

SERVIDOR NAT

Configuración de un servidor NAT en Windows y Linux



MAURO SAMPAYO HERNÁNDEZ
ESCUELA SUPERIOR DE CÓMPUTO
Redes de Computadoras Grupo 2CM9

Índice:

❖ Introducción.....	2
❖ Conceptos Generales.....	3
❖ ¿Cómo funciona una NAT?.....	4
❖ Configuración de Servidor NAT en Windows.....	5
❖ Configuración de Servidor NAT en Linux.....	8

Introducción

En sus inicios, Internet no había sido pensado para ser una red tan extensa como lo es actualmente, por ese mismo motivo se reservaron sólo 32 bits para direcciones, el equivalente a 4,294,967,296 direcciones únicas; más, sin embargo, el número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP comenzaron a agotarse.

Es por ello que surgió la NAT o Network Address Translation (Traducción de Direcciones de Red en español), la cual consiste en hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Es por ello que hoy en día, resulta importante tener un conocimiento adecuado del funcionamiento de las NAT, pues estas resultan indispensables al momento de hacer una traducción de direcciones privadas de tal forma que las diferentes redes puedan comunicarse sin problemas.

Es por ello, que en este manual se analizara y explicara mas a fondo el funcionamiento de las NAT, así como también, la manera en que se puede configurar una NAT en los sistemas operativos Windows y Linux; con el objetivo de orientar al lector en la creación y configuración de este sistema, para que este pueda realizar la comunicación entre redes de datos, cuyas direcciones IP sean mutuamente incompatibles.

Conceptos Generales

- **NAT (Network Address Translation):** NAT significa Traducción de Direcciones de Red. La función NAT está diseñada para simplificar y conservar direcciones IP. Permite que las interredes IP privadas que usan direcciones IP no registradas puedan conectarse a Internet. NAT se ejecuten en un router, generalmente, conectando dos redes juntas, y traduce las direcciones privadas (no universalmente únicas) de la red interna en direcciones legales antes de reenviar paquetes a otra red. Como parte de esta funcionalidad, NAT se puede configurar para anunciar una o muy pocas direcciones para toda la red al mundo exterior. De esta forma, se ofrece más seguridad y se oculta de forma efectiva toda la red interna del mundo que está detrás de dicha dirección. NAT ofrece una doble función de seguridad y conservación de red, y generalmente, se implementa en entornos de acceso remoto.
- **Intranet:** Es una red de equipos de cómputo privada, basada en protocolos de internet, que se utiliza para compartir recursos y para agilizar tareas entre ellas.
- **Extranet:** Una Extranet es en realidad una Intranet que es parcialmente accesible para personas externas autorizadas. El servidor real (el equipo que sirve las páginas web) residirá detrás de un firewall. El firewall ayuda a controlar el acceso entre la Intranet e Internet permitiendo el acceso a la Intranet sólo a las personas que están debidamente autorizadas
- **Internet:** Es un sistema mundial de redes informáticas, una red de redes en la que los usuarios de cualquier computadora pueden obtener información de cualquier otro ordenador y en ocasiones hablar directamente con los usuarios en otros ordenadores.
- **DHCP (Dynamic Host Configuration Protocol):** Es el protocolo que usan las computadoras para obtener información de configuración. El DHCP permite asignar una dirección IP a una computadora sin requerir que un administrador configure la información sobre la computadora en la base de datos de un servidor.
- **DNS (Domain Name Service):** Es el encargado de traducir las complicadas series de números que conforman una dirección IP en palabras que el usuario pueda recordar fácilmente.

¿Cómo funciona una NAT?

En la NAT existen varios tipos de funcionamiento:

Estática:

Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet.

Dinámica:

El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública.

Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando.

Sobrecarga:

La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos, ya que es el utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. Además del ahorro económico, también se ahorran direcciones IPv4, ya que, aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública.

Para poder hacer esto el router hace uso de los puertos. En los protocolos TCP y UDP se disponen de 65.536 puertos para establecer conexiones. De modo que cuando una máquina quiere establecer una conexión, el router guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar. Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.

Solapamiento:

Cuando una dirección IP privada de una red es una dirección IP pública en uso, el router se encarga de reemplazar dicha dirección IP por otra para evitar el conflicto de direcciones.

