

Universidad Estatal a Distancia

Vicerrectoría Académica

Escuela De Ciencias Exactas y Naturales

Carrera de Diplomado en Ingeniería Informática

Asignatura: Telemática y redes

Código: 00883

Proyecto final

Estudiante:

Francisco Campos Sandi

114750560

Sede: San Vito

Grupo 04

Tutor: Jorge Moraga Moreno

II Cuatrimestre 2024

Contenido

Introducción.....	4
Desarrollo.....	5
Link del video con la creación de la red:	5
1. Preparación del Entorno: https://youtu.be/yBE7obzgSx8	5
Paso 1, 2 y 3:.....	5
Paso 4: Tabla de subneteo	6
Paso 5: Configuración de la topología.....	6
Paso 6:	12
Investigar la configuración de Telnet.....	12
Seguridad con Telnet	12
Realice una captura de tráfico con Wireshark.....	14
Paso 7: Configuración de VLAN.....	18
Realice pruebas de conectividad y presente en el video las	20
pruebas de conexiones.	20
Ping Pc8 a pc1 y pc23.....	20
Ping Pc28 a pc4 y pc20.....	20
Paso 8: Aplicación de comandos:	21
Conclusión	24
Referencias	25

Tabla de ilustraciones

Ilustración 1 Paso 1,2 y 3	5
Ilustración 2 Tabla de subneteo.....	6
Ilustración 3 captura de tráfico con Wireshark	14
Ilustración 4 Configuraciones	16
Ilustración 5 Prueba de ACL.....	19
Ilustración 6 Ping Pc8 a pc1 y pc23.....	20
Ilustración 7 Ping Pc28 a pc4 y pc20.....	20
Ilustración 8 encapsulation dot1Q 10.....	21
Ilustración 9 access-list 100 deny icmp.....	22
Ilustración 10 show running-config	23

Introducción

El presente documento corresponde a una tarea práctica e investigativa sobre importancia de las capas de red y transporte en las redes en el mundo de la informática es necesario poder crear comunicación entre los diferentes dispositivos, las capas de red se encargan principalmente del enrutamiento de los datos por medio de la red permitiendo que la información llegue desde su punto de origen al destino deseado entre las diferentes redes de la topología lo cual es importante al trabajar con múltiples dispositivos para poder así asegurar que la información llegue.

Desde una perspectiva objetiva, esta tarea busca proporcionar una base sólida de conocimientos sobre como configurar una topología de red sencilla, hasta una más elaborada en la cual se debe de crear con ayuda del programa GNS3 en donde se debe de instalar un dos Router y dos Switch con las imágenes sugeridas en el documento, además de poder colocar las direcciones ip a las veinte ocho pcs, y que se debe configurar el Router y los dos switches con ciertos comandos para el correcto funcionamiento en la red

La importancia de la tarea radica en su capacidad para equipar a los estudiantes con los conocimientos y habilidades para poder configurar topologías con diferentes VLANs y que la información llegue de manera precisa, en el caso de la tarea que se de verificar si hay conexiones entre los diferentes dispositivos.

En la misma se exploran los fundamentos y la terminología esencial en el ámbito de las redes de computadoras y el transporte de la información, lo cual es buen aprendizaje mediante la simulación en el software GNS3, cada ocasión se van adquiriendo más conocimientos en el mundo de las redes que son vitales para el área de la informática.

Desarrollo

Link del video con la creación de la red:

1. Preparación del Entorno: <https://youtu.be/TooVyQWjVHg>

Se realiza la construcción de la red con la guía de la tutoría por el profesor **Alejandro**

Rodríguez, se adaptan a las necesidades de la tarea (*Telemática y Redes Tutoría Virtual N°3 Alejandro Rodríguez Pérez, 2024*).

Paso 1, 2 y 3:

Se realiza la tarea en GNS3, se instalan 2 **Routers c3725** y 2 **Switchs c3745**, de acuerdo a las indicaciones del proyecto final, con la cantidad de **28 pcs** requeridas:

