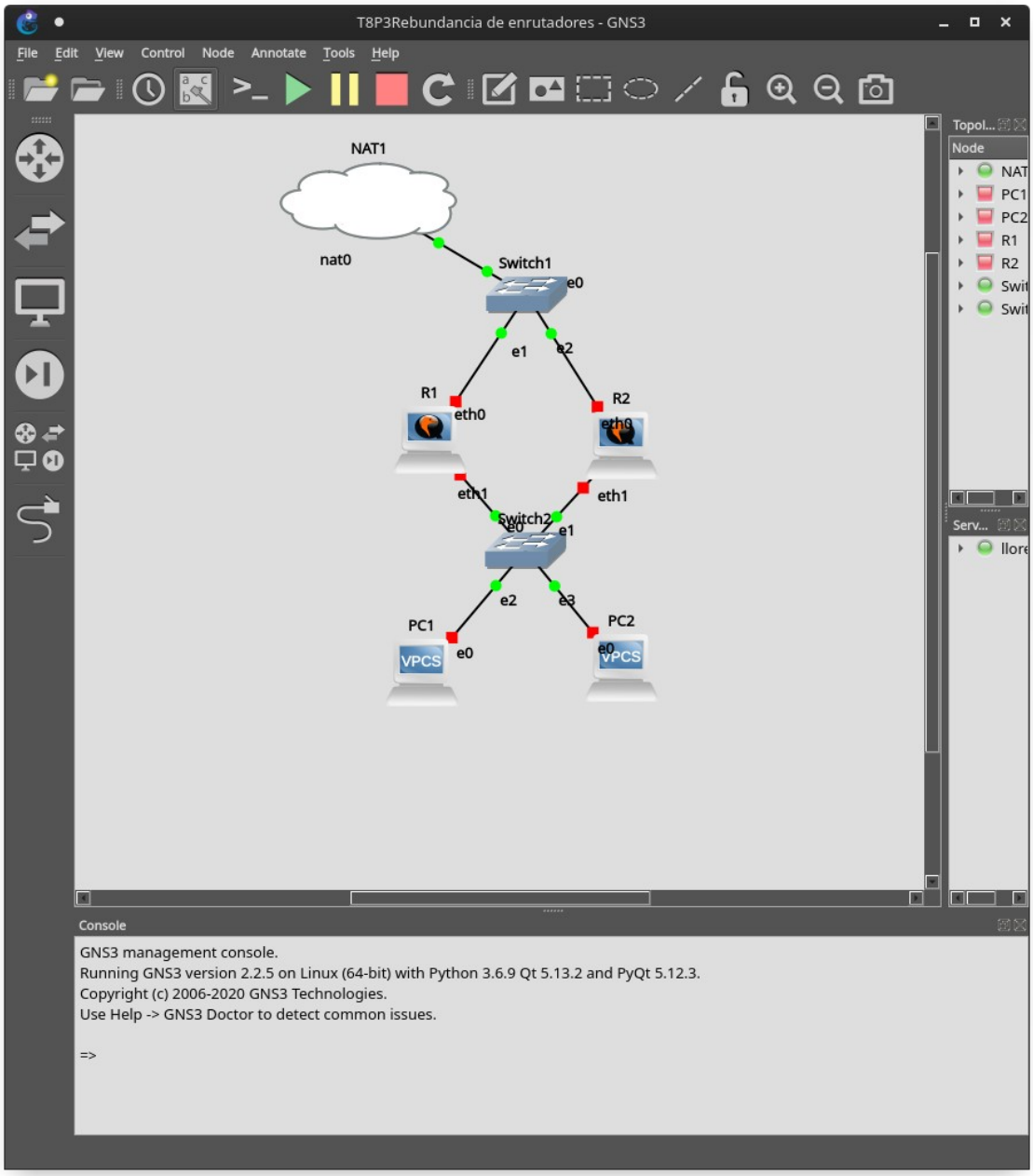
Redundancia de enrutadores

Esta practica la realizaremos con GNS3 la verdad que el programa esta bien pero es un continuo tira y alfloja con el por problemas de configuración, las ventanas por VNC a veces me da problemas por que se visualiza mal,etc.

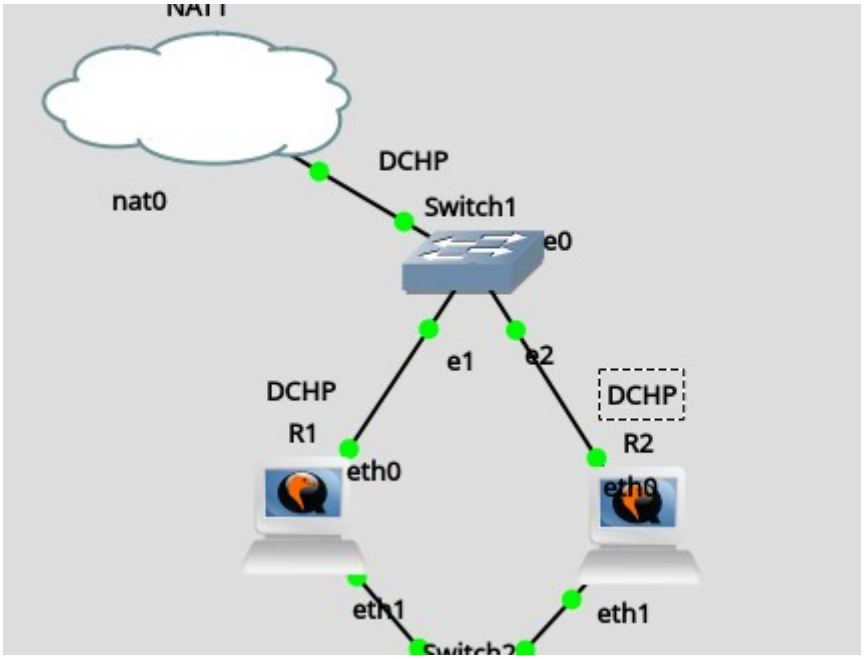
De todas formas vamos a por el.

Primeramente preparo el proyecto como sugieres en el enunciado de la practica.



Redundancia de enrutadores

Seguidamente preparamos para que todos los routers tengan internet que como siempre la nube NAT debe estar en DCHP para que logre conectar por lo tanto las interfaces eth0 del dibujo estarán en DCHP para que el router les asigne una IP.