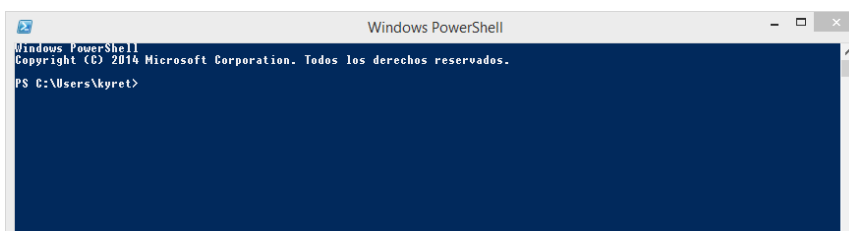
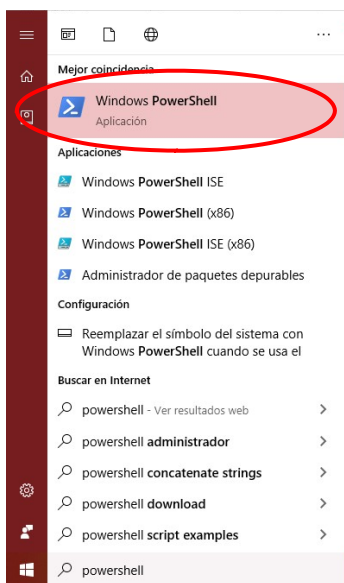
Configuración de Servidor NAT en Windows 10

Requisitos:

- Tener Windows Server, o Windows 10 Pro, Enterprise o Education
- Tener instalado Hiper-V en el sistema operativo

Pasos:

1. Accedemos a la consola de Powershell como Administrador



2. Creamos un switch interno, colocando el siguiente comando:

```
New-VMSwitch -SwitchName "SwitchName" -SwitchType Internal
```

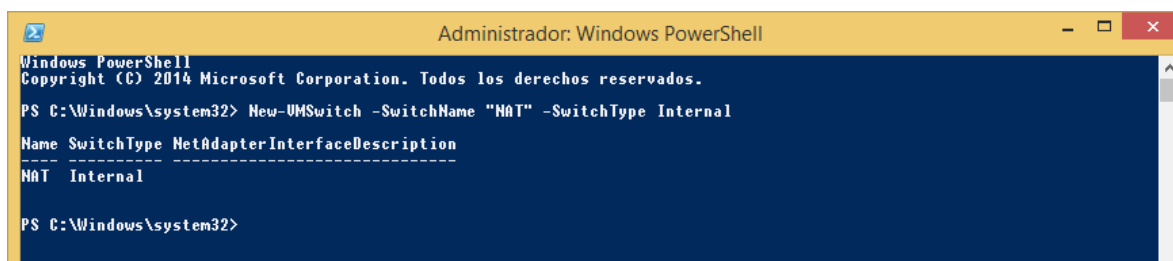
New-VMSwitch: Instrucción principal para crear el switch

-SwitchName: Parámetro de la función principal, que indica el nombre del switch

“SwitchName”: Valor del parámetro que indica el nombre del switch, y puede ser cambiado a conveniencia del usuario.

-SwitchType: Parámetro de la función principal, que indica el tipo de switch.

Internal: Valor del parámetro -SwitchType, en el cual se indica el tipo del switch. En este caso el switch será interno.



3. Encuentre el índice de la interfaz del switch virtual que creo en el paso anterior. Esto se puede realizar utilizando el comando **Get-NetAdapter**.

```
PS C:\Windows\system32> Get-NetAdapter

Name                           InterfaceDescription          ifIndex Status      MacAddress           LinkSpeed
----                           -
vEthernet (NAT)                Adaptador virtual de Ethernet para...#3  31 Up         00-15-50-00-00-01    10 Gbps
vEthernet (SwitchName)        Adaptador virtual de Ethernet para...#2  21 Up         00-15-50-00-00-00    10 Gbps
Wi-Fi                          Adaptador de red inalámbrica Qualcom...  3 Up         50-B7-C3-09-10-05    72.2 Mbps
Conexión de red Bluetooth      Dispositivo Bluetooth (Red de área p...  5 Disconnected 50-B7-C3-09-10-06    3 Mbps

PS C:\Windows\system32>
```

El switch interno tendrá un nombre parecido a **vEthernet(SwitchName)**, y un Descriptor de Interfaz de **Hyper-V Virtual Ethernet Adapter**. Tome nota de su **ifindex**, pues este será usado en el paso siguiente.

