

## **Actividad | #1 | Escenario LAN**

### **Administración de Redes y Servidores.**

---

Ingeniería en Desarrollo de  
Software



**TUTOR: Marco Alonso Rodríguez Tapia**

---

**ALUMNO: Sarahi Jaqueline Gómez Juárez**

---

**FECHA: sábado, 19 de julio de 2025.**

---

## Índice

<b>Índice.....</b>	<b>2</b>
<b>Introducción .....</b>	<b>4</b>
<b>Descripción: .....</b>	<b>7</b>
<b>Justificación:.....</b>	<b>10</b>
<b>Desarrollo: .....</b>	<b>12</b>
<b>Etapla 1- Escenario LAN.....</b>	<b>12</b>
<b>Contextualización: .....</b>	<b>12</b>
<i>Ejemplo de la Estructura:.....</i>	<i>12</i>
<i>Topología Inicial - Dispositivos sin conexión.....</i>	<i>14</i>
<i>Conexiones Físicas Establecidas entre Dispositivos.....</i>	<i>15</i>
<i>Estado de puertos en Switch0 (antes de asignar VLANs): .....</i>	<i>16</i>
<i>Estado de puertos en Switch1 (antes de configurar VLANs):.....</i>	<i>18</i>
<i>Selección de interfaz GigabitEthernet0/1 en Switch1: .....</i>	<i>19</i>
<i>Segmentación por Pisos y VLANs con Enlace Troncal: .....</i>	<i>20</i>
<i>Configuración de VLANs en Switch0 (Parte I):.....</i>	<i>21</i>
<i>Verificación de VLANs en Switch0.....</i>	<i>23</i>
<i>Configuración de VLANs en Switch1:.....</i>	<i>24</i>
<i>Verificación de VLANs en Switch1:.....</i>	<i>26</i>
<i>Estado de Puertos Switch0 – VLAN 10 (Gerencia): .....</i>	<i>27</i>
<i>Red Final con Conexión Troncal y Segmentación Aplicada:.....</i>	<i>28</i>
<i>Switch1 con PC2 (Gerencia) y Trunk Activado:.....</i>	<i>29</i>
<i>Activación de Puertos VLAN Gerencia y Trunk en Switch0: .....</i>	<i>30</i>

<i>Switch1 – VLAN 20 (Operativos) Funcionando:</i> .....	31
<i>Enlace para visualizar el Archivo .pkt de Cisco en GitHub:</i> .....	31
<b>Conclusión .....</b>	<b>32</b>
<b>Referencias: .....</b>	<b>34</b>

## Introducción

En el ámbito de las redes informáticas, el diseño y la configuración adecuada de una infraestructura de comunicación son aspectos fundamentales para garantizar el rendimiento, la seguridad y la escalabilidad de los sistemas, una de las prácticas más comunes en entornos corporativos para alcanzar estos objetivos es la segmentación lógica mediante VLANs (Virtual Local Area Networks), técnica que permite dividir una red física en múltiples dominios de broadcast independientes, esto optimiza el tráfico, reduce colisiones y mejora el control de acceso.

El presente informe tiene como propósito documentar detalladamente el proceso de diseño, implementación y verificación de una red empresarial segmentada mediante VLANs, utilizando la herramienta de simulación **Cisco Packet Tracer**, a través de una secuencia de dieciséis figuras ilustrativas, se expone desde la topología inicial sin conexión hasta la configuración completa de puertos, enlaces troncales y validación final del sistema, cada figura incluye una imagen representativa, un título descriptivo y una nota técnica en estilo académico, que explica el propósito del diseño, los comandos aplicados, su función dentro de la infraestructura, así como las consecuencias derivadas de una configuración errónea u omitida.

En los entornos empresariales actuales, disponer de una red LAN (Local Area Network) bien estructurada y segmentada es crucial para garantizar la eficiencia operativa, la seguridad de la información y la capacidad de crecimiento de la infraestructura. Las redes LAN permiten conectar múltiples dispositivos dentro de una misma ubicación física como oficinas o departamentos facilitando la comunicación interna, el acceso compartido a recursos y una administración centralizada, sin embargo, a medida que la red se expande, su gestión se vuelve más compleja, haciendo indispensable la adopción de soluciones como las VLANs.

