



MINISTERIO
DE EDUCACIÓN
Y CIENCIA

SECRETARÍA GENERAL
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL

DIRECCIÓN GENERAL
DE EDUCACIÓN,
FORMACIÓN PROFESIONAL
E INNOVACIÓN EDUCATIVA

CENTRO NACIONAL
DE INFORMACIÓN Y
COMUNICACIÓN EDUCATIVA

Redes de área local Aplicaciones y Servicios Linux

Enrutamiento



SERVICIO DE
FORMACIÓN DEL
PROFESORADO

Índice de contenido

Enrutamiento.....	3
Activar enrutamiento en Linux.....	4
Activación del enrutamiento en Linux.....	4
Creación del script para activar enrutamiento.....	5

Enrutamiento

Se puede definir el enrutamiento como la capacidad de transmitir datos entre redes interconectadas. Al agente encargado de realizar este encaminamiento de información entre redes se conoce como **enrutador o router** pudiendo ser de tipo hardware si es un dispositivo físico dedicado al encaminamiento y de tipo software en caso de ser un PC que ejecuta una aplicación que realice las funciones propias del enrutamiento.

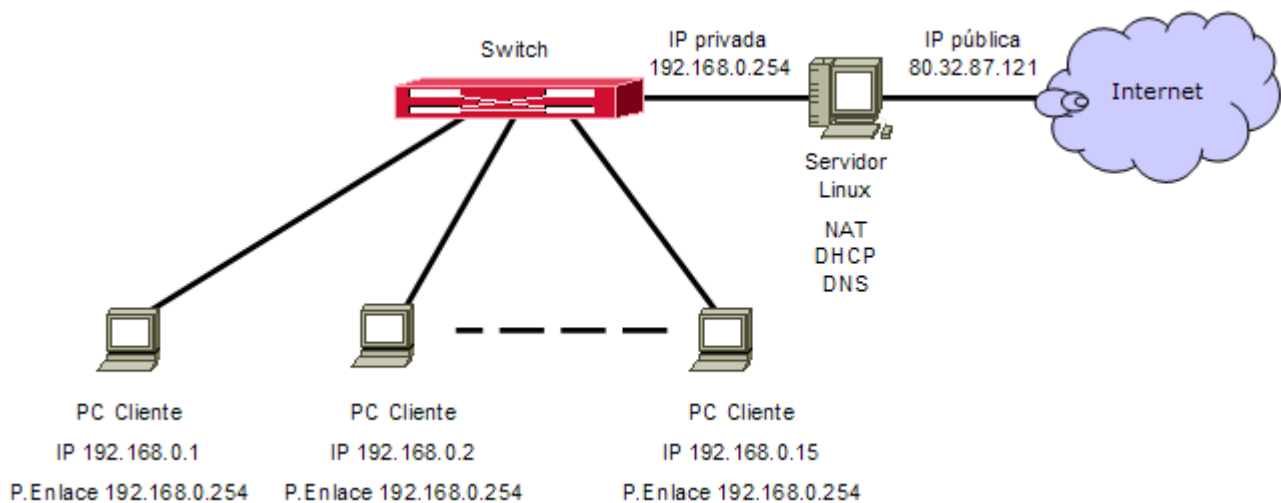
Con el software adecuado, nuestro servidor Linux podrá actuar de enrutador en nuestra red de manera que permitirá que los equipos de la red local se conecten a Internet como si lo hicieran a través de un router.

La tecnología empleada para permitir que los equipos de la red local se conecten a Internet a través de nuestro servidor Linux se denomina NAT - Network Address Translation (Traducción de Direcciones de Red). El software NAT que se ejecuta en nuestro servidor permite, que con una única dirección IP pública en el servidor, tengan acceso a Internet el resto de PCs de la red.

En los PCs de la red local se deberá configurar como puerta de enlace (gateway) la dirección IP interna del servidor para que sea éste quien reciba y procese los paquetes provenientes de la red interna y con destino hacia Internet.

Cuando desde un PC de la red local se quiere acceder a Internet, el paquete de datos se enviará al servidor linux ya que es la puerta de enlace. El software NAT del servidor cambiará en el paquete de datos la dirección IP de origen del PC de la red local por la dirección IP pública del servidor y lanzará el paquete de datos hacia Internet. En una tabla interna almacenará el puerto de salida del paquete junto con la IP del PC de la red local con la finalidad de que cuando llegue la respuesta desde Internet, realizar el proceso inverso y poder redirigirlo hacia el PC que lanzó la petición.

Si nuestro servidor Linux, dispone además de servidor DHCP, la configuración de las direcciones IP, la puerta de enlace y el servidor DNS de nuestros PCs, podrá ser establecida automáticamente por el servidor DHCP.



