

Práctica 9: Configuración de NAT y DHCP

Material necesario: maqueta de routers, cables de red y consola y ordenadores de consola.

IMPORTANTE: En los ejemplos utilizados se hace mención a uno de los routers de la maqueta, “**Lab-A**>”, pero puede generalizarse al resto “**Lab-B**>”, “**Lab-C**>”, ...

Objetivos:

En esta práctica de laboratorio vamos a poner en práctica dos mecanismos diferentes:

- DHCP: Dynamic Host Configuration Protocol. Sirve para configurar automáticamente parámetros de configuración ip en los hosts de una red.
- NAT: Network Address Translation. Sirve para traducir una serie de direcciones en otras según una tabla de equivalencias. Muy usado para conectar a Internet redes IP que usan rangos privados (RFC 1918: 10.*.*.*, 172.16-31.*.*, 192.168.0-255.*). Suele realizarla el router que conecta la red con el exterior.

En la primera parte configuraremos los routers Lab-A, Lab-B, Lab-C y Lab-E como servidores DHCP y probaremos los comandos de monitorización de DHCP.

En la segunda parte configuraremos NAT overload (PAT) en esos mismos routers y probaremos también algunos comandos relacionados.

Práctica:

Parte A : Configurar Routers como servidor DHCP

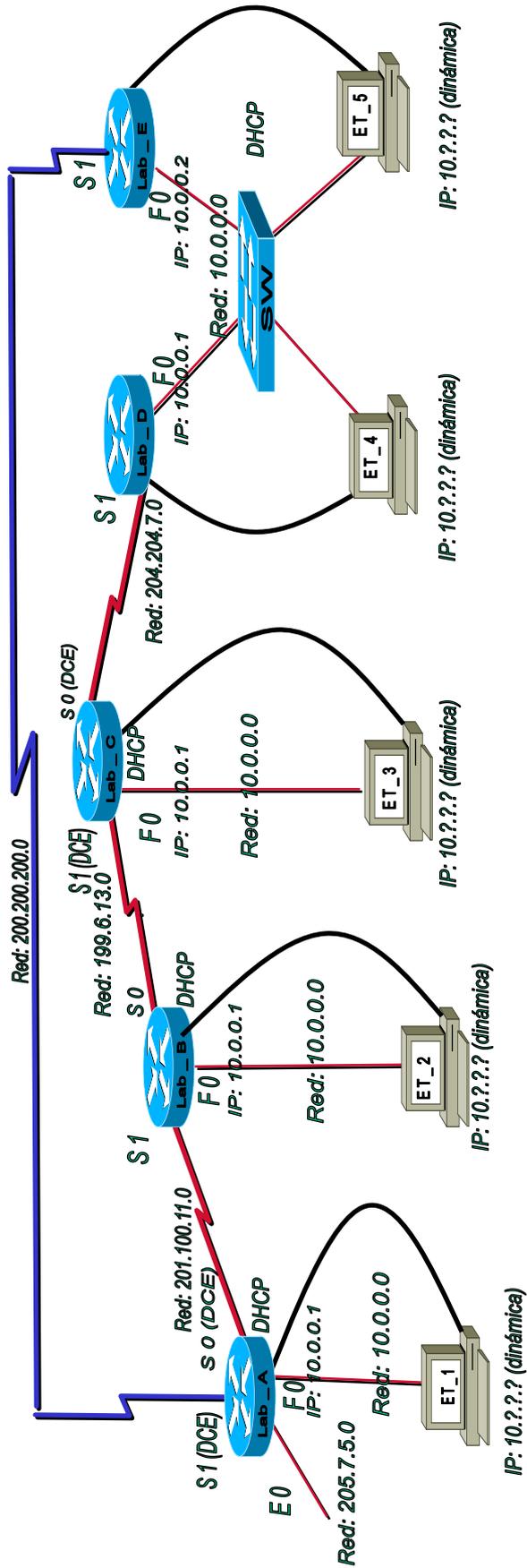
Partiendo de la maqueta de siempre, vamos a cambiar el direccionamiento de las redes locales conectadas a F0 en cada router para que sea en todas la misma red privada: 10.0.0.0/8. Es decir, todas las LAN de la maqueta tendrán las mismas direcciones IP, existirá solapamiento. La nueva configuración de estas redes la haremos con estos dos pasos:

- Configuraremos la interfaz F0 de cada router como 10.0.0.1 (Como el interfaz F0 de Lab-D y Lab-E está en la misma red, el de Lab-E lo configuraremos como 10.0.0.2).
- las posibles direcciones de los hosts de cada red las configuraremos automáticamente por DHCP.