Una **VLAN** es una técnica de segmentación lógica que permite subdividir una red física en múltiples subredes independientes, sin necesidad de modificar la infraestructura física, cada VLAN opera como un dominio de broadcast separado, impidiendo que el tráfico de una VLAN sea visible por dispositivos de otras, salvo mediante dispositivos de capa 3 como routers o switches multicapa.

Las VLANs ofrecen múltiples beneficios, entre ellos:

**Aumento de la seguridad**, al aislar grupos de trabajo o departamentos.

**Reducción del tráfico de red innecesario**, limitando los dominios de broadcast.

**Mejora en la administración**, agrupando dispositivos según función, ubicación o nivel de acceso.

**Facilidad de escalabilidad**, permitiendo reorganizaciones sin alteraciones físicas.

La implementación de VLANs se realiza directamente sobre switches administrables mediante comandos específicos del sistema operativo de red (como Cisco IOS), esto permite a los administradores definir políticas de acceso, segmentar el tráfico y garantizar que cada segmento lógico funcione de forma autónoma y segura.

El proyecto aquí descrito simula un escenario empresarial realista, en el que se parte de una topología sin conexiones físicas para luego avanzar progresivamente hacia una red segmentada completamente por VLANs, se configuran enlaces troncales, se asignan puertos a VLANs específicas y se verifica el funcionamiento correcto del sistema mediante comandos especializados del sistema operativo de Cisco.

Cada etapa está documentada con análisis técnico detallado de los comandos utilizados, su propósito dentro de la arquitectura de red y el impacto de su omisión o mala configuración. Este enfoque no solo permite una comprensión práctica de los conceptos involucrados, sino que

fortalece las competencias necesarias en la administración de redes empresariales.

Finalmente, es importante destacar que la **Administración de Redes y Servidores** es una disciplina esencial dentro del campo de las tecnologías de la información, se encarga del diseño, implementación, monitoreo y mantenimiento de la infraestructura necesaria para asegurar la disponibilidad, seguridad y eficiencia de los servicios de red, entre sus funciones clave se encuentran:

Configuración y gestión de dispositivos de red (switches, routers, puntos de acceso).

Segmentación lógica mediante VLANs y políticas de control de tráfico.

Instalación y mantenimiento de servicios críticos (DNS, DHCP, servidores de archivos, correo, web).

Supervisión del rendimiento y respuesta ante incidentes.

Documentación y respaldo de configuraciones.

Una gestión adecuada de redes y servidores no solo garantiza la operatividad continua de los sistemas, sino que también protege la integridad de los datos y la continuidad del negocio.

### **Descripción:**

En el contexto de las tecnologías de la información, el diseño, la implementación y la administración de redes informáticas representan pilares fundamentales para garantizar la operatividad, seguridad y escalabilidad de los sistemas organizacionales, el documento aborda con precisión estos elementos, mediante el desarrollo de un proyecto de simulación que ejemplifica el uso de VLANs (Virtual Local Area Networks) dentro de una red empresarial segmentada, implementada y verificada en Cisco Packet Tracer.

Este informe integra conceptos teóricos y su aplicación práctica mediante una serie de configuraciones y verificaciones técnicas, el propósito principal es evidenciar cómo la segmentación lógica a través de VLANs mejora significativamente la eficiencia y seguridad de una red LAN, así como desarrollar las competencias necesarias en la administración de redes y servidores, a través de un enfoque guiado y documentado con figuras, comandos y análisis técnico, se presenta un escenario realista que simula las condiciones de trabajo de un administrador de sistemas.

En este escenario se propone una red segmentada en dos departamentos clave: **Gerencia** y **Operativos**, cada uno con su propia VLAN y direccionamiento IP, esta división permite aislar el tráfico de red entre grupos funcionales, una estrategia indispensable en organizaciones modernas que buscan optimizar el flujo de datos y reducir la exposición a riesgos de seguridad.

La base de este proyecto es la comprensión y correcta aplicación del concepto de **VLAN**, el cual permite dividir una red física en múltiples redes lógicas, a diferencia de una red tradicional, en la que todos los dispositivos comparten el mismo dominio de broadcast, las VLANs permiten que los dispositivos operen como si estuvieran conectados a redes distintas,

aunque compartan el mismo hardware, entre sus beneficios más destacados se encuentran el aumento de la seguridad, la reducción del tráfico innecesario, la mejora en la administración y la posibilidad de escalar o reorganizar la red sin modificar su infraestructura física.