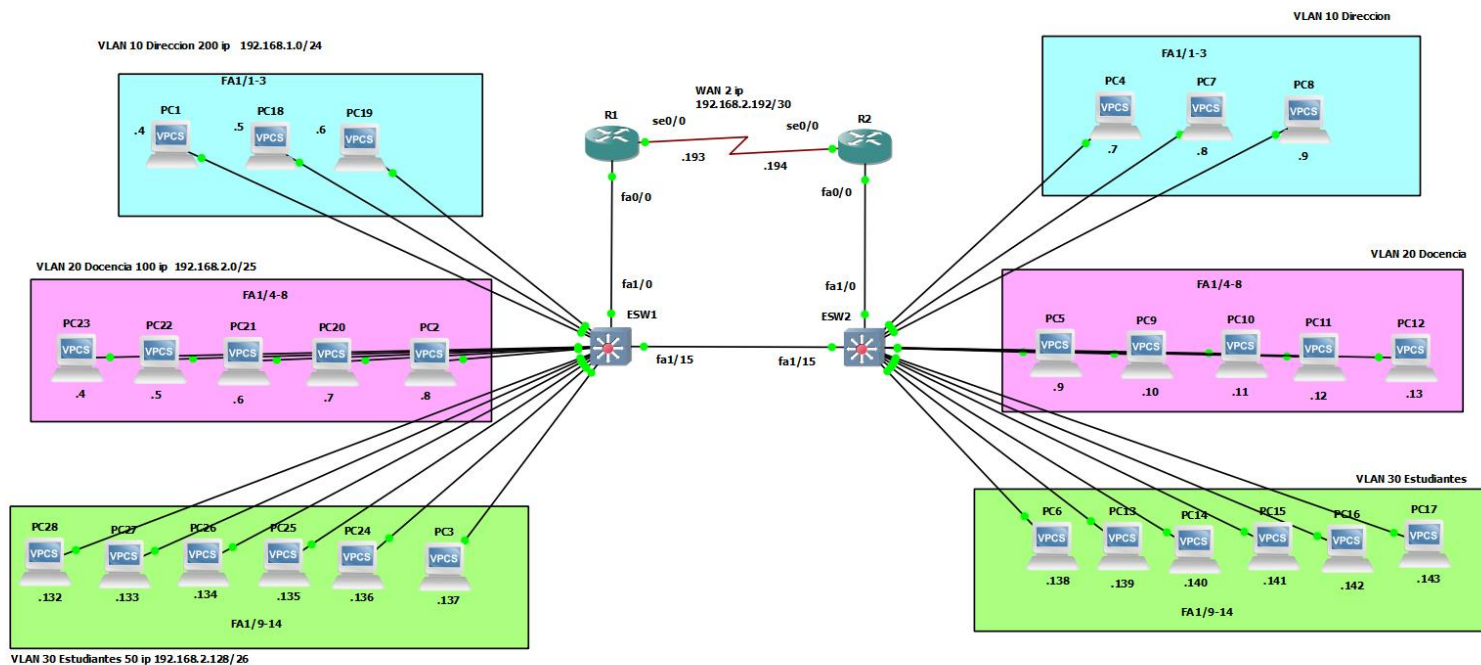


Ilustración 1 Paso 1,2 y 3

Paso 4: Tabla de subneteo

RED					
192.168.1.0					
Dirección Sub Red	Mascara de Red	PREFIJO	Dirección BroadCast	Cantidad de Host	Rango de Host
192.168.1.0	255.255.255.0	/24	192.168.1.255	200	192.168.1.1 -192.168.1.254
192.168.2.0	255.255.255.128	/25	192.168.2.127	100	192.168.2.1 -192.168.2.126
192.168.2.128	255.255.255.192	/26	192.168.2.191	50	192.168.2.129 -192.168.2.190
192.168.2.192	255.255.255.252	/30	192.168.2.195	2	192.168.2.193 -192.168.2.194

Ilustración 2 Tabla de subneteo

Paso 5: Configuración de la topología

Se realiza la configuración del Router con los siguientes comandos:

R1:

Habilitar y configurar la terminal, además de la configuración de la interfaz serial0/0. Luego, se seleccionó la interfaz serial0/0 y se activó con no shutdown.**sh vlan-s**

enable

configure terminal

interface serial0/0

ip address 192.168.2.193 255.255.255.252

no shutdown

exit

se habilita la interfaz fastethernet0/0 y se activa con no shutdown.

interface fastethernet0/0

no shutdown

exit

Configuración de las subinterfases y VLAN. Se crean subinterfases en fastethernet0/0 para diferentes VLANs. Cada subinterfaz tiene una encapsulación dot1Q y una dirección IP específica. Esta configuración es útil para segmentar la red en diferentes VLANs y permitir que el router enrute entre ellas.

```
interface fastethernet0/0.10
encapsulation dot1q 10
ip address 192.168.1.2 255.255.255.0
standby 10 ip 192.168.1.1
standby 10 priority 150
standby 10 preempt
do write
exit
```

```
interface fastethernet0/0.20
encapsulation dot1q 20
ip address 192.168.2.2 255.255.255.128
standby 20 ip 192.168.2.1
standby 20 priority 150
standby 20 preempt
do write
exit
```

```
interface fastethernet0/0.30
encapsulation dot1q 30
ip address 192.168.2.130 255.255.255.192
standby 30 ip 192.168.2.129
standby 30 priority 150
standby 30 preempt
do write
exit
```

Se verifica que todo esté correcto con 'sh running-config' muestra la configuración actual y 'sh ip int br' da un resumen rápido del estado de las interfaces IP, luego se guarda la configuración actual para que los cambios sean permanentes.

```
sh running-config
```

```
sh ip int br
```

```
Copy running-config startup-config
```

R2:

Habilitar y configurar la interfaz serial0/0. Primero, se configura la dirección IP y la máscara de subred, luego se activa la interfaz con no shutdown

```
interface serial0/0
ip address 192.168.2.194 255.255.255.252
no shutdown
exit
```

Habilitar la interfaz fastethernet0/0 y activarla con no shutdown.

```
interface fastethernet0/0
no shutdown
exit
```

Configuración de subinterfaces y VLAN. Se crean subinterfaces en fastethernet0/0 para diferentes VLANs. Cada subinterfaz tiene encapsulación dot1Q y una dirección IP específica, además de configurar el protocolo de enrutamiento de alta disponibilidad.**sh vlan-s**

```
interface fastethernet0/0.10
encapsulation dot1q 10
ip address 192.168.1.3 255.255.255.0
standby 10 ip 192.168.1.1
do write
exit
interface fastethernet0/0.20
encapsulation dot1q 20
ip address 192.168.2.3 255.255.255.128
standby 20 ip 192.168.2.1
do write
exit
interface fastethernet0/0.30
encapsulation dot1q 30
ip address 192.168.2.131 255.255.255.192
standby 30 ip 192.168.2.129
do write
exit
```


ESW1:

Configuración de VLANs se definen las VLANs con sus nombres correspondientes.

```

vlan database
vlan 10 name Direccion
vlan 20 name Docencia
vlan 30 name Estudiantes
exit

```

Se configura los puertos en el rango fastethernet1/0 a fastethernet1/15 como puertos de troncal

```

configure terminal
interface range fastethernet1/0, fastethernet1/15
switchport mode trunk
exit
do write

```

Se asigna las VLANs a puertos de acceso.

```

interface range fastethernet1/1 - 3
switchport mode access
switchport access vlan 10
exit

```

```

interface range fastethernet1/4 - 8
switchport mode access
switchport access vlan 20
exit

```

```

interface range fastethernet1/9 - 14
switchport mode access
switchport access vlan 30
exit

```

se finaliza la configuración y guardo los cambios

```

end
copy running-config startup-config

```

ESW2:

Configuración de VLANs se definen las VLANs con sus nombres correspondientes.

```
vlan database
vlan 10 name Direccion
vlan 20 name Docencia
vlan 30 name Estudiantes
exit
```

Luego, se entra en el modo de configuración global y se configuran los puertos fastethernet1/0 a fastethernet1/15 como puertos de troncal.

```
enable
configure terminal
interface range fastethernet1/0 , fastethernet1/15
switchport mode trunk
exit
do write
```

Se asigna las VLANs a puertos de acceso.

```
interface range fastethernet1/1 - 3
switchport mode access
switchport access vlan 10
exit
interface range fastethernet1/4 - 8
switchport mode access
switchport access vlan 20
exit
interface range fastethernet1/9 - 14
switchport mode access
switchport access vlan 30
exit
```

se finaliza la configuración y guardo los cambios

```
end
copy running-config startup-config
```

