

Routers, Edificios y Servidores NFS - Manual Técnico

Fernando Rubén Ocaña Ixcot 201830121

Universidad de San Carlos de Guatemala

Centro Universitario de Occidente

División de Ciencias de la Ingeniería

Ingeniería en Ciencias y Sistemas

Laboratorio de Redes de Computadoras 1

Ing. Juan Francisco Rojas, Aux. Willy Jessiel Ardiano

Quetzaltenango, 09 de mayo de 2023

Indice

Requisitos y Herramientas Utilizadas	3
Herramientas Utilizadas:	3
Interfaces:	3
Ip route:	3
Iptables:	3
NFS Server:	4
NFS Common:	4
SSH:	4
Diagrama de Red	5
Direcciones IP de Dispositivos	5
Tablas de Enrutamiento	7
Router 1:	7
Router 2:	7
Router 3:	8
Router 4:	8
Router 5:	9
Router 6:	9
Router 7:	10
Router 8:	10

MANUAL TÉCNICO - CONFIGURACION DE ROUTERS, EDIFICIOS

Requisitos y Herramientas Utilizadas

- **Repositorio:** <https://github.com/froi0409/Configuracion-Routers.git>
- **General**
 - **Sistema Operativo de Desarrollo:** Debían 11 Bullseye
- **Máquinas Virtuales:**
 - **Sistema Operativo:** Debian 11 Bullseyes (nonfree), sin entorno gráfico.
 - **Almacenamiento:** 10 GB (cada máquina)
 - **RAM:** 2GB (cada máquina)

Herramientas Utilizadas:

Interfaces:

Para establecer las interfaces que el router, PC o servidor utilizarán, es importante agregarlas directamente a la máquina virtual, ya que dichas interfaces serán las que dichos dispositivos utilizarán para comunicarse entre sí. Las interfaces se configuran en el archivo “/etc/network/interfaces” y se habilitan con los comandos ifdown e ifup.

Ip route:

Comando que tiene como finalidad, establecer la tabla de enrutamiento que cada router maneja, esto es lo que permite que la comunicación entre dispositivos de diferentes edificios pueda llevarse a cabo.

Iptables:

Comando que sirve para indicar al router las rutas que no deben tener alguna comunicación.

NFS Server:

Permite que los servidores puedan manejar un sistema de archivos compartido, es decir, permite que múltiples PC puedan acceder y manipular ciertos archivos que estén almacenados en el servidor.

NFS Common:

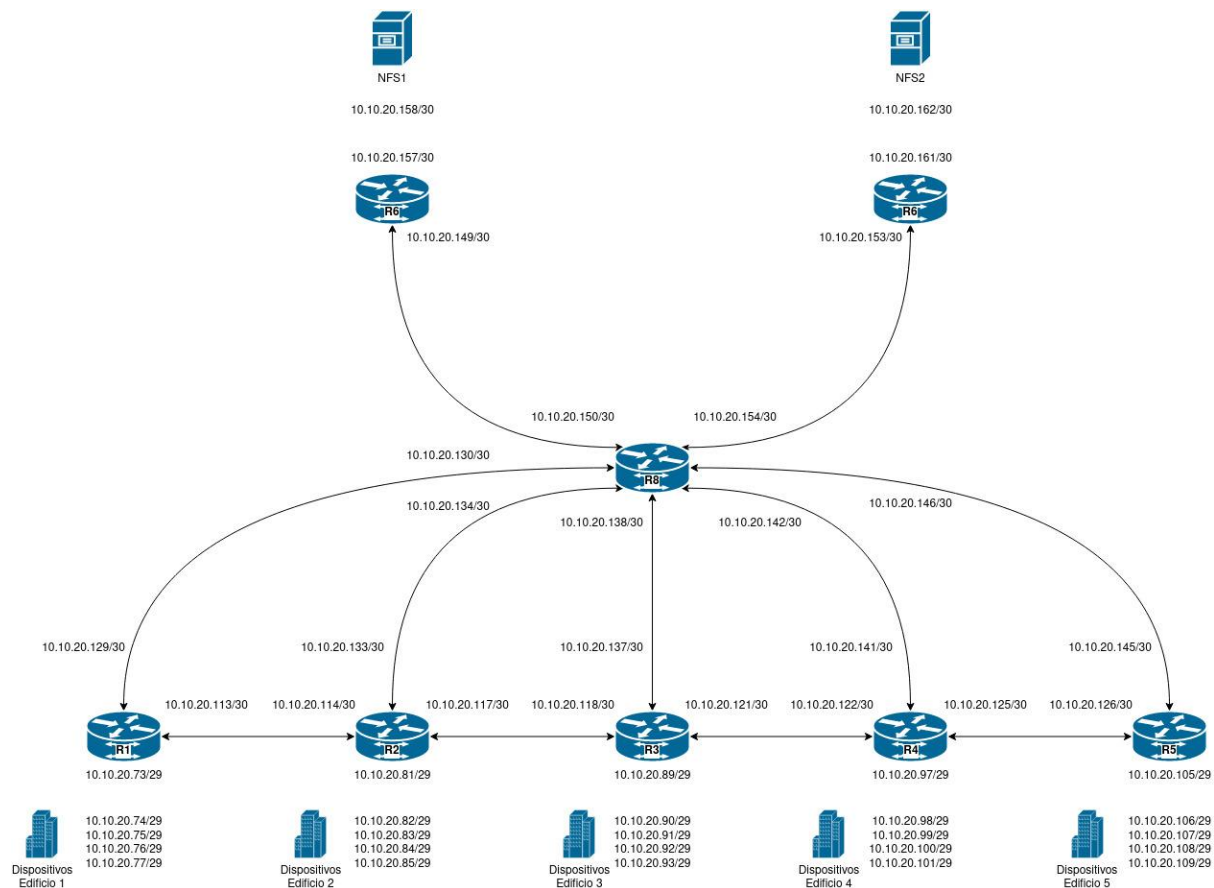
Permite a los dispositivos cliente (las PC que cada edificio tiene) acceder a los archivos que estén ubicados en algún servidor NFS.