Estas redes virtuales se configuran directamente en los switches mediante comandos especializados, como se muestra en el proyecto, donde se utiliza el sistema operativo Cisco IOS para crear las VLANs, asignar puertos y establecer enlaces troncales (trunking) que permiten la comunicación entre switches. Esta capacidad técnica permite a los administradores de red establecer límites funcionales entre departamentos, asegurando que los datos viajen únicamente dentro de su segmento lógico correspondiente.

La **LAN (Local Area Network)**, en la cual se basa la estructura del escenario, es una red de área local que conecta dispositivos dentro de una ubicación física determinada, su papel es esencial en la comunicación interna de una empresa, ya que posibilita el acceso compartido a recursos como archivos, impresoras y servidores. Sin embargo, conforme la red crece en número de dispositivos y usuarios, también lo hace la complejidad de su administración, es aquí donde las VLANs y una adecuada planificación de la infraestructura cobran especial relevancia, permitiendo mantener el control y orden lógico del sistema.

Dentro del documento, el **Escenario LAN** se desarrolla paso a paso, comienza con una topología sin conexiones físicas y evoluciona hasta una red completamente segmentada y funcional, que refleja fielmente un entorno de trabajo real, cada etapa está acompañada por configuraciones técnicas y análisis del estado de puertos, verificación de enlaces y comandos aplicados. La conexión entre switches mediante enlaces troncales y el uso de subinterfaces en routers (router-on-a-stick) para permitir la comunicación entre VLANs son aspectos claves de este diseño.



Todo este proceso está enmarcado en la disciplina de la **Administración de Redes y Servidores**, que abarca desde el diseño y la configuración de la infraestructura hasta el monitoreo y mantenimiento continuo de los servicios de red, esta área no solo se limita a la parte técnica, sino que también contempla la documentación precisa de cada configuración, la implementación de políticas de seguridad, la respuesta ante incidentes y la gestión de servidores críticos como DNS, DHCP, correo electrónico o servidores web.

El documento no se limita a describir una actividad práctica, sino que ofrece una comprensión profunda de cómo se interrelacionan estos elementos en un entorno de red profesional, muestra cómo una buena administración permite garantizar la disponibilidad de los servicios, proteger la integridad de la información y asegurar la continuidad operativa de una organización.

En conclusión, el proyecto presentado es un ejemplo integral de cómo las redes LAN modernas, apoyadas en tecnologías como las VLANs y gestionadas bajo principios sólidos de administración de redes y servidores, pueden ser configuradas para cumplir con los estándares de eficiencia, seguridad y escalabilidad que demandan los entornos empresariales actuales, este tipo de ejercicios fortalece el perfil del profesional en formación, al proporcionarle no solo habilidades técnicas, sino también una visión estructurada y estratégica del diseño de redes empresariales.

### **Justificación:**

El desarrollo de escenarios prácticos como el planteado en este proyecto responde a la necesidad de fortalecer la comprensión técnica y operativa en el área de redes informáticas, en un entorno cada vez más digitalizado y dependiente de la conectividad, la correcta segmentación lógica de una red mediante VLANs se ha convertido en una competencia esencial para garantizar el orden, la seguridad y la eficiencia de la infraestructura tecnológica de cualquier organización.

La simulación de una red LAN empresarial utilizando herramientas como Cisco Packet Tracer permite aplicar conocimientos teóricos a situaciones reales, ofreciendo un entorno controlado donde se pueden diseñar, visualizar y analizar topologías de red antes de su implementación física, esta aproximación no solo mejora la capacidad de análisis técnico del estudiante, sino que también fomenta la toma de decisiones fundamentadas en la planificación de redes escalables y seguras.

La elección de trabajar con VLANs dentro del escenario LAN tiene un fundamento claro: estas permiten segmentar una red física en dominios lógicos, lo que reduce el tráfico innecesario, mejora el rendimiento de la red y proporciona una gestión más eficiente, implementar esta solución desde la fase de diseño impulsa el desarrollo de habilidades clave en la Administración de Redes y Servidores, como la asignación de direcciones IP, la jerarquización de dispositivos, la previsión de enlaces troncales y la preparación para el enrutamiento entre VLANs.

Este proyecto se justifica también por su aplicabilidad directa al ámbito profesional. En la vida laboral, el dominio de estas herramientas y conceptos permite a los egresados desempeñarse en roles técnicos con mayor eficiencia, adaptarse a las necesidades cambiantes de las organizaciones y contribuir a la mejora continua de sus sistemas de comunicación, asimismo, en

la vida cotidiana, el conocimiento sobre redes mejora la autonomía tecnológica y la capacidad de comprender el funcionamiento de los entornos digitales que nos rodean.