4. Configure la puerta de enlace del NAT, usando la función **New-NetIPAddress**, utilizando el siguiente comando:

New-NetIPAddress -IPAddress <NAT Gateway IP> **-PrefixLength** <NAT Subnet Prefix Length> **-InterfaceIndex** <ifIndex>

Para configurar la Puerta de enlace, se requerirá la siguiente información de tu network:

- **IPAddress:** La IP de Puerta de enlace de la NAT, especifica la dirección del IPv4 o del IPv6 a usar. La forma genérica de esta IP será a.b.c.1 (por ejemplo: 172.16.0.1). Por otro lado, la posición final no debe de ser forzosamente .1, pero usualmente lo es.
- **PrefixLength:** El Prefijo de la longitud de Subred de la NAT, define el tamaño de la subred local de la NAT (máscara de la subred). El prefijo de la longitud de la subred será un valor entre 0 y 32.

0 mapearía la red entera, 32 solo permitiría mapear una sola IP. Los valores más comunes, están en el rango del 24 al 32 dependiendo de cuantas IPs deben de ser adjuntadas a la NAT.

- **InterfaceIndex:** "ifindex" es el índice de la interfaz del switch virtual, el cual fue determinado en el paso anterior.

```
PS C:\Windows\system32> New-NetIPAddress -IPAddress 169.254.53.10 -PrefixLength 16 -InterfaceIndex 31

IPAddress      : 169.254.53.10
InterfaceIndex : 31
InterfaceAlias  : vEthernet (NAT)
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 16
PrefixOrigin    : Manual
SuffixOrigin    : Manual
AddressState    : Tentative
ValidLifetime   : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : ActiveStore

IPAddress      : 169.254.53.10
InterfaceIndex : 31
InterfaceAlias  : vEthernet (NAT)
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 16
PrefixOrigin    : Manual
SuffixOrigin    : Manual
AddressState    : Invalid
ValidLifetime   : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : PersistentStore

PS C:\Windows\system32>
```

5. Configure la network del NAT usando New-NetNat, usando el siguiente comando:

```
New-NetNat -Name <NATOutsideName> -InternalIPInterfaceAddressPrefix <NAT subnet prefix>
```

Para configurar la Puerta de enlace, se necesitará que se provea información acerca del network y la Puerta de enlace de la NAT.

- **Name:** NATOutsideName describe el nombre del network de la NAT. Este parámetro se usará para remover la network de la NAT.
- **InternalIPInterfaceAddressPrefix:** El prefijo de la Subred de la NAT describe tanto el prefijo de la IP de la Puerta de enlace de la NAT por encima de la Subred, como la Longitud de el prefijo de la Subred de la NAT, también por encima de la red

La forma genérica será a.b.c.0/NAT

```
PS C:\Windows\system32> New-NetNat -Name "MyNATnetwork" -InternalIPInterfaceAddressPrefix 169.254.0.0/16
```

Con estos pasos tendremos configurado un servidor NAT en Windows 10 y podremos compartir internet hacía otra computadora mediante un cable de red.

Configuración de Servidor NAT en Linux

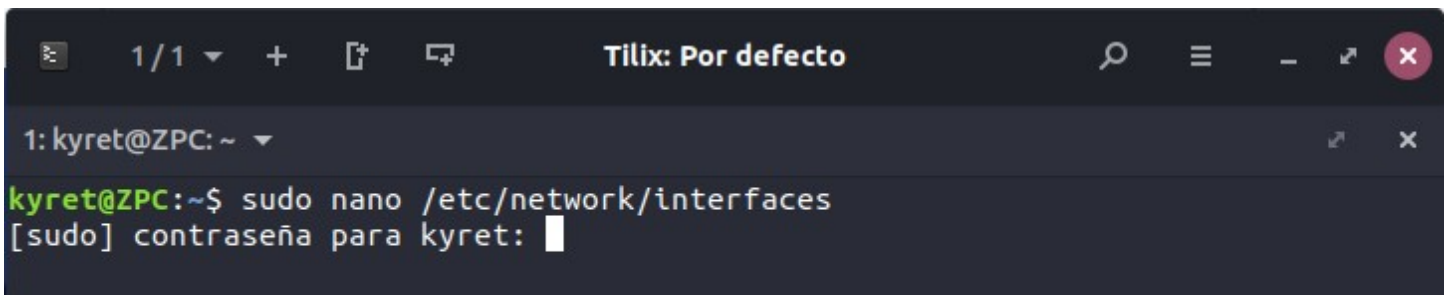
Requisitos:

- Tener al menos 2 interfaces de red, una será usada para comunicarnos con el exterior (internet), y la otra se usará para poder establecer comunicación con el resto de PC's. Pueden ser tarjetas de red Ethernet o Wi-Fi
- Tener instalado iptables, el cual nos servirá para administrar conexiones y aplicar reglas. En caso de no tenerlo instalado se debe abrir una terminal, y ejecutar **sudo apt-get install iptables**.
- Tener instalado dnsmasq, el cual nos servirá para asignar ips y dns de forma automática al resto de máquinas que lo soliciten. En caso de no tenerlo instalado se debe abrir una terminal, y ejecutar **sudo apt-get install dnsmasq**.

Pasos:

Suponiendo que ya tenemos nuestra máquina conectada a internet; imaginemos que nuestro servidor está conectado a un modem por cable de red, y que tenemos otra tarjeta libre. Estas conexiones serían eth0(la cual sería nuestra red pública) y eth1(la cual sería nuestra red privada) respectivamente.

1. Abrimos el archivo /etc/network/interfaces por medio del código **sudo nano /etc/network/interfaces**



```
Tilix: Por defecto
1: kyret@ZPC: ~
kyret@ZPC:~$ sudo nano /etc/network/interfaces
[sudo] contraseña para kyret:
```

Al abrirlo tendremos el siguiente contenido:



```
Tilix: Por defecto
1: kyret@ZPC: ~
GNU nano 2.9.3 /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
```

Se deben de agregar las dos tarjetas de red que tenemos. Esto se realiza escribiendo en el archivo lo siguiente:

```
auto eth0
```

```
iface eth0 inet dhcp
```

Esto quiere decir que tenemos configurada la tarjeta de red eth0 para obtener una IP por DHCP. Sin embargo no hay ninguna mención para eth1, por lo cual tendremos que ponerla de forma manual, para así poder crear una red con esta interfaz. Esto lo haremos colocando el siguiente código;

```
auto eth1
```

```
iface eth1 inet static
```

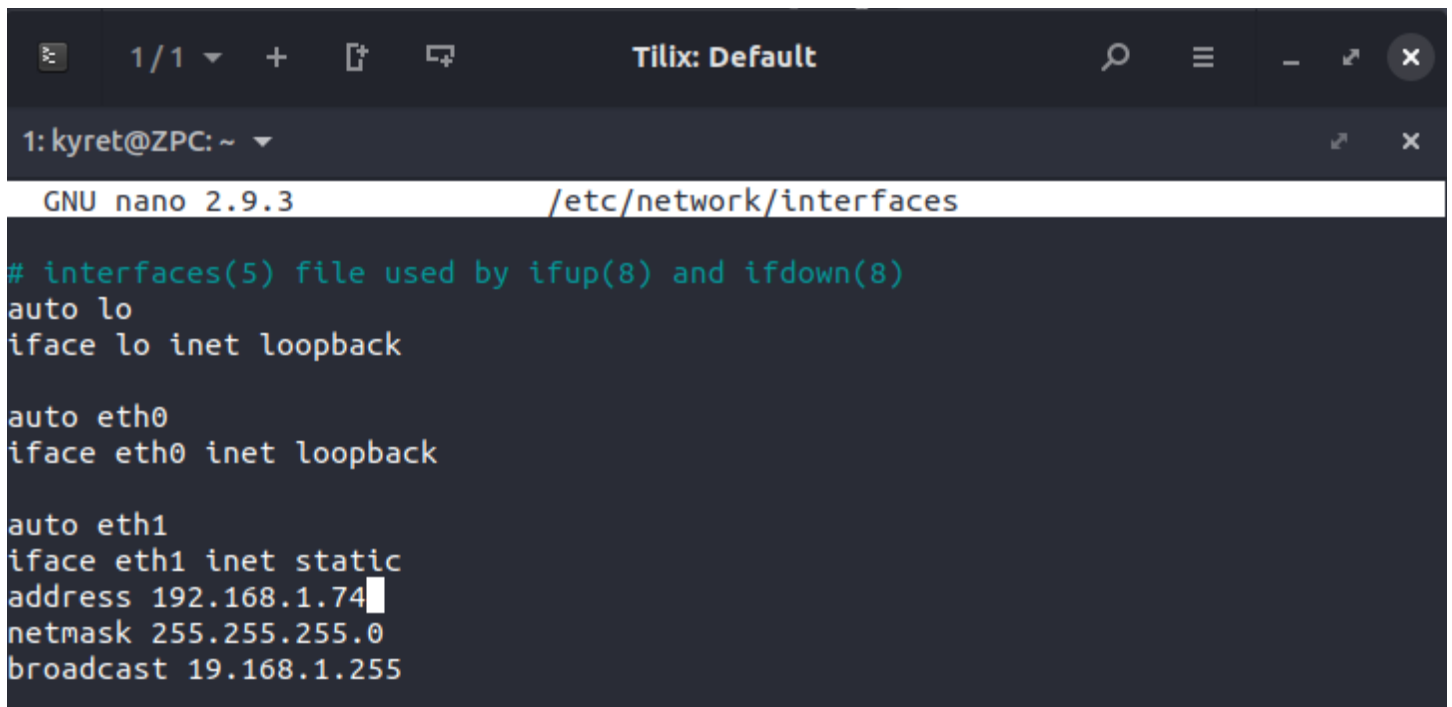
```
address 192.168.0.1*
```

```
netmask 255.255.255.0*
```

```
broadcast 192.168.0.255*
```