Seguidamente para que a los VPCS que harán de cliente vamos a configurar el firewall de los 2 routers para que tengan internet. En practicas anteriores ya lo hicimos. Dejo el recorte por mera información.

Redundancia de enrutadores

Habilitar ip forwarding

Para habilitar el **ip forwarding** (enrutamiento) en GNU/Linux se puede proceder de la siguiente forma:

- Editar como root el **/etc/sysctl.conf** y poner **net.ipv4.ip_forward=1**
- Aplicar con **sysctl -p**

Habilitar NAT de origen

Para habilitar el **NAT** de origen (realmente es PAT) en el router de la sede, de forma que enmascare las direcciones privadas reemplazándolas por la dirección ip de su interfaz pública, se puede ejecutar como root el comando:

```
iptables -t nat -A POSTROUTING -s 172.20.0.0/24 -o eth0 -j
MASQUERADE
```

Este comando se realizaría en el equipo que hace de router en la sede 1, suponiendo que la interfaz WAN con la ip 192.168.0.20 de la figura, es la eth0. En un entorno de producción, este comando debería ejecutarse en un script de inicio en el sistema, para que sea persistente entre reinicios del router.

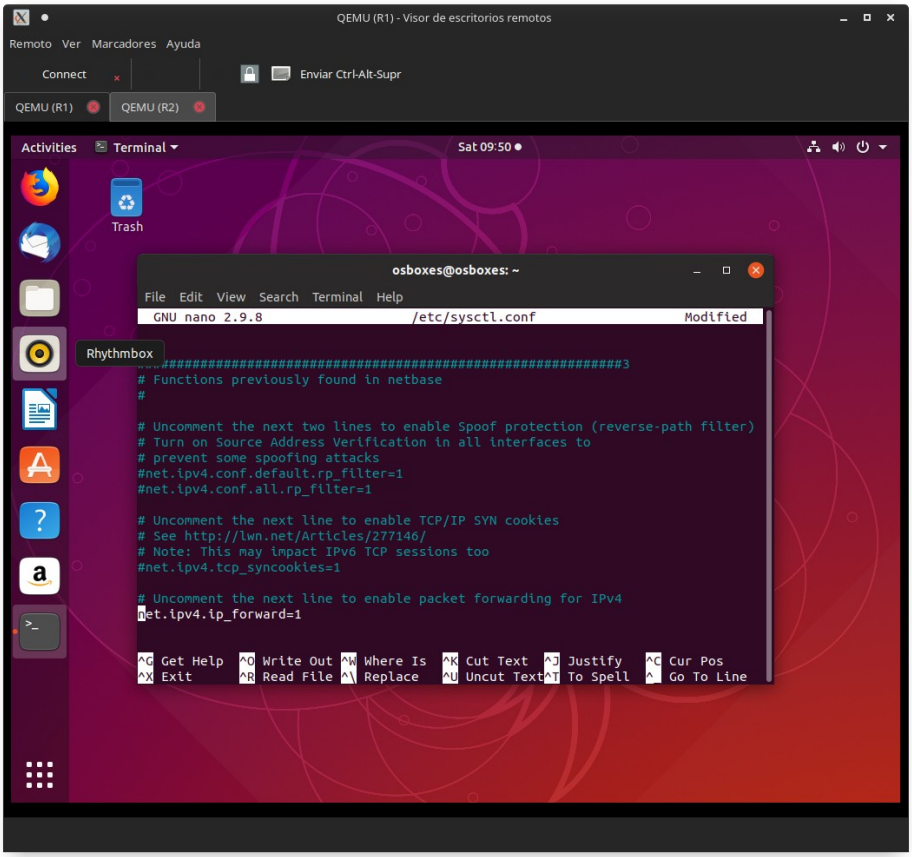
Problemas que podemos encontrarnos

Depende de la distribución GNU/Linux usada, en el router puede haber reglas de firewall o no. En caso de que las haya, es necesario deshabilitarlas para la práctica, bien con **iptables -F** o con el comando necesario para parar el firewall como **service iptables stop** o **systemctl stop firewalld.service**. Consultar la documentación de la distribución.

Es posible que tengas que **deshabilitar el firewall de Windows** si los clientes son Windows (pueden ser GNU/Linux perfectamente), para que funcione el ping entre ambos PC una vez establecida la VPN. Puedes pensar que no funciona la VPN y realmente es el firewall de Windows que elimina el ICMP entrante por defecto. La solución más elegante es crear una regla de entrada que permita el ICMP entrante en ambos PC.