Por lo tanto, la elaboración de este escenario constituye una inversión formativa de alto valor para el desarrollo integral de competencias en tecnologías de la información, preparándonos a los para enfrentar los desafíos del mercado laboral y de la sociedad conectada actual.

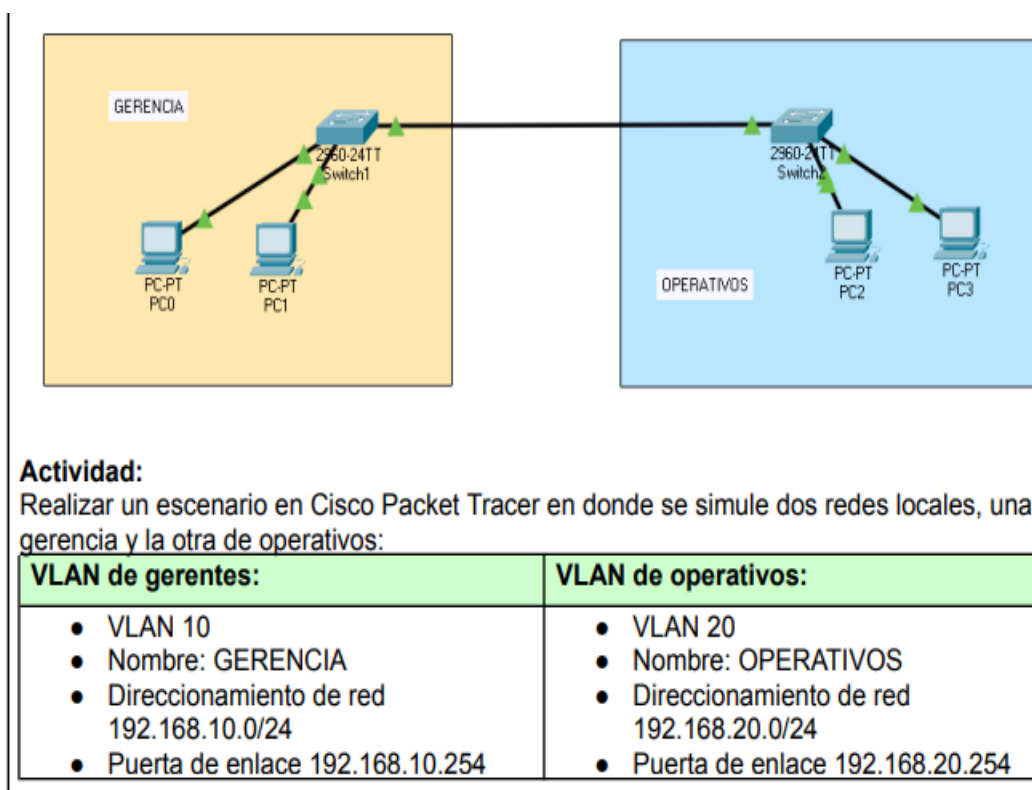
## Desarrollo:

### Etapa 1- Escenario LAN

**Contextualización:** Rogelio aplicando para el puesto de administrador de sistemas, por tanto, se le solicita realizar una propuesta gráfica y simulada para dos redes locales.

**Figura 1**

*Ejemplo de la Estructura:*



*Nota:* La actividad consiste en el diseño y simulación de una red en **Cisco Packet Tracer** que represente la segmentación lógica de dos departamentos dentro de una empresa: **Gerencia** y **Operativos**, para ello, se implementan **dos VLANs independientes** sobre switches distintos, lo que permite aislar el tráfico de red entre ambas áreas, mejorar la seguridad y optimizar el control del flujo de datos.

La **VLAN 10**, identificada como *GERENCIA*, agrupa a los equipos del área administrativa con direccionamiento de red **192.168.10.0/24** y puerta de enlace **192.168.10.254**.

La **VLAN 20**, denominada *OPERATIVOS*, incluye a los dispositivos del personal operativo con direccionamiento **192.168.20.0/24** y puerta de enlace **192.168.20.254**.