***NOTA:** En estos apartados se deben de colocar la dirección IP, la netmask y el broadcast perteneciente a su máquina. Si desea consultar que direcciones tienen estos apartados en su máquina, debe colocaren la consola el comando **ifconfig** En caso de no tener este comando instalado, debe de ejecutar **sudo apt-get install ifconfig** para proceder con su instalación

El archivo debe quedar de la siguiente forma, como se muestra en la imagen:

A screenshot of a terminal window titled 'Tilix: Default'. The terminal shows the user 'kyret@ZPC' editing the file '/etc/network/interfaces' with 'GNU nano 2.9.3'. The content of the file is as follows:

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet loopback

auto eth1
iface eth1 inet static
address 192.168.1.74
netmask 255.255.255.0
broadcast 19.168.1.255
```

Guardamos presionando Ctrl+O y cerramos el archivo presionando Ctrl+X.

La configuración quedaría de la siguiente manera:

IP de la máquina: 192.168.1.74

Máscara de red: 255.255.255.0


Dirección de difusión: 192.168.0.255

2. Reiniciamos el servicio de red por medio del código **sudo /etc/init.d/networking restart**



```
Tilix: Default
1: kyret@ZPC: ~
kyret@ZPC:~$ sudo /etc/init.d/networking restart
[sudo] contraseña para kyret: 
```

Nos abrirá un archivo como el que se muestra en la imagen



```
Tilix: Default
1: kyret@ZPC: ~
[1/2] /etc/init.d/networking

```

Ahora deberemos de activar “ip_forward” para que nuestro servidor no ignore los paquetes que no vayan destinados a si mismo, ya que pueden ser paquetes para otros equipos y esto haría que esos equipos no obtuviesen respuesta del exterior.

Hay dos formas de realizar esta activación:

- 1) **Provisionalmente (se pierde al reiniciar):** Sobre el mismo archivo que abrimos previamente colocamos el código: **echo 1 > /proc/sys/net/ipv4/ip_forward**



