }
```

Bloqueo/Permiso de forma explícita

- Se puede controlar de forma explícita la asignación y el bloqueo de IPs en un rango explícito.

```
pool {
   deny all clients;
   range 10.0.0.10 10.0.0.99;
}

pool {
   allow all clients;
   range 10.0.0.100 10.0.0.199;
}
```

Configuración estática de DHCP

- Es posible mezclar asignaciones DHCP estáticas con asignaciones DHCP dinámicas.

- Si un servidor tiene una asignación estática, tomará esa dirección, y en otro caso se le asignará una dirección dinámica dentro del rango establecido.

- Este proceso es más complejo, pero se asegura que se provee la dirección deseada a un cliente.

Configuración estática de DHCP

- Por ejemplo. Supongamos que queremos asignarle a un host con dirección MAC DE:AD:C0:DE:CA:FE una dirección IP fija 10.0.2.14. Entonces debemos añadir:

```
host aso {
     hardware ethernet DE:AD:C0:DE:CA:FE;
     fixed-address    10.0.2.14;
  }
```

- Es posible añadir en este fichero tantas declaraciones como necesitemos, siempre que tengan una MAC única y una IP única para cada host añadido.

- La dirección MAC de un servidor o equipo se puede obtener de la información proporcionada por el comando “ip a”.

Declaración de grupos

- La declaración de grupo se usa para aplicar uno o más parámetros a un conjunto de declaraciones. Se puede utilizar para agrupar hosts, redes compartidas, subredes o incluso otros grupos.

```
group {
  option routers                192.168.1.254;
  option subnet-mask            255.255.255.0;

  option domain-name            ”aso.uma.es";
  option domain-name-servers    192.168.1.1, x.x.x.x;

  subnet 192.168.1.0 netmask 255.255.255.0 {
      range 192.168.1.1 192.168.1.31;
   }

  host aso1 {
    option host-name "aso1.uma.es";
    hardware ethernet 00:A1:DD:74:C3:F2;
    fixed-address 192.168.1.6;
  }
}
```

Ejercicio de clase

- Define un asignación en DHCP para la interfaz de red 192.168.1.0/24 que cumpla los siguientes requisitos:

1. El router está en la IP 192.168.1.1, y es común a todas las configuraciones.
2. El nombre del dominio es “aso.uma.es” y los servidores DNS “dns1.aso.uma.es” y “dns2.uma.es”, aplicable en todas las configuraciones.
3. Las direcciones IP válidas van desde la IP 192.168.1.2 hasta la IP 192.168.1.125, con un tiempo máximo de licencia 1 día.
4. Las IPs 192.168.1.126, se deben de asignar a la MACs 00:0a:95:9d:68:16 y 00:0a:95:9d:68:17 respectivamente, y deben de tener asignados los hostnames “aso126” y “aso127” respectivamente.
5. El rango de IPs de 128 hasta 200 se debe de permitir únicamente a clientes conocidos.
6. El resto de IPs hasta la IP 192.168.1.254 se debe de bloquear de forma explícita.

Opciones avanzadas: filtrado de clases

- Se pueden declarar grupos de clientes y definir asignación de IP en base a ciertos criterios:

```
class ”rasp" {
  match if substring (option vendor-class-identifier, 0, 4) = ”RASP";
}
group {
  subnet 10.17.224.0 netmask 255.255.255.0 {
    option routers rtr-224.example.org;
  }
  subnet 10.0.29.0 netmask 255.255.255.0 {
    option routers rtr-29.example.org;
  }
  pool {
    allow members of "rasp";
    range 10.17.224.10 10.17.224.250;
  }
  pool {
    deny members of "rasp";
    range 10.0.29.10 10.0.29.230;
 }}
```

Configuración dinámica a través de OMAPI

- La interfaz OMAPI permite **modificar la configuración** agregando objetos host, subredes, etc., de un servidor en **tiempo de ejecución**.
- Lo primero que hay que realizar es configurar el puerto de la API OMAPI (por defecto 7911) y una clave, en el fichero principal de configuración de DHCP y reiniciar el servidor. Por ejemplo:

```
omapi-port 7911;
omapi-key omapi_key;
key omapi_key {
   algorithm hmac-md5;
   secret Ofakekeyfakekeyfakekey==;
}
```

OMAPI omshell

- Omshell es un comando para interactuar con la API OMAPI. Se inicia con:
  - `$ omshell`
- Una vez dentro hay que conectarse al servidor:
  - `server localhost`
  - `port 7911`
  - `key omapi_key Ofakekeyfakekeyfakekey==`
  - `connect`
- Ahora podemos crear un nuevo host:
  - `new host`
  - `set name = "aso-host"`
  - `set hardware-address = 00:80:c7:84:b1:94`
  - `set ip-address = 192.168.4.40`
  - `create`

Configuración estática de IP en Ubuntu

Añadir un fichero a la carpeta /etc/netplan y añadir la configuración de IP estática como el siguiente ejemplo. Haced `sudo netplan apply` para aplicar los cambios

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses:
        - 10.0.2.15/24
      dhcp4: false
      gateway4: "10.0.2.2"
      nameservers:
        addresses:
          - "8.8.8.8"
          - "8.8.4.4"
  renderer: networkd
```

Bibliografía

- Dynamic Host Configuration Protocol (DHCP) https://ubuntu.com/server/docs/network-dhcp
- Tutorial servicio DHCP https://www.fpgenred.es/DHCP/index.html
- dhcp.conf https://manpages.ubuntu.com/manpages/focal/en/man5/dhcpd.conf.5.html
- Servicios de red e Internet (DHCP) https://serviciosgs.readthedocs.io/es/latest/dhcp/index.html
- Top nmap commands https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts
- Omshell: https://linux.die.net/man/1/omshell
- OMAPI: https://kb.isc.org/docs/aa-00475