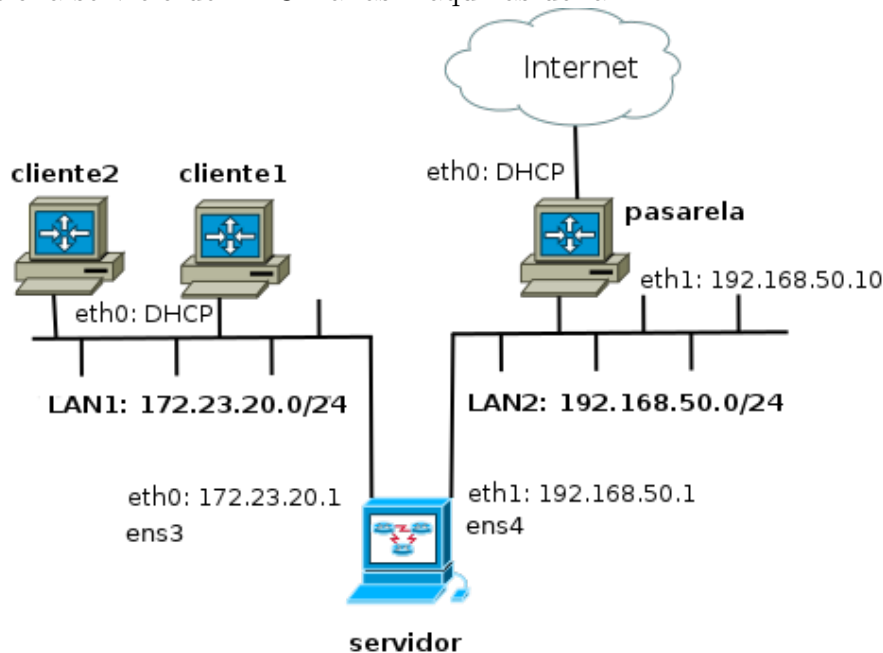


## 7. Prácticas de gestión de redes

**Entrega:** Enseñar al profesor en el aula las 4 máquinas funcionando con conexión a Internet, así como un fichero de texto con los comandos utilizados en la configuración.

### Esquema de la red

En nuestra nueva empresa disponemos de un servidor Linux que proporciona servicios a dos redes, LAN1 y LAN2, como se muestra en el diagrama adjunto. A su vez, una de las máquinas de la LAN sirve de pasarela cara Internet. El servidor proporciona servicio de DHCP a las máquinas de la LAN1.



### Configuración de las máquinas virtuales:

Para realizar esta práctica necesitaremos cuatro máquinas. Crearemos todas las máquinas usando como base la imagen que ya tenemos creada (`cliente1.img`). Pasos:

- Renombra `cliente1.img` y dale permisos de solo lectura

```
$ mv cliente1.img cliente-base.img  
$ chmod -w cliente-base.img
```

- Crea las cuatro máquinas

```
$ qemu-img create -b cliente-base.img -f qcow2 cliente1.img
```

```
$ qemu-img create -b cliente-base.img -f qcow2 cliente2.img
$ qemu-img create -b cliente-base.img -f qcow2 pasarela.img
$ qemu-img create -b cliente-base.img -f qcow2 servidor.img
```

Una vez creadas, arranca las cuatro máquinas con los scripts indicados a continuación (se puede escribir todo en el mismo script). Se dan dos posibles soluciones, siendo preferible la primera.

Nota: debido a la configuración de red que estamos usando, el servidor siempre tiene que ser la primera máquina en iniciarse, y la última en apagarse.

### Conexión mediante sockets UDP

La conexión de red entre máquinas puede simularse en KVM usando sockets UDP. Para la conexión hay que elegir dos puertos mayores que 1024. Puesto que las transmisiones son multicast, para que las conexiones de diferentes ordenadores del aula no se mezclen, deberán usarse puertos diferentes, lo que en la práctica puede hacerse eligiéndolos aleatoriamente (este problema solo ocurre en la red de cable de la USC, pues la red inalámbrica filtra las transmisiones multicast).

#### ■ Servidor:

```
$ PORT1=elegir un puerto mayor que 1024
$ PORT2=elegir otro puerto mayor que 1024
$ kvm -name "Servidor" -m 512M -hda servidor.img \
    -net nic,vlan=1,macaddr=52:54:00:12:34:56 \
    -net socket,vlan=1,name=lan1,mcast=224.0.0.1:$PORT1 \
    -net nic,vlan=2,macaddr=52:54:00:12:34:57 \
    -net socket,vlan=2,name=lan2,mcast=224.0.0.1:$PORT2 &
```

#### ■ Pasarela:

```
$ kvm -name "Pasarela" -m 256M -hda pasarela.img \
    -net nic,macaddr=52:54:00:12:34:58 \
    -net user,hostfwd=tcp::2222-:22 \
    -net nic,vlan=2,macaddr=52:54:00:12:34:59 \
    -net socket,vlan=2,name=lan2,mcast=224.0.0.1:$PORT2 &
```

#### ■ Cliente 1:

```
$ kvm -name "Cliente1" -m 256M -hda cliente1.img \
    -net nic,vlan=1,macaddr=52:54:00:12:34:60 \
    -net socket,vlan=1,name=lan1,mcast=224.0.0.1:$PORT1 &
```

- Cliente 2:

```
$ kvm -name "Cliente2" -m 256M -hda cliente2.img \
-net nic,vlan=1,macaddr=52:54:00:12:34:61 \
-net socket,vlan=1,name=lan1,mcast=224.0.0.1:$PORT1 &
```

## Conexión mediante sockets TCP

En el caso de no poder usar el esquema anterior, se puede realizar la conexión entre las máquinas KVM mediante sockets TCP. En las nuevas versiones de KVM esta configuración tiene el problema de que solo nos dejará conectar un cliente.