Configuración de todas las pcs

PC1:

ip 192.168.1.4/24 192.168.1.1

PC18:

ip 192.168.1.5/24 192.168.1.1

PC19:

ip 192.168.1.6/24 192.168.1.1

PC4:

ip 192.168.1.7/24 192.168.1.1

PC7:

ip 192.168.1.8/24 192.168.1.1

PC8:

ip 192.168.1.9/24 192.168.1.1

PC23:

ip 192.168.2.4/25 192.168.2.1

PC22:

ip 192.168.2.5/25 192.168.2.1

PC21:

ip 192.168.2.6/25 192.168.2.1

PC20:

ip 192.168.2.7/25 192.168.2.1

PC2:

ip 192.168.2.8/25 192.168.2.1

PC5:

ip 192.168.2.9/25 192.168.2.1

PC9:

ip 192.168.2.10/25 192.168.2.1

PC10:

ip 192.168.2.11/25 192.168.2.1

PC11:

ip 192.168.2.12/25 192.168.2.1

PC12:

ip 192.168.2.13/25 192.168.2.1

PC28:

ip 192.168.2.132/26 192.168.2.129

PC27:

ip 192.168.2.133/26 192.168.2.129

PC26:

ip 192.168.2.134/26 192.168.2.129

PC25:

ip 192.168.2.135/26 192.168.2.129

PC24:

ip 192.168.2.136/26 192.168.2.129

PC3:

ip 192.168.2.137/26 192.168.2.129

PC6:

ip 192.168.2.138/26 192.168.2.129

PC13:

ip 192.168.2.139/26 192.168.2.129

PC14:

ip 192.168.2.140/26 192.168.2.129

PC15:

ip 192.168.2.141/26 192.168.2.129

PC16:

ip 192.168.2.142/26 192.168.2.129

PC17:

ip 192.168.2.143/26 192.168.2.129

Paso 6: Paso 6 Telnet: El estudiante debe configurar el Protocolo de red de teletipo entre los dispositivos R1 y R2.

Investigar la configuración de Telnet

Seguridad con Telnet

Telnet es un protocolo de red que se usa para acceder a dispositivos de forma remota, pero no es seguro. Esto se debe a que transmite los datos en texto claro, lo que significa que cualquier persona que intercepte la comunicación puede leer la información sin ningún problema.

Además, Telnet no tiene cifrado, usa una autenticación débil y no garantiza que los datos no hayan sido alterados durante la transmisión. *(IBM i 7.5, 2024)*

Existen alternativas mucho más seguras que Telnet, como SSH, que cifra toda la sesión y utiliza criptografía de clave pública para la autenticación. También tenemos SSL/TLS, VPNs y Kerberos, que proporcionan conexiones seguras y cifradas. Entre estas alternativas, SSH es la más común para reemplazar Telnet, gracias a sus robustas características de seguridad, como el cifrado y la autenticación de dos factores. Con SSH, se garantiza una comunicación segura y protegida en las redes *(Singh, 2023)*

Primero, se deshabilita la búsqueda de dominio y se establece una contraseña secreta

```
no ip domain-lookup
```

```
enable secret telematica123456
```

Luego, se configura la consola para iniciar sesión y se establece una contraseña.

```
line console 0
```

```
logging synchronous
```

```
pass telematica12
```

```
login
```

```
exit
```

Se activa el servicio de cifrado de contraseñas y se establece un mensaje de banner.

```
service password-encryption
```

```
banner motd $ACCESO RESTRINGIDO$
```

```
do wr
```

Configuración TELNET:

Se configuran las líneas virtuales de terminal (vty) para permitir el acceso Telnet y se establece una contraseña.

```
line vty 0 15
```

```
transport input telnet
```

```
password tele12
```

```
login
```

```
exit
```

Se activa el servicio de cifrado de contraseñas y se guardan los cambios.

```
service password-encryption
```

```
do wr
```

Realice una captura de tráfico con Wireshark: Sobre un paquete Telnet, analice el resultado de la captura, y brinde una breve explicación del análisis que se presenta sobre la captura, especialmente sobre temas de seguridad

Si seguimos el número de paquete y filtramos el flujo de TCP con respecto a TELNET, podemos ver la contraseña del R1 en texto claro. Esto ocurre porque el protocolo TELNET tiene bajos niveles de seguridad y no encripta la contraseña ni los datos transmitidos. Esto hace que cualquier persona que pueda interceptar el tráfico de red tenga acceso directo a información sensible, como las credenciales de acceso. Por esta razón, es crucial evitar el uso de TELNET y optar por alternativas más seguras como SSH, que cifra toda la sesión y protege la información de posibles interceptaciones

The image displays a Wireshark packet capture of Telnet traffic. The packet list on the left shows several Telnet sessions. The packet details pane on the right shows the structure of a Telnet packet, including the 'User Access Verification' section where the password 'telematica123' is visible in plaintext. The packet bytes pane at the bottom shows the raw data.

No.	Source	Destination	Protocol	Length	Info
7809	192.168.2.193	192.168.2.194	TELNET	45	Telnet Data ...
3099	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=117 Ac
5603	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
6607	192.168.2.193	192.168.2.194	TELNET	45	Telnet Data ...
2021	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=118 Ac
3450	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
5449	192.168.2.193	192.168.2.194	TELNET	45	Telnet Data ...
3079	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=119 Ac
4893	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
6892	192.168.2.193	192.168.2.194	TELNET	45	Telnet Data ...
3443	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
1438	192.168.2.193	192.168.2.194	TELNET	59	Telnet Data ...
3667	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=121 Ac
1926	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
2925	192.168.2.193	192.168.2.194	TELNET	45	Telnet Data ...
5458	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=122 Ac
7468	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
8467	192.168.2.193	192.168.2.194	TELNET	45	Telnet Data ...
7356	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
9358	192.168.2.193	192.168.2.194	TELNET	45	Telnet Data ...
7801	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=124 Ac
1854	192.168.2.194	192.168.2.193	TELNET	45	Telnet Data ...
3869	192.168.2.193	192.168.2.194	TELNET	68	Telnet Data ...
7750	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=125 Ac
9477	192.168.2.194	192.168.2.193	TELNET	46	Telnet Data ...
0479	192.168.2.193	192.168.2.194	TELNET	46	Telnet Data ...
3479	192.168.2.193	192.168.2.194	TELNET	118	Telnet Data ...
7324	192.168.2.194	192.168.2.193	TCP	44	23630 → 23 [ACK] Seq=127 Ac

