



INSTITUTO POLITÉCNICO NACIONAL  
ESCUELA SUPERIOR DE CÓMPUTO



ADMINISTRACIÓN DE SERVICIOS EN RED

Actividad

Proyecto Final

EQUIPO 1

INTEGRANTES:

Arellano Aguillón Shu Nashy Nizarely

Banderas Solórzano Midori

Montaño Morales Angeles Aranza

Servín Quinterio Damaris Angelina

GRUPO: 4CV12

PROFESORA: Leticia Henestrosa Carrasco

## Introducción

El término “red de computadoras” hace referencia al conjunto de computadoras autónomas interconectadas mediante una sola tecnología.

Existen diferentes tipos de redes, entre las cuales cabe destacar:

**LAN:** Es una red de área local cuyo alcance se restringe a un radio de unos cuantos cientos de metros.

**VLAN:** Es una red virtual que se instala en una red local switchheada tomando como base el número del puerto de switch al cual se conecta la computadora.

**Internet:** Es un conjunto descentralizado de redes de comunicaciones interconectadas, que utilizan la familia de protocolos TCP/IP, constituye una red lógica única de alcance mundial.

El enrutamiento es la manera en la que un paquete busca la ruta más corta para llegar a su destino dentro de una red.

Los protocolos de enrutamiento administran la actividad de enrutamiento en un sistema. Los enrutadores intercambian información de enrutamiento con otros hosts para mantener las rutas conocidas a las redes remotas. Para este proyecto se utilizó el protocolo de enrutamiento OSPF.

**OSPF (Open Shortest Path First)** es un protocolo de enrutamiento dinámico interior (IGP – Internal Gateway Protocol -). Usa un algoritmo de tipo Estado de Enlace. OSPF ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.

Se aplicará direccionamiento con **VLSM: Máscara de Subred de Longitud Variable**, en la división en subredes tradicional se asigna la misma cantidad de direcciones a cada subred. Sin embargo, las subredes que requieren menos direcciones tienen direcciones sin utilizar (desperdiciadas). Por ejemplo, los enlaces WAN solo necesitan dos direcciones. Así que, la máscara de subred de longitud variable (VLSM), permite un uso más eficiente de las direcciones.

Los mecanismos básicos de seguridad serán implementados con: VLAN, NAT y ACL EXTENDIDAS:

**NAT (Network Address Translation = Traducción de Direcciones de Red)** tiene muchos usos, pero el principal es conservar las direcciones IPv4 públicas.

Esto se logra al permitir que las redes utilicen direcciones IPv4 privadas internamente y al proporcionar la traducción a una dirección pública solo cuando sea necesario.

**Port Address Translations (PAT)** es una extensión de la traducción de direcciones de red (NAT) que permite asignar varios dispositivos en una LAN a una única dirección IP pública para conservar las direcciones IP. En otras palabras, se puede utilizar una única dirección IPv4 pública para cientos, incluso miles de direcciones IPv4 privadas internas.

Las **ACL extendidas** se utilizan con más frecuencia que las ACL estándar, porque proporcionan un mayor grado de control. Pueden filtrar por dirección de origen, dirección de destino, protocolo (es decir, IP, TCP, UDP, ICMP) y número de puerto. Esto proporciona una gama de criterios más amplia sobre la cual basar la ACL. Por ejemplo, una ACL extendida puede permitir el tráfico de correo electrónico de una red a un destino específico y, simultáneamente, denegar la transferencia de archivos y la navegación web.

Los servicios que habilitaremos en las máquinas virtuales son SNMP, DNS, DHCP, HTTP y FTP:

**SNMP (Protocolo simple de administración de red)** es un protocolo de capa de aplicación que proporciona un formato de mensaje para la comunicación entre administradores y agentes. Se desarrolló para permitir que los administradores puedan administrar los nodos, como los servidores, las estaciones de trabajo, los routers, los switches y los dispositivos de seguridad, en una red IP. Permite que los administradores de red administren el rendimiento de la red, detecten y resuelvan problemas de red, y planifiquen el crecimiento de la red.

El **Sistema de nombres de dominio (Domain Name System o DNS)** es un sistema de nombres jerárquico que permite la comunicación entre dispositivos en una red. Traduce nombres de dominio legibles para humanos a una dirección de Protocolo de Internet (IP) que una computadora puede entender. Esencialmente, DNS nos permite conectarnos a sitios web sin tener que memorizar una serie de números; todo lo que necesitamos saber es el nombre del sitio web.

El **Servidor DHCP (Dynamic Host configuration Protocol)**, es un servidor de Red el cual permite una asignación automática de direcciones IP, gateways predeterminadas, así como otros parámetros de red que necesiten los

clientes. El sistema DHCP envía automáticamente todos los parámetros para que los clientes se comuniquen sin problema dentro de la red.

El **Protocolo de transferencia de hipertexto (HTTP)** es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. El cliente (se le suele llamar "agente de usuario", en inglés user agent) realiza una petición enviando un mensaje, con cierto formato al servidor. El servidor (se le suele llamar un servidor web) le envía un mensaje de respuesta.

**FTP** (File Transfer Protocol o Protocolo de Transferencia de Archivos), su principal objetivo, es la transferencia de archivos entre dos equipos. Los servidores FTP son las aplicaciones de software que permiten la transferencia de archivos de un dispositivo a otro. El FTP se suele utilizar para manejar grandes cantidades de archivos, por lo que a menudo puede resultar útil en el desarrollo de la web.

Para la creación de la topología y la implementación de los servicios se utilizará la herramienta de GNS3.

**GNS3** es un simulador gráfico de red lanzado en 2008, que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos,<sup>123</sup> permitiendo la combinación de dispositivos tanto reales como virtuales.



Imagen. Logo de GNS3

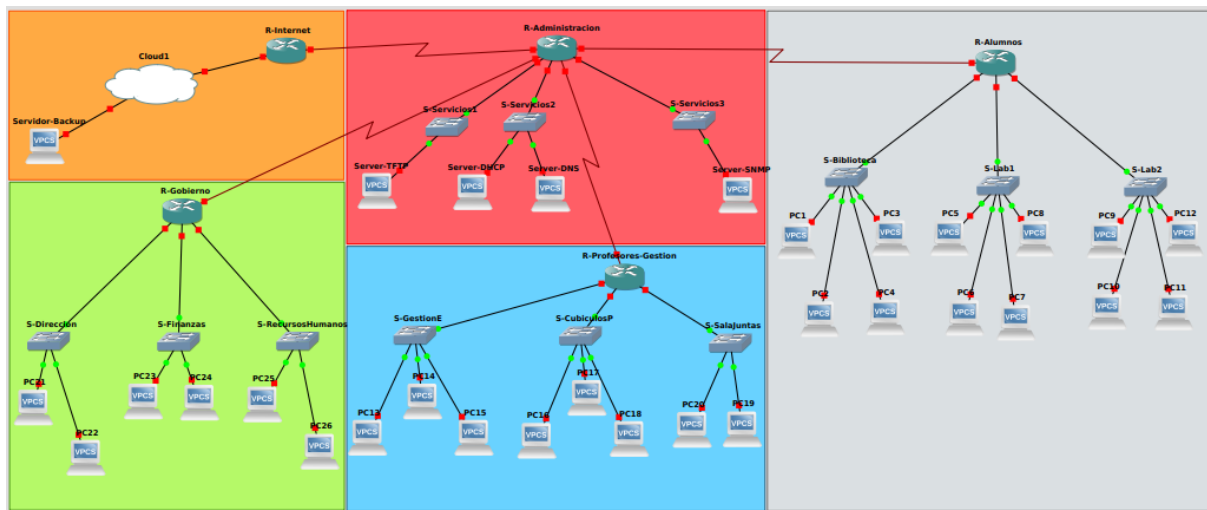
# Objetivos

Los objetivos de este proyecto son:

- Utilizar GNS3 como herramienta de simulación de redes.
- Crear y administrar nuestra propia red.
- Implementar servicios básicos de una red.
- Aplicar los conocimientos adquiridos durante el curso de Administración de Servicios en Red.

## Desarrollo

La topología de la red es la siguiente:



Como se puede apreciar se tienen 5 routers cada uno representa un área dentro de una institución educativa.

En el área administrativa se tiene una granja de servidores donde se encuentran los servicios de la red.

Se tiene un área de gobierno, de alumnos y de profesores.

Por último, se encuentra el router de frontera que se conecta al internet.

Se implementarán los siguientes servicios:

- SNMP
- DNS
- DHCP
- HTTP
- FTP

A continuación, se muestra la tabla de direccionamiento.

Área de alumnos				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-Alumnos	S3/0	172.16.4.253	255.255.255.252	
	Fa0/0	172.16.15.254	255.255.248.0	
	Fa1/0	172.16.4.62	255.255.255.192	
	Fa2/0	172.16.4.126	255.255.255.192	
Área de Gestión Escolar y Profesores				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-ProfGest	S3/0	172.16.3.253	255.255.255.252	
	Fa2/0	172.16.3.62	255.255.255.192	
	Fa1/0	172.16.3.94	255.255.255.224	
	Fa0/0	172.16.3.110	255.255.255.240	
Área de Gobierno				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-Gobierno	S1/0	172.16.2.253	255.255.255.252	
	Fa0/0	172.16.2.62	255.255.255.192	
	Fa2/0	172.16.2.126	255.255.255.192	
	Fa4/0	172.16.2.158	255.255.255.224	
Área de Administración de Red				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-Administración	S3/0	172.16.1.254	255.255.255.252	
	S3/1	172.16.4.254	255.255.255.252	
	S3/2	172.16.3.254	255.255.255.252	
	S3/3	172.16.2.254	255.255.255.252	
	Fa0/0	172.16.17.1	255.255.255.248	
	Fa1/0	172.16.17.9	255.255.255.248	

	Fa2/0	172.16.17.17	255.255.255.248	
Server DHCP	ens3	172.16.17.2	255.255.255.248	172.16.17.1
Server TFTP	E0	172.16.17.10	255.255.255.248	172.16.17.9
Server DNS	E0	172.16.17.11	255.255.255.248	172.16.17.9
Server SNMP	E0	172.16.17.18	255.255.255.248	172.16.17.17
Server HTTP	E0	172.16.17.19	255.255.255.248	172.16.17.17
<b>Área de internet</b>				
<b>Dispositivo</b>	<b>Interfaz</b>	<b>Dirección IP</b>	<b>Máscara de subred</b>	<b>Gateway</b>
R-Internet	S3/0	172.16.1.253	255.255.255.252	
	Fa0/0	192.168.122.2	255.255.255.0	
Cloud	vibr0	192.168.122.1	255.255.255.0	

Para empezar con la configuración de la red se siguen los siguientes pasos.

## Configuración

### Paso 1. Configuraciones básicas

Se configuran todos los routers de la red con los siguientes puntos:

- Configurar una contraseña EXEC privilegiada. **(team1-pass1)**
- Configurar un mensaje del día.
- Establecer una contraseña para las conexiones a consola. **(team1-pass2)**
- Configurar una contraseña para las conexiones vty. **(team1-pass3)**
- Establecer las direcciones IP correspondientes en todos los routers.

*#configure terminal*

*(config)#enable password team1-pass1*

*(config)#banner motd #User Access Verification##*

*(config)#line console 0*

*(config-line)# password team1-pass2*

*(config-line)# login*

*(config-line)# exit*

*(config)#line vty 0 4*

*(config-line)# password team1-pass3*

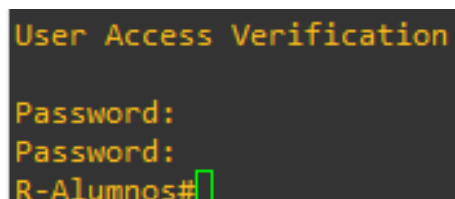
*(config-line)# login*

*(config-line)# exit*



```
R-Alumnos
*Dec 9 23:10:36.519: %LINK-5-CHANGED: Interface Serial3/6, changed state to administratively down
R-Alumnos#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R-Alumnos(config)#banner motd #Solo acceso autorizado!!!#
R-Alumnos(config)#enable password team1-pass1
R-Alumnos(config)#line console 0
R-Alumnos(config-line)#password team1-pass2
R-Alumnos(config-line)#login
R-Alumnos(config-line)#line vty 0
R-Alumnos(config-line)#password team1-pass3
R-Alumnos(config-line)#login
R-Alumnos(config-line)#ex
```

Figura 1. Configuraciones básicas en el router R-Alumnos



```
User Access Verification

Password:
Password:
R-Alumnos#
```

