Universidad Estatal a Distancia

Vicerrectoría Académica

Escuela De Ciencias Exactas y Naturales

Carrera de Diplomado en Ingeniería Informática

Asignatura: Telemática y redes

Código: 00883

Tarea #3

Estudiante:

Francisco Campos Sandi

114750560

Sede: San Vito

Grupo 04

Tutor: Jorge Moraga Moreno

II Cuatrimestre 2024

Contenido

ntrodu	cción	4		
Desarrollo5				
ink del video con la creación de la red:5				
1. F	Preparación del Entorno:	5		
Paso	o 1 y 2:	5		
Paso	3: Crear un nuevo proyecto en GNS3	6		
Paso	4: Configure el Router los Switchs:	6		
Paso	5:1	1		
Paso	o 6:	2		
Expli	ique los siguientes comandos:1	5		
Int	erface fa0/0.#1	5		
En	capsulation dot1Q1	5		
Sw	vitchport mode trunk1	5		
Sw	vitchport mode access1	5		
Paso	719	5		
En	el router: Show running-config1	6		
En el swicth: Show Vlan-Switch1				
ΟŚ	Cuáles pings fueron exitosos?1	9		
۵ś	De cuál destino a cuál final?1	9		
La	principal razón de estos pings exitosos2	0		
Paso 8: Facilite los scripts21				
Conclusión22				
Refere	Referencias23			

Tabla de ilustraciones

Ilustración 1 Paso 1 y 2	5
Ilustración 2 TOPOLOGÍA DE RED TAREA 3	6
Ilustración 3 ping de la PC1 a las demás pcs	.13
Ilustración 4 ping de la PC5 a las demás pcs	.14
Ilustración 5 router: Show running-config	.17
Ilustración 6 Show Vlan-Switch 1	.18
Ilustración 7 Show Vlan-Switch 2	19

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 en la cual se debe de crear con ayuda del programa GNS3 en donde se debe de instalar un Rauter y dos Switch con las imágenes sugeridas en el documento, además de poder colocar las direcciones ip a las seis pcs, y que se debe configurar el Router y los dos switchs 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

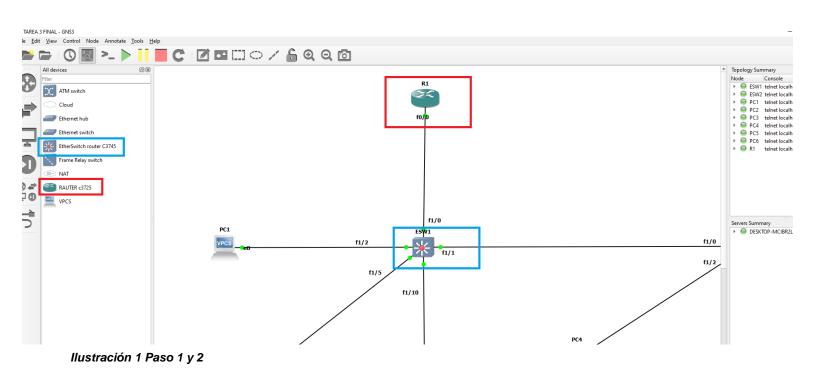
Link del video con la creación de la red:

1. Preparación del Entorno: https://youtu.be/LHGbwwg1Z9k

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 y 2:

Se realiza la tarea en GNS3, se instalan Router c3725 y Switch c3745, de acuerdo a las indicaciones de la tarea 3:



TOPOLOGÍA DE RED TAREA 3

R1

10.0

10.0

10.0

11/0

10.0

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

11/10

SISTEMAS Vlan 10 10.0.10.2.254/24

> OPERACIONES Vlan 20 10.0.20.1.254/24

Paso 3: Crear un nuevo proyecto en GNS3

Ilustración 2 TOPOLOGÍA DE RED TAREA 3

Paso 4: Configure el Router los Switchs:

Se realiza la configuración del Router con los siguientes comandos:

R1:

Estos comandos ayudan a ver cómo está configurado el dispositivo antes de iniciar.