8 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface -, id 0

Protocol Version 4, Src: 192.168.2.193, Dst: 192.168.2.194

Control Protocol, Src Port: 23, Dst Port: 23630, Seq: 204, Ack: 125, Len: 24

Wireshark · Seguir secuencia TCP (tcp.stream eq 2) · -

.....!.....ACCESO RESTRINGIDO

User Access Verification

Password:P.....!.....telematica12

Password: telematica123

Password: tele12

R1>enn

R1>enable

Password: telematica12

Password: tele12

Password: telematica123456

R1#ennaablllee

R1#ccoonnffii

R1#configure tteerr

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#

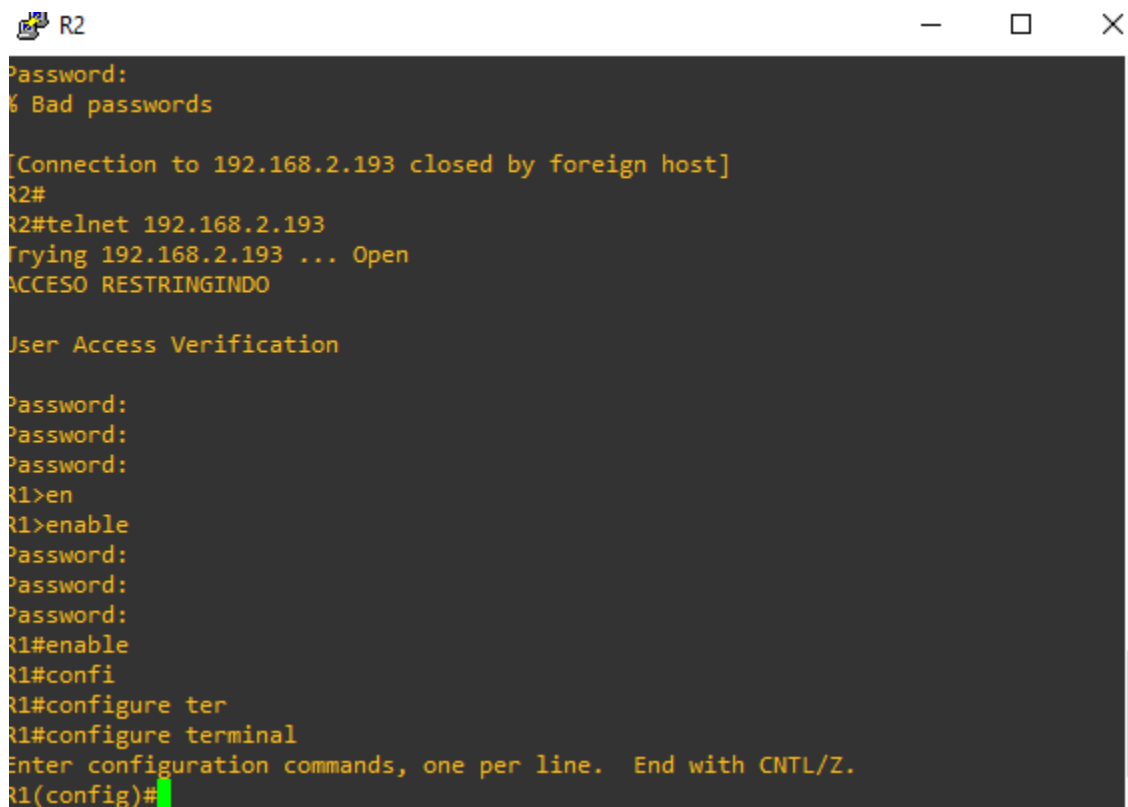
97 client pkt(s), 37 server pkt(s), 59 turn(s)

Conversación completa (429 bytes)

Mostrar datos como ASCII

Ilustración 3 captura de tráfico con Wireshark

- Posterior de configurar el protocolo Telnet, debe acceder desde R2 a R1, y realizar las siguientes configuraciones.



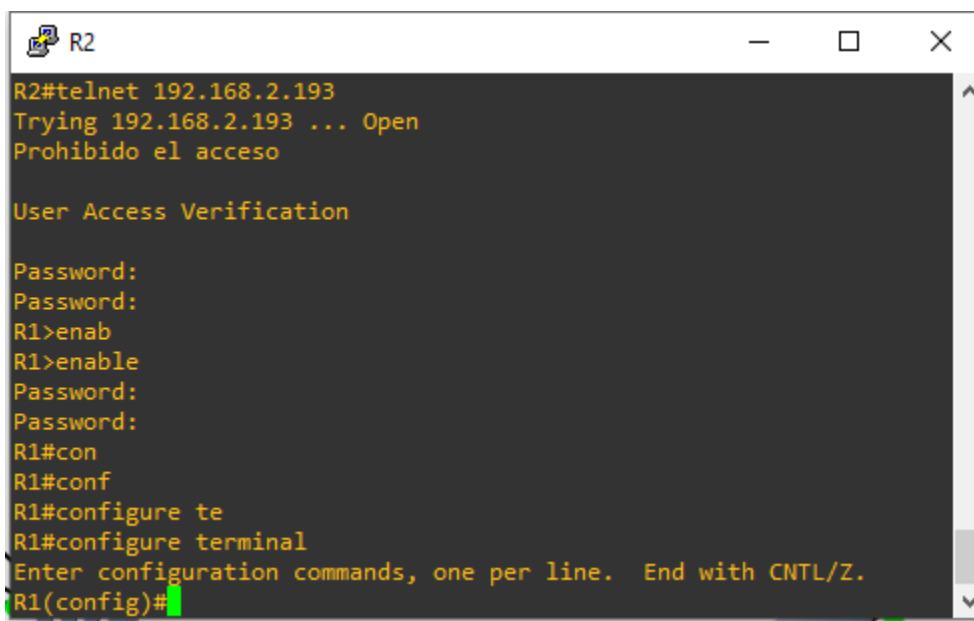
```
R2
Password:
% Bad passwords

[Connection to 192.168.2.193 closed by foreign host]
R2#
R2#telnet 192.168.2.193
Trying 192.168.2.193 ... Open
ACCESO RESTRINGIDO

User Access Verification

Password:
Password:
Password:
R1>en
R1>enable
Password:
Password:
Password:
R1#enable
R1#confi
R1#configure ter
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
```

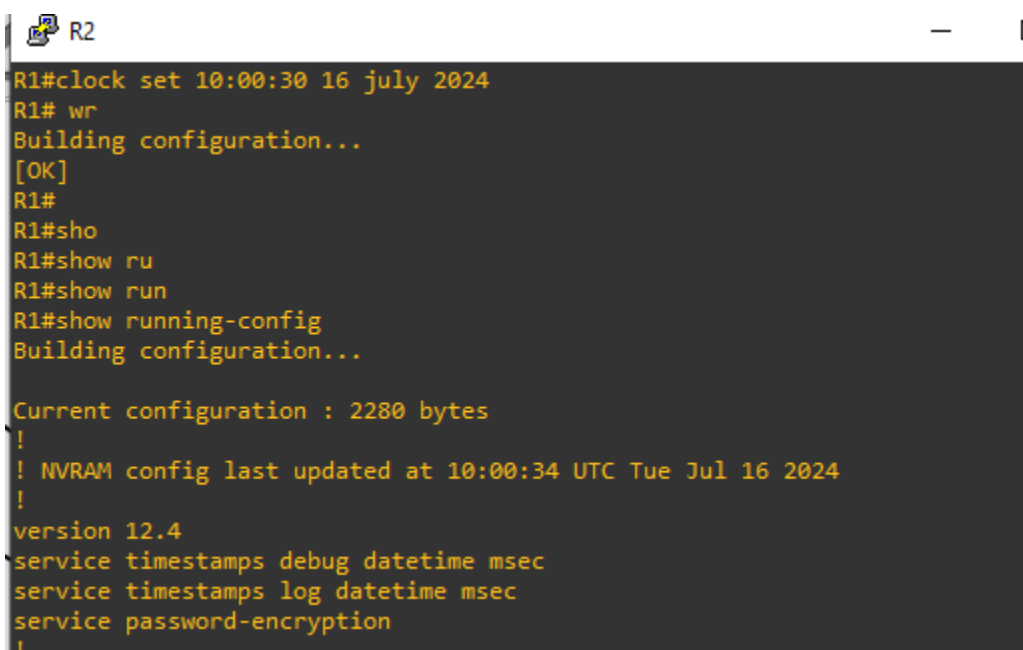
Posterior de configurar el protocolo Telnet, debe acceder desde R2 a R1, y realizar las siguientes configuraciones



```
R2
R2#telnet 192.168.2.193
Trying 192.168.2.193 ... Open
Prohibido el acceso

User Access Verification

Password:
Password:
R1>enab
R1>enable
Password:
Password:
R1#con
R1#conf
R1#configure te
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
```



```
R2
R1#clock set 10:00:30 16 july 2024
R1# wr
Building configuration...
[OK]
R1#
R1#sho
R1#show ru
R1#show run
R1#show running-config
Building configuration...

Current configuration : 2280 bytes
!
! NVRAM config last updated at 10:00:34 UTC Tue Jul 16 2024
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

Ilustración 4 Configuraciones

R2:

```
Hostname R1
no ip domain-lookup
service password-encryption
banner motd $Prohibido el acceso$
exit
clock set 10:00:30 16 july 2024
wr
```

a. Colocar un banner

El comando `banner motd $Prohibido el acceso$` se usa para configurar un Mensaje del Día (MOTD) en el router. Este mensaje aparece a todos los usuarios que se conectan al dispositivo. Es útil para advertir sobre políticas de uso o para dar información importante. Por ejemplo, se puede usar para avisar a los usuarios que el acceso está prohibido (Configurar banner en dispositivos Cisco | Configuración de mensajes en Cisco - ManageEngine Network Configuration Manager, s. f.)

b. Cambiar el nombre del host

El comando `hostname R1` cambia el nombre del dispositivo a "R1". Esto es útil para identificar el dispositivo en la red y para administración y documentación. (*Asignar nombre de host de dispositivo en switches gestionados serie 300 mediante la interfaz de línea de comandos*, s. f.)

c. Ajuste el reloj en el router a la hora y fecha de hoy

El comando `clock set 8:00:30 19 july 2024` establece la hora y fecha del reloj interno del router

d. Inhabilite la búsqueda DNS

El comando `no ip domain-lookup` deshabilita la búsqueda de nombres de dominio por parte del router. Esto evita que el router intente resolver nombres de dominio incorrectos, lo que puede retrasar la configuración y resolución de comandos erróneos. (Configuración de DNS en los routers, s. f.)

Paso 7: Configuración de VLAN

El estudiante debe configurar las VLANs correspondientes (acorde a lo

aprendido en a lo largo del curso) realizando la siguiente asignación:

- VLAN 10 = Dirección (3 host por edificio)
- VLAN 20 = Docencia (5 host por edificio)
- VLAN 30 = Estudiantes (6 host por edificio)

Configuración de VLANs se definen las VLANs con sus nombres correspondientes.

```
vlan database
```

```
vlan 10 name Direccion
```

```
vlan 20 name Docencia
```

```
vlan 30 name Estudiantes
```

```
exit
```

- a) El estudiante debe limitar la conectividad por VLAN, en donde los dispositivos asignados a una VLAN especifican, solo pueden acceder a ese segmento como tal.

R1-2: (ACL extendida numerada, que la pc1 de vlan 10 no pueda comunicarse por ICMP con la pc12 de vlan 20):

Crear una ACL extendida numerada que deniegue el tráfico ICMP entre las dos PC y permita todo el tráfico restante.

```
Access-list 100 deny icmp host 192.168.1.4 host 192.168.2.13
```

```
Access-list 100 permit ip any any
```

Aplicar la ACL a las interfaces relevantes. Primero, se aplica a la interfaz serial **se0/0**

```
Inter se0/0
```

```
Ip access-group 100 out
```

```
Exit
```

Luego, se aplica a la subinterfaz **fa0/0.20**

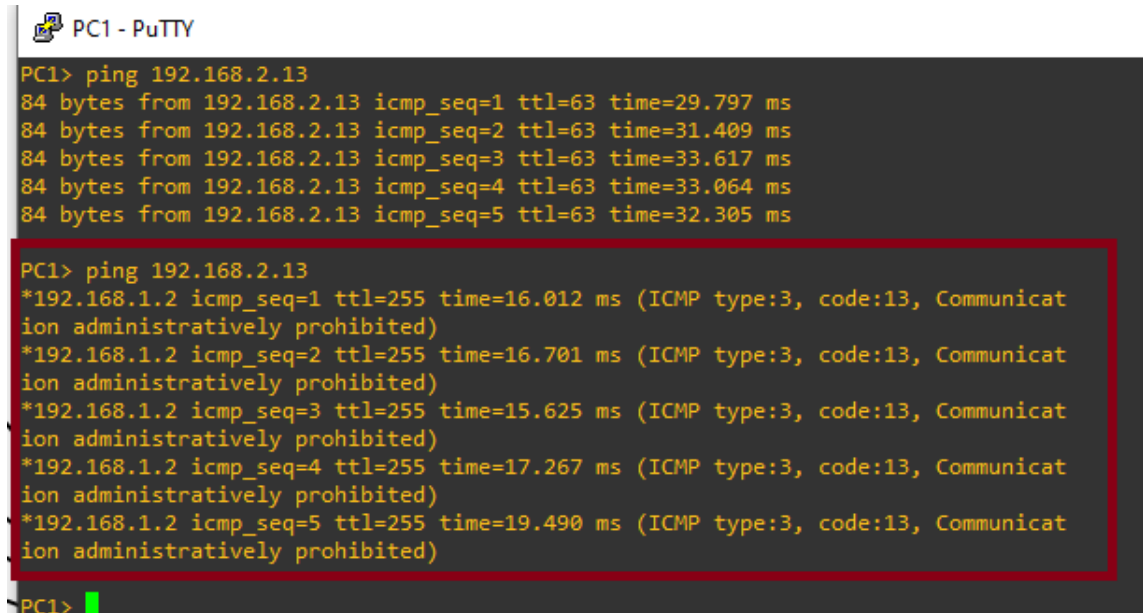
```
Inter fa0/0.20
```

```
Ip access-group 100 out
```

```
Exit
```

```
Do wr
```

Primero se realiza ping sin la configuración ACL y luego con la configuración ACL