Figura 2. Visualización del mensaje del día en el router R-Alumnos



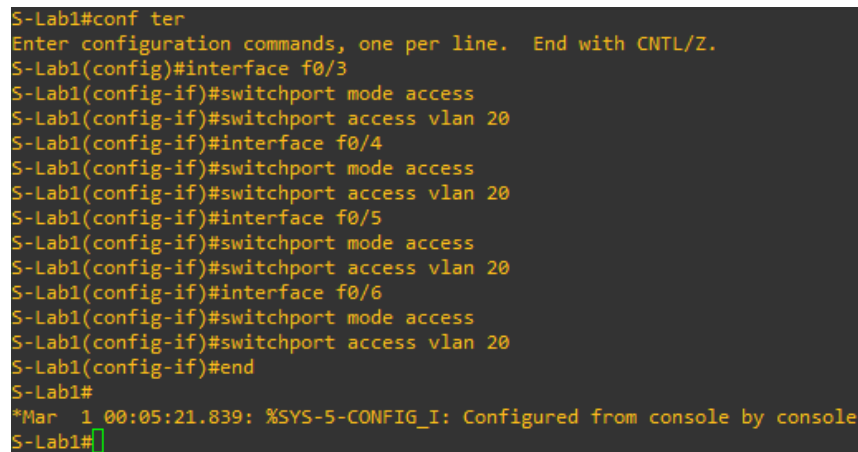
## Paso 2. Configuración de las VLAN

La creación de las VLAN se realiza con los siguientes comandos:

- *S1#configure terminal*
- *S1(config)#vlan database*
- *S1(config)#vlan <vlan-id>*
- *S1(config-vlan)#end*

Para asignar los puertos a las VLAN se usan los siguientes comandos:

- *S1#configure terminal*
- *S1(config)#interface <interface-id>*
- *S1(config-if)#switchport mode access*
- *S1(config-if)#switchport access vlan <vlan-id>*
- *S1(config-if)#end*

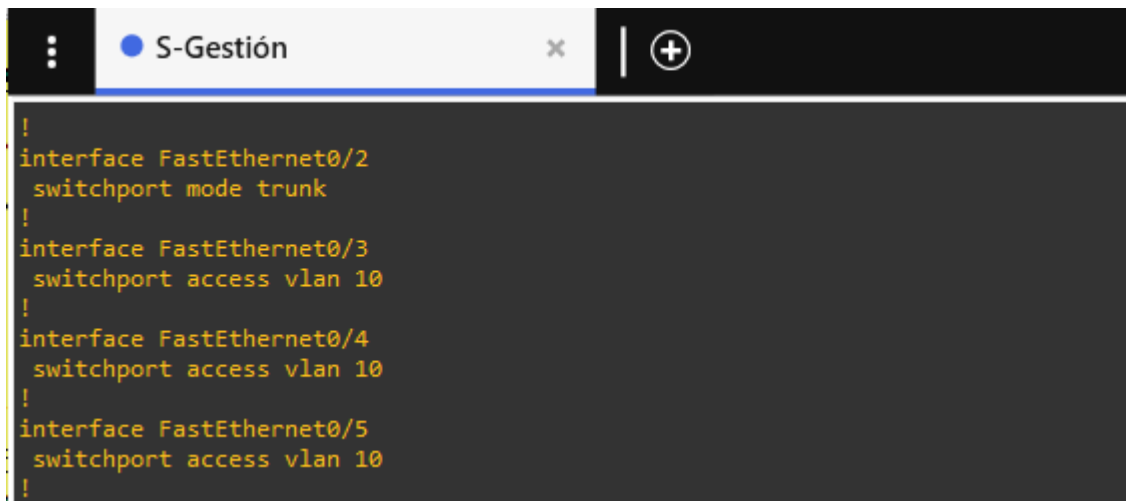


```
S-Lab1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
S-Lab1(config)#interface f0/3
S-Lab1(config-if)#switchport mode access
S-Lab1(config-if)#switchport access vlan 20
S-Lab1(config-if)#interface f0/4
S-Lab1(config-if)#switchport mode access
S-Lab1(config-if)#switchport access vlan 20
S-Lab1(config-if)#interface f0/5
S-Lab1(config-if)#switchport mode access
S-Lab1(config-if)#switchport access vlan 20
S-Lab1(config-if)#interface f0/6
S-Lab1(config-if)#switchport mode access
S-Lab1(config-if)#switchport access vlan 20
S-Lab1(config-if)#end
S-Lab1#
*Mar  1 00:05:21.839: %SYS-5-CONFIG_I: Configured from console by console
S-Lab1#
```

Figura 3. Configuración de VLAN en el switch S-Lab1

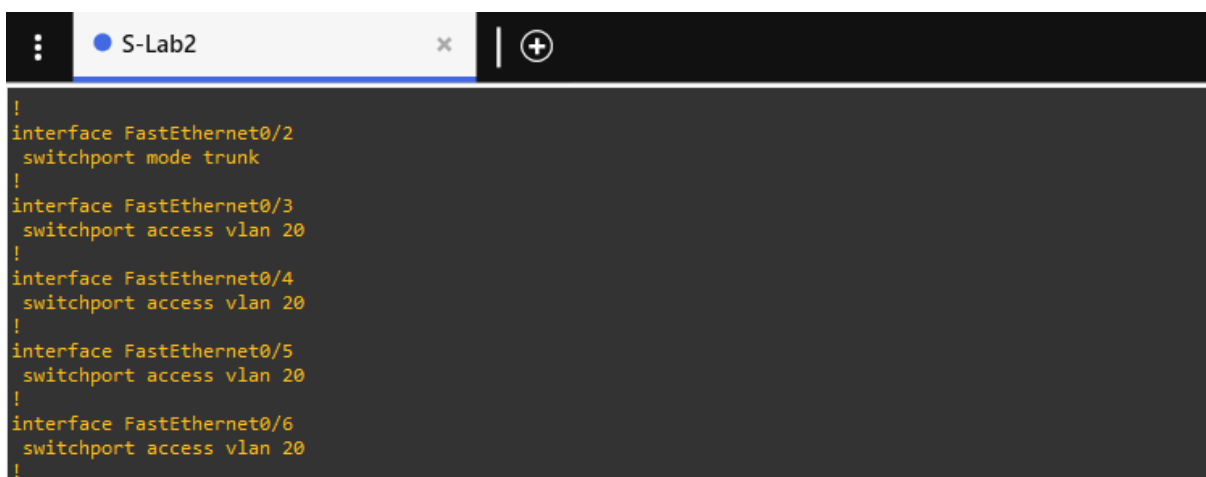
Finalmente se configuran los enlaces truncales:

- *S1#configure terminal*
- *S1(config)#interface <interface-id>*
- *S1(config-if)#switchport trunk encapsulation dot1q*
- *S1(config-if)#switchport mode trunk*
- *S1(config-if)#end*



```
!
interface FastEthernet0/2
  switchport mode trunk
!
interface FastEthernet0/3
  switchport access vlan 10
!
interface FastEthernet0/4
  switchport access vlan 10
!
interface FastEthernet0/5
  switchport access vlan 10
!
```

Figura 4. Configuración de VLAN 10 en el switch S-Gestión



```
!
interface FastEthernet0/2
  switchport mode trunk
!
interface FastEthernet0/3
  switchport access vlan 20
!
interface FastEthernet0/4
  switchport access vlan 20
!
interface FastEthernet0/5
  switchport access vlan 20
!
interface FastEthernet0/6
  switchport access vlan 20
!
```

Figura 5. Configuración de VLAN 20 en el switch S-Lab2

### Paso 3. Configuración enrutamiento con OSPF

Para llevar a cabo el enrutamiento es necesario ingresar a cada uno de los routers e ingresar los siguientes comandos:

- *configure terminal*
- *router ospf 1*
- *network <ip de la interfaz> <wildcard de la red> area <número de área> (0 para este caso)*

El último comando se tendrá que repetir de acuerdo con el número de interfaces que estén conectadas al router. Al final, el enrutamiento queda configurado.

A continuación, se muestran algunos ejemplos de la configuración de OSPF en los routers de la red implementada.

```

R-Alumnos#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.15.254
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.4.0 0.0.0.63 area 0
    172.16.4.64 0.0.0.63 area 0
    172.16.4.252 0.0.0.3 area 0
    172.16.8.0 0.0.7.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

```

Figura 6. Configuración de OSPF en el router R-Alumnos

```

R-Profesores-Gestion#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.3.253
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.3.0 0.0.0.63 area 0
    172.16.3.64 0.0.0.31 area 0
    172.16.3.96 0.0.0.15 area 0
    172.16.3.252 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  192.168.122.2      110          00:37:29
  172.16.2.253       110          01:16:51
  172.16.15.254      110          01:16:51
  172.16.17.17       110          00:37:39
  Distance: (default is 110)

```

Figura 7. Configuración de OSPF en el router R-Profesores-Gestion

```

R-Gobierno#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.2.253
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.2.0 0.0.0.63 area 0
    172.16.2.64 0.0.0.63 area 0
    172.16.2.128 0.0.0.31 area 0
    172.16.2.252 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  192.168.122.2      110          00:39:00
  172.16.3.253       110          01:12:12
  172.16.15.254      110          01:12:12
  172.16.17.17       110          00:39:10
  Distance: (default is 110)

```

Figura 8. Configuración de OSPF en el router R-Gobierno

## Paso 4. Configuración ACL's

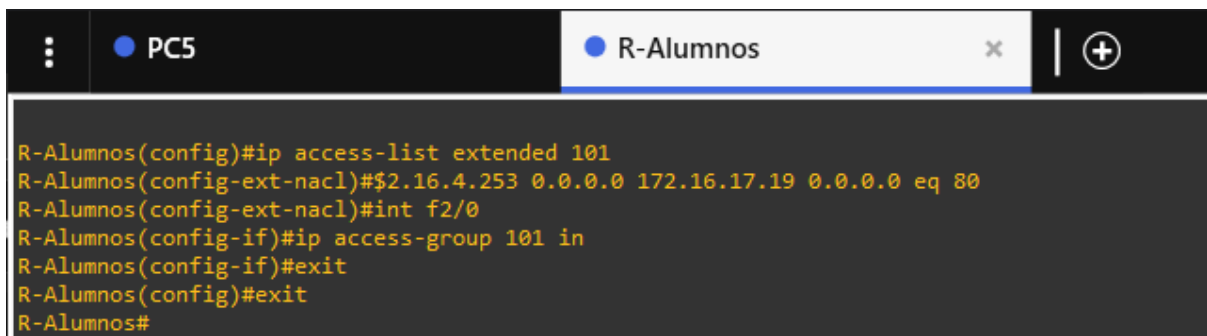
Sintaxis de la ACL extendida:

(cofig)#access-list **n** {permit | deny} **protocol** **source** {source-mask} **destination** {destination-mask} **eq** [destination-port]

Las ACL's que se crearán servirán para los siguientes propósitos:

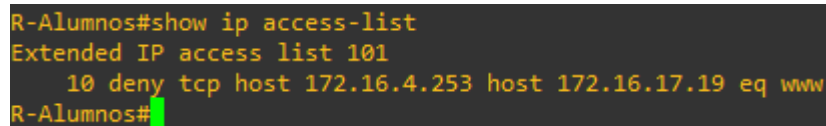
→ Denegar a los dispositivos pertenecientes al área de Alumnos la salida a internet.

→ (cofig)#access-list **101** deny **tcp** host **172.16.4.253** host **172.16.17.19** eq **80**



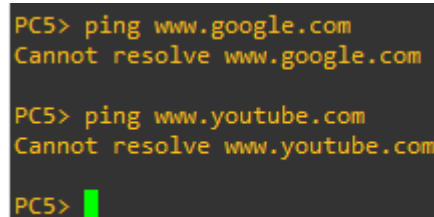
```
R-Alumnos(config)#ip access-list extended 101
R-Alumnos(config-ext-nacl)#172.16.4.253 0.0.0.0 172.16.17.19 0.0.0.0 eq 80
R-Alumnos(config-ext-nacl)#int f2/0
R-Alumnos(config-if)#ip access-group 101 in
R-Alumnos(config-if)#exit
R-Alumnos(config)#exit
R-Alumnos#
```

Figura 9. Configuración de la ACL en el router R-Alumnos



```
R-Alumnos#show ip access-list
Extended IP access list 101
  10 deny tcp host 172.16.4.253 host 172.16.17.19 eq www
R-Alumnos#
```

Figura 10. Comprobando la creación de la ACL en el router R-Alumnos



```
PC5> ping www.google.com
Cannot resolve www.google.com

PC5> ping www.youtube.com
Cannot resolve www.youtube.com

PC5>
```

Figura 11. Denegando la conexión a internet desde la PC5

→ Denegar a los dispositivos pertenecientes a las áreas de Gobierno, Profesores y Gestión Escolar, Alumnos, el tráfico hacia los servidores FTP (telnet y tftp) y SNMP (telnet y tftp).