- Servidor:

```
$ PORT1=1234
$ PORT2=2345
$ kvm -name "Servidor" -m 1G -hda servidor.img \
-net nic,vlan=1,macaddr=52:54:00:12:34:56 \
-net socket,vlan=1,name=lan1,listen=$PORT1 \
-net nic,vlan=2,macaddr=52:54:00:12:34:57 \
-net socket,vlan=2,name=lan2,listen=$PORT2 &
```

- Pasarela:

```
$ sleep 1
$ kvm -name "Pasarela" -m 256M -hda pasarela.img \
-net nic,macaddr=52:54:00:12:34:58 \
-net user,hostfwd=tcp::2222-:22 \
-net nic,vlan=2,macaddr=52:54:00:12:34:59 \
-net socket,vlan=2,name=lan2,connect=127.0.0.1:$PORT2 &
```

- Cliente 1:

```
$ sleep 1
$ kvm -name "Cliente1" -m 256M -hda cliente1.img \
-net nic,vlan=1,macaddr=52:54:00:12:34:60 \
-net socket,vlan=1,name=lan1,connect=127.0.0.1:$PORT1 &
```

- Cliente 2:

```
$ sleep 1
$ kvm -name "Cliente2" -m 256M -hda cliente2.img \
-net nic,vlan=1,macaddr=52:54:00:12:34:61 \
-net socket,vlan=1,name=lan1,connect=127.0.0.1:$PORT1 &
```

## Ajustes

- Obtén con el comando `ifconfig -a` el nombre de los interfaces de red:

Distribución:	<i>jessie</i>	<i>buster</i>
servidor y pasarela:	eth0 y eth1	ens3 y ens4
cliente1 y cliente2:	eth0	ens3

- Cambia el nombre a las máquinas `pasarela.img`, `servidor.img` y `cliente2.img` modificando los ficheros `/etc/hosts` y `/etc/hostname` y llámale `pasarela`, `servidor` y `cliente2`, respectivamente.
- Reinicia las cuatro máquinas.

### 7.1. Configuración de la pasarela (2 puntos)

1. Esta máquina presenta dos interfaces de red, de las cuales el conectado a Internet ya debería estar configurado mediante el servicio DHCP del KVM, incluyendo la pasarela por defecto de la máquina.

Para el interfaz conectado a la LAN2, edita el fichero de configuración de red de la pasarela, `/etc/network/interfaces`, y configura de forma manual los datos estáticos: IP, máscara, dirección de red y dirección de broadcast. Este interfaz no tiene pasarela por defecto, puesto que solo hay que poner una por máquina y el otro interface ya tiene una. Incluye también en este fichero una ruta hacia la red de los clientes:

```
address (deducir los valores de la figura anterior)
netmask
network
broadcast
up route add -net 172.23.20.0/24 gw 192.168.50.1
```

2. Para que servidor pueda acceder a Internet a través de pasarela es necesario en pasarela activar el IP forwarding. Para ello activar en el fichero `/etc/sysctl.conf` la característica `net.ipv4.ip_forward`.
3. Para poder acceder a Internet desde servidor hay que hacer traducción de direcciones (NAT): los paquetes con origen en el servidor (y por tanto, con dirección privada `192.168.50.1`) cambian esta IP por la IP “real” de pasarela. El comando para hacer esto es (en pasarela):

```
$ iptables -t nat -A POSTROUTING -s 192.168.50.0/24 \
! -d 192.168.50.0/24 -j MASQUERADE
```

Es decir, “enmascara” (cambia la IP origen por la IP real de pasarela) los paquetes que vengan de la red 192.168.50.0/24 y que no tengan como destino esa misma red.

De igual forma, para que los clientes puedan acceder a Internet:

```
$ iptables -t nat -A POSTROUTING -s 172.23.20.0/24 \
! -d 192.168.50.0/24 -j MASQUERADE
```

Es decir, “enmascara” (cambia la IP origen por la IP real de pasarela) los paquetes que lleguen a pasarela desde la red 172.23.20.0/24 y que no tengan como destino la red LAN2 (es decir, que vayan hacia Internet).

Comprueba con `iptables-save` o con `iptables -L -t nat` las reglas introducidas.

4. Para hacer la configuración de traducción de direcciones permanente, instala el siguiente paquete:

```
$ apt-get install iptables-persistent
```

Si posteriormente se modifican las *iptables* debemos reconfigurar el paquete para que se haga permanente la nueva configuración: `dpkg-reconfigure iptables-persistent`.