```
PC1 - PuTTY
PC1> ping 192.168.2.13
84 bytes from 192.168.2.13 icmp_seq=1 ttl=63 time=29.797 ms
84 bytes from 192.168.2.13 icmp_seq=2 ttl=63 time=31.409 ms
84 bytes from 192.168.2.13 icmp_seq=3 ttl=63 time=33.617 ms
84 bytes from 192.168.2.13 icmp_seq=4 ttl=63 time=33.064 ms
84 bytes from 192.168.2.13 icmp_seq=5 ttl=63 time=32.305 ms

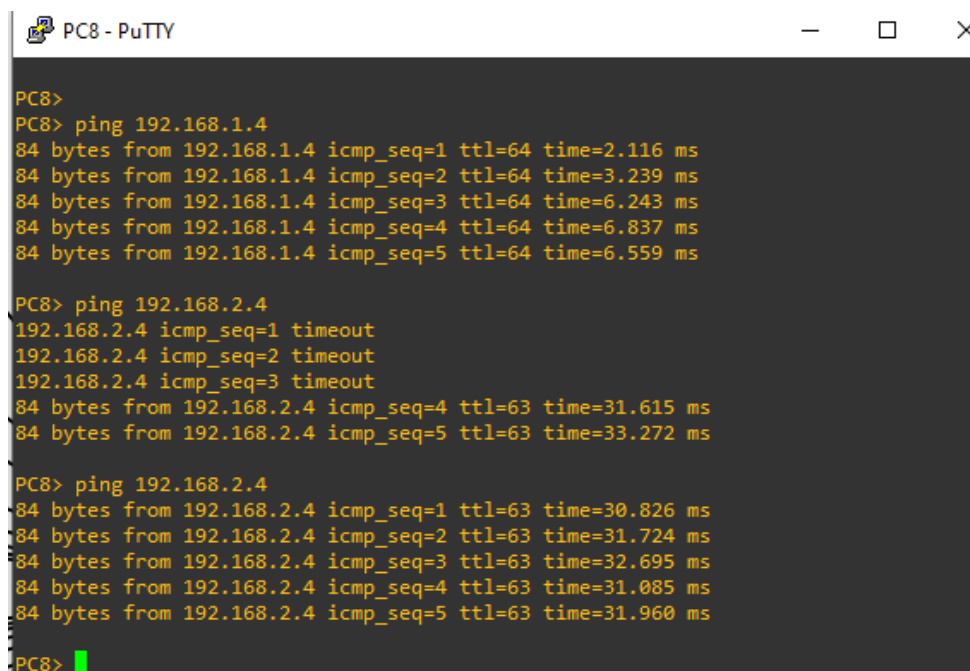
PC1> ping 192.168.2.13
*192.168.1.2 icmp_seq=1 ttl=255 time=16.012 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.2 icmp_seq=2 ttl=255 time=16.701 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.2 icmp_seq=3 ttl=255 time=15.625 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.2 icmp_seq=4 ttl=255 time=17.267 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.2 icmp_seq=5 ttl=255 time=19.490 ms (ICMP type:3, code:13, Communication administratively prohibited)

PC1>
```

Ilustración 5 Prueba de ACL

Realice pruebas de conectividad y presente en el video las pruebas de conexiones.

Ping Pc8 a pc1 y pc23



```
PC8>
PC8> ping 192.168.1.4
84 bytes from 192.168.1.4 icmp_seq=1 ttl=64 time=2.116 ms
84 bytes from 192.168.1.4 icmp_seq=2 ttl=64 time=3.239 ms
84 bytes from 192.168.1.4 icmp_seq=3 ttl=64 time=6.243 ms
84 bytes from 192.168.1.4 icmp_seq=4 ttl=64 time=6.837 ms
84 bytes from 192.168.1.4 icmp_seq=5 ttl=64 time=6.559 ms

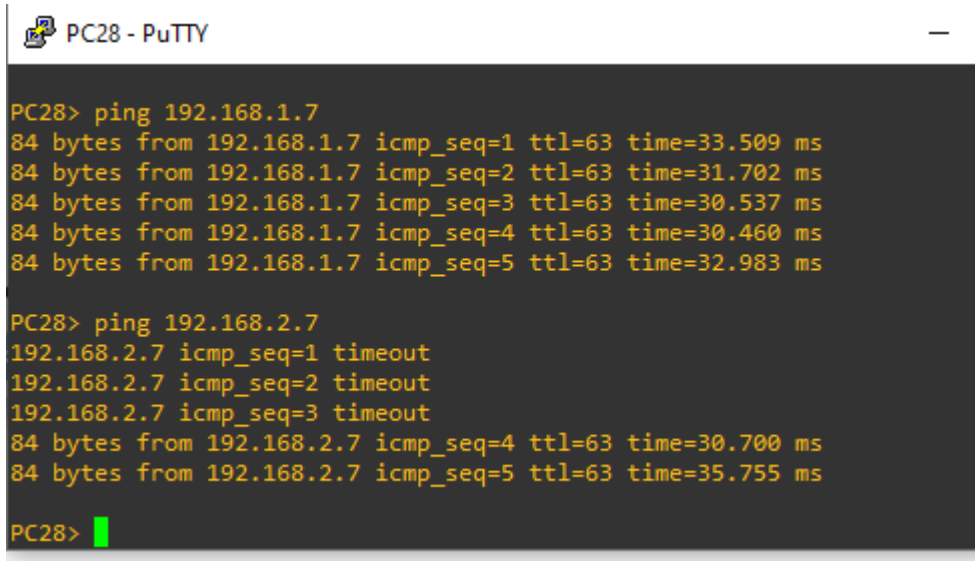
PC8> ping 192.168.2.4
192.168.2.4 icmp_seq=1 timeout
192.168.2.4 icmp_seq=2 timeout
192.168.2.4 icmp_seq=3 timeout
84 bytes from 192.168.2.4 icmp_seq=4 ttl=63 time=31.615 ms
84 bytes from 192.168.2.4 icmp_seq=5 ttl=63 time=33.272 ms

PC8> ping 192.168.2.4
84 bytes from 192.168.2.4 icmp_seq=1 ttl=63 time=30.826 ms
84 bytes from 192.168.2.4 icmp_seq=2 ttl=63 time=31.724 ms
84 bytes from 192.168.2.4 icmp_seq=3 ttl=63 time=32.695 ms
84 bytes from 192.168.2.4 icmp_seq=4 ttl=63 time=31.085 ms
84 bytes from 192.168.2.4 icmp_seq=5 ttl=63 time=31.960 ms