FTP (telnet y ftp) (Gobierno)

- (cofig)#access-list 105 deny tcp host 172.16.2.253 host 172.16.17.10 eq telnet
- (cofig)#access-list 105 permit ip any any
- (cofig)#access-list 111 deny tcp host 172.16.2.253 host 172.16.17.10 eq ftp
- (cofig)#access-list 111 permit ip any any

```
R-Gobierno#telnet 172.16.2.253
Trying 172.16.2.253 ... Open
User Access Verification
User Access Verification

Password:
R-Gobierno>exit

[Connection to 172.16.2.253 closed by foreign host]
```

Figura 12. Comprando acceso a Telnet antes de aplicar la ACL

```
R-Gobierno#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R-Gobierno(config)#ip access-list extended 105
R-Gobierno(config-ext-nacl)#$st 172.16.2.253 host 172.16.17.10 eq 23
R-Gobierno(config-ext-nacl)#permit ip any any
R-Gobierno(config-ext-nacl)#int s1/0
R-Gobierno(config-if)#ip access-group 105 out
R-Gobierno(config-if)#exit
R-Gobierno(config)#
```

Figura 13. Creación de la ACL en el router R-Gobierno

```
R-Gobierno#show ip access-list
Extended IP access list 105
  10 deny tcp host 172.16.2.253 host 172.16.17.10 eq telnet
  20 permit ip any any
R-Gobierno#
```

Figura 14. Comprobando configuraciones de la ACL desde el router R-Gobierno

```
R-Gobierno#telnet 172.16.17.10
Trying 172.16.17.10 ...
% Connection refused by remote host

R-Gobierno#
```

Figura 15. Bloqueo Telnet desde el router R-Gobierno

FTP (telnet y ftp) (Profesores y Gestión Escolar)

- (cofig)#access-list 106 deny tcp host 172.16.3.253 host 172.16.17.10 eq telnet
- (cofig)#access-list 106 permit ip any any
- (cofig)#access-list 112 deny tcp host 172.16.3.253 host 172.16.17.10 eq ftp
- (cofig)#access-list 112 permit ip any any

FTP (telnet y ftp) (Alumnos)

- (cofig)#access-list 107 deny tcp host 172.16.4.253 host 172.16.17.10 eq telnet
- (cofig)#access-list 107 permit ip any any
- (cofig)#access-list 113 deny tcp host 172.16.4.253 host 172.16.17.10 eq ftp
- (cofig)#access-list 113 permit ip any any

SNMP (telnet y tftp) (Gobierno)

- (cofig)#access-list 108 deny tcp host 172.16.2.253 host 172.16.17.18 eq telnet
- (cofig)#access-list 108 permit ip any any
- (cofig)#access-list 114 deny tcp host 172.16.2.253 host 172.16.17.18 eq ftp
- (cofig)#access-list 114 permit ip any any

SNMP (telnet y tftp) (Profesores y Gestión Escolar)

- (cofig)#access-list 109 deny tcp host 172.16.3.253 host 172.16.17.18 eq telnet
- (cofig)#access-list 109 permit ip any any
- (cofig)#access-list 115 deny tcp host 172.16.3.253 host 172.16.17.18 eq ftp
- (cofig)#access-list 115 permit ip any any

SNMP (telnet y tftp) (Alumnos)

- (cofig)#access-list 110 deny tcp host 172.16.4.253 host 172.16.17.18 eq telnet
- (cofig)#access-list 110 permit ip any any
- (cofig)#access-list 116 deny tcp host 172.16.4.253 host 172.16.17.18 eq ftp
- (cofig)#access-list 116 permit ip any any

## Paso 5. Configuración PAT

Configurar PAT en esta topología nos servirá para que todos los dispositivos conectados en nuestra red privada puedan tener acceso a internet. Dentro de la topología de red, se tiene un área especial llamada “Internet”, la cual se conforma de una nube llamada “Internet”, la cual tiene dos interfaces de red (vibr0 y eth0), las cuales son interfaces pertenecientes a la máquina virtual de Azure que tienen acceso a internet; hacia esta nube está conectado en su interfaz vibr0 un router llamado R-Internet a través de su puerto fastEthernet 0/0, el cual tiene como dirección IP 192.168.122.2/24. Esta es una dirección perteneciente a la red de vibr0.

Una vez se ha configurado la IP de la interfaz FastEthernet 0/0, se agrega la siguiente ruta dentro de R-Internet:

```
ip route 0.0.0.0 0.0.0.0 192.168.122.1
```

Y procedemos también a configurar el ruteo con OSPF, agregando la instrucción default-information originate. Con lo anterior, R-Internet tendrá acceso a internet, sin embargo, para que los demás dispositivos de la red privada puedan tener acceso a internet es necesario que tengan asignada una dirección IP perteneciente a la red 192.168.122.0/24, sin embargo, en la red privada que estamos configurando las direcciones IP pertenecen a 172.16.0.0/16. Es por ello que necesitamos configurar PAT, para realizar las traducciones de las direcciones de nuestra red 172.16.0.0/16 hacia una dirección perteneciente a 192.168.122.0/24, que en este caso será la usada en la interfaz FastEthernet 0/0. Para realizar esta configuración se lleva a cabo lo siguiente.

```

enP29997s1: flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST> mtu 1500
ether 00:0d:3a:54:2d:2d txqueuelen 1000 (Ethernet)
RX packets 1133958 bytes 1615724697 (1.6 GB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 432428 bytes 53884422 (53.8 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.4 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::20d:3aff:fe54:2d2d prefixlen 64 scopeid 0x20<link>
ether 00:0d:3a:54:2d:2d txqueuelen 1000 (Ethernet)
RX packets 985569 bytes 1600398082 (1.6 GB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 426880 bytes 51574708 (51.5 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

gns3tap0-0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 ::d86a:76ff:fe5f:ecbc prefixlen 64 scopeid 0x20<link>
ether da:6a:76:5f:ec:bc txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2945 bytes 183629 (183.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

gns3tap0-2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::70e7:9cff:fe54:8aa9 prefixlen 64 scopeid 0x20<link>
ether 72:e7:9c:54:8a:a9 txqueuelen 1000 (Ethernet)
RX packets 785 bytes 77373 (77.3 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2583 bytes 144808 (144.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 3301821 bytes 3583713732 (3.5 GB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3301821 bytes 3583713732 (3.5 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
ether 52:54:00:32:16:e4 txqueuelen 1000 (Ethernet)
RX packets 1434 bytes 118234 (118.2 KB)
RX errors 0 dropped 17 overruns 0 frame 0
TX packets 232 bytes 23720 (23.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

admin@GNS3@gns3vm:~$

```

Figura 16. Interfaces de red disponibles en la máquina virtual gns3vm en Azure.

1. Configurar un pool de direcciones para NAT.

***ip nat pool <nombre del pool> <IP inicial> <IP final> netmask <máscara de red>***

***ip nat pool NAT-INTERNET 192.168.122.2 192.168.122.2 netmask 255.255.255.0***

2. Crear una lista de acceso (ACL) para permitir que todos los hosts de la red privada puedan acceder a internet.

***access-list <número de ACL> permit <id de red> <wildcard>***  
***access-list 24 permit 172.16.0.0 0.0.255.255***

3. Configurar el PAT con la ACL para lograr la traducción de direcciones.

***ip nat inside source list <número de ACL> pool <nombre del pool>***  
***overload***

***ip nat inside source list 24 pool NAT-INTERNET overload***



Una vez realizado lo anterior, el PAT ha quedado configurado, quedando lo siguiente en el router R-Internet.

```
interface FastEthernet0/0
 ip address 192.168.122.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex half
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
!
interface Serial3/0
 ip address 172.16.1.253 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 serial restart-delay 0
!
```

**Figura 17.** Configuración de las interfaces del router R-Internet.

```
router ospf 1
 network 172.16.1.252 0.0.0.3 area 0
 network 192.168.122.0 0.0.0.255 area 0
 default-information originate
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat pool NAT-INTERNET 192.168.122.2 192.168.122.2 netmask 255.255.255.0
ip nat inside source list 24 pool NAT-INTERNET overload
ip route 0.0.0.0 0.0.0.0 192.168.122.1
!
access-list 24 permit 172.16.0.0 0.0.255.255
no cdp log mismatch duplex
!
```

**Figura 18.** Configuración de la ACL y PAT en el router R-Internet.

A modo de comprobación, se comprueba la conexión a internet en el router R-Administración y en una máquina virtual cliente perteneciente al Área de alumnos-biblioteca.

```

R-Administracion#ping www.google.com
Translating "www.google.com"...domain server (192.168.122.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 142.251.45.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/56/132 ms
R-Administracion#ping www.youtube.com
Translating "www.youtube.com"...domain server (192.168.122.1) [OK]

Translating "www.youtube.com"...domain server (192.168.122.1) [OK]

Translating "www.youtube.com"...domain server (192.168.122.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.13.238, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/27/32 ms
R-Administracion#

```

Figura 19. Comprobación de conexión a internet desde el router R-Administración.

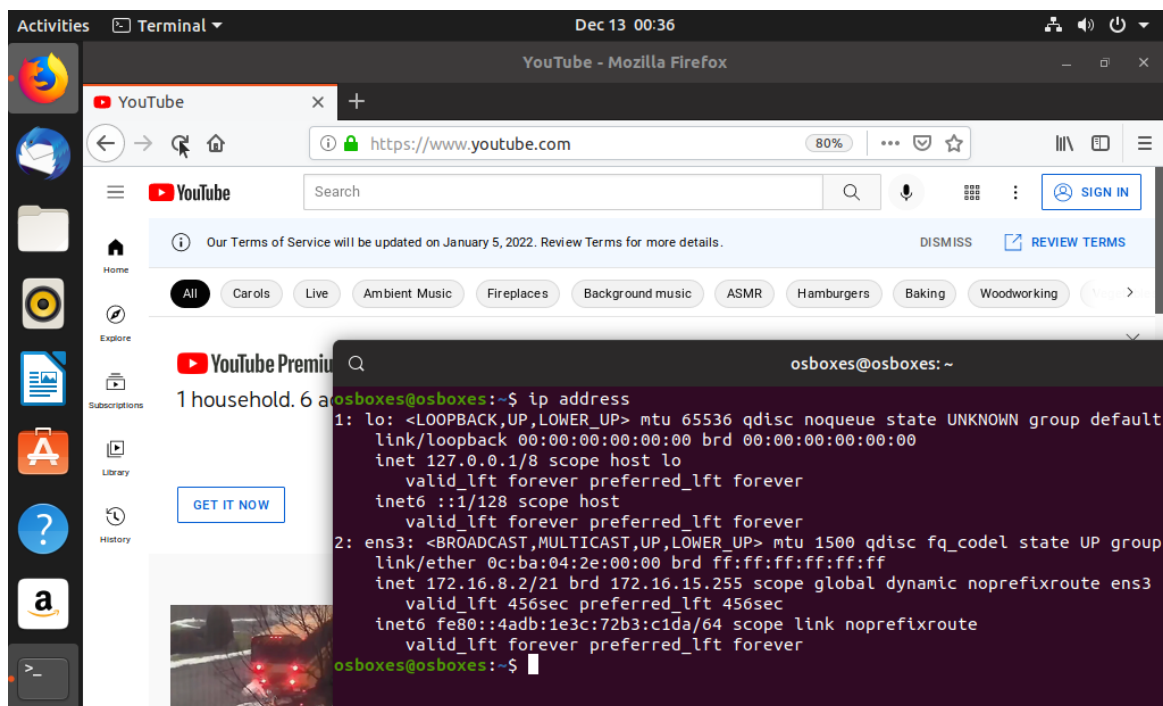


Figura 20. Conexión a internet a través de un cliente Ubuntu ubicado en el área de alumnos.

Finalmente, se muestra el comando “show ip nat translations” para visualizar la traducción realizada por el router R-Internet.

```

R-Internet#sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 192.168.122.2:3832 172.16.8.2:3832   142.250.31.105:3832 142.250.31.105:3832
udp 192.168.122.2:32818 172.16.8.2:32818 192.168.122.1:53    192.168.122.1:53
udp 192.168.122.2:35278 172.16.8.2:35278 192.168.122.1:53    192.168.122.1:53
udp 192.168.122.2:36398 172.16.8.2:36398 192.168.122.1:53    192.168.122.1:53
udp 192.168.122.2:38565 172.16.8.2:38565 192.168.122.1:53    192.168.122.1:53
tcp 192.168.122.2:39316 172.16.8.2:39316 99.84.216.7:443     99.84.216.7:443
udp 192.168.122.2:39865 172.16.8.2:39865 192.168.122.1:53    192.168.122.1:53
udp 192.168.122.2:40909 172.16.8.2:40909 192.168.122.1:53    192.168.122.1:53
tcp 192.168.122.2:41542 172.16.8.2:41542 142.250.73.227:80   142.250.73.227:80
tcp 192.168.122.2:41544 172.16.8.2:41544 142.250.73.227:80   142.250.73.227:80
tcp 192.168.122.2:41646 172.16.8.2:41646 172.217.13.86:443    172.217.13.86:443
tcp 192.168.122.2:41668 172.16.8.2:41668 52.85.131.17:443    52.85.131.17:443
tcp 192.168.122.2:42086 172.16.8.2:42086 34.107.221.82:80     34.107.221.82:80
tcp 192.168.122.2:42106 172.16.8.2:42106 34.107.221.82:80     34.107.221.82:80
tcp 192.168.122.2:42108 172.16.8.2:42108 34.107.221.82:80     34.107.221.82:80
udp 192.168.122.2:42497 172.16.8.2:42497 91.189.89.198:123    91.189.89.198:123
udp 192.168.122.2:48201 172.16.8.2:48201 192.168.122.1:53    192.168.122.1:53
tcp 192.168.122.2:50438 172.16.8.2:50438 172.217.0.35:443     172.217.0.35:443
udp 192.168.122.2:53178 172.16.8.2:53178 192.168.122.1:53    192.168.122.1:53
tcp 192.168.122.2:54776 172.16.8.2:54776 172.217.15.78:443    172.217.15.78:443
tcp 192.168.122.2:54778 172.16.8.2:54778 172.217.15.78:443    172.217.15.78:443
udp 192.168.122.2:54848 172.16.8.2:54848 192.168.122.1:53    192.168.122.1:53
udp 192.168.122.2:57039 172.16.8.2:57039 91.189.89.198:123    91.189.89.198:123
udp 192.168.122.2:58145 172.16.8.2:58145 192.168.122.1:53    192.168.122.1:53
tcp 192.168.122.2:58426 172.16.8.2:58426 172.217.0.42:443     172.217.0.42:443
tcp 192.168.122.2:60974 172.16.8.2:60974 142.251.16.84:443    142.251.16.84:443

```

Figura 21. Ejecución del comando “show ip nat translations” en R-Internet.