Ambas VLANs se interconectan mediante un **router configurado con subinterfaces (router-on-a-stick)**, el cual facilita la comunicación entre redes virtuales (inter-VLAN routing) sin comprometer la segmentación lógica, la implementación también contempla la asignación de IPs estáticas a cada host, la configuración de puertos en modo acceso o trunk según corresponda, y la verificación de conectividad entre dispositivos.

Este escenario permite comprender conceptos clave de redes como:

VLANs y su configuración en switches

Subinterfaces en routers

Trunking 802.1Q

Segmentación de red y enrutamiento entre VLANs

Enlace para visualizarlo a detalle:

[file:///C:/Users/sara/Downloads/Actividad\\_1\\_Administracion\\_de\\_Netes\\_y\\_Servicios\\_V4.docx](file:///C:/Users/sara/Downloads/Actividad_1_Administracion_de_Netes_y_Servicios_V4.docx)

[%20\(1\).pdf](#) , **Creación de la Universidad Corporativa.**

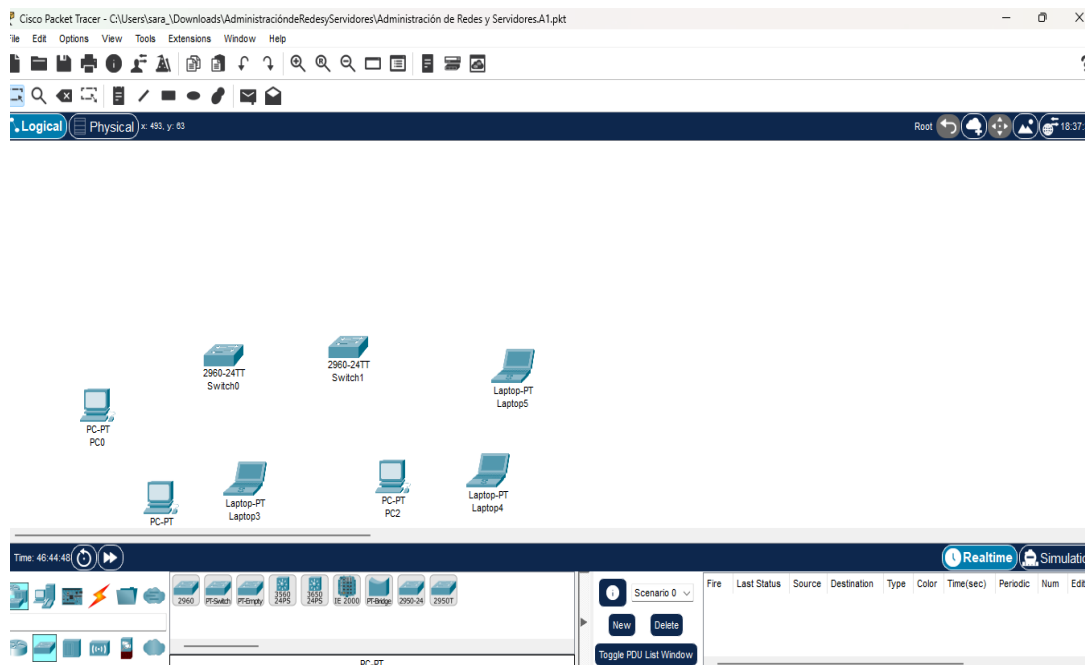
Crear el escenario mostrado en la imagen de la sección de contextualización con dos switches y 4 PC y conectarlas

Configurar el switch 1 de gerencia con los datos de la tabla en la pestaña de CLI.

Configurar el switch 2 de operativos con los datos de la tabla en la pestaña de CLI

Documentar los comandos utilizados en el Switch 1 y el Switch 2.

Tomar captura de pantalla del escenario creado.

**Figura 2*****Topología Inicial - Dispositivos sin conexión***

*Nota:* En esta fase preliminar del proyecto, se ha establecido la disposición lógica inicial de los dispositivos en Cisco Packet Tracer, sin aplicar aún conexiones físicas entre ellos.

**Descripción física y cableado:**

La infraestructura muestra dos switches modelo Cisco 2960-24TT (Switch0 y Switch1), acompañados de tres computadoras de escritorio (PCs) y tres laptops (Laptop-PT), distribuidos sin enlaces de red.

**Función principal:**

Visualizar la estructura base de la red, facilitando una organización jerárquica inicial antes de aplicar configuraciones físicas o lógicas.

**Relevancia técnica:**

Este diseño inicial permite planear una red escalable y ordenada, segmentada por áreas físicas o