PC8> 
```

Ilustración 6 Ping Pc8 a pc1 y pc23

Ping Pc28 a pc4 y pc20



```
PC28> ping 192.168.1.7
84 bytes from 192.168.1.7 icmp_seq=1 ttl=63 time=33.509 ms
84 bytes from 192.168.1.7 icmp_seq=2 ttl=63 time=31.702 ms
84 bytes from 192.168.1.7 icmp_seq=3 ttl=63 time=30.537 ms
84 bytes from 192.168.1.7 icmp_seq=4 ttl=63 time=30.460 ms
84 bytes from 192.168.1.7 icmp_seq=5 ttl=63 time=32.983 ms

PC28> ping 192.168.2.7
192.168.2.7 icmp_seq=1 timeout
192.168.2.7 icmp_seq=2 timeout
192.168.2.7 icmp_seq=3 timeout
84 bytes from 192.168.2.7 icmp_seq=4 ttl=63 time=30.700 ms
84 bytes from 192.168.2.7 icmp_seq=5 ttl=63 time=35.755 ms

PC28> 
```

Ilustración 7 Ping Pc28 a pc4 y pc20

Paso 8: Aplicación de comandos:

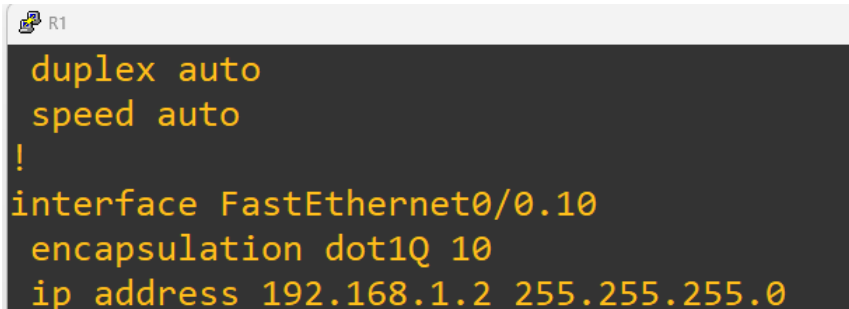
a. Investigue con cual comando se puede encriptar todas las contraseñas. (Explique en el documento).

El comando **"service password-encryption"** en un router sirve para encriptar todas las contraseñas que se configuran en el dispositivo. Esto incluye las contraseñas de acceso, de consola, de líneas vty y de enable. Aunque la encriptación no es muy fuerte, evita que las contraseñas se vean en texto claro cuando se muestra la configuración del router. Así, añade una capa extra de seguridad y hace más difícil que alguien no autorizado vea las contraseñas. («Passwords en los Routers Cisco», s. f.)

b. Desarrollo 3 comandos de captura de información (show) útiles dentro de las configuraciones realizadas. (Explique en el documento).

El comando **encapsulation dot1Q 10** se usa en un router o switch para configurar una subinterfaz con el protocolo de encapsulación 802.1Q y asignarle una VLAN específica, en este caso, la VLAN 10. Esto permite que el dispositivo maneje tráfico etiquetado para esa VLAN en particular, facilitando la segmentación y gestión del tráfico de red dentro de entornos de red que usan VLANs para separar el tráfico. Además, se asigna la dirección IP **192.168.1.2** con una máscara de subred **255.255.255.0** a esta subinterfaz utilizando el comando **ip address 192.168.1.2 255.255.255.0**, lo que permite la comunicación en la subred 192.168.1.0/24. (► *Configuración de VLAN [Comandos]* » CCNA desde Cero, s. f.)

El



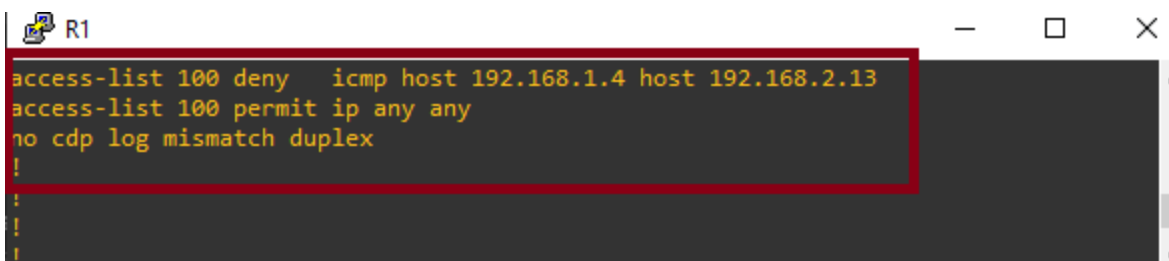
comando

```
R1
duplex auto
speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.2 255.255.255.0
```

Ilustración 8 encapsulation dot1Q 10

access-list 100 deny icmp se usa para crear una lista de control de acceso (ACL) numerada, específicamente la número 100, que bloquea todo el tráfico ICMP (como los mensajes de ping) que pasa por el router o switch donde se configura. Al añadir esta línea a una ACL, se impide que cualquier paquete ICMP sea permitido a través de esa lista de acceso, lo cual puede ser útil para limitar ciertas actividades de diagnóstico de red o ataques basados en ICMP. (Walton, 2020)

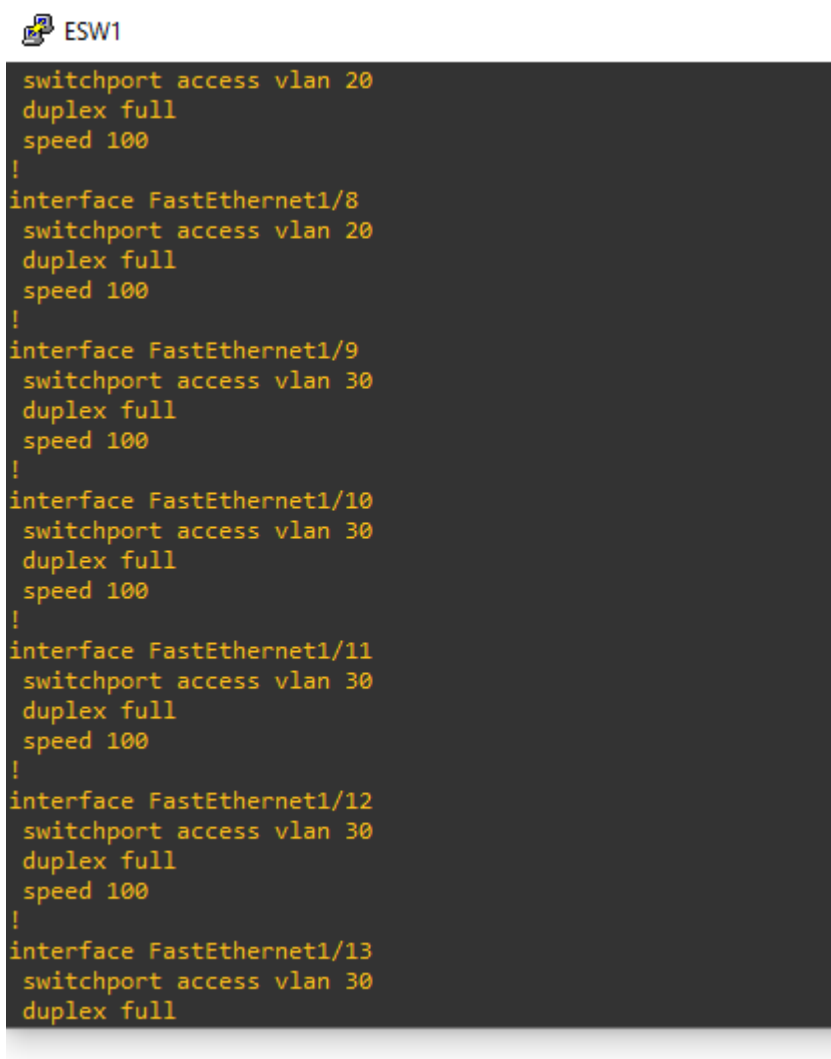
El comando (`access-list 100 deny icmp host 192.168.1.4 host 192.168.2.13`) bloquea todo el tráfico ICMP (como el tráfico de ping) entre el host con dirección IP 192.168.1.4 y el host con dirección IP 192.168.2.13. La segunda entrada (`access-list 100 permit ip any any`) permite todo el tráfico IP entre cualquier origen y cualquier destino.

A screenshot of a network configuration window titled 'R1'. The window contains a list of configuration commands in a monospaced font. The first two lines are highlighted with a red rectangular box. The commands are: 'access-list 100 deny icmp host 192.168.1.4 host 192.168.2.13' and 'access-list 100 permit ip any any'. Below these, there are two more lines: 'no cdp log mismatch duplex' and a single exclamation mark '!' on the next line. The window has standard OS controls (minimize, maximize, close) in the top right corner.