Editamos el archivo sysctl.conf

Redundancia de enrutadores

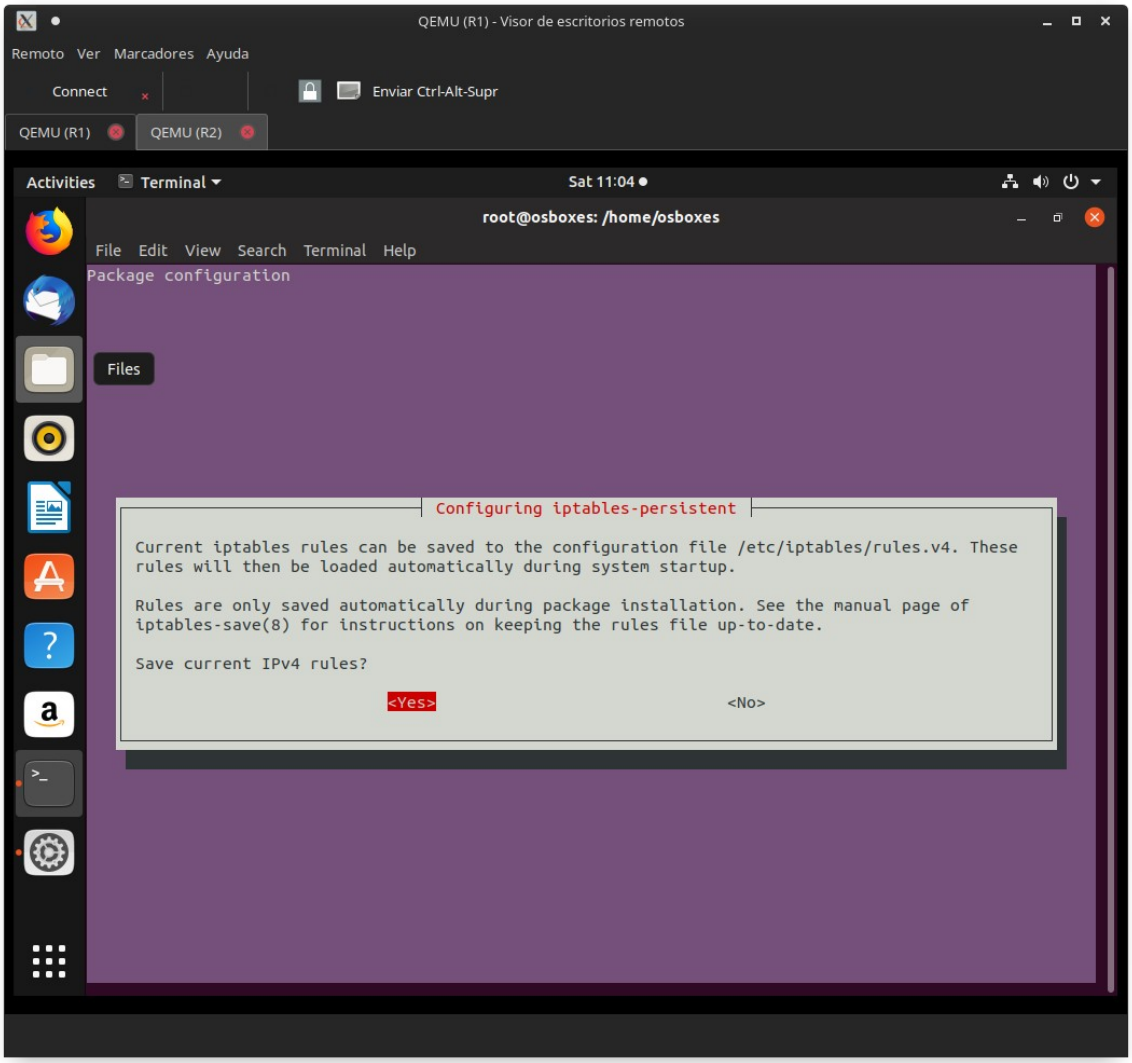


Aplicamos la regla del firewall

```
root@osboxes:/home/osboxes# iptables -t nat -A POSTROUTING -s 192.168.100.1/24 -o ens3 -j MASQUERADE
root@osboxes:/home/osboxes#
```

Despues instalamos `iptables-persistent` (aprendido de la web de la practica anterior) para que se mantenga la reglas del firewall cuando reiniciemos.

Redundancia de enrutadores



Seguidamente ya configuramos la red interna y el cliente que ahora describire para documentarlo dado que el GNS3 lo malo es que las maquinas tienen las interfaces un nombre y el dibujo otra. Se que se puede configurar editar pero falta tiempo xD

Pero comprobamos que el cliente VPCS tiene internet con un ping a 8.8.8.8

```
PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=54 time=9.975 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=54 time=9.785 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=54 time=10.404 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=54 time=9.587 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=54 time=10.291 ms
```

