Linux como router

Para conigurar un equipo con Debian/Ubuntu como router se ten máis dun interface de rede, basta con habilitar o *ip forwarding* ou reenvio de paquetes.

Isto consíguese poñendo un 1 en vez do 0 que hai no ficheiro `/proc/sys/net/ipv4/ip_forward`

O principal problema é que cando reiniciamos a máquina volve a estar un 0 onde escribimos un 1, e deshabilita o reenvío de paquetes.

Para facer eses cambios permanentes, editamos o ficheiro `/etc/sysctl.conf` e descomentamos a seguinte liña:

```
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

##############################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#
```

Para aplicar a configuración nova, podemos reiniciar o equipo, ou executar

```
sysctl -p
```

Como probablemente, as redes as que está conectado o router, son redes privadas, necesitaremios, activar a tradución de enderezos (NAT) mediante *iptables*. Supoñendo que eth0 é o interface de rede que conecta o router co exterior.

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Para gardar todo isto, instalamos o paquete **iptables-persistent** e indicamos que queremos gardar as regras actuais.