sh vlan-s

sh ip int brief

Habilitar y configurar la terminal, además de la configuración de la Interfaz fa0/, luego se seleccionó la interfaz FastEthernet 0/0 y la activo con 'no shut'

enable

configure terminal

Interface fa0/0

No shutdown

Configuración de las subinterfaces y VLAN, se Crean subinterfaces en fa0/0 para diferentes VLANs, Cada subinterfaz tiene una encapsulación dot1Q y una dirección IP específica, es útil para segmentar la red en diferentes VLANs y permitir que el Router enrute entre ellas.

interface fa0/0.10
encapsulation dot1Q 10
ip address 10.0.10.1 255.255.255.0
no shut
exit
interface fa0/0.20
encapsulation dot1Q 20
ip address 10.0.20.1 255.255.255.0
No shut
exit
interface fa0/0.30
encapsulation dot1Q 30
ip address 10.0.30.1 255.255.255.0
no shut
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

ESW1:

Se verifica la configuración actual del switch y las VLANs configuradas antes de hacer cambios.

```
sh running-config
sh vlan-s
```

Habilitar y configurar las VLAN, se crean las VLANs 10, 20 y 30 y se les asignan sus respectivos nombres.

```
Enable
vlan database
vlan 10 name Sistemas
vlan 20 name Operaciones
vlan 30 name Gerencia
exit
```

Se verifica nuevamente las VLANs para asegurarme de que se crearon correctamente.

```
sh vlan-s
```

Luego la configuración del Modo Trunk, así se configura el rango de interfaces fa1/0 - 1 como trunk para permitir el tráfico de todas las VLANs.

```
enable
configure terminal
interface range fa1/0 - 1
switchport mode trunk
no shut
exit
```

Luego se configura los diferentes rangos de interfaces como access y se les asigna a las VLANs creadas previamente.

Asigno interfaces fa1/2 - 4 a la VLAN 10

```
interface range fa1/2 - 4
switchport mode access
switchport access vlan 10
no shut
exit
```

Asigno interfaces fa1/5 - 9 a la VLAN 20.

```
interface range fa1/5 - 9
switchport mode access
switchport access vlan 20
no shut
exit
```

Asigno interfaces fa1/10 - 15 a la VLAN 30.

```
interface range fa1/10 - 15
switchport mode access
switchport access vlan 30
no shut
exit
```

se finaliza la configuración y guardo los cambios

end

copy running-config startup-config

ESW2:

Se verifica la configuración actual del switch y las VLANs configuradas antes de hacer cambios.

```
sh running-config
sh vlan-s
```

Habilitar y configurar las VLAN, se crean las VLANs 10, 20 y 30 y se les asignan sus respectivos nombres.

```
enable
vlan database
vlan 10 name Sistemas
vlan 20 name Operaciones
vlan 30 name Gerencia
exit
```

Se verifica nuevamente las VLANs para asegurarme de que se crearon correctamente.

```
sh vlan-s
```

Luego la configuración del Modo Trunk, así se configura el rango de interfaces fa1/0 - 1 como trunk para permitir el tráfico de todas las VLANs.

```
enable

configure terminal

interface range fa1/0 - 1

switchport mode trunk

no shut

exit
```

Luego se configura los diferentes rangos de interfaces como access y se les asigna a las VLANs creadas previamente.

Asigno interfaces fa1/2 - 4 a la VLAN 10

```
interface range fa1/2 - 4
switchport mode access
switchport access vlan 10
no shut
exit
```

Asigno interfaces fa1/5 - 9 a la VLAN 20.

```
interface range fa1/5 - 9
switchport mode access
switchport access vlan 20
no shut
exit
```

Asigno interfaces fa1/10 - 15 a la VLAN 30.

```
interface range fa1/10 - 15
switchport mode access
switchport access vlan 30
exit
```

se finaliza la configuración y guardo los cambios

end
copy running-config startup-config

Paso 5: Configurar los hosts bajo la siguiente referencia, de acuerdo a las indicaciones de la tabla 2 de la tarea se procede a las configuraciones de las direcciones IP de cada pc con una máscara de subred /24 y establezco la puerta de enlace predeterminada.