## Paso 6. Configuración servidor DHCP

Para esta red se utilizará una máquina virtual con Debian como sistema operativo para dar el servicio de DHCP a los clientes de la red, los cuales son todos los dispositivos finales conectados a cada una de las áreas que componen la red. Entonces, como primer paso es instalar en esta máquina virtual llamada Server-DHCP el paquete de servidor de DHCP con el siguiente comando:

*apt install isc-dhcp-server*

Luego de la instalación, se deberán de editar los siguientes archivos: */etc/defaults/isc-dhcp-server* y */etc/dhcp/dhcpd.conf*.

En el primero únicamente se especifica la interfaz por donde el servidor dará el servicio, que para este caso es la interfaz con nombre **ens3**.

```
GNU nano 3.2                                isc-dhcp-server

# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#   Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#   Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens3"
INTERFACESv6=""
```

**Figura 22.** Configuración del archivo isc-dhcp-server

En el segundo archivo se tendrán que especificar cada uno de los pool de direcciones a las que asignará en un futuro, también se especifica el nombre DNS para el servicio, su dirección IP y el tiempo que un cliente será propietario de la IP asignada.

```
# dhcpd.conf
# Sample configuration file for ISC dhcpd

# option definitions common to all supported networks...
option domain-name "172.16.17.2";
option domain-name-servers team1-dhcp-server.com;

default-lease-time 600;
max-lease-time 7200;
```

**Figura 23.** Edición del archivo dhcpd.conf

```
#Gobierno-Finanzas
subnet 172.16.2.64 netmask 255.255.255.192{
    range 172.16.2.65 172.16.2.125
    option routers 172.16.2.126
    option broadcast-address 172.16.2.127
}

#Gobierno-Recursos Humanos
subnet 172.16.2.128 netmask 255.255.255.224{
    range 172.16.2.129 172.16.2.157
    option routers 172.16.2.158
    option broadcast-address 172.16.2.159
}

#---Área de profesores y gestión
#Área gestión escolar
subnet 172.16.3.0 netmask 255.255.255.192{
    range 172.16.3.1 172.16.3.61
    option routers 172.16.3.62
    option broadcast-address 172.16.3.63
}
```

Figura 24. Parte de la edición del archivo dhcpd.conf.

Finalmente, reiniciamos el servicio para que se apliquen los cambios realizados en el archivo. Como se puede observar en la siguiente imagen, al reiniciar y consultar el estatus del servicio, éste se encuentra activo de forma satisfactoria.

```
root@debian-gns3:/etc/default# systemctl restart isc-dhcp-server
root@debian-gns3:/etc/default# systemctl status isc-dhcp-server.service
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Sat 2021-12-11 18:54:52 EST; 27s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 489 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 2359)
   Memory: 5.5M
    CGroup: /system.slice/isc-dhcp-server.service
            └─501 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens3

Dec 11 18:54:49 debian-gns3 systemd[1]: Starting LSB: DHCP server...
Dec 11 18:54:50 debian-gns3 isc-dhcp-server[489]: Launching IPv4 server only.
Dec 11 18:54:50 debian-gns3 dhcpd[501]: Wrote 0 leases to leases file.
Dec 11 18:54:50 debian-gns3 dhcpd[501]: Server starting service.
Dec 11 18:54:52 debian-gns3 isc-dhcp-server[489]: Starting ISC DHCPv4 server: dhcpd.
Dec 11 18:54:52 debian-gns3 systemd[1]: Started LSB: DHCP server.
root@debian-gns3:/etc/default#
```

Figura 25. Estado del servicio de DHCP.

Como forma de corroborar que el servicio está activo, se solicitará desde una PC el servicio de DHCP, en el cual se le debe asignar una IP una vez establecida la comunicación con el servidor. Para este caso, la PC3 del área de alumnos solicita una dirección IP al servidor DHCP y éste le contesta y le asigna una IP.

```

PC3> ip dhcp
DDORA IP 172.16.8.1/21 GW 172.16.15.254

PC3> sh ip

NAME          : PC3[1]
IP/MASK       : 172.16.8.1/21
GATEWAY       : 172.16.15.254
DNS           :
DHCP SERVER   : 172.16.17.2
DHCP LEASE    : 456, 600/300/525
MAC           : 00:50:79:66:68:10
LPORT        : 20252
RHOST:PORT    : 127.0.0.1:20253
MTU           : 1500

```

Figura 26. Solicitud del servicio de DHCP en la PC3.

```

root@debian-gns3:~# systemctl status isc-dhcp-server.service
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Sat 2021-12-11 22:34:02 EST; 1min 9s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 576 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 2359)
   Memory: 5.3M
    CGroup: /system.slice/isc-dhcp-server.service
            └─588 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens3

Dec 11 22:34:00 debian-gns3 systemd[1]: Starting LSB: DHCP server...
Dec 11 22:34:00 debian-gns3 isc-dhcp-server[576]: Launching IPv4 server only.
Dec 11 22:34:00 debian-gns3 dhcpd[588]: Wrote 0 leases to leases file.
Dec 11 22:34:00 debian-gns3 dhcpd[588]: Server starting service.
Dec 11 22:34:02 debian-gns3 isc-dhcp-server[576]: Starting ISC DHCPv4 server: dhcpd.
Dec 11 22:34:02 debian-gns3 systemd[1]: Started LSB: DHCP server.
Dec 11 22:34:53 debian-gns3 dhcpd[588]: DHCPDISCOVER from 00:50:79:66:68:10 via 172.16.15.254
Dec 11 22:34:54 debian-gns3 dhcpd[588]: DHCPOFFER on 172.16.8.1 to 00:50:79:66:68:10 (PC3) via 172.16.15.254
Dec 11 22:34:57 debian-gns3 dhcpd[588]: DHCPREQUEST for 172.16.8.1 (172.16.17.2) from 00:50:79:66:68:10 (PC3) via 172.16.15.254
Dec 11 22:34:57 debian-gns3 dhcpd[588]: DHCPACK on 172.16.8.1 to 00:50:79:66:68:10 (PC3) via 172.16.15.254

```

Figura 27. Estado del servicio DHCP en el servidor DHCP.

## Paso 7. Configuración servidor HTTP

Para nuestra red daremos el servicio de HTTP para dos páginas web diferentes, una será destinada para el área de alumnos y otra para el área de profesores, esto porque en cada página se podría colocar información relevante para ambos grupos, y es conveniente que cada uno pueda acceder a dos páginas web diferentes. Para lograr lo anterior, es necesario tener dos interfaces de red y modificar ambas para que proporcionen el servicio, existen muchas formas de configurar este servicio y para este caso crearemos una interfaz de red virtual derivada de la interfaz de red llamada ens3, la interfaz principal ens3 será quien dará servicio a la página web de los alumnos y tendrá asignada la IP 172.16.17.19, y la interfaz virtual ens3:0 dará el servicio a la página web de los profesores con dirección 172.16.17.20 La configuración del servidor se muestra a continuación.

```
GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
    address 172.16.17.19
    netmask 255.255.255.248
    gateway 172.16.17.17
auto ens3:0
iface ens3:0 inet static
    address 172.16.17.20
    netmask 255.255.255.248
    gateway 172.16.17.17

auto ens4
iface ens4 inet dhcp
```

Figura 28. Configuración de la interfaz ens3 y la interfaz virtual ens3:0 en el servidor.

Luego, tras instalar el servidor apache dentro del servidor usando la instrucción **sudo apt install apache2**, deberemos crear un archivo con la configuración de la página web de los profesores dentro del directorio **/etc/apache2/sites-available**, puesto que es la perteneciente a la interfaz de red virtual. Tomamos como plantilla el archivo llamado **000-default.conf**, editamos la información y nombramos a este archivo con la dirección que tendrá la página web de los profesores (**172.16.17.20.conf**). En este archivo se especifica el nombre del servidor (**ServerName "172.16.17.20"**) y la ubicación del archivo html de la página de los profesores (**DocumentRoot /var/www/sites-profesores**).

```
root@debian-gns3:/etc/apache2/sites-available# ls
000-default.conf 172.16.17.20.conf default-ssl.conf
```

Figura 29. Creación del archivo 172.16.17.20.conf usando la plantilla 000-default.conf.

```
GNU nano 3.2 172.16.17.20.conf
<VirtualHost 172.16.17.20>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    ServerName "172.16.17.20"

    DocumentRoot /var/www/site-profesores

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Figura 30. Edición del archivo 172.16.17.20.conf.

Una vez hecho esto, nos ubicamos en el directorio **/var/www** y creamos el directorio **"site-profesores"**, dentro de él creamos el archivo **index.html**. Por otro lado, en el directorio **/var/www/html** creamos el archivo **index.html**, el cual será la página web de los alumnos. También tendremos en ambos directorios una carpeta llamada **images**, en la cual se guardarán las imágenes usadas por las páginas web.

```
root@debian-gns3:/var/www# ls
html site-alumnos site-profesores
root@debian-gns3:/var/www# cd html
root@debian-gns3:/var/www/html# ls
images index.html
root@debian-gns3:/var/www/html# cd ..
root@debian-gns3:/var/www# cd site-profesores
root@debian-gns3:/var/www/site-profesores# ls
images index.html
root@debian-gns3:/var/www/site-profesores#
```

Figura 31. Creación de los directorios y archivos dentro del directorio /var/www.

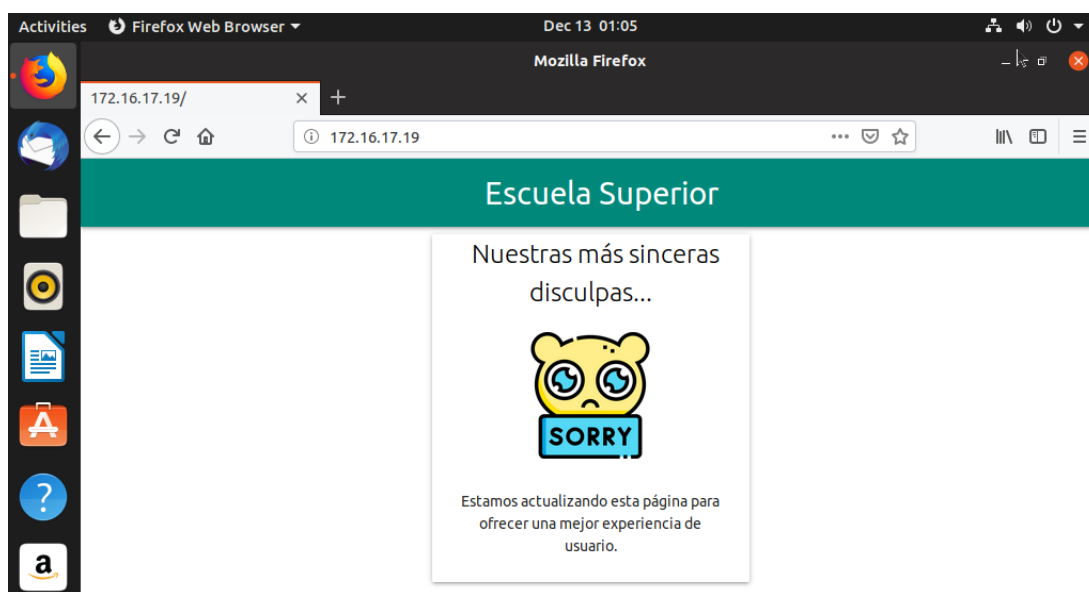
Como siguiente paso, se **"activa"** el sitio correspondiente a los profesores con la instrucción **"a2ensite 172.16.17.20"**, para el caso del sitio de los alumnos no se realiza este paso, puesto que por default ya viene activado el sitio ubicado en **/var/www/html**. Luego, se reinicia el servicio HTTP para que se apliquen los cambios realizados con la instrucción **"service apache2 reload"**.