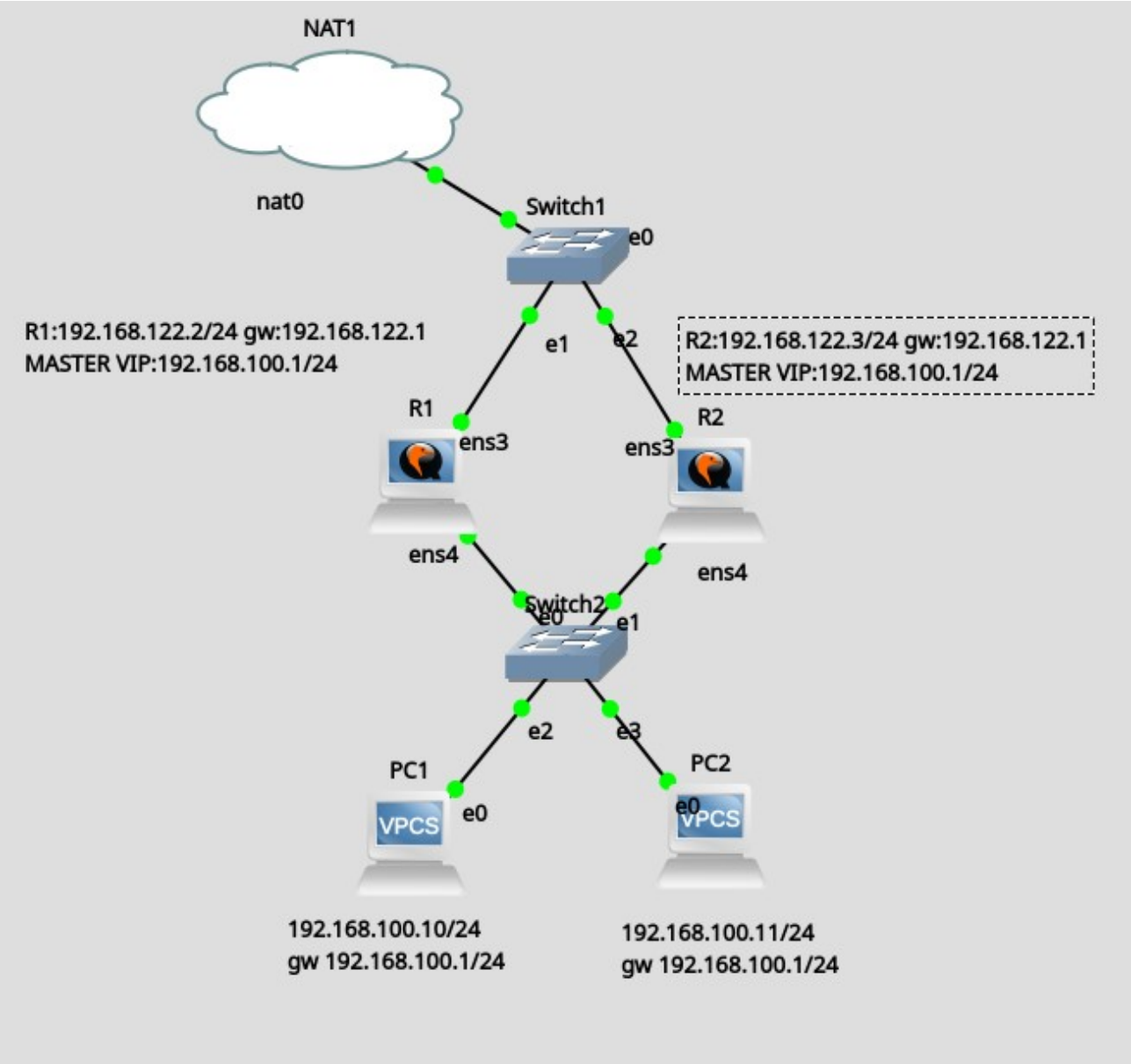
NAT en GNS3

Ahora vamos averiguar la NAT en GNS3 mirando por intenet sabemos 2 cosas

Redundancia de enrutadores

que si queremos Internet debe de tener un rango de IP 192.168.122.0/24 y el la puerta de enlace es 192.168.122.1 que es el que asigna el DCHP automáticamente y es la primera IP de la red

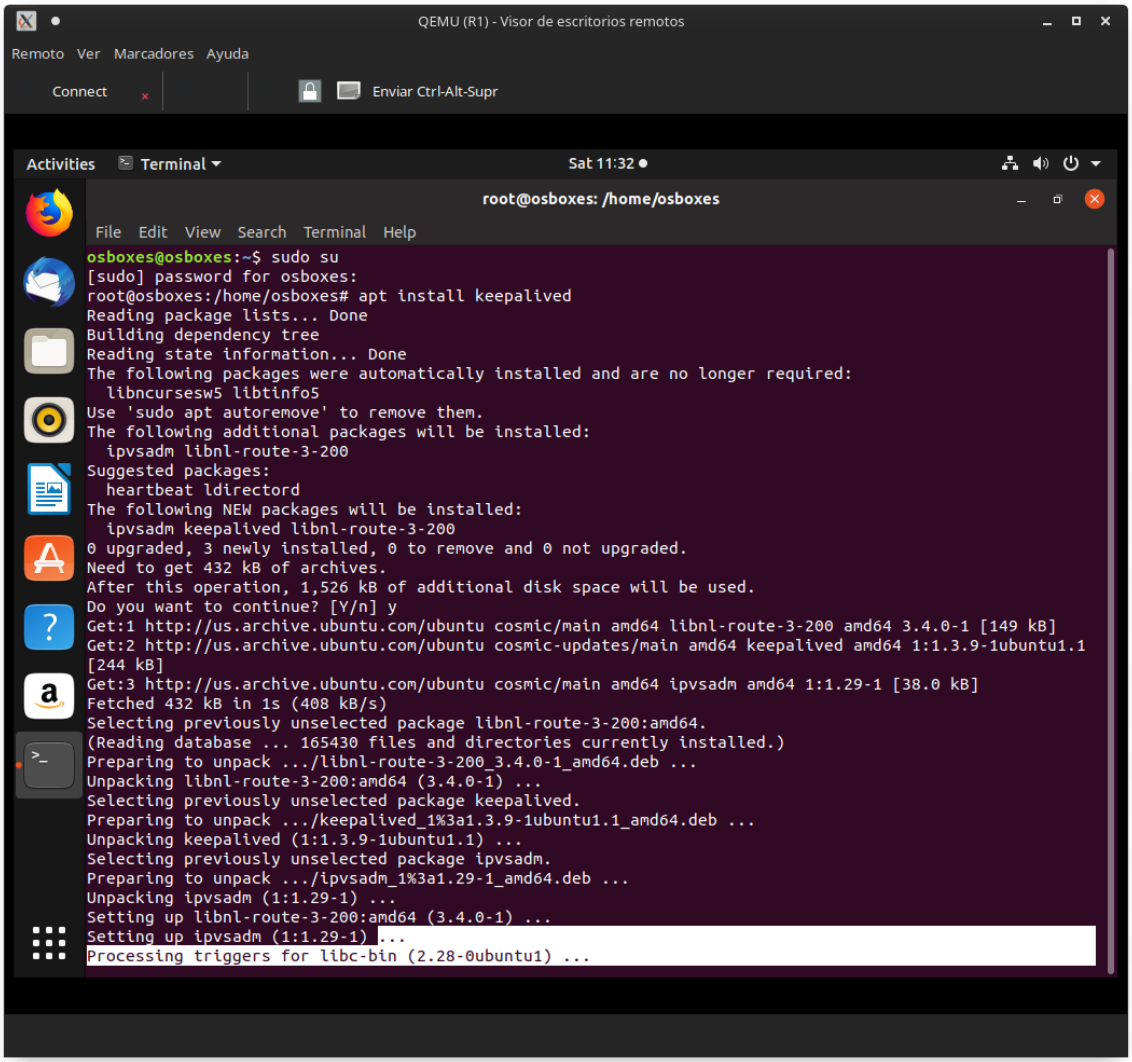
Por lo tanto asi queda la topologia.