Host	Configuración		
	IP	Mascara	Gateway
PC1	10.0.10.2	255.255.255.0	10.0.10.1
PC2	10.0.20.2	255.255.255.0	10.0.20.1
PC3	10.0.30.2	255.255.255.0	10.0.30.1
PC4	10.0.10.254	255.255.255.0	10.0.10.1
PC5	10.0.20.254	255.255.255.0	10.0.20.1
PC6	10.0.30.254	255.255.255.0	10.0.30.1

Tabla 2 Direccionamiento Host

PC1:	PC4:
ip 10.0.10.2/24 10.0.10.1	ip 10.0.10.254/24 10.0.10.1
save	save
PC2:	PC5:
ip 10.0.20.2/24 10.0.20.1	ip 10.0.20.254/24 10.0.20.1
save	save
PC3:	PC6:
ip 10.0.30.2/24 10.0.30.1	ip 10.0.30.254/24 10.0.30.1, Save

save

Paso 6: Realice pruebas para ver si se puede acceder al dispositivo a través de la red. Dicho en otras palabras, realice un ping desde cada una de las PCs a las otras 5 disponibles.

Se realiza ping de la PC1 a las demás pcs


```
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
PC1> ip 10.0.10.2/24 10.0.10.1
Checking for duplicate address...
PC1 : 10.0.10.2 255.255.255.0 gateway 10.0.10.1
PC1> save
Saving startup configuration to startup.vpc
PC1> ping 10.0.10.2

10.0.10.2 icmp_seq=1 ttl=64 time=0.001 ms

10.0.10.2 icmp_seq=2 ttl=64 time=0.001 ms

10.0.10.2 icmp_seq=3 ttl=64 time=0.001 ms

10.0.10.2 icmp_seq=4 ttl=64 time=0.001 ms

10.0.10.2 icmp_seq=5 ttl=64 time=0.001 ms
PC1> ping 10.0.20.2
10.0.20.2 icmp_seq=1 timeout
84 bytes from 10.0.20.2 icmp_seq=2 ttl=63 time=30.659 ms
84 bytes from 10.0.20.2 icmp_seq=3 ttl=63 time=30.241 ms
84 bytes from 10.0.20.2 icmp_seq=4 ttl=63 time=30.454 ms
84 bytes from 10.0.20.2 icmp_seq=5 ttl=63 time=30.277 ms
PC1> ping 10.0.30.2
10.0.30.2 icmp_seq=1 timeout
84 bytes from 10.0.30.2 icmp_seq=2 ttl=63 time=30.739 ms
84 bytes from 10.0.30.2 icmp_seq=3 ttl=63 time=30.530 ms
84 bytes from 10.0.30.2 icmp_seq=4 ttl=63 time=30.111 ms
84 bytes from 10.0.30.2 icmp_seq=5 ttl=63 time=30.331 ms
PC1> ping 10.0.10.254
84 bytes from 10.0.10.254 icmp_seq=1 ttl=64 time=0.909 ms
84 bytes from 10.0.10.254 icmp_seq=1 ttl=64 time=1.417 ms
84 bytes from 10.0.10.254 icmp_seq=3 ttl=64 time=1.429 ms
84 bytes from 10.0.10.254 icmp_seq=4 ttl=64 time=1.559 ms
84 bytes from 10.0.10.254 icmp_seq=5 ttl=64 time=1.030 ms
PC1> ping 10.0.20.254
10.0.20.254 icmp_seq=1 timeout
84 bytes from 10.0.20.254 icmp_seq=2 ttl=63 time=29.993 ms
84 bytes from 10.0.20.254 icmp_seq=3 ttl=63 time=30.143 ms
84 bytes from 10.0.20.254 icmp_seq=4 ttl=63 time=30.444 ms
84 bytes from 10.0.20.254 icmp_seq=5 ttl=63 time=33.870 ms
PC1> ping 10.0.30.254
10.0.30.254 icmp_seq=1 timeout
84 bytes from 10.0.30.254 icmp_seq=2 ttl=63 time=30.337 ms
84 bytes from 10.0.30.254 icmp_seq=3 ttl=63 time=30.532 ms
84 bytes from 10.0.30.254 icmp_seq=4 ttl=63 time=30.292 ms
84 bytes from 10.0.30.254 icmp_seq=5 ttl=63 time=40.632 ms
```