```
Tilix: Default
1: kyret@ZPC: ~
[1/2] /etc/init.d/networking
echo 1 > /proc/sys/net/ipv4/ip_forward

```

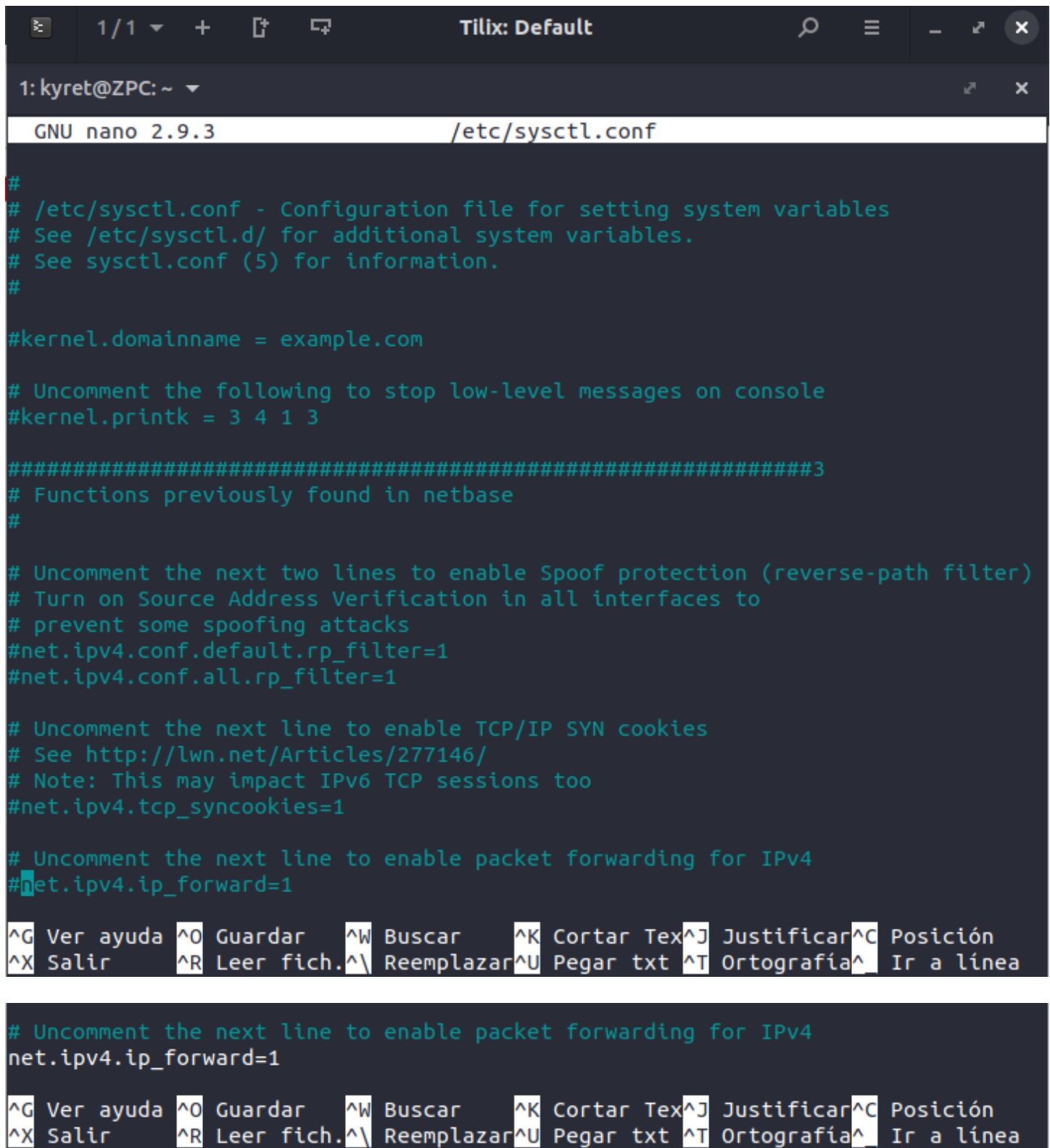
Guardamos presionando Ctrl+O y cerramos el archivo presionando Ctrl+X.

- 2) **De manera permanente:** Colocamos el siguiente código en la consola: **sudo nano /etc/sysctl.conf**



```
Tilix: Default
1: kyret@ZPC: ~
kyret@ZPC:~$ sudo nano /etc/sysctl.conf
[sudo] contraseña para kyret: 
```

Nos abrirá un archivo como el que se muestra en la imagen. Debemos de buscar y descomentar la línea `#net.ipv4.ip_forward=1` quitándole el carácter “#” de manera que nos quede así:
`net.ipv4.ip_forward=1`



```
1: kyret@ZPC: ~  
GNU nano 2.9.3 /etc/sysctl.conf  
#  
# /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  
net.ipv4.ip_forward=1  
  
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición  
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea  
  
# Uncomment the next line to enable packet forwarding for IPv4  
net.ipv4.ip_forward=1  
  
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición  
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Guardamos presionando Ctrl+O y cerramos el archivo presionando Ctrl+X.