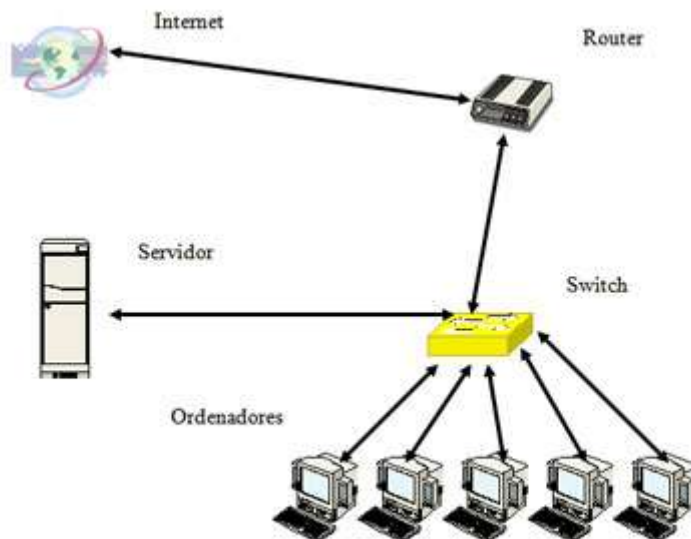
Una alternativa podría ser instalar en el servidor un proxy como **squid**, de esa forma las páginas accedidas por los clientes serían cacheadas en el servidor con lo cual se aceleraría la conexión a Internet, especialmente cuando son muchos los clientes que acceden a los mismos sitios. Un proxy facilita también el control de la conexión impidiéndola o restringiéndola a medida de nuestras necesidades. El inconveniente de compartir una conexión a Internet con un proxy es que trabaja a nivel de aplicación y por tanto del protocolo de cada aplicación (HTTP, FTP, SMTP, etc...). Esto obliga a configurar las aplicaciones (navegador, clientes de correo, clientes ftp, etc...) para que utilicen el proxy, cosa que no es necesario hacer cuando se dispone de un router ya que el router NAT trabaja a nivel de red TCP/IP y es totalmente transparente a las aplicaciones.

Otro servicio que se podría disponer en el servidor es un cortafuegos como **iptables** que permite filtrar qué paquetes de datos pueden entrar y qué paquetes de datos pueden salir, con la finalidad de controlar el acceso a Internet y ganar en seguridad frente a ataques externos.

Activar enrutamiento en Linux

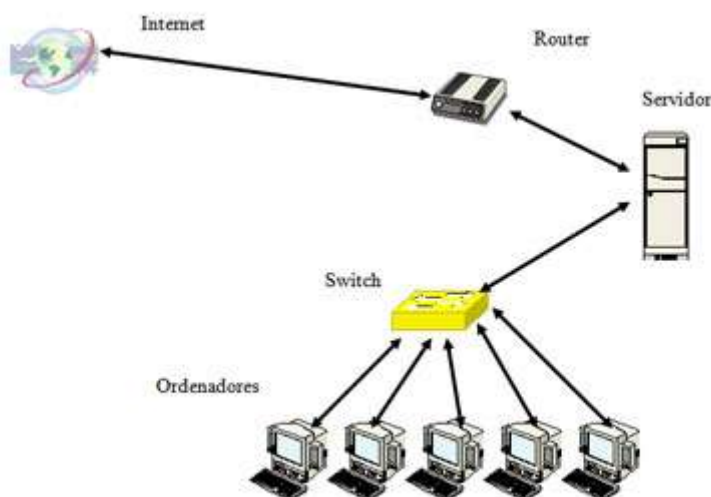
En nuestro Centro Educativo hemos venido detectando problemas de saturación de la línea de conexión a Internet sin motivo justificado. Hemos detectado que en algún ordenador de la sala de profesorado y de algún departamento hay instalados programas de P2P (descarga masiva) y somos conscientes de que estos programas saturan el canal de salida a Internet del centro, además sospechamos que el alumnado también utiliza este tipo de programas.

El router ADSL está conectado a un switch y por lo tanto a través de múltiples utilidades es fácil conocer su dirección IP y configurar nuestro equipo como puerta de enlace, con el consiguiente acceso libre a Internet y a la descarga masiva. Es decir nos encontramos con un esquema del tipo:



Este esquema no permite controlar el tráfico de red puesto que los PCs tienen acceso directo al router.

Situando el servidor entre la red y el router, todo el tráfico hacia Internet pasa por el servidor lo que nos permitirá analizarlo, generar estadísticas, filtrar accesos, instalar un proxy-caché, etc., de forma sencilla y centralizada.



Activación del enrutamiento en Linux

Las funciones de enrutamiento mediante NAT son realizadas por el cortafuegos que analizará los paquetes provenientes de la red local interna cuyo destino sea Internet y los modificará convenientemente para que

salgan hacia Internet como si fueran emitidos por el servidor. A partir del núcleo 2.4 de Linux, el cortafuegos empleado es **iptables**.

Para posibilitar que nuestro servidor Linux sea capaz de comportarse como un router y hacer de puerta de enlace para los PCs de nuestra red local, será necesario crear un script que configure el cortafuegos iptables para que realice NAT desde dentro de la red local hacia Internet.

Creación del script para activar enrutamiento

Para activar el enrutamiento en un sistema Linux, tan solo basta con poner a '1' la variable `ip_forward` del sistema, es decir, basta con ejecutar desde una consola de root:

```
// Activar el enrutamiento en un sistema Linux
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Posteriormente tendríamos que configurar el filtrado de paquetes para que acepte el redireccionamiento de paquetes desde dentro hacia fuera de nuestra red y mediante NAT permita que los PCs de la red interna naveguen con la dirección IP 'pública' del servidor. Supongamos que el router Linux tiene una tarjeta (`eth0`) conectada a la red local (`192.168.0.254/255.255.255.0`) y que tenemos una tarjeta (`eth1`) conectada al router, con la ip `10.0.0.1`, los comandos a ejecutar serían:

```
// Haciendo NAT en el servidor
# iptables -A FORWARD -j ACCEPT

# iptables -t nat -A POSTROUTING -s 192.168.0.254/24 -o eth1 -j SNAT
-to-source 10.0.0.1
```

Podríamos realizar un script que activara el enrutamiento y el NAT y otro para desactivarlo:

```
// activar-enrutamiento.sh
echo "1" > /proc/sys/net/ipv4/ip_forward

iptables -A FORWARD -j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.0.254/24 -o eth1 -j SNAT
-to-source 10.0.0.1

// desactivar-enrutamiento.sh
echo "0" > /proc/sys/net/ipv4/ip_forward
```