Ilustración 3 ping de la PC1 a las demás pcs

Se realiza ping de la PC5 a las demás pcs

```
PC5 - PuTTY
 Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
PC5> ip 10.0.20.254/24 10.0.20.1
Checking for duplicate address...
PC1 : 10.0.20.254 255.255.255.0 gateway 10.0.20.1
Saving startup configuration to startup.vpc
PC5> ping 10.0.10.2
10.0.10.2 icmp_seq=1 timeout
10.0.10.2 icmp_seq=2 timeout
84 bytes from 10.0.10.2 icmp_seq=3 ttl=63 time=32.477 ms
84 bytes from 10.0.10.2 icmp_seq=5 ttl=63 time=30.786 ms
PC5> ping 10.0.20.2

84 bytes from 10.0.20.2 icmp_seq=1 ttl=64 time=3.925 ms

84 bytes from 10.0.20.2 icmp_seq=2 ttl=64 time=2.305 ms

84 bytes from 10.0.20.2 icmp_seq=3 ttl=64 time=3.868 ms

84 bytes from 10.0.20.2 icmp_seq=4 ttl=64 time=0.978 ms

84 bytes from 10.0.20.2 icmp_seq=5 ttl=64 time=1.256 ms
PC5> ping 10.0.30.2
10.0.30.2 icmp_seq=1 timeout
10.0.30.2 icmp_seq=2 timeout
84 bytes from 10.0.30.2 icmp_seq=3 ttl=63 time=30.351 ms
84 bytes from 10.0.30.2 icmp_seq=4 ttl=63 time=31.874 ms
84 bytes from 10.0.30.2 icmp_seq=5 ttl=63 time=31.919 ms
 PC5> ping 10.0.10.254
10.0.10.254 icmp_seq=1 timeout
84 bytes from 10.0.10.254 icmp_seq=2 ttl=63 time=31.551 ms
84 bytes from 10.0.10.254 icmp_seq=3 ttl=63 time=30.726 ms
84 bytes from 10.0.10.254 icmp_seq=4 ttl=63 time=32.075 ms
84 bytes from 10.0.10.254 icmp_seq=5 ttl=63 time=31.776 ms
PC5> ping 10.0.20.254
10.0.20.254 icmp_seq=1 ttl=64 time=0.001 ms
10.0.20.254 icmp_seq=1 ttl=64 time=0.001 ms
10.0.20.254 icmp_seq=3 ttl=64 time=0.001 ms
10.0.20.254 icmp_seq=3 ttl=64 time=0.001 ms
10.0.20.254 icmp_seq=4 ttl=64 time=0.001 ms
10.0.20.254 icmp_seq=5 ttl=64 time=0.001 ms
PC5> ping 10.0.30.254
10.0.30.254 icmp_seq=1 timeout
10.0.30.254 icmp_seq=2 timeout
84 bytes from 10.0.30.254 icmp_seq=3 ttl=63 time=31.031 ms
84 bytes from 10.0.30.254 icmp_seq=4 ttl=63 time=30.525 ms
84 bytes from 10.0.30.254 icmp_seq=5 ttl=63 time=31.848 ms
```

Ilustración 4 ping de la PC5 a las demás pcs

Explique los siguientes comandos:

Interface fa0/0.#

El comando **interface fa0/0.#** nos permite configurar subinterfaces en un router, lo cual es útil para crear varias interfaces lógicas dentro de una única interfaz física. En nuestro caso, en el router R1 estamos configurando subinterfaces para las VLANs 10, 20 y 30.

Luego, en la subinterfaz **fa0/0.10**, la configuramos para la **VLAN 10** usando el comando encapsulation dot1Q 10 para etiquetar el tráfico de esta VLAN. Asignamos la dirección IP 10.0.10.1 con una máscara de subred 255.255.255.0.

También, configuramos la subinterfaz **fa0/0.20** para la **VLAN 20** con encapsulation dot1Q 20 y asignamos la dirección IP 10.0.20.1.

Por último, configuramos la subinterfaz fa0/0.30 para la **VLAN 30** con encapsulation dot1Q 30 y asignamos la dirección IP 10.0.30.1. (*Your First Cisco Topology | GNS3 Documentation*, s. f.)

Encapsulation dot1Q

El comando encapsulation dot1Q es esencial porque nos permite etiquetar tráfico Ethernet con información de VLAN. Esto es crucial cuando queremos segmentar y gestionar tráfico de diferentes VLANs en un solo dispositivo de red, como un router. (Marcelo, 2019)

Switchport mode trunk

Se utiliza para configurar un puerto en modo trunk usando switchport mode trunk es importante al trabajar con redes con múltiples VLANs. Esto permite que el puerto transporte tráfico de todas las VLANs configuradas, utilizando etiquetas para identificar a qué VLAN pertenece cada trama Ethernet. Es muy útil cuando necesitamos que diferentes VLANs se comuniquen entre sí a través de switches. (3.2.2.1 Configuración de enlaces troncales IEEE 802.1Q, s. f.)