Instalación de Keepalived

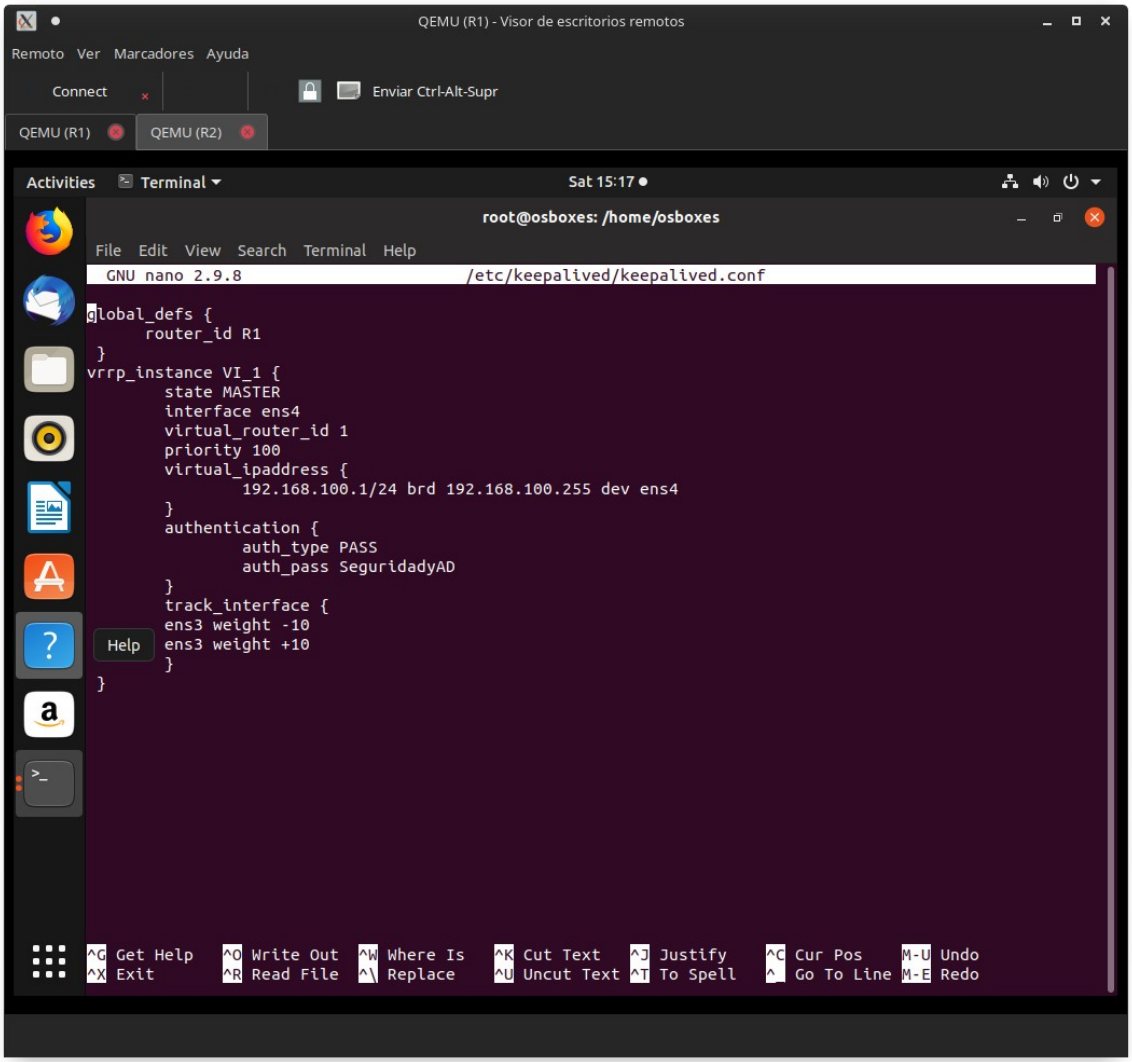
Redundancia de enrutadores

Siguiendo la practica pasamos a configurar el router1



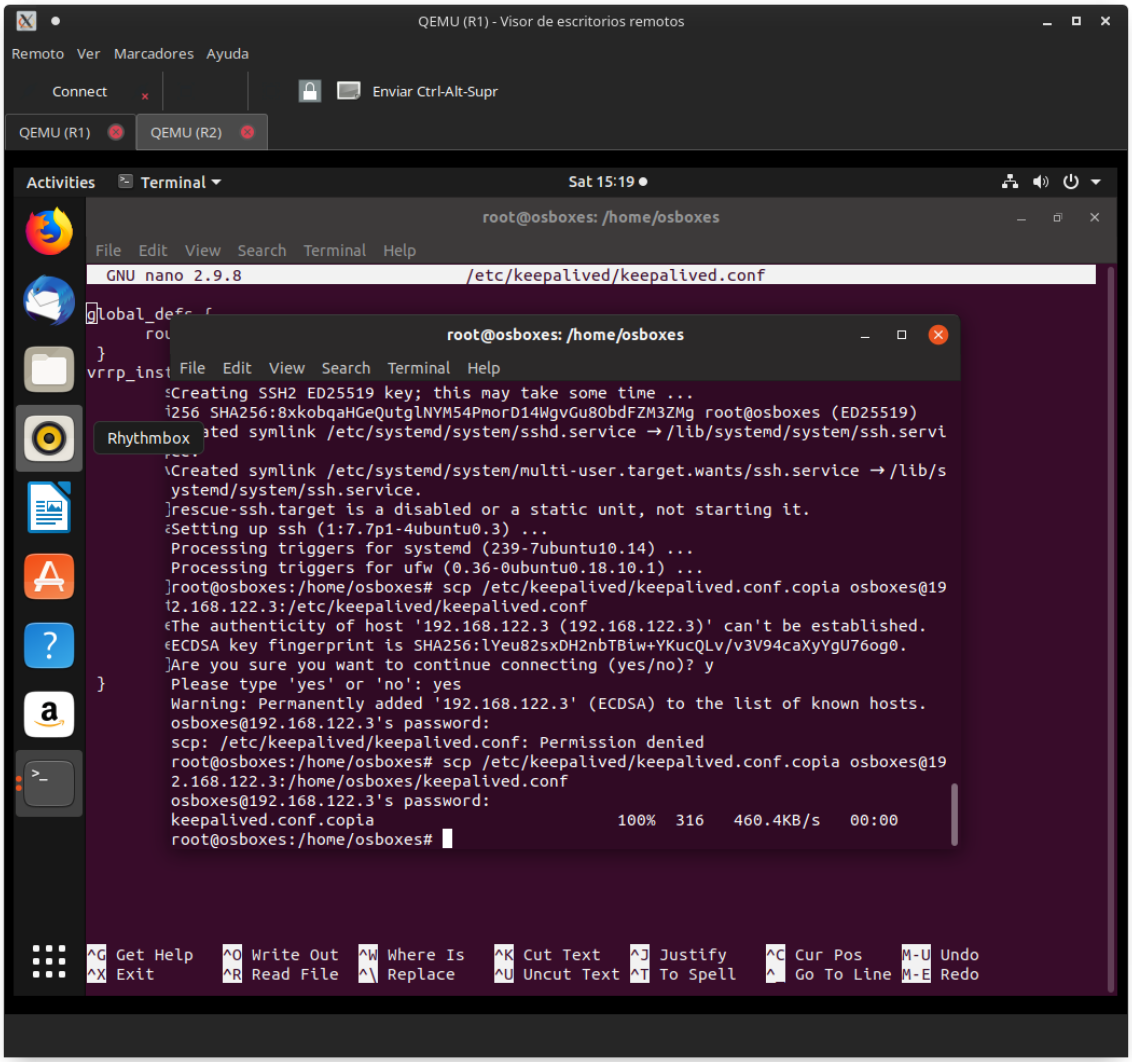
Creamos el archivo de configuración de keepalived