3. Activamos la NAT para que los equipos que estén conectados a nuestro servidor puedan salir a internet mediante la IP del servidor. Para esto utilizaremos iptables con el siguiente comando: **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE.**

- **iptables:** Comando para modificar las reglas.
- **-t:** Especifica el tipo de tabla a la que van dirigidas las reglas.
- **Nat:** Es el tipo de tabla.
- **-A:** Añade la regla a las ya existentes.
- **POSTROUTING:** Modifica los paquetes justo antes de reenviarlos a las máquinas correspondientes.
- **-o:** Sirve para especificar hacia que tarjeta van redirigidos los paquetes.
- **eth0:** Es nuestra tarjeta conectada a internet.
- **-j:** Especifica hacia donde se aplican las reglas
- **MASQUERADE:** Indica el enmascaramiento ip.

Este comando hará que todo lo que entre a nuestro PC por algún puerto que no sea eth0, se enmascarará para reenviarlo a la tarjeta eth0. Esto solo aplicará durante la sesión, pues, cuando reiniciemos la PC, se desactivará.

```
Tilix: Default
1: root@ZPC: /home/kyret
kyret@ZPC:~$ sudo su
[sudo] contraseña para kyret:
root@ZPC:/home/kyret# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@ZPC:/home/kyret#
```

4. Cualquier PC conectado a nuestra tarjeta eth1 tendría acceso a internet, sin embargo, primero se deben de configurar las direcciones IP y la DNS manualmente, puesto a que DHCP aun no está activo. Esto se puede realizar con el programa dnsmasq. Ejecutamos el comando: **sudo nano /etc/dnsmasq.conf**

```
Tilix: Default
1: root@ZPC: /home/kyret
kyret@ZPC:~$ sudo su
[sudo] contraseña para kyret:
root@ZPC:/home/kyret# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@ZPC:/home/kyret# sudo nano /etc/dnsmasq.conf
```

Buscamos las líneas siguientes usando Ctrl+W y las modificamos para que queden así:

```
listen-address=192.168.0.1
bind-interfaces
dhcp-range=192.168.0.2,192.168.0.254,12h
```

```
Tilix: Default
1: root@ZPC: /home/kyret
GNU nano 2.9.3 /etc/dnsmasq.conf

listen-address=192.168.1.74
# If you want dnsmasq to provide only DNS service on an interface,
# configure it as shown above, and then use the following line to
# disable DHCP and TFTP on it.
#no-dhcp-interface=

# On systems which support it, dnsmasq binds the wildcard address,
# even when it is listening on only some interfaces. It then discards
# requests that it shouldn't reply to. This has the advantage of
# working even when interfaces come and go and change address. If you
# want dnsmasq to really bind only the interfaces it is listening on,
# uncomment this option. About the only time you may need this is when
# running another nameserver on the same machine.
bind-interfaces

# If you don't want dnsmasq to read /etc/hosts, uncomment the
# following line.
#no-hosts
# or if you want it to read another file, as well as /etc/hosts, use

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

```
Tilix: Default
1: root@ZPC: /home/kyret
GNU nano 2.9.3 /etc/dnsmasq.conf

# Uncomment this to enable the integrated DHCP server, you need
# to supply the range of addresses available for lease and optionally
# a lease time. If you have more than one network, you will need to
# repeat this for each network on which you want to supply DHCP
# service.
dhcp-range=192.168.1.2,192.168.0.254,12h

# This is an example of a DHCP range where the netmask is given. This
# is needed for networks we reach the dnsmasq DHCP server via a relay
# agent. If you don't know what a DHCP relay agent is, you probably
# don't need to worry about this.
#dhcp-range=192.168.0.50,192.168.0.150,255.255.255.0,12h

# This is an example of a DHCP range which sets a tag, so that
# some DHCP options may be set only for this network.
#dhcp-range=set:red,192.168.0.50,192.168.0.150

# Use this DHCP range only when the tag "green" is set.
[ 666 líneas escritas ]

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

5. Reiniciamos el servicio usando el código **sudo /etc/init.d/dnsmasq restart**

```
root@ZPC:/home/kyret# sudo /etc/init.d/dnsmasq restart
[ ok ] Restarting dnsmasq (via systemctl): dnsmasq.service.
root@ZPC:/home/kyret#
```

Con estos pasos tendremos configurado un servidor NAT en Windows 10 y podremos compartir internet hacia otra computadora mediante un cable de red.