Switchport mode access

Se utiliza para configurar un puerto en modo access con **switchport mode access** restringe el tráfico a una sola VLAN específica. Esto es ideal para dispositivos finales como computadoras o impresoras, donde no necesitamos segmentar el tráfico y queremos mantener la simplicidad en la gestión de la red. Esta configuración nos ayuda a mejorar la seguridad y eficiencia de la red al asegurar que el tráfico esté correctamente etiquetado y segmentado según las necesidades de cada dispositivo y VLAN. (Alvarez, 2023)

En el caso de los switches ESW1 y ESW2, los puertos Fa1/2 a Fa1/15 están configurados en modo access

Paso 7: Responda las siguientes cuestionantes:

En el router: Show running-config

"El comando show running-config (o show run) probablemente es el comando más valioso para ayudar a determinar el estado actual de un router, ya que muestra el archivo de configuración activo que se ejecuta en la RAM" .(CCNA2_lab_3_1_4_es.pdf, s. f.)

El comando show running-config en el router nos permite ver la configuración actual del dispositivo. Así cuando ejecutamos este comando, podemos ver cómo están configuradas las subinterfaces FastEthernet0/0.10, FastEthernet0/0.20 y FastEthernet0/0.30. Cada una de estas subinterfaces usa encapsulation dot1Q para VLANs específicas (10, 20 y 30), lo que permite que diferentes segmentos de red se comuniquen a través de una sola interfaz física usando etiquetas VLAN para separar el tráfico.

Por ejemplo, en la configuración de la red:

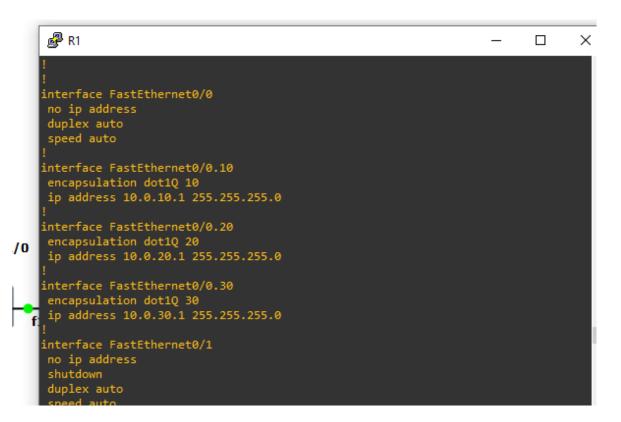
FastEthernet0/0.10: Está configurada para la VLAN 10 con encapsulation dot1Q 10. La dirección IP asignada es 10.0.10.1 con una máscara 255.255.255.0.

FastEthernet0/0.20: Está configurada para la VLAN 20 con encapsulation dot1Q 20. La dirección IP asignada es 10.0.20.1 con una máscara 255.255.255.0.

FastEthernet0/0.30: Está configurada para la VLAN 30 con encapsulation dot1Q 30. La dirección IP asignada es 10.0.30.1 con una máscara 255.255.255.0.

Esta configuración es súper importante porque permite que el router enrute el tráfico entre las diferentes VLANs y subredes. Al usar etiquetas VLAN, el router puede manejar el tráfico de manera eficiente y segura, asegurando que los datos de una VLAN no se mezclen con los de otra. Esto es crucial en redes complejas donde necesitamos segmentar el tráfico para mejorar el rendimiento y la seguridad. Además, usar una sola interfaz física para manejar múltiples

VLANs ayuda a optimizar los recursos de la red y facilita la administración(*▷ Comandos SHOW Cisco* ✓, s. f.).



En el swicth: Show Vlan-Switch

Configuración de VLANs en el Switch ESW1

Al revisar la configuración de VLANs en el switch ESW1, podemos ver la información detallada de las VLANs configuradas, incluyendo su estado y los puertos asociados a cada una. Esta configuración importante porque nos permite segmentar la red en diferentes dominios de broadcast, mejorando tanto la seguridad como el rendimiento al separar el tráfico de diferentes departamentos (Engineering, 2018).