SSH:

Secure Shell (SSH), es un protocolo que permite a un usuario comunicarse de forma segura con algún dispositivo remoto (en este caso con una máquina virtual), Es ampliamente utilizado en el mundo de la administración de sistemas y la informática para permitir la administración remota de servidores y dispositivos de red.

En este caso, se usa el protocolo SSH para poder manejar las máquinas virtuales a nivel del sistema operativo que tiene instalado la computadora, esto es viable debido a que no es necesario hacer uso de un entorno gráfico.

Diagrama de Red



* En el repositorio de GitHub se puede encontrar una copia del diagrama de red en formato PDF, por motivos de calidad de imagen.

Direcciones IP de Dispositivos

Edificio	No.	Dirección IP	Máscara de Subred	Router
Edificio 1	1	10.10.20.74	255.255.255.248	10.10.20.73
	2	10.10.20.75	255.255.255.248	
	3	10.10.20.76	255.255.255.248	
	4	10.10.20.77	255.255.255.248	
Edificio 2	1	10.10.20.82	255.255.255.248	10.10.20.81
	2	10.10.20.83	255.255.255.248	
	3	10.10.20.84	255.255.255.248	
	4	10.10.20.85	255.255.255.248	

Edificio 3	1	10.10.20.90	255.255.255.248	10.10.20.89
	2	10.10.20.91	255.255.255.248	
	3	10.10.20.92	255.255.255.248	
	4	10.10.20.93	255.255.255.248	
Edificio 4	1	10.10.20.98	255.255.255.248	10.10.20.97
	2	10.10.20.99	255.255.255.248	
	3	10.10.20.100	255.255.255.248	
	4	10.10.20.101	255.255.255.248	
Edificio 5	1	10.10.20.106	255.255.255.248	10.10.20.105
	2	10.10.20.107	255.255.255.248	
	3	10.10.20.108	255.255.255.248	
	4	10.10.20.109	255.255.255.248	
Edificio 6	1	10.10.20.158	255.255.255.252	10.10.20.157
Edificio 7	1	10.10.20.162	255.255.255.252	10.10.20.161

Tablas de Enrutamiento

Router 1:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.80/29	enp10s0	10.10.20.113/30
10.10.20.88/29	enp10s0	10.10.20.113/30
10.10.20.96/29	enp10s0	10.10.20.113/30
10.10.20.104/29	enp10s0	10.10.20.113/30
10.10.20.156/30	enp11s0	10.10.20.129/30
10.10.20.160/30	enp11s0	10.10.20.129/30

Router 2:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.72/29	enp8s0	10.10.20.114/30
10.10.20.88/29	enp9s0	10.10.20.117/30
10.10.20.96/29	enp9s0	10.10.20.117/30
10.10.20.104/29	enp9s0	10.10.20.117/30
10.10.20.156/30	enp10s0	10.10.20.133/30
10.10.20.160/30	enp10s0	10.10.20.113/30