Redundancia de enrutadores



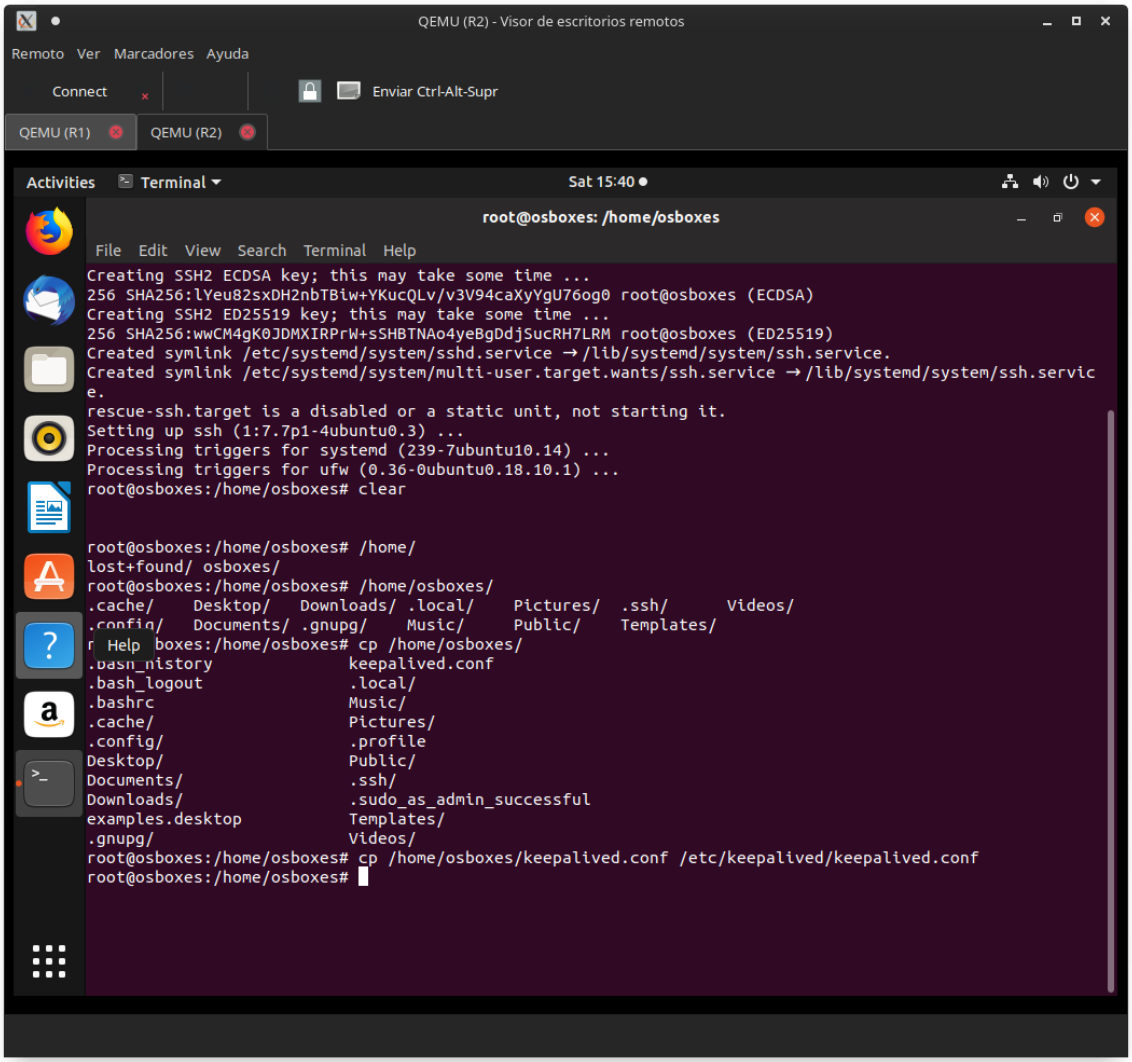
Redundancia de enrutadores

Instalamos SSH y mandamos una copia del archivo al R2 dado que lo he escrito a mano y mas adelante nos ara falta para configurarlo.