```
access-list 100 deny icmp host 192.168.1.4 host 192.168.2.13
access-list 100 permit ip any any
no cdp log mismatch duplex
!
```

Ilustración 9 access-list 100 deny icmp

La configuración que se muestra con el comando **show running-config** en el switch establece parámetros específicos para las interfaces FastEthernet1/9 a FastEthernet1/14. Cada una de estas interfaces está asignada a la VLAN 30 usando el comando `switchport access vlan 30`, lo que ayuda a segmentar el tráfico de red y a mejorar la administración y seguridad. Además, las interfaces están configuradas en modo dúplex completo (`duplex full`), lo que permite transmitir y recibir datos al mismo tiempo, mejorando el rendimiento en comparación con el modo medio dúplex. También, la velocidad de cada interfaz está fijada en 100 Mbps (`speed 100`), asegurando una transmisión de datos adecuada para las necesidades de la red. (Aprende Redes.com » Comandos Show, s. f.)



```
ESW1
switchport access vlan 20
duplex full
speed 100
!
interface FastEthernet1/8
switchport access vlan 20
duplex full
speed 100
!
interface FastEthernet1/9
switchport access vlan 30
duplex full
speed 100
!
interface FastEthernet1/10
switchport access vlan 30
duplex full
speed 100
!
interface FastEthernet1/11
switchport access vlan 30
duplex full
speed 100
!
interface FastEthernet1/12
switchport access vlan 30
duplex full
speed 100
!
interface FastEthernet1/13
switchport access vlan 30
duplex full
```

Ilustración 10 show running-config

Conclusión

En conclusión, la elaboración de esta tarea ha permitido una comprensión profunda de los conceptos fundamentales y la terminología esenciales al trabajar con redes y las capas de enlace de la importancia que tiene al transmitir información entre dispositivos al lograr realizar las conexiones necesarias, además mediante la configuración práctica de enrutamiento inter-VLAN utilizando Router y switches, se logra adquirir estos conceptos teóricos los cuales se transforman en soluciones prácticas que mejoran la eficiencia, seguridad y rendimiento de las redes.

Por otro lado, se ha adquirido un entendimiento claro de como poder configurar la instalación de Routers, switches, y PCs y poder crear una topología con un perfecto funcionamiento para poder transmitir la información entre los mismos, implementando comandos esenciales desde la terminal de GNS3.

Además, se destaca la importancia de poder entender los conceptos en términos la configuración adecuada de enrutamiento inter-VLAN, ACL, para poder lograr la comunicación entre los diferentes tipos de dispositivos en edificios distintos y que existen entre las VLANs creadas, lo cual podemos verificar al realizar las pruebas mediante los pings, lo cual es una manera segura de poder verificar que las configuraciones de los dispositivos están bien, además de poder restringir ciertos dispositivos.

El trabajo ha permitido poder comprender y aplicar los conceptos de las diferentes capas de red y transporte de información en entornos de simulación con el programa GNS3, lo cual hace un acercamiento a lo que se debe de realizar en la práctica en entornos reales, y así poder conocer un poco los conceptos de las redes.

Referencias

▷ *Configuración de VLAN [Comandos] » CCNA desde Cero*. (s. f.). Recuperado 30 de julio de 2024, de <https://ccnadesdecero.es/configuracion-vlan/>

Aprende Redes.com » Comandos Show. (s. f.). Recuperado 30 de julio de 2024, de <https://aprenderedes.com/2019/08/comandos-show/>

Asignar nombre de host de dispositivo en switches gestionados serie 300 mediante la interfaz de línea de comandos. (s. f.). Cisco. Recuperado 30 de julio de 2024, de https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb1388-assign-device-host-name-on-300-series-managed-switches-using.html

Configuración de DNS en los routers. (s. f.). Cisco. Recuperado 30 de julio de 2024, de https://www.cisco.com/c/es_mx/support/docs/ip/domain-name-system-dns/24182-reversedns.html

Configurar banner en dispositivos Cisco | Configuración de mensajes en Cisco—ManageEngine Network Configuration Manager. (s. f.). Recuperado 30 de julio de 2024, de <https://www.manageengine.com/latam/network-configuration-manager/configuracion-banner-dispositivos-cisco.html>

IBM i 7.5. (2024, mayo 7). <https://www.ibm.com/docs/es/i/7.5?topic=server-telnet-security>

Passwords en los Routers Cisco. (s. f.). *Seguridad y Redes*. Recuperado 30 de julio de 2024, de <https://delfirosales.blogspot.com/2014/04/passwords-en-los-routers-cisco.html>

Singh, N. (2023, abril 17). *SSH vs. Telnet: La opción más segura para el acceso remoto [2024]* | *Geekflare*. Geekflare Spain. <https://geekflare.com/es/ssh-vs-telnet-for-remote-access/>

Telemática y Redes Tutoría Virtual N°3 Alejandro Rodríguez Pérez. (2024, julio 6). [Video recording]. <https://www.youtube.com/watch?v=n3m7s8jvoIM>

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