```
root@debian-gns3:/etc/apache2# service apache2 reload
root@debian-gns3:/etc/apache2# apache2ctl -t
AH00558: apache2: Could not reliably determine the server's
irrective globally to suppress this message
Syntax OK
root@debian-gns3:/etc/apache2# _
```

**Figura 32.** Reinicio del servicio HTTP para aplicar los cambios.

Se pueden editar las páginas web incluso después de reiniciar el servidor, por lo que es el siguiente paso a realizar, y puesto que realizar una página web está fuera de los objetivos de este proyecto, no se mostrará la forma de crearlas. Finalmente, como forma de comprobar el funcionamiento del servidor, se accede a las páginas correspondientes a la de alumnos y profesores desde el área de alumnos. Se observa que en el navegador se ingresan las IPs correspondientes a cada servicio.



**Figura 33.** Comprobación del funcionamiento del servidor HTTP ingresando a la página de alumnos.

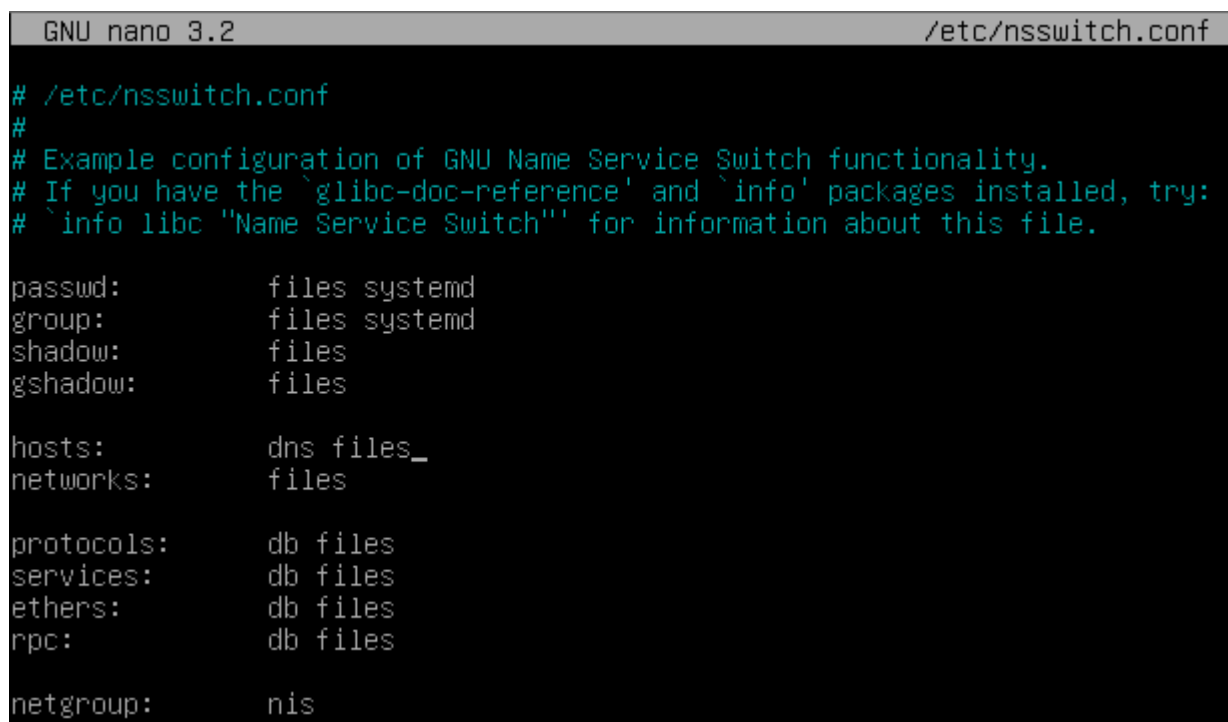


**Figura 34.** Comprobación del funcionamiento del servidor HTTP ingresando a la página de profesores.

Ahora bien, es importante configurar un servidor DNS dentro de la red para que pueda traducir las direcciones IP correspondientes a las páginas web creadas, por lo que es el siguiente paso a seguir.

## Paso 8. Configuración servidor DNS

Luego de descargar e instalar el paquete bind9 en una máquina virtual Debian 10, procedemos a configurar los siguientes archivos.



```
GNU nano 3.2 /etc/nsswitch.conf

# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      files systemd
group:       files systemd
shadow:      files
gshadow:     files

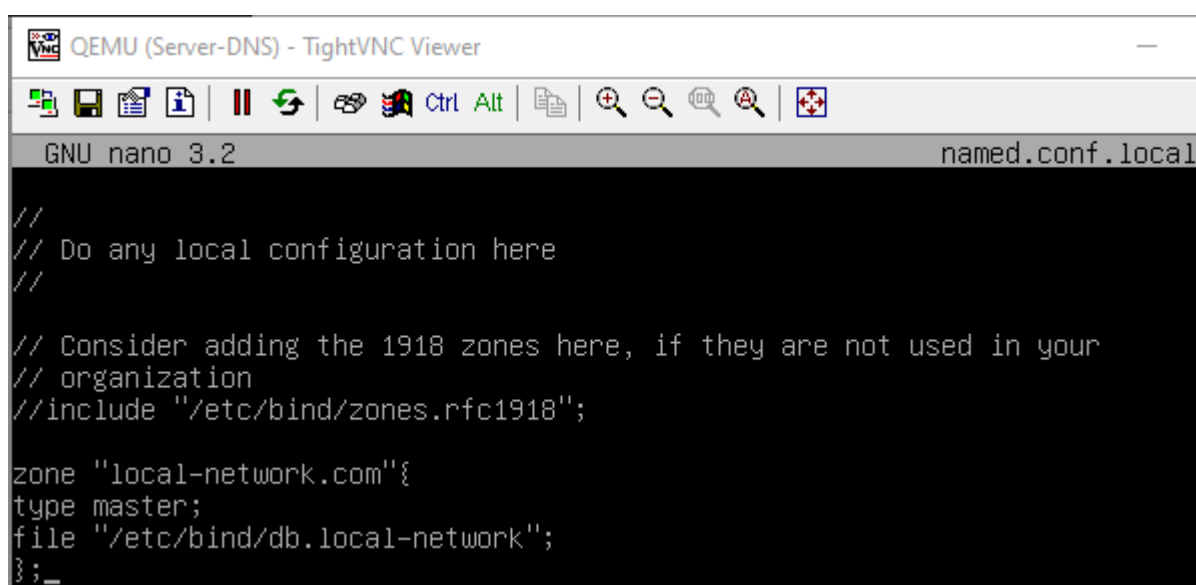
hosts:       dns files_
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

Figura 35. Edición del archivo /etc/nsswitch.conf

En /etc/nsswitch.conf únicamente colocamos “dns” al principio de hosts.



```
QEMU (Server-DNS) - TightVNC Viewer

GNU nano 3.2 named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "local-network.com"{
type master;
file "/etc/bind/db.local-network";
};_
```

Figura 36. Edición del archivo named.conf.local

En el archivo anterior, se agrega la zona DNS, que para este caso se llamará “local-network”. Indicamos que será de tipo master y la configuración de la zona estará en /etc/bind/db.local-network.

Luego, editamos el archivo db.local-network., indicando las IPs de la zona local.

```
GNU nano 3.2 db.local-network
;
; Fichero de registros de recursos BIND para la zona de local-network.com
;
$TTL 604800
@ IN SOA servidor.local-network.com. root.local-network.com. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
;
servidor IN NS servidor.local-network.com.
servidor IN A 172.16.17.11
servidor-ftp IN A 172.16.17.10
```

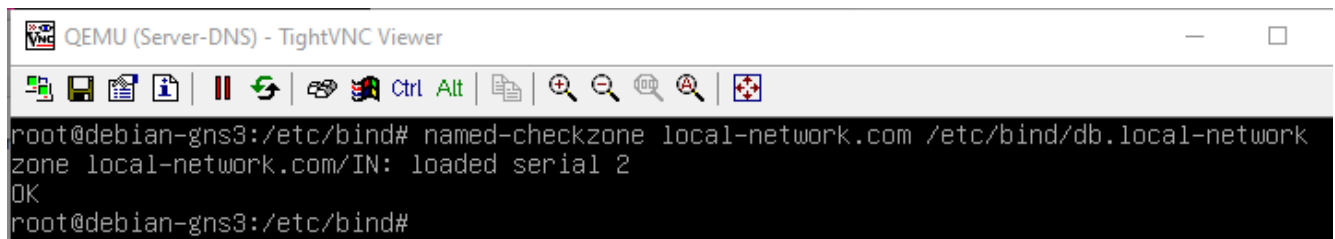
Figura 37. Edición del archivo db.local-network.

Después, editamos la zona inversa, la cual está contenida en db.11.17.16.172

```
GNU nano 3.2 db.11.17.16.172
;
; Fichero de registros de recursos BIND para la zona inversa 17.16.172
;
$TTL 604800
@ IN SOA servidor.local-network.com. root.local-network.com. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
;
IN NS servidor.local-network.com.
11 IN PTR servidor.local-network.com.
10 IN PTR servidor.servidor-ftp.com._
```

Figura 38. Edición del archivo db.11.17.16.172

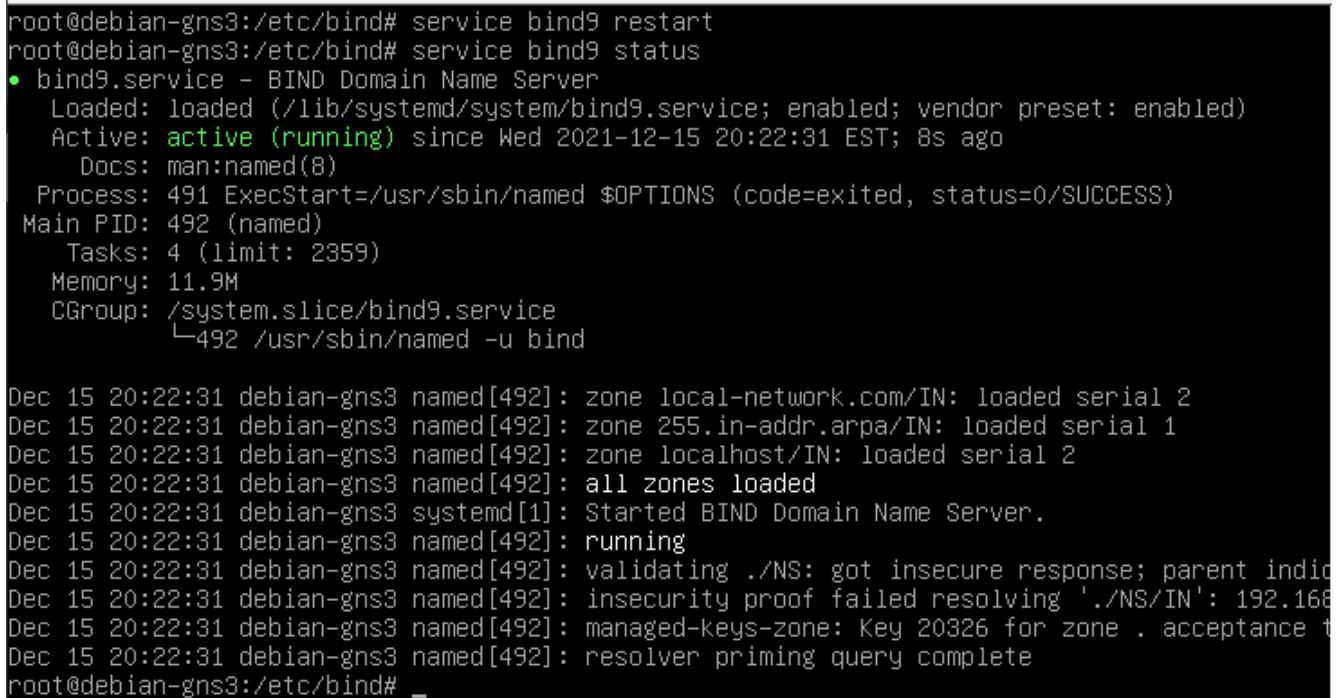
Luego, checamos que ambos archivos no tengan errores con el comando `named-checkzone local-network /etc/bind/db.local-network.`



```
QEMU (Server-DNS) - TightVNC Viewer
root@debian-gns3:/etc/bind# named-checkzone local-network.com /etc/bind/db.local-network
zone local-network.com/IN: loaded serial 2
OK
root@debian-gns3:/etc/bind#
```

Figura 39. Comprobación de la correcta edición de los archivos.