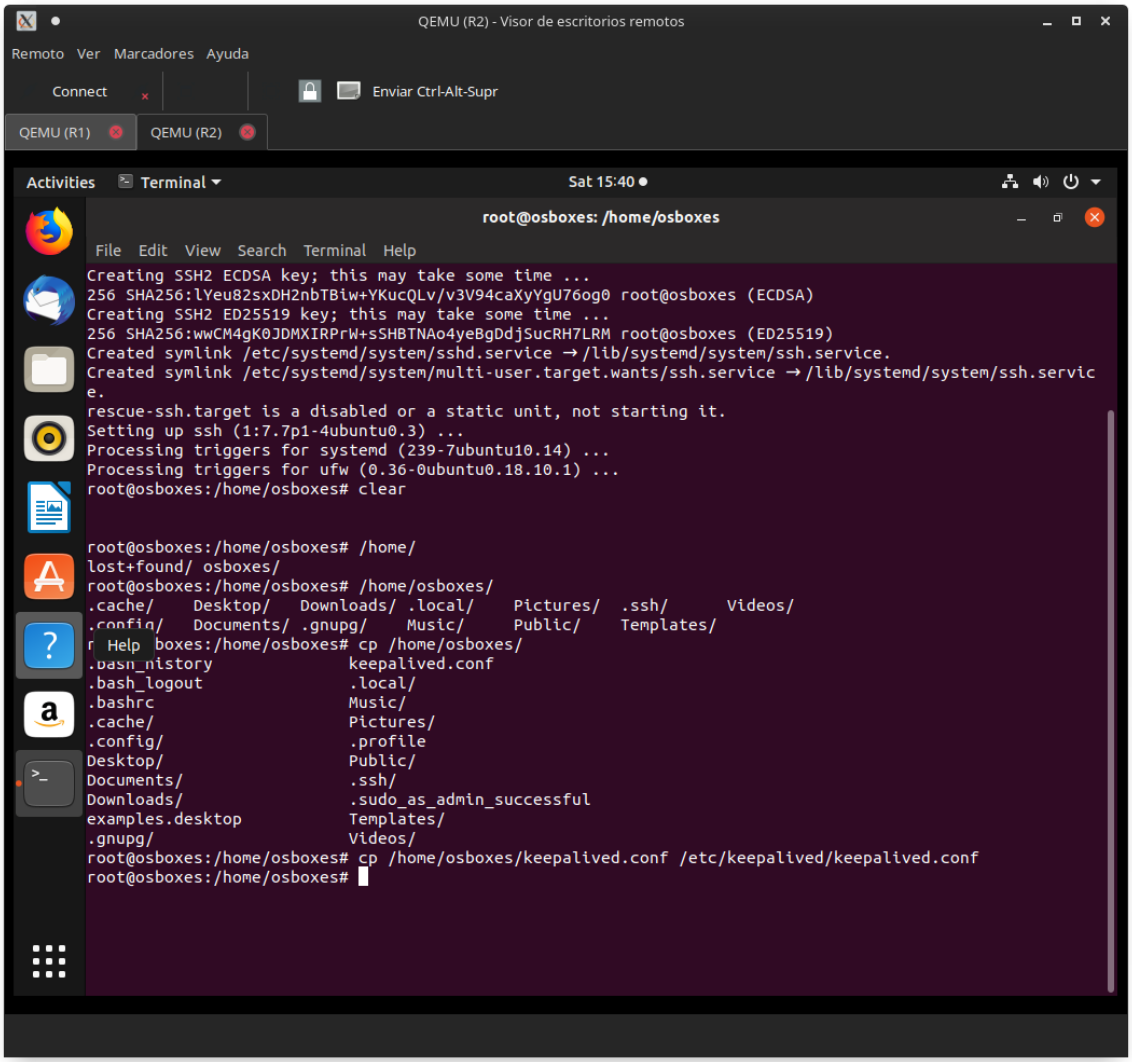
Redundancia de enrutadores

Ahora nos vamos al R2 y copiamos el archivo de configuración que esta en /home/osboxes y lo editaremos según indica la practica.



Redundancia de enrutadores

Editamos…



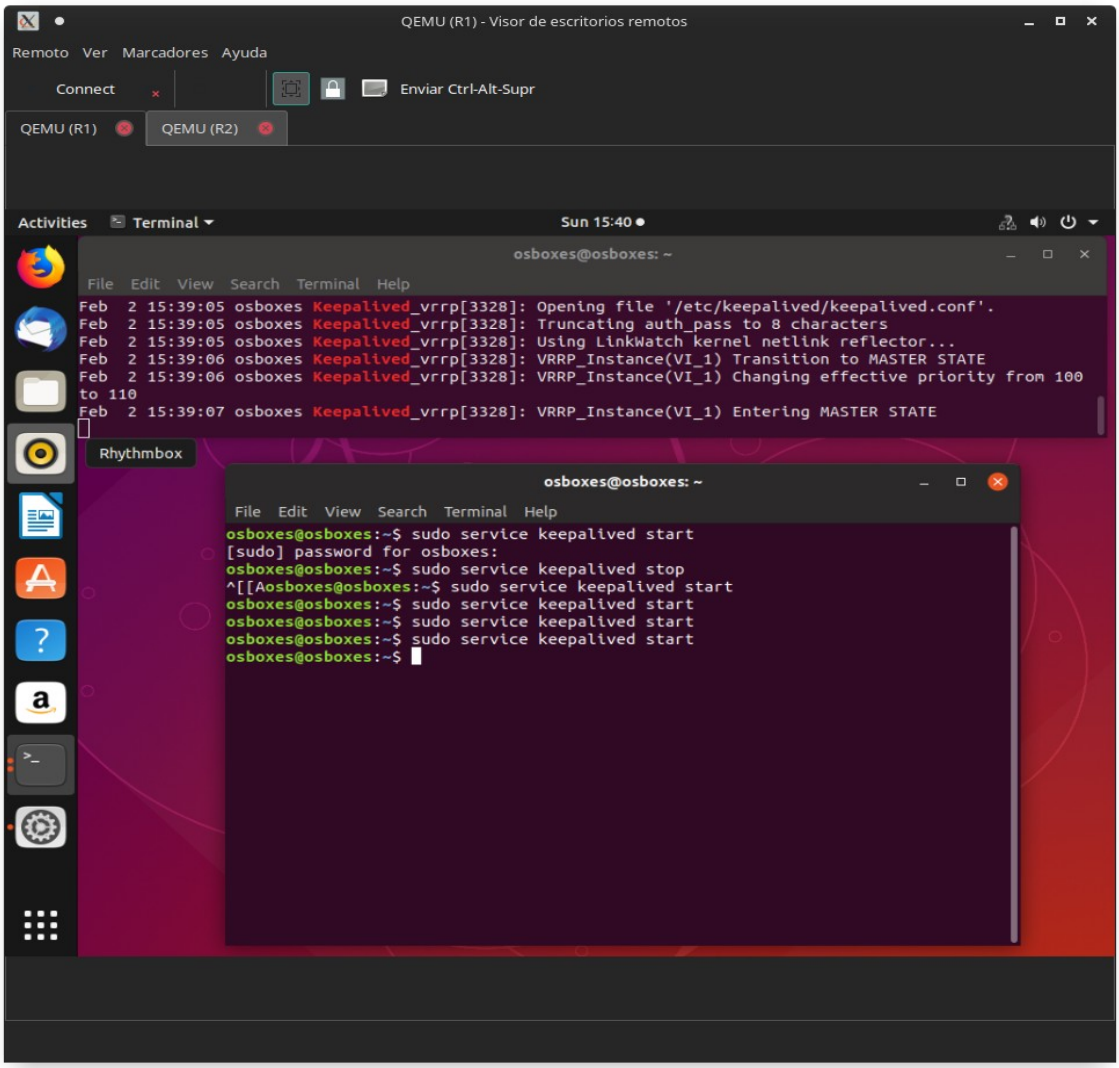
Y finalmente activaremos el servicio.