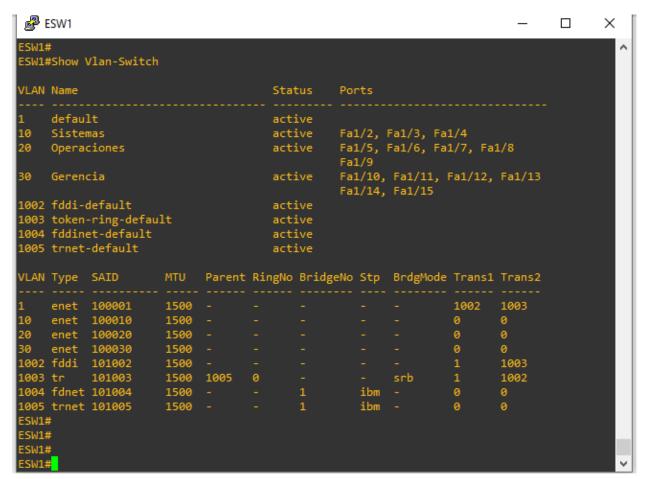


Ilustración 6 Show Vlan-Switch 1

Al revisar la configuración de VLANs en el switch ESW2, podemos observar que es similar a la del switch ESW1. La configuración muestra la información detallada de las VLANs configuradas, incluyendo su estado y los puertos asociados a cada una. Esta configuración permite segmentar la red en diferentes dominios de broadcast, mejorando tanto la seguridad como el rendimiento al separar el tráfico de diferentes departamentos (Engineering, 2018).

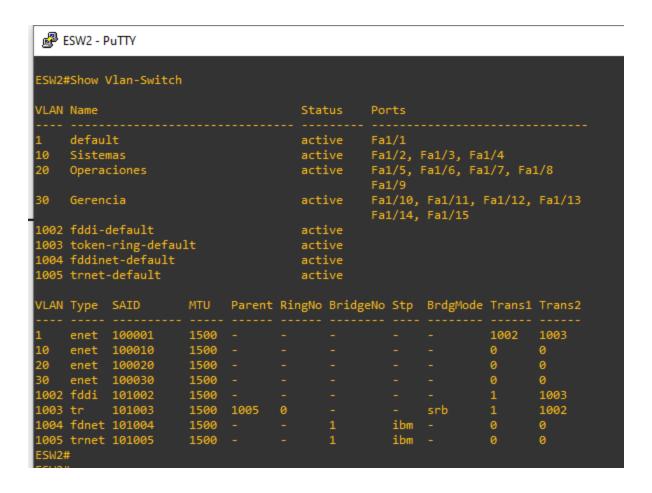


Ilustración 7 Show Vlan-Switch 2

¿Cuáles pings fueron exitosos?

Se realizaron las pruebas con los ping en todas las pcs hace las demás y en todas las pruebas fueron resultados exitosos debido a las configuraciones que se realizaron anteriormente para las comunicación entre las diferentes VLANs.

¿De cuál destino a cuál final?

La comunicación fue exitosa desde cualquier dispositivo final a cualquier otro dispositivo final, así como entre los dispositivos finales y el router. Esto significa que, independientemente de la VLAN a la que pertenecieran, los dispositivos pudieron intercambiar tráfico correctamente debido a la configuración de enrutamiento entre VLANs en el router y la segmentación adecuada en los switches.

Esta conectividad asegura que los dispositivos de todas las VLANs (Sistemas, Operaciones, Gerencia y la VLAN por defecto) puedan comunicarse entre sí y con el router, garantizando un funcionamiento fluido de la red eficiente del tráfico (Walton, 2020).

Principal Razón de los Pings Exitosos

La principal razón de estos pings exitosos

En la tarea realizada, la comunicación exitosa entre las PCs en las VLANs 10, 20 y 30 mediante pings se debe a la correcta configuración del enrutamiento inter-VLAN en el router. Esto incluye la creación de subinterfaces con etiquetado 802.1Q y la asignación de direcciones IP para cada VLAN específica. El router opera eficazmente como un router-on-a-stick, permitiendo el tráfico entre VLANs a través de una única interfaz física subdividida en subinterfaces lógicas. Los switches están configurados adecuadamente con puertos en modo trunk para mantener las etiquetas VLAN y puertos en modo access para conectar dispositivos finales a sus VLANs respectivas. Esta configuración garantiza una comunicación eficiente y segura entre diferentes segmentos de red, mejorando el rendimiento general y facilitando la gestión del tráfico. (*Ping - Definition and details*, s. f.)