Router 3:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.72/29	enp8s0	10.10.20.118/30
10.10.20.80/29	enp8s0	10.10.20.118/30
10.10.20.96/29	enp9s0	10.10.20.121/30
10.10.20.104/29	enp9s0	10.10.20.121/30
10.10.20.156/30	enp10s0	10.10.20.137/30
10.10.20.160/30	enp10s0	10.10.20.137/30

Router 4:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.72/29	enp8s0	10.10.20.122/30
10.10.20.80/29	enp8s0	10.10.20.122/30
10.10.20.88/29	enp8s0	10.10.20.122/30
10.10.20.104/29	enp9s0	10.10.20.125/30
10.10.20.156/30	enp10s0	10.10.20.141/30
10.10.20.160/30	enp10s0	10.10.20.141/30

Router 5:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.72/29	enp10s0	10.10.20.126/30
10.10.20.80/29	enp10s0	10.10.20.126/30
10.10.20.88/29	enp10s0	10.10.20.126/30
10.10.20.96/29	enp10s0	10.10.20.126/30
10.10.20.156/30	enp11s0	10.10.20.145/30
10.10.20.160/30	enp11s0	10.10.20.145/30

Router 6:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.72/29	enp8s0	10.10.20.149/30
10.10.20.80/29	enp8s0	10.10.20.149/30
10.10.20.88/29	enp8s0	10.10.20.149/30
10.10.20.96/29	enp8s0	10.10.20.149/30
10.10.20.14/30	enp8s0	10.10.20.149/30

Router 7:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.72/29	enp8s0	10.10.20.153/30
10.10.20.80/29	enp8s0	10.10.20.153/30
10.10.20.88/29	enp8s0	10.10.20.153/30
10.10.20.96/29	enp8s0	10.10.20.153/30
10.10.20.14/30	enp8s0	10.10.20.153/30

Router 8:

Red Destino	Interfaz	Dirección Interfaz
10.10.20.72/29	enp7s0	10.10.20.130/30
10.10.20.80/29	enp8s0	10.10.20.134/30
10.10.20.88/29	enp9s0	10.10.20.138/30
10.10.20.96/29	enp10s0	10.10.20.142/30
10.10.20.104/30	enp11s0	10.10.20.146/30
10.10.20.156/30	enp12s0	10.10.20.150/30
10.10.20.160/30	enp13s0	10.10.20.154/30

Matriz de Permisos

Se debe tomar en cuenta que todas las direcciones IP son de formato 10.10.20.N,
donde N es el número que aparece en los encabezados de filas y columnas:

Cliente	Clientes																				Servidores	
	74	75	76	77	82	83	84	85	90	91	92	93	98	99	100	101	106	107	108	109	158	162
74	X	X	X	X				X		X			X		X	X			X		X	
75	X	X	X	X		X				X		X						X				X
76	X	X	X	X					X					X		X			X			
77	X	X	X	X								X		X	X		X	X				
82					X	X	X	X		X				X		X						X
83		X		X	X	X	X	X		X												
84			X		X	X	X	X				X		X			X		X			X
85	X	X			X	X	X	X							X		X		X			
90									X	X	X	X									X	
91							X		X	X	X	X									X	
92		X		X					X	X	X	X		X				X				X
93					X				X	X	X	X										X
98		X											X	X	X	X						
99								X					X	X	X	X		X			X	
100				X							X		X	X	X	X						X
101			X							X		X	X	X	X	X						
106						X					X						X	X	X	X		
107				X													X	X	X	X		X
108	X						X					X					X	X	X	X	X	
109			X	X	X											X	X	X	X	X	X	X

Funcionamiento de Dispositivos PC:

Los dispositivos PC, poseen dos archivos .sh que administran la configuración y funcionamiento de los mismos. Los archivos se especifican a continuación:

Configuración de IP e Interfaces:

Archivo que se basa en solicitar al usuario que ingrese el número de edificio y dispositivo que se quiere conectar, para esto se utiliza el formato “N_M”, donde N es el número de edificio y M es el número del dispositivo del edificio que se quiere conectar.

```
# Indicamos el usuario que queremos conectar
echo "Ingrese el número de dispositivo que se conectará";
read dispositivo;
```