Redundancia de enrutadores

Pruebas

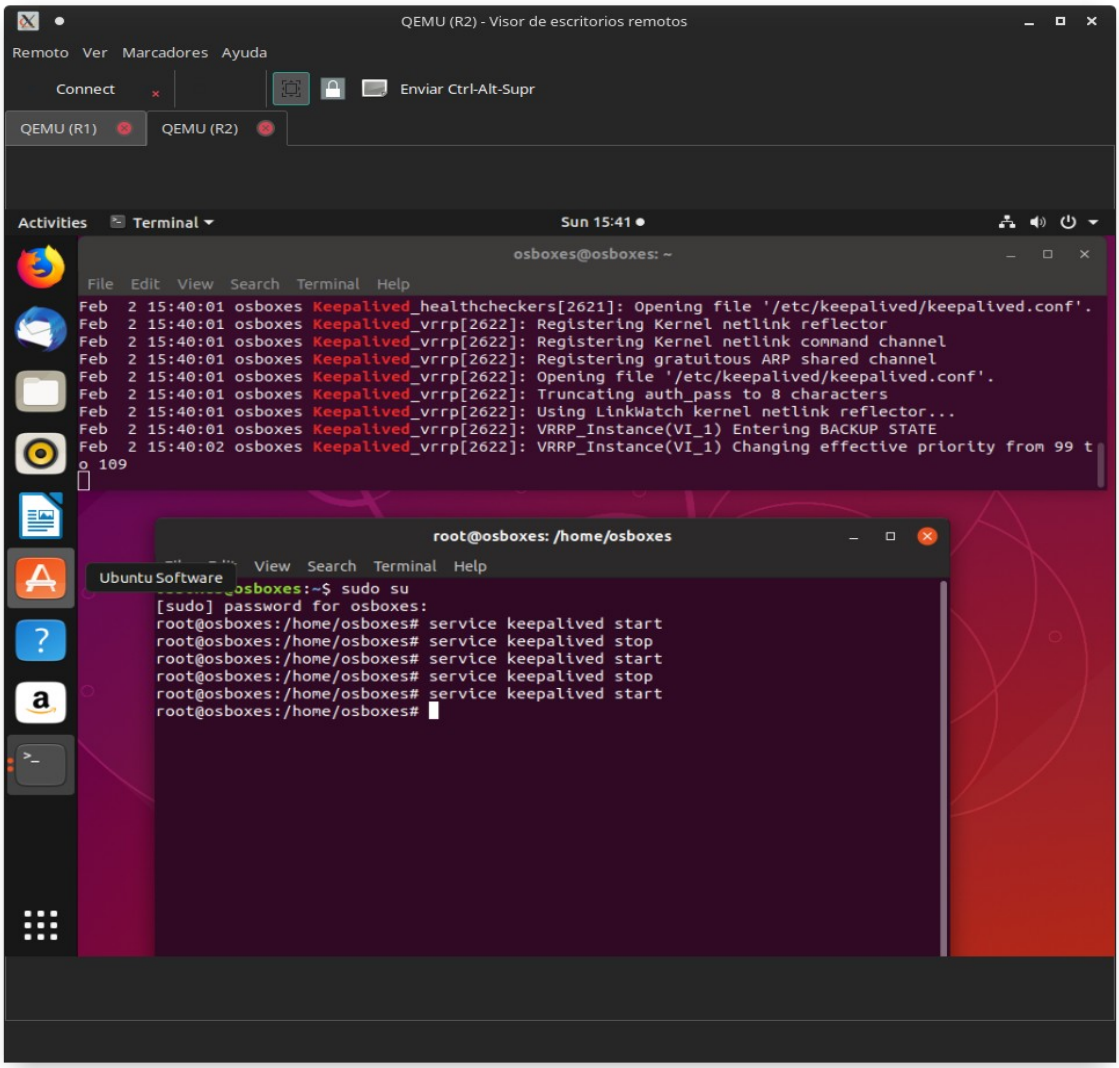
Ya con los 2 servicios activos comprobamos el estado actual

R1 esta en MASTER



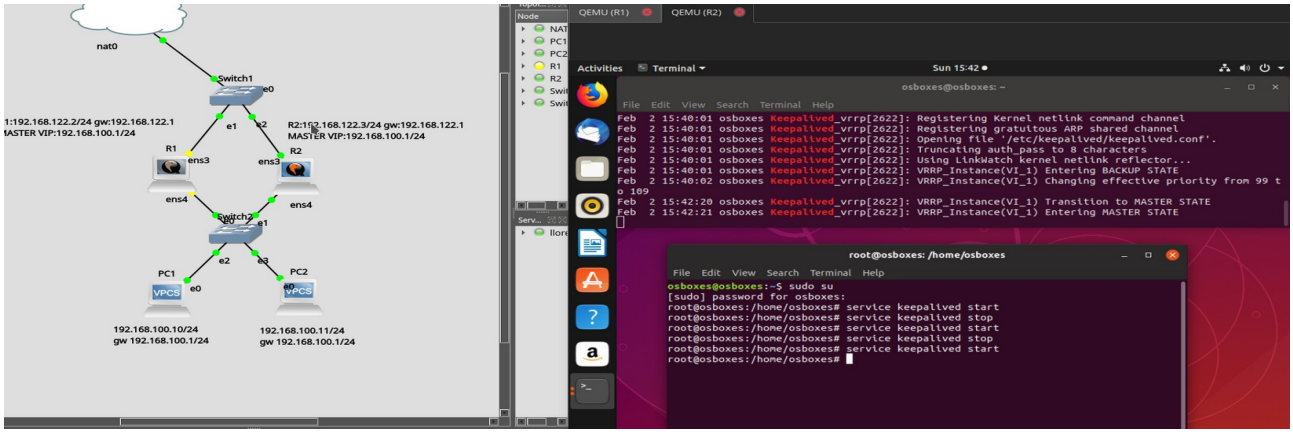
Redundancia de enrutadores

Y el R2 estara en BACKUP



Redundancia de enrutadores

Sin embargo como se aprecia en la misma captura suspendemos R1 y el estado del servicio R2 se vuelve MASTER automaticamente



Y vemos como los clientes aun siguen teniendo acceso a Internet

```
PC2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=54 time=10.864 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=54 time=10.729 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=54 time=10.658 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=54 time=10.873 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=54 time=11.101 ms
```