5. Reinicia la pasarela
6. Comprueba que la configuración es correcta:
  - Comprueba las direcciones IP con el correspondiente comando.
  - Comprueba las rutas con el correspondiente comando.
  - Comprueba el fichero `/proc/sys/net/ipv4/ip_forward`.
  - Comprueba la traducción de direcciones:

```
$ iptables -L -t nat
```
  - Comprueba el fichero del servicio de nombres `/etc/resolv.conf`
  - Comprueba que se puede acceder a Internet, por ejemplo, ejecutando `apt-get update`.

## 7.2. Configuración del servidor (2 puntos)

1. En el fichero de configuración de red del servidor elimina el *allow-hotplug* y el *dhcpc* e incluye las dos interfaces con las direcciones IPs estáticas de la máquina.

En la interfaz que conecta con la pasarela ha de fijarse IP, máscara, dirección de red, dirección de broadcast y *gateway*. Tened en cuenta que la dirección

de la gateway es la dirección del interface de la máquina con la que se conecta, no de la propia máquina.

En la interfaz que conecta con la red interna (LAN1) ha de fijarse IP, máscara, dirección de red y dirección de broadcast. Esta interface no tiene dirección de *gateway*, pues solo se pone una ruta por defecto por máquina.

2. Activa el IP forwarding.
3. Reinicia el servidor.
4. Comprueba direcciones IP, ruta por defecto, IP forwarding y el fichero del servicio de nombres.
5. Comprueba que la conexión a la pasarela funciona mediante un `ping` a los dos interfaces de la pasarela.
6. Comprueba que la conexión al exterior funciona mediante un `ssh` a la IP del host (ordenador del laboratorio o portátil).
7. Comprueba que se puede hacer `apt-get update`.

### 7.3. Configuración de los clientes mediante comandos (2 puntos)

En este apartado las configuraciones que vamos a realizar son temporales, es decir, se borran cuando se reinicia la máquina. Por tanto, guardar los comandos en un fichero en la correspondiente máquina, para poder recuperarlos rápidamente.

1. Configura la IP de los clientes con el comando `ifconfig`. Para ello asignarles una dirección IP de acuerdo con la red a la que pertenecen.
2. Configura la ruta por defecto con el comando `route`.
3. Comprueba que el servicio de nombres del fichero `/etc/resolv.conf` es correcto, comparando con el que se encuentra en el servidor o la pasarela.
4. Configura el IP forwarding (realmente los clientes no lo necesitan, pero lo haremos como ejercicio):

```
$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

5. Haz las comprobaciones pertinentes y asegúrate que los clientes pueden conectarse a Internet.

## 7.4. Configuración del servidor de DHCP (3 puntos)

1. En la máquina servidor instala el servidor de DHCP, disponible en el paquete `isc-dhcp-server`.
2. Configura el servidor de DHCP para que los sistemas en la red LAN1 puedan obtener su configuración de red del servidor.

En `/etc/default/isc-dhcp-server` indica el interface que conecta con la LAN1. Considera solo IPv4, si hay alguna línea de IPv6 coméntala.

3. En `/etc/dhcp/dhcpd.conf` va el nombre de dominio (`nombre.apellido1.apellido2`), servidores DNS (podemos poner todos, los de KVM: 10.0.2.3, Google: 8.8.8.8 y 8.8.4.4 y USC: 193.144.75.9 y 193.144.75.12) y añadimos una subnet definida por la dirección de red y la máscara (obten los datos a partir de la figura) y proporcione el rango de IPs (172.23.20.2 172.23.20.199), dirección de broadcast y pasarela (routers).
4. Adicionalmente, configura el servidor de DHCP para que la máquina *cliente1* obtenga siempre la misma IP 172.23.20.200 (el resto de sistemas de la LAN1, es decir, *cliente2*, deben seguir obteniendo una IP dinámica). El servidor detecta al cliente1 a través de su dirección Ethernet (busca cuál es con el comando `ifconfig eth0/ens3` en cliente1).
5. Reinicia el servicio de DHCP con: `systemctl restart isc-dhcp-server`. Fíjate en que no dé error (en caso de error, mira los ficheros de log, incluyendo el fichero `/var/log/syslog`).
6. Haz que los clientes obtengan los datos de red con `dhclient eth0/ens3`.
7. Comprueba que la red de los clientes está correctamente configurada, que se puede hacer ping entre el servidor y los clientes y que los clientes pueden acceder a Internet.
8. Verifica en los clientes que el fichero `/etc/network/interfaces` tiene la configuración por DHCP (si no tocamos nada debería ser así). Reinicia los clientes y comprueba.

## 7.5. Configuración de nombres (1 punto)

1. Para terminar, modifica en las cuatro máquinas los ficheros necesarios para poder referirnos a *servidor*, *pasarela* y *cliente1* usando nombres en lugar de IPs (por ejemplo, `ping pasarela.nombre.apellido1.apellido2` o `ping servidor`).
2. Como última comprobación, reinicia las cuatro máquinas y comprueba que todo funciona correctamente.