En base a la información ingresada anteriormente, se realiza la configuración del ip y la dirección gateway de la siguiente manera:

```
case $dispositivo in
    "1_1" )
        ip_addr="10.10.20.74";
        gate_addr="10.10.20.73";
        ;;
    "1_2" )
        ip_addr="10.10.20.75";
        gate_addr="10.10.20.73";
        ;;
```

Donde al final, solamente se realiza la configuración de las interfaces en el archivo /etc/network/interfaces, de la siguiente forma:

```
# Configuración de interfaces
cat <<EOF > /etc/network/interfaces
# The loopback network interface
auto lo
iface lo inet loopback

# SSH
auto enp1s0
iface enp1s0 inet static
    address 192.168.122.30
    netmask 255.255.255.0
    gateway 192.168.122.1

# Configuración de Red
allow-hotplug enp7s0
iface enp7s0 inet static
    address $ip_addr
    netmask 255.255.255.248
    gateway $gate_addr

EOF

echo "Se terminaron de configurar las interfaces"
```

Configuración y Funcionamiento de NFS Common:

Como se mencionó anteriormente, NFS common nos servirá para poder acceder a los archivos que estén ubicados en algún servidor NFS. Para esto existen dos scripts .sh, ya que se debe montar una carpeta que pueda acceder a un servidor en específico, y en este caso contamos con dos servidores, por lo que cada script sirve para acceder a un servidor NFS en específico. El funcionamiento del script se da de la siguiente manera:

```
mount 10.10.20.162:/nfsshare /mnt
df -h

chmod 777 /mnt
```

Funcionamiento de Servidores NFS

En un servidor NFS, se debe indicar las direcciones de red válidas, las cuales podrán acceder a la carpeta (siempre que el enrutamiento lo permita), para indicar dichas direcciones se debe editar el archivo /etc/exports de la siguiente manera:

```
/nfsshare 10.10.20.72/29(rw,sync,no_subtree_check)
/nfsshare 10.10.20.80/29(rw,sync,no_subtree_check)
/nfsshare 10.10.20.88/29(rw,sync,no_subtree_check)
/nfsshare 10.10.20.96/29(rw,sync,no_subtree_check)
/nfsshare 10.10.20.104/29(rw,sync,no_subtree_check)
```

Donde “/nfsshare” es la carpeta del servidor que contiene los archivos que serán compartidos, y las direcciones ip, son las direcciones de las redes que podrán acceder a la carpeta “/nfsshare”.

Posteriormente se debe dar permisos de lectura y escritura a la carpeta compartida, esto se realiza de la siguiente manera:

```
chown nobody:nogroup /nfsshare
chmod 755 /nfsshare
chmod -R 777 /nfsshare
```

Funcionamiento de Routers

El funcionamiento de un router debe ser gestionado de la siguiente manera:

Levantamiento de Interfaces:

Prepara las interfaces para que las mismas estén actualizadas y configuradas según su respectivo archivo “/etc/network/interfaces”. Se levantan haciendo uso de ifdown e ifup:

```
ifdown enp8s0
ifdown enp9s0
ifdown enp10s0
ifup enp8s0
ifup enp9s0
ifup enp10s0
```

Configuración de Rutas con Routes:

Se agregan direcciones de red, de las redes a las cuales el router podrá enviar paquetes, también se debe indicar la interfaz sobre la cual deben salir los paquetes para llegar a una red en específico. La configuración se da de la siguiente manera:

```
ip route add 10.10.20.72/29 dev enp8s0
ip route add 10.10.20.88/29 dev enp9s0
ip route add 10.10.20.96/29 dev enp9s0
ip route add 10.10.20.104/29 dev enp9s0
ip route add 10.10.20.156/30 dev enp10s0
ip route add 10.10.20.160/30 dev enp10s0
```

Bloqueo de Rutas con Iptables:

Dado que no todos los dispositivos de la red se pueden enviar paquetes entre sí, es importante bloquear las rutas a las que no se puede acceder, las cuales deben ser bloqueadas con iptables de la siguiente manera:

```
# Dispositivo 5 - 10.10.20.82
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.74 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.75 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.76 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.77 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.90 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.92 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.93 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.98 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.100 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.106 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.107 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.108 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.109 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -s 10.10.20.82 -d 10.10.20.158 -j DROP
```

Donde la primera dirección ip es la dirección ip de origen (que normalmente debería ser la dirección ip de algún dispositivo que se encuentre en la red del router) y la segunda dirección, es la dirección a la cual no se pueden enviar paquetes.