Finalmente, reiniciamos el servicio DNS y comprobamos su funcionamiento, observamos que está activo y sin errores.



```
root@debian-gns3:/etc/bind# service bind9 restart
root@debian-gns3:/etc/bind# service bind9 status
• bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-12-15 20:22:31 EST; 8s ago
     Docs: man:named(8)
  Process: 491 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 492 (named)
    Tasks: 4 (limit: 2359)
   Memory: 11.9M
    CGroup: /system.slice/bind9.service
            └─492 /usr/sbin/named -u bind

Dec 15 20:22:31 debian-gns3 named[492]: zone local-network.com/IN: loaded serial 2
Dec 15 20:22:31 debian-gns3 named[492]: zone 255.in-addr.arpa/IN: loaded serial 1
Dec 15 20:22:31 debian-gns3 named[492]: zone localhost/IN: loaded serial 2
Dec 15 20:22:31 debian-gns3 named[492]: all zones loaded
Dec 15 20:22:31 debian-gns3 systemd[1]: Started BIND Domain Name Server.
Dec 15 20:22:31 debian-gns3 named[492]: running
Dec 15 20:22:31 debian-gns3 named[492]: validating ./NS: got insecure response; parent indic
Dec 15 20:22:31 debian-gns3 named[492]: insecurity proof failed resolving './NS/IN': 192.168
Dec 15 20:22:31 debian-gns3 named[492]: managed-keys-zone: Key 20326 for zone . acceptance t
Dec 15 20:22:31 debian-gns3 named[492]: resolver priming query complete
root@debian-gns3:/etc/bind# _
```

Figura 40. Comprobación del funcionamiento del servicio DNS

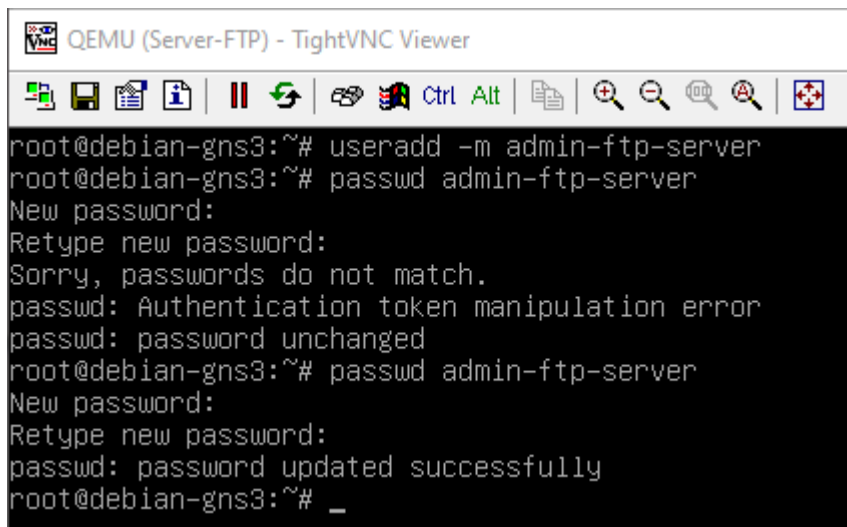
Sin embargo, al intentar comprobar el funcionamiento de este servicio no se pudo acceder a las IP con los dominios configurados, pese intentar cambiar una y otra vez las configuraciones para DNS.

## Paso 9. Configuración servidor FTP

El servidor FTP se instalará y ejecutará en una máquina virtual con Linux Debian 10. Como primer paso en la configuración del servidor es necesario instalar el paquete para el servidor FTP, para ello ejecutamos el siguiente comando:

**sudo apt install vsftpd**

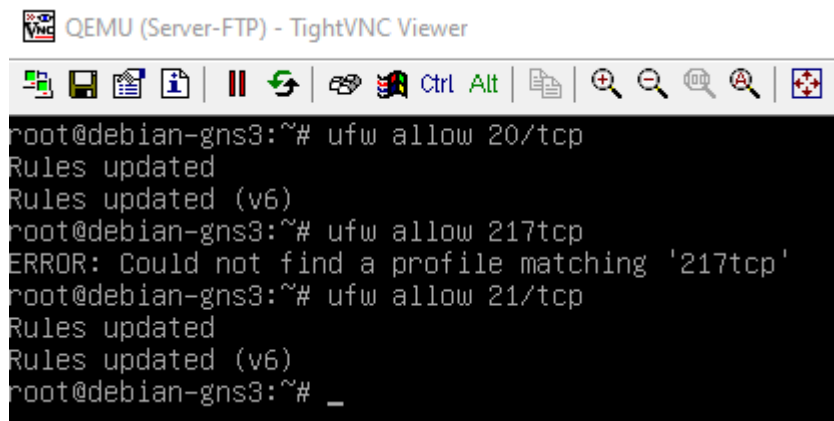
Una vez hecho lo anterior, procedemos a crear un nuevo usuario FTP para poder acceder al servidor, en este caso se establece el usuario **admin-ftp-server** y contraseña **pass-ftp-server**.



```
root@debian-gns3:~# useradd -m admin-ftp-server
root@debian-gns3:~# passwd admin-ftp-server
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
root@debian-gns3:~# passwd admin-ftp-server
New password:
Retype new password:
passwd: password updated successfully
root@debian-gns3:~# _
```

Figura 41. Establecimiento de un nuevo usuario con contraseña para el acceso al servidor FTP.

Luego, será necesario abrir los puertos 20 y 21 del servidor para que pueda aceptar conexiones.

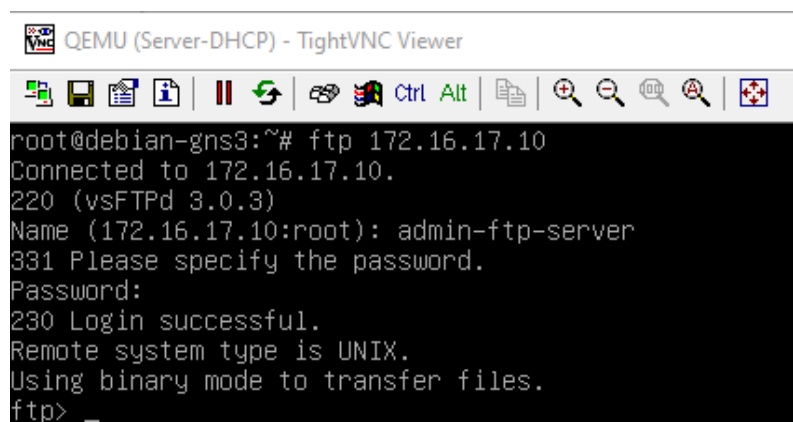


```
root@debian-gns3:~# ufw allow 20/tcp
Rules updated
Rules updated (v6)
root@debian-gns3:~# ufw allow 217tcp
ERROR: Could not find a profile matching '217tcp'
root@debian-gns3:~# ufw allow 21/tcp
Rules updated
Rules updated (v6)
root@debian-gns3:~# _
```

Figura 42. Apertura de los puertos 20 y 21 del servidor FTP.

Con la configuración anterior, el servidor FTP está listo para usarse, se prueba su funcionamiento conectándose a este servidor a través del servidor DHCP con el comando

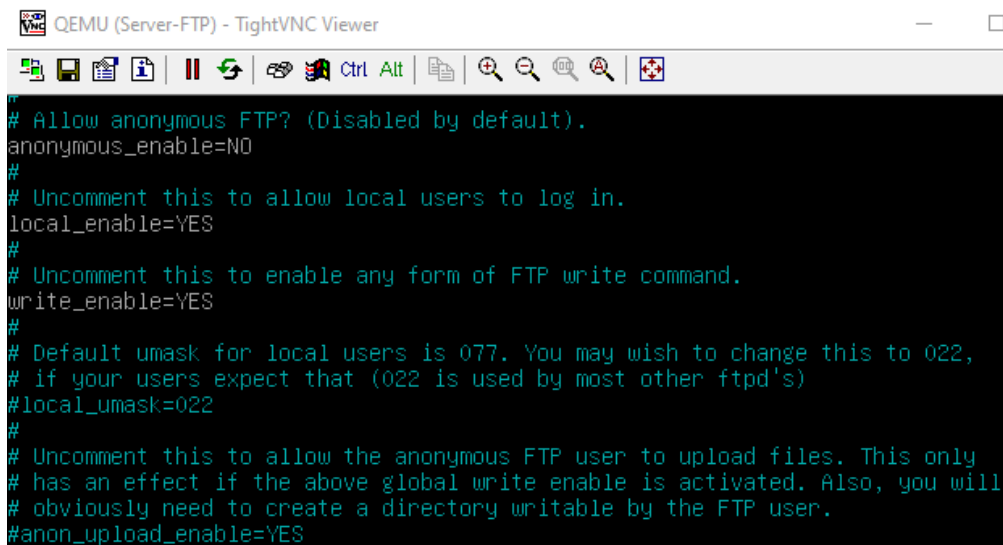
**ftp <dirección ip del servidor FTP>**  
**ftp 172.16.17.10**



```
root@debian-gns3:~# ftp 172.16.17.10
Connected to 172.16.17.10.
220 (vsFTPD 3.0.3)
Name (172.16.17.10:root): admin-ftp-server
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

**Figura 43.** Conexión hacia el servidor FTP desde el servidor DHCP.

Finalmente, para permitir que los usuarios que ingresen al servidor FTP puedan escribir en el directorio, editaremos el archivo `/etc/vsftpd.conf` habilitando la instrucción `write_enable=YES`. Guardamos los cambios y reiniciamos el servicio.

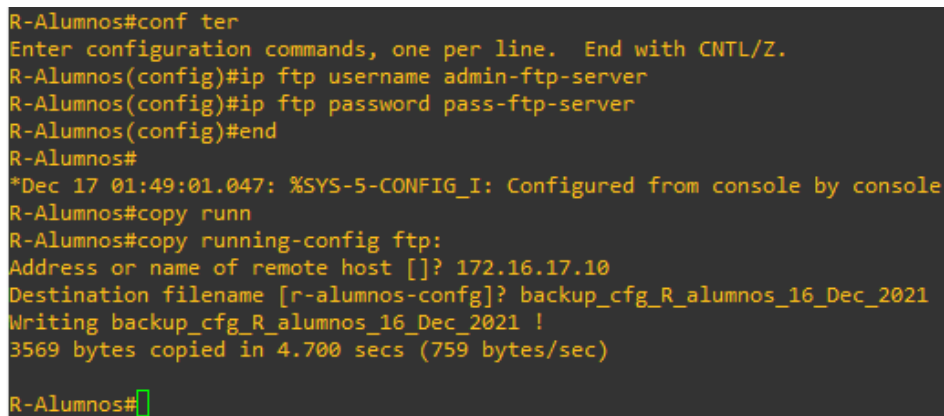


```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
```

**Figura 44.** Edición del archivo vsftpd.conf para permitir la escritura en el directorio.

Finalmente, volvemos a probar el servicio ingresando nuevamente al servidor por medio del servidor DHCP, no sin antes crear un documento en el servidor FTP con nombre `test.txt`, el cual contiene lo siguiente: *“Esta es una prueba del funcionamiento de FTP, este archivo puede ser descargado por los clientes FTP.”* El archivo mencionado anteriormente se consigue usando el comando `get test.txt`. Al desconectarse del servidor podemos observar que el archivo obtenido se encuentra en el servidor DHCP, y si leemos su contenido es tal cual el que se encuentra en el servidor FTP.

También probaremos que los routers puedan ser capaces de establecer una conexión con este servidor para que este sea el lugar donde se guardarán las copias de seguridad de sus configuraciones y/o imágenes.



```
R-Alumnos#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R-Alumnos(config)#ip ftp username admin-ftp-server
R-Alumnos(config)#ip ftp password pass-ftp-server
R-Alumnos(config)#end
R-Alumnos#
*Dec 17 01:49:01.047: %SYS-5-CONFIG_I: Configured from console by console
R-Alumnos#copy runn
R-Alumnos#copy running-config ftp:
Address or name of remote host []? 172.16.17.10
Destination filename [r-alumnos-config]? backup_cfg_R_alumnos_16_Dec_2021
Writing backup_cfg_R_alumnos_16_Dec_2021 !
3569 bytes copied in 4.700 secs (759 bytes/sec)
R-Alumnos#
```

**Figura 45.** Conexión al servidor FTP desde el router R-Alumnos para crear copia de seguridad.

```
root@debian-gns3:/home/admin-ftp-server# ls
backup_cfg_R_alumnos_16_Dec_2021
root@debian-gns3:/home/admin-ftp-server# _
```

**Figura 46.** Copia de seguridad del router R-Alumnos en el servidor FTP.