Para que el DHCP funcione es necesario hacer 2 cosas:

- Configurar un DHCP en cada red (en nuestro caso serán los routers Lab-A, Lab-B, Lab-C, Lab-E)
- Configurar los PCs como clientes DHCP

La maqueta modificada para esta práctica tendrá este aspecto:



Paso A.1 (tareas similares a otras prácticas)

En primer lugar, vamos a configurar la maqueta de forma similar a las anteriores prácticas:

1. Configurar las interfaces **serie** con las IP de siempre
2. Configurar las interfaces LAN (F0) de los routers con las IP de 10.0.0.1/8. En el caso de Lab-E, usar 10.0.0.2/8 (para evitar que coincida con Lab-D).
3. Configurar el protocolo de enrutamiento (EIGRP 100), para poder visualizar y acceder a todas las interfaces serie, pero NO las interfaces LAN, dado que tendríamos conflicto por duplicidad de IP.

Paso A.2. Configuración de DHCP en los routers

Hay que configurar un DHCP en cada LAN, para ello usaremos Lab-A, Lab-B, Lab-C y Lab-E.

Nota sobre el caso especial de la LAN donde están Lab-D y Lab-E: Como la LAN de ambos routers es la misma, sólo hace falta configurar un servidor: tomaremos Lab-E, que además va a actuar como puerta de enlace predeterminada de su LAN.

DHCP sirve para configurar IP automáticamente. Esto incluye además de las direcciones IP y el router por defecto, otras posibilidades, de las que vamos a tomar como ejemplo el servidor DNS y el nombre de dominio.

Tomemos como ejemplo la configuración de **Lab-A** para ver los comandos que tenemos que aplicar y para qué sirven:

Comando	Qué hace
Lab-A (config) #service dhcp	Activar servicio DHCP
Lab-A (config) #ip dhcp pool red-10	Da el nombre red-10 al pool de direcciones (ámbito, conjunto de direcciones) a utilizar
Lab-A (dhcp-config) #network 10.0.0.0 255.0.0.0	Indica el ámbito (10.*.*) (conjunto de direcciones que se van a asignar a los hosts). Cada host tomará una de esas direcciones que repartirá DHCP.
	A partir de aquí se trata de otras opciones de la configuración IP que serán aplicadas a cada host cliente de este DHCP:
Lab-A (dhcp-config) #default-router 10.0.0.1	Puerta de enlace predeterminada (router por defecto)
Lab-A (dhcp-config) #dns-server 10.0.0.3	Servidor DNS
Lab-A (dhcp-config) #domain-name lab-a.net	Nombre de Dominio

Además, normalmente siempre hay que excluir una serie de direcciones (es habitual tomar las primeras) que no conviene que sean dinámicas, que estarán reservadas a dispositivos que querremos que tengan una ip fija, siempre la misma (routers, servidores...). Para ello usaremos esta otra instrucción:

Lab-A (config) #ip dhcp excluded-address 10.0.0.1 10.0.0.10	Reservar las 10 primeras direcciones 10.0.0.1-10, excluirlas del pool red-10 .
--	---

Paso A.3. Configuración de Clientes DHCP

Nota sobre entorno Windows: para que un PC busque un servidor DHCP para su configuración IP, suele verse como "obtener dirección IP automáticamente" dentro de su configuración TCP/IP, lo que permite obtener la ip al arrancar el PC. El comando ipconfig permite ciertas opciones de DHCP (renovación, etc...).

En el entorno Linux de los PCs del laboratorio, lo que haremos es activar el cliente DHCP y forzar una petición de configuración tecleando lo siguiente:

```
dhclient
```

Paso A.4. Comprobación del funcionamiento de DHCP en los PCs

Ahora podemos comprobar el funcionamiento del DHCP, para ello tras haber solicitado la configuración automática de IP mediante DHCP desde un PC cliente, por ejemplo tecleando dhclient en ET-1, podemos revisar la configuración IP para ver que todo se ha asignado tal y como definimos en nuestro servidor DHCP, es decir:

- Se ha asignado como dirección IP de forma automática una del pool, normalmente será la primera (10.0.0.11/8) → Lo podremos ver con ifconfig. Comprobar especialmente las direcciones IP de los PCs ET-4 y ET-5 que están en la misma LAN.
- Se ha asignado como router por defecto el que pusimos en DHCP → Lo podremos ver con route -n.

NOTA: Si esto no funciona, introducir manualmente el router por defecto y volver a comprobar que está bien introducido con route -n

- El servidor dns y el nombre del dominio son los que pusimos en DHCP → Lo podremos ver entrando en la configuración de red del Linux.

Paso A.5. Monitorización de DHCP en router

Utiliza el comando `show ip dhcp ?` y apunta las opciones

Utiliza las opciones **conflict** y **binding** y observa los resultados.

Utiliza también estos 2 comandos y observa los resultados:

```
show ip dhcp pool
show ip dhcp server statistics.
```

Realiza ahora las siguientes pruebas de conectividad (ping) desde los PCs. Anota los resultados y trata de explicarlos:

- a.- hacia las interfaces F0 y S0 y S1 de tu router
- b.- hacia las interfaces S0 o S1 de uno de tus routers vecinos

Parte B : Configuración de NAT Overload (PAT) en el router

Dado que las IP asignadas son privadas y además duplicadas, vamos a configurar NAT para que nos haga traducción de IP y puerto, de forma controlada, para evitar el solape de direcciones.