Paso 8: Facilite los scripts

1.R1: Sh vlan-s Sh vlan-switch Sh ip int

brief

enable configure terminal Interface fa0/0 No shut

interface fa0/0.10 encapsulation dot1Q 10 ip address 10.0.10.1 255.255.255.0 no shut exit

interface fa0/0.20 encapsulation dot1Q 20 ip address 10.0.20.1 255.255.255.0 No shut exit

interface fa0/0.30 encapsulation dot1Q 30 ip address 10.0.30.1 255.255.255.0 no shut exit

sh runningconfig Sh ip int br running-config startup-config

2.ESW1:

Sh runningconfig Sh vlan-s

enable
vlan database
vlan 10 name
Sistemas
vlan 20 name
Operaciones
vlan 30 name
Gerencia
Exit

sh vlan-s Enable Configure terminal

interface
range fa1/0 -1
switchport
mode trunk
No shut
exit

Asignación del rango de interfaz a la vlan interface range fal/2 - 4 switchport mode access switchport access vlan 10 No shut exit

interface range fa1/5 - 9 switchport mode access switchport access vlan 20 No shut exit interface range fal/10 - 15 switchport mode access switchport access vlan 30 exit End copy runningconfig startup-config

3.ESW2:

Sh runningconfig Sh vlan-s

enable
vlan database
vlan 10 name
Sistemas
vlan 20 name
Operaciones
vlan 30 name
Gerencia
Exit

sh vlan-s Enable Configure terminal

enable
interface
fa1/0
switchport
mode trunk
No shut
exit

interface range fa1/1 - 4 switchport mode access switchport access vlan 10 No shut exit

interface range fa1/5 - 9

switchport mode access switchport access vlan 20 No shut exit

interface range fa1/10 - 15 switchport mode access switchport access vlan 30 No shut Exit end running-config startup-config

4.PC1:

ip 10.0.10.2/24 10.0.10.1 save PC2: ip 10.0.20.2/24 10.0.20.1 save PC3: ip 10.0.30.2/24 10.0.30.1 save PC4: 10.0.10.254/24 10.0.10.1 save PC5: ip 10.0.20.254/24 10.0.20.1 save PC6: ip 10.0.30.254/24

10.0.30.1

Save

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 Rauters, swicht, y pcs y poder crear una topología con un perfecto funcionamiento para poder transmitir la información entre los mismos, implementado 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 para poder lograr la comunicación entre los diferentes tipos de dispositivos 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.

El trabajado 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

- 3.2.2.1 Configuración de enlaces troncales IEEE 802.1Q. (s. f.). Recuperado 9 de julio de 2024, de https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.2.2.1/3.2.2.1.html
- Alvarez, F. (2023, marzo 23). *Configuración de Puertos en Switch Cisco*. DotBugs. https://dotbugs.com/configuracion-puertos-switch-cisco/
- CCNA2_lab_3_1_4_es.pdf. (s. f.). Recuperado 9 de julio de 2024, de http://www.utez.edu.mx/curriculas/ccna2_ES/pdf/knet-1076521137663/CCNA2_lab_3_1_4_es.pdf
- Engineering, N. (2018, julio 24). Ingeniería de redes, telecomunicaciones y ciberseguridad en Barcelona.

 Net Cloud Engineering. https://netcloudengineering.com/configuracion-vlan-cisco-switch/
- Marcelo. (2019, agosto 30). Enrutamiento Intra VLAN. *CCNA Desde Cero*. https://ccnadesdecero.com/curso/enrutamiento-intra-vlan/
- Ping—Definition and details. (s. f.). Recuperado 10 de julio de 2024, de https://www.paessler.com/es/it-explained/ping
- 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, junio 10). *▶ Configuración de VLAN [Comandos] » CCNA desde Cero*. CCNA desde Cero. https://ccnadesdecero.es/configuracion-vlan/
- Your First Cisco Topology | GNS3 Documentation. (s. f.). Recuperado 9 de julio de 2024, de https://mother.github.io/docs/getting-started/your-first-cisco-topology/