```
root@debian-gns3:~# ftp 172.16.17.10
Connected to 172.16.17.10.
220 (vsFTPD 3.0.3)
Name (172.16.17.10:root): admin-ftp-server
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/admin-ftp-server" is the current directory
ftp> lpwd
?Invalid command
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd /srv/ftp/data-network
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      102 Dec 14 01:40 test.txt
226 Directory send OK.
ftp> get test.txt
local: test.txt remote: test.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for test.txt (102 bytes).
226 Transfer complete.
102 bytes received in 0.00 secs (229.5147 kB/s)
ftp> quit
221 Goodbye.
root@debian-gns3:~# ls
README  resize_disk.sh  scripts  test  test.txt
root@debian-gns3:~# cat test.txt
Esta es una prueba del funcionamiento de FTP, este archivo puede ser descargado por los clientes FTP.
root@debian-gns3:~# _
```

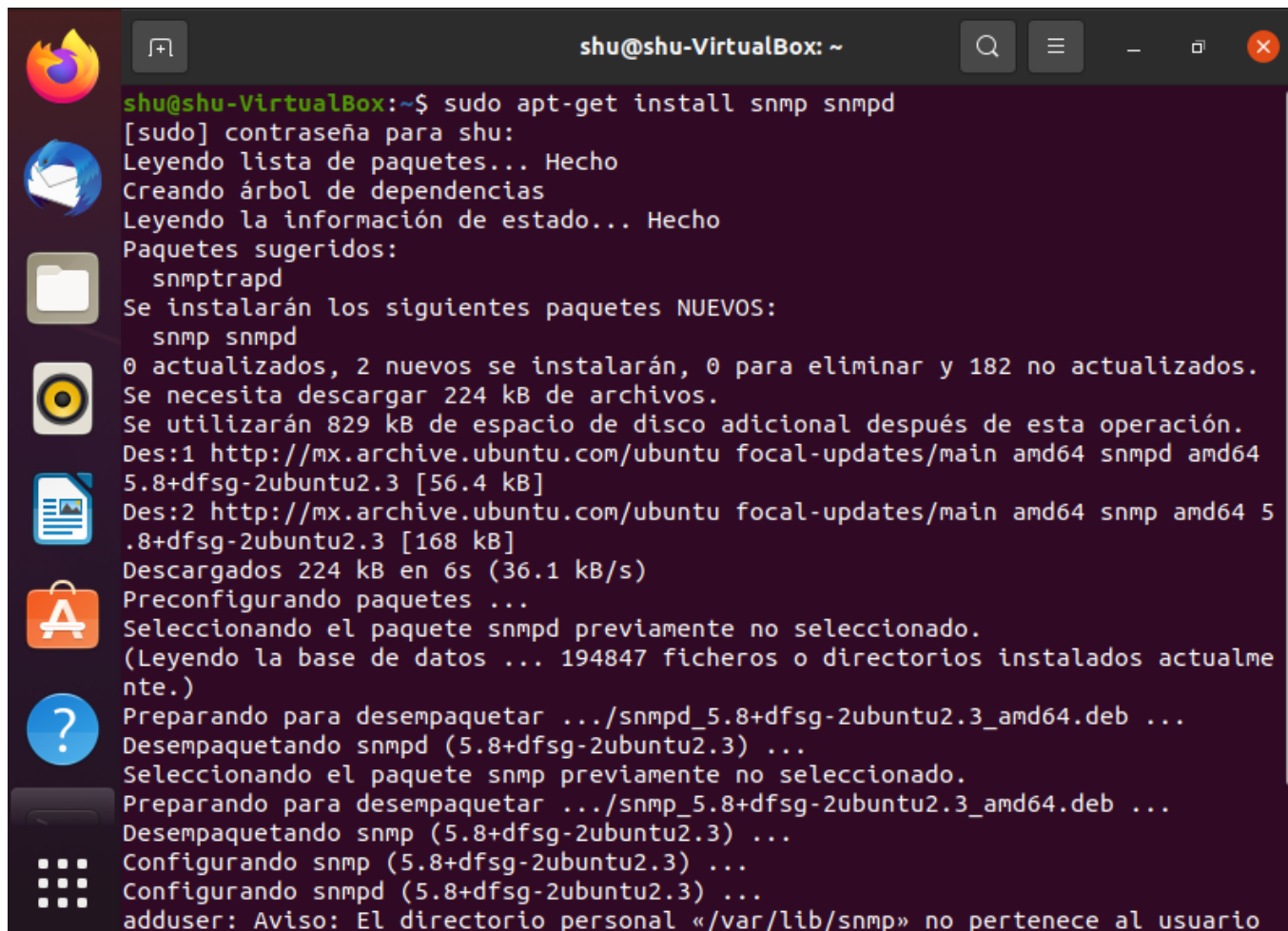
**Figura 47.** Conexión y pruebas del servidor FTP desde el servidor DHCP.

## Paso 10. Configuración servidor SNMP

### Instalación del servidor SNMP

El único paquete que se requiere en el sitio del servidor es `snmpd`, el daemon de SNMP. Para instalarlo usamos el siguiente comando:

**`sudo apt-get install snmpd`**



```
shu@shu-VirtualBox: ~  
shu@shu-VirtualBox:~$ sudo apt-get install snmp snmpd  
[sudo] contraseña para shu:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Paquetes sugeridos:  
  snmptrapd  
Se instalarán los siguientes paquetes NUEVOS:  
  snmp snmpd  
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 182 no actualizados.  
Se necesita descargar 224 kB de archivos.  
Se utilizarán 829 kB de espacio de disco adicional después de esta operación.  
Des:1 http://mx.archive.ubuntu.com/ubuntu focal-updates/main amd64 snmpd amd64  
5.8+dfsg-2ubuntu2.3 [56.4 kB]  
Des:2 http://mx.archive.ubuntu.com/ubuntu focal-updates/main amd64 snmp amd64 5  
.8+dfsg-2ubuntu2.3 [168 kB]  
Descargados 224 kB en 6s (36.1 kB/s)  
Preconfigurando paquetes ...  
Seleccionando el paquete snmpd previamente no seleccionado.  
(Leyendo la base de datos ... 194847 ficheros o directorios instalados actualme  
nte.)  
Preparando para desempaquetar .../snmpd_5.8+dfsg-2ubuntu2.3_amd64.deb ...  
Desempaquetando snmpd (5.8+dfsg-2ubuntu2.3) ...  
Seleccionando el paquete snmp previamente no seleccionado.  
Preparando para desempaquetar .../snmp_5.8+dfsg-2ubuntu2.3_amd64.deb ...  
Desempaquetando snmp (5.8+dfsg-2ubuntu2.3) ...  
Configurando snmp (5.8+dfsg-2ubuntu2.3) ...  
Configurando snmpd (5.8+dfsg-2ubuntu2.3) ...  
adduser: Aviso: El directorio personal «/var/lib/snmp» no pertenece al usuario
```

Figura 48. Instalación del servidor SNMP

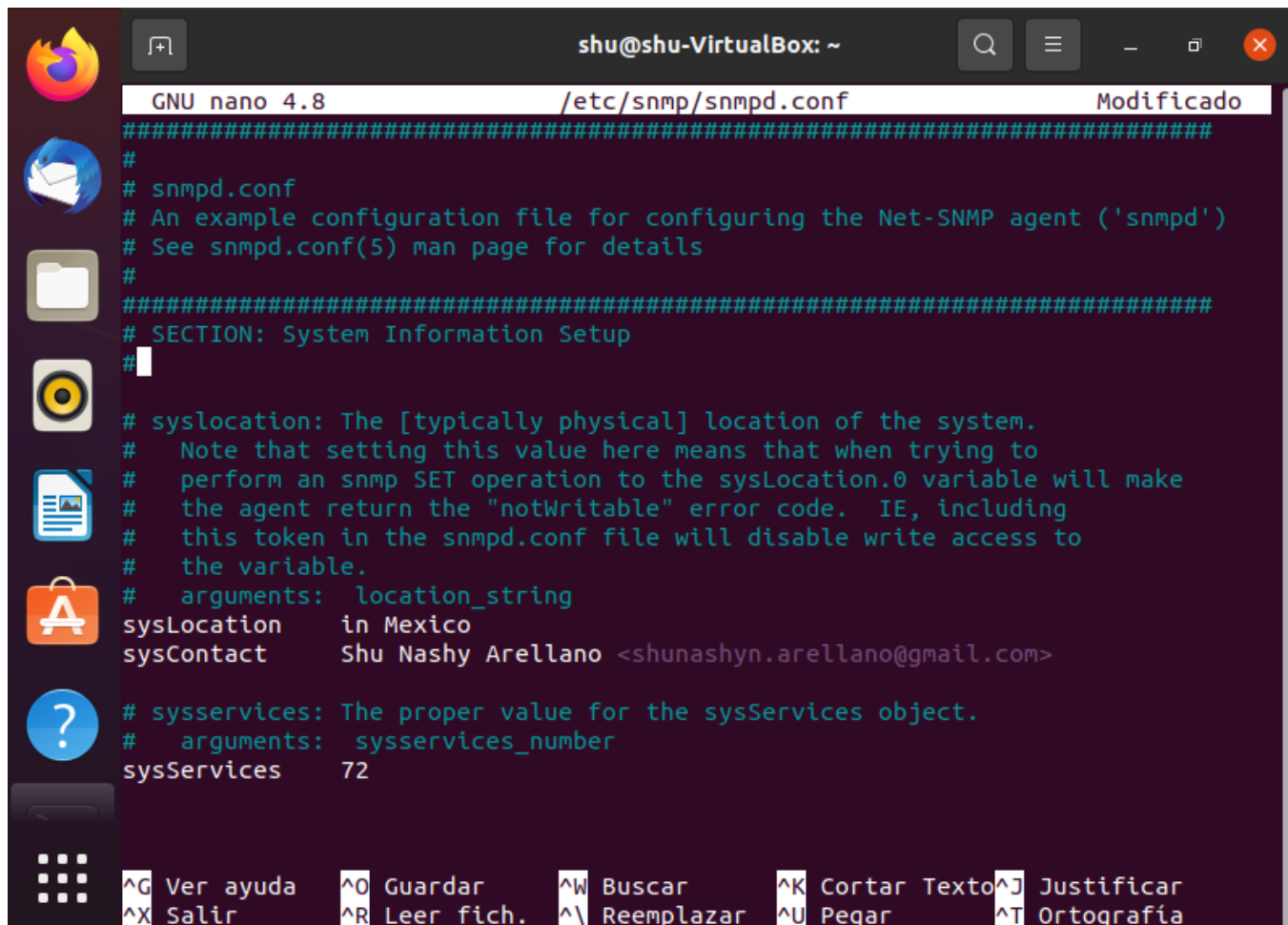
De este modo snmpd ya está instalado, pero todavía tenemos que modificarlo un poco para que funcione como queremos.

### Configuración del protocolo SNMP

Desde el servidor administrador, abra el archivo */etc/snmp/snmpd.conf* en el editor de texto con privilegios sudo.

`sudo nano /etc/snmp/snmpd.conf`





```
shu@shu-VirtualBox: ~
GNU nano 4.8 /etc/snmp/snmpd.conf Modificado
#####
#
# snmpd.conf
# An example configuration file for configuring the Net-SNMP agent ('snmpd')
# See snmpd.conf(5) man page for details
#
#####
# SECTION: System Information Setup
#
# syslocation: The [typically physical] location of the system.
# Note that setting this value here means that when trying to
# perform an snmp SET operation to the sysLocation.0 variable will make
# the agent return the "notWritable" error code. IE, including
# this token in the snmpd.conf file will disable write access to
# the variable.
# arguments: location_string
sysLocation      in Mexico
sysContact       Shu Nashy Arellano <shunashyn.arellano@gmail.com>
# syservices: The proper value for the sysServices object.
# arguments: syservices_number
sysServices      72

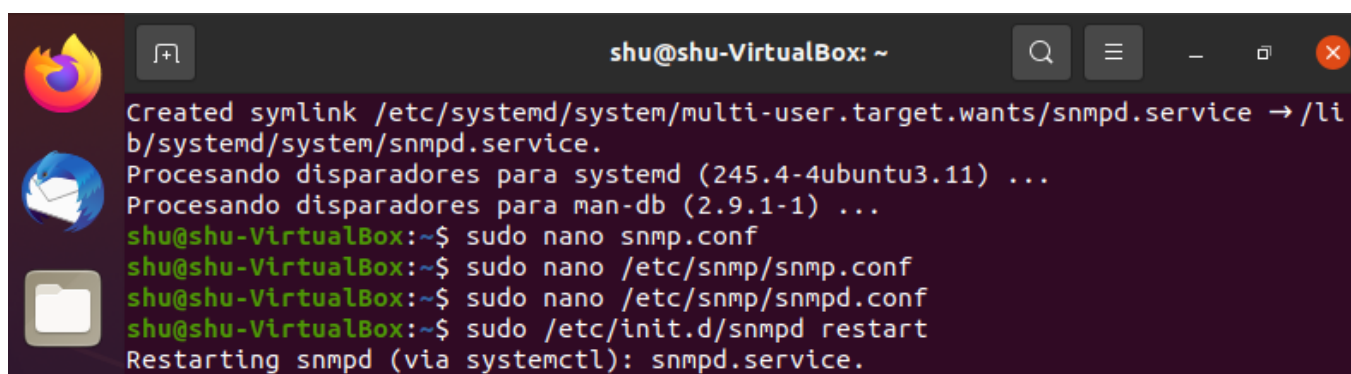
^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Texto ^J Justificar
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar        ^T Ortografía
```

Figura 49. Modificación del archivo snmpd.conf

### Reinicio del servidor

Tecleamos el siguiente comando para reiniciar el servidor:

`sudo /etc/init.d/snmpd restart`