Vamos además a suponer que no disponemos de muchas IP y por eso usaremos la misma IP de las interfaces serie, que supondremos que son públicas y están asignadas por el operador para realizar PAT (NAT overload) sobre ellas.

Además, hay que tener en cuenta, que el NAT sólo se configura en un único punto de salida de toda la red, esto es importante tenerlo en cuenta en la LAN de Lab-D y Lab-E. En esta LAN tomaremos como router para hacer NAT el mismo que hemos usado para DHCP, y que hemos configurado en los clientes como router por defecto, es decir Lab-E.

Paso B.1. Configuración de NAT

Para configurar NAT con la opción de overload, hay que realizar la siguiente configuración:

Comando	Qué hace
Router(config)# ip nat pool <i>name start-ip end-ip</i> { netmask <i>netmask</i> prefix-length <i>prefix-length</i> }	Definir pool o conjunto de ip disponibles sobre las que se va a realizar NAT.
Router(config)# access-list <i>access-list-number</i> permit source [<i>source-wildcard</i>]	Definir el tráfico al que se va a permitir hacer NAT
Router(config)# ip nat inside source list <i>access-list-numb</i> pool <i>name</i> [<i>overload</i>]	Definir el proceso de NAT de las direcciones inside (internas) modificando la dirección de origen (source)

En nuestro caso (ej: Lab-A):

Lab-A(config)# ip nat pool <i>MILABA</i> 201.100.11.1 201.100.11.1 netmask 255.255.255.252	MILABA es el nombre (interno al router) que hemos dado al pool. Como dirección hay que usar una cualquiera de las dos de los dos serial. En este caso se está usando la dirección 201.100.11.1 del S0 de Lab-A, ip que debe ser alcanzable por todos los routers de la maqueta
Lab-A(config)# access-list 50 permit 10.0.0.0 0.255.255.255	
Lab-A(config)# ip nat inside source list 50 pool <i>MILABA</i> <u>overload</u>	

Para completar la configuración de NAT es necesario identificar qué interfaces van a ser internas y cuales van a ser externas con los siguientes comandos:

```
Lab-A(config)#interface fastethernet0
```

```
Lab-A(config-if)#ip nat inside
```

```
Lab-A(config)#inteface serial0
```

```
Lab-A(config-if)#ip nat outside
```

```
Lab-A(config-if)#interface serial1
```

```
Lab-A(config)#ip nat outside
```

NOTA: Cabe destacar que **otra forma de realizar la misma configuración** hubiera sido con:

```
Router(config)#ip nat inside source list access-list-number interface  
if-name
```

Donde el nombre de la interfaz sería la que utilizaría para obtener la IP (en vez de asignársela por el pool), para realizar el NAT overload (o PAT).

Paso B.2. Comprobación funcionamiento NAT

Ahora podemos comprobar el funcionamiento del NAT, haciendo ping desde los hosts a las interfaces serie de los routers. Con ello, podremos comprobar que recibimos respuesta porque nuestros paquetes IP saldrán con la IP modificada, utilizando overload sobre la IP serie de nuestro router por defecto.

Paso B.3. Monitorización del funcionamiento de NAT

Para ver información sobre el funcionamiento de NAT, podemos probar los siguientes comandos desde el router (probarlos, hacer pings, volverlos a probar...):

```
Router#show ip nat translations verbose  
Router#show ip nat statistics
```

Ahora vamos a realizar la siguiente prueba. En primer lugar borramos las asignaciones realizadas y a continuación activamos la depuración de NAT:

```
Router#clear ip nat translation *  
Router#debug ip nat
```

Ahora volvemos a comprobar el funcionamiento del NAT, haciendo ping desde los hosts a las interfaces serie de los routers.

Para desactivar la depuración: Router#**undebug all**

Paso B.4. Repaso de Conceptos

Responda a las siguientes preguntas:

- 1.- Hemos comprobado que la conexión desde el interior al exterior funciona, siempre y cuando el interior inicie la conexión (cliente). ¿Qué pasa en caso contrario, es decir si desde el exterior (ej. Otro router) queremos conectarnos a una IP interior?

- 2.- En el caso de tener servidores internos, por ejemplo servidores web, ¿qué solución le daría para que pudieran ser accedidos desde el exterior?

- 3.- Podrían dos hosts de dos LAN diferentes comunicarse tal como hemos configurado la maqueta ¿por qué?

- 4.- Discute sobre ¿cuál debería ser la utilización de NAT y DHCP cuando en nuestra LAN tenemos servidores? Ten en cuenta que los servidores requieren una IP fija y que DHCP en principio entrega las IP de forma dinámica.

- 5.- ¿Por qué en una LAN, el NAT se ha de realizar en un único punto, y si tenemos 2 routers como Lab-D y Lab-E, sólo se realiza en uno de ellos?.