```
shu@shu-VirtualBox: ~
Created symlink /etc/systemd/system/multi-user.target.wants/snmpd.service → /li
b/systemd/system/snmpd.service.
Procesando disparadores para systemd (245.4-4ubuntu3.11) ...
Procesando disparadores para man-db (2.9.1-1) ...
shu@shu-VirtualBox:~$ sudo nano snmp.conf
shu@shu-VirtualBox:~$ sudo nano /etc/snmp/snmp.conf
shu@shu-VirtualBox:~$ sudo nano /etc/snmp/snmpd.conf
shu@shu-VirtualBox:~$ sudo /etc/init.d/snmpd restart
Restarting snmpd (via systemctl): snmpd.service.
```

Figura 50. Reinicio del servidor SNMP

Y dentro de la ruta específica, tecleamos el siguiente comando para poder modificar el archivo de configuración de SNMP:

`sudo nano /etc/default/snmpd`

Actividades Terminal 20 de dic 14:17

shu@shu-VirtualBox: ~

```
GNU nano 4.8 /etc/default/snmpd
# This file controls the behaviour of /etc/init.d/snmpd
# but not of the corresponding systemd service file.
# If needed, create an override file in
# /etc/systemd/system/snmpd.service.d/local.conf
# see man 5 systemd.unit and man 5 systemd.service

# Don't load any MIBs by default.
# You might comment this lines once you have the MIBs downloaded.
export MIBS=

# snmpd options (use syslog priority warning, close stdin/out/err).
#SNMPDOPTS='-LSwd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux,mteTrig>
SNMPDRUN=yes

SNMPDOPTS='-LSwd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux,mteTrigg>
```

[ 16 líneas leídas ]

^G Ver ayuda	^O Guardar	^W Buscar	^K Cortar Texto	^J Justificar
^X Salir	^R Leer fich.	^\ Reemplazar	^U Pegar	^T Ortografía

Figura 51. Modificación del archivo snmpd

## Conclusiones

Todos los dispositivos inteligentes pertenecen a una red, es decir, vivimos rodeados de redes de computadoras, pero muchas veces no nos damos cuenta de la cantidad de operaciones que se están realizando simultáneamente.

En los dos cursos pasados de redes aprendimos las características que tiene una red de computadoras, cómo lograr que dos o más computadoras envíen y reciban mensajes y entender qué significan los protocolos con los que se comunican.

En esta unidad de aprendizaje estudiamos los servicios básicos que una red debe de tener y que como futuras ingenieras en sistemas computacionales debemos de conocer para poder administrarlas.

Al realizar este proyecto implementamos protocolos como SNMP, DHCP, y TFTP en la herramienta de GNS3. La parte más difícil fue trabajar con un simulador que ninguna de nosotras conocía y que causaba constantes problemas durante su uso. A pesar de este inconveniente logramos construir nuestra red y cumplir con los objetivos planteados.

## Fuentes de Consulta

Sosa, C. R. (1999). *Redes de computadoras*. IPN.

Amaya Carrión, E. W. (2018). *Redes de computadoras*. Introducción a las redes, necesidad de una red, tipo y equipos de redes, topología de una red, diseño de redes, instalación y administración de redes LAN.

[https://docs.oracle.com/cd/E56339\\_01/html/E53805/ipref-13.html#:~:text=Los%20protocolos%20de%20enrutamiento%20administran,pueden%20ejecutar%20protocolos%20de%20enrutamiento.](https://docs.oracle.com/cd/E56339_01/html/E53805/ipref-13.html#:~:text=Los%20protocolos%20de%20enrutamiento%20administran,pueden%20ejecutar%20protocolos%20de%20enrutamiento.)

*Introducción a OSPF*. (2020, 10 agosto). CCNA Desde Cero. Recuperado 8 de diciembre de 2021, de <https://ccnadesdecero.com/curso/ospf/>

Walton, A. (2018, 15 febrero). *Implementación Básica de OSPFv2 y OSPFv3*. CCNA desde Cero. Recuperado 8 de diciembre de 2021, de [https://ccnadesdecero.es/implementacion-ospf-ospfv2-ospfv3/#2\\_Open\\_Shortest\\_Path\\_First\\_OSPF](https://ccnadesdecero.es/implementacion-ospf-ospfv2-ospfv3/#2_Open_Shortest_Path_First_OSPF)

Walton, A. (2021, 22 febrero). *VLSM: Máscaras de Subred de Longitud Variable » CCNA 200-301*. CCNA desde Cero. Recuperado 8 de diciembre de 2021, de [https://ccnadesdecero.es/vlsm-mascaras-subred-longitud-variable/#4\\_VLSM](https://ccnadesdecero.es/vlsm-mascaras-subred-longitud-variable/#4_VLSM)

Walton, A. (2020, 15 enero). *¿Qué es y cómo funciona la NAT?* CCNA desde Cero. Recuperado 8 de diciembre de 2021, de [https://ccnadesdecero.es/nat-network-address-translation/#2\\_%C2%BFQue\\_es\\_NAT](https://ccnadesdecero.es/nat-network-address-translation/#2_%C2%BFQue_es_NAT)

Walton, A. (2020b, septiembre 3). *Configuración de ACL Extendidas IPv4*. CCNA desde Cero. Recuperado 8 de diciembre de 2021, de <https://ccnadesdecero.es/configurar-acl-extendidas/>

Walton, A. (2018b, febrero 15). *SNMP: Funcionamiento y Configuración*. CCNA desde Cero. Recuperado 8 de diciembre de 2021, de <https://ccnadesdecero.es/snmp-funcionamiento-configuracion/>

Walton, A. (2021b, febrero 27). ¿Qué es DNS?: Explicación sencilla. CCNA desde Cero. Recuperado 8 de diciembre de 2021, de <https://ccnadesdecero.es/que-es-dns/>

*Port Address Translation.* (s. f.). Cisco. Recuperado 12 de diciembre de 2021, de [https://www.cisco.com/assets/sol/sb/RV320\\_Emulators/RV320\\_Emulator\\_v1-1-0-09/help/Setup13.html](https://www.cisco.com/assets/sol/sb/RV320_Emulators/RV320_Emulator_v1-1-0-09/help/Setup13.html)

Walton, A. (2018a, febrero 15). *Configuración de PAT (NAT con sobrecarga)*. CCNA desde Cero. Recuperado 12 de diciembre de 2021, de <https://ccnadesdecero.es/configuracion-pat-nat-sobrecarga/>

*How To Install and configure FTP Server on Ubuntu With VSFTPD.* (2019, junio 6). Knowledge Base by PhoenixNAP. <https://phoenixnap.com/kb/install-ftp-server-on-ubuntu-vsftpd>

*How to monitor Linux servers with SNMP and Cacti.* (s. f.). Linux FAQ. <https://www.xmodulo.com/monitor-linux-servers-snmp-cacti.html>

*Habilitar SNMP Linux.* (s. f.). QQDrile. <http://qqdrile.com/wp/componentes/habilitar-snmp-linux/>

ANEXOS

Área de alumnos				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-Alumnos	S3/0	172.16.4.253	255.255.255.252	
	Fa0/0	172.16.15.254	255.255.248.0	
	Fa1/0	172.16.4.62	255.255.255.192	
	Fa2/0	172.16.4.126	255.255.255.192	
PC1	E0	172.16.8.1	255.255.248.0	172.16.15.254
PC2	E0	172.16.8.2	255.255.248.0	172.16.15.254
PC3	E0	172.16.8.3	255.255.248.0	172.16.15.254
PC4	E0	172.16.8.4	255.255.248.0	172.16.15.254
PC5	E0	172.16.4.1	255.255.255.192	172.16.4.62
PC6	E0	172.16.4.2	255.255.255.192	172.16.4.62
PC7	E0	172.16.4.3	255.255.255.192	172.16.4.62
PC8	E0	172.16.4.4	255.255.255.192	172.16.4.62
PC9	E0	172.16.4.65	255.255.255.192	172.16.4.126
PC10	E0	172.16.4.66	255.255.255.192	172.16.4.126
PC11	E0	172.16.4.67	255.255.255.192	172.16.4.126
PC12	E0	172.16.4.68	255.255.255.192	172.16.4.126
Área de Gestión Escolar y Profesores				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-ProfGest	S3/0	172.16.3.253	255.255.255.252	
	Fa2/0	172.16.3.62	255.255.255.192	
	Fa1/0	172.16.3.94	255.255.255.224	
	Fa0/0	172.16.3.110	255.255.255.240	
PC13	E0	172.16.3.1	255.255.255.192	172.16.3.62
PC14	E0	172.16.3.2	255.255.255.192	172.16.3.62
PC15	E0	172.16.3.3	255.255.255.192	172.16.3.62

PC16	E0	172.16.3.65	255.255.255.224	172.16.3.94
PC17	E0	172.16.3.66	255.255.255.224	172.16.3.94
PC18	E0	172.16.3.67	255.255.255.224	172.16.3.94
PC19	E0	172.16.3.97	255.255.255.240	172.16.3.110
PC20	E0	172.16.3.98	255.255.255.240	172.16.3.110
Área de Gobierno				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-Gobierno	S1/0	172.16.2.253	255.255.255.252	
	Fa0/0	172.16.2.62	255.255.255.192	
	Fa2/0	172.16.2.126	255.255.255.192	
	Fa4/0	172.16.2.158	255.255.255.224	
Área de Administración de Red				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-Administración	S3/0	172.16.1.254	255.255.255.252	
	S3/1	172.16.4.254	255.255.255.252	
	S3/2	172.16.3.254	255.255.255.252	
	S3/3	172.16.2.254	255.255.255.252	
	Fa0/0	172.16.17.1	255.255.255.248	
	Fa1/0	172.16.17.9	255.255.255.248	
	Fa2/0	172.16.17.17	255.255.255.248	
Server DHCP	ens3	172.16.17.2	255.255.255.248	172.16.17.1
Server TFTP	E0	172.16.17.10	255.255.255.248	172.16.17.9
Server DNS	E0	172.16.17.11	255.255.255.248	172.16.17.9
Server SNMP	E0	172.16.17.18	255.255.255.248	172.16.17.17
Server HTTP	E0	172.16.17.19	255.255.255.248	172.16.17.17
Área de internet				
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
R-Internet	S3/0	172.16.1.253	255.255.255.252	
Cloud	E6/0			

	Eth0			
	enp5...			
Servidor B.	E0			

Device	Interfaz	Dirección Ip	Máscara de Subred	Gateway
R0	S0/0/0			
	S0/0/1	172.16.1.253	255.255.255.252	
R1	S0/0/0	172.16.1.254	255.255.255.252	
	S0/0/1	172.16.2.254	255.255.255.252	
	S0/1/0	172.16.3.254	255.255.255.252	
	S0/1/1	172.16.4.254	255.255.255.252	
R2	S0/0/0	172.16.2.253	255.255.255.252	
	Gi0/0	172.16.2.62	255.255.255.192	
	Gi0/1	172.16.2.126	255.255.255.192	
	Gi0/2	172.16.2.158	255.255.255.224	
R3	S0/0/0	172.16.3.253	255.255.255.252	
	Gi0/0	172.16.3.62	255.255.255.192	
	Gi0/1	172.16.3.94	255.255.255.224	
	Gi0/2	172.16.3.110	255.255.255.240	

R4	S0/0/0	172.16.4.253	255.255.255.252	
	Gi0/0	172.16.15.254	255.255.224.0	
	Gi0/1	172.16.4.62	255.255.255.192	
	Gi0/2	172.16.4.126	255.255.255.192	
PC0	Fa0	172.16.2.1	255.255.255.192	172.16.2.62
PC1	Fa0	172.16.2.2	255.255.255.192	172.16.2.62
PC2	Fa0	172.16.2.65	255.255.255.192	172.16.2.126
PC3	Fa0	172.16.2.66	255.255.255.192	172.16.2.126
PC4	Fa0	172.16.2.129	255.255.255.224	172.16.2.158
PC5	Fa0	172.16.2.130	255.255.255.224	172.16.2.158
PC6	Fa0	172.16.3.1	255.255.255.192	172.16.3.62
PC7	Fa0	172.16.3.2	255.255.255.192	172.16.3.62
PC8	Fa0	172.16.3.3	255.255.255.192	172.16.3.62
PC9	Fa0	172.16.3.65	255.255.255.224	172.16.3.94
PC10	Fa0	172.16.3.66	255.255.255.224	172.16.3.94



PC11	Fa0	172.16.3.67	255.255.255.224	172.16.3.94
PC12	Fa0	172.16.3.97	255.255.255.240	172.16.3.110
PC13	Fa0	172.16.3.98	255.255.255.240	172.16.3.110
PC14	Fa0	172.16.3.99	255.255.255.240	172.16.3.110
PC15	Fa0	172.16.8.1	255.255.224.0	172.16.15.254
PC16	Fa0	172.16.8.2	255.255.224.0	172.16.15.254
PC17	Fa0	172.16.8.3	255.255.224.0	172.16.15.254
PC18	Fa0	172.16.8.4	255.255.224.0	172.16.15.254
PC19	Fa0	172.16.4.1	255.255.255.192	172.16.4.62
PC20	Fa0	172.16.4.2	255.255.255.192	172.16.4.62
PC21	Fa0	172.16.4.3	255.255.255.192	172.16.4.62
PC22	Fa0	172.16.4.65	255.255.255.192	172.16.4.126
PC23	Fa0	172.16.4.66	255.255.255.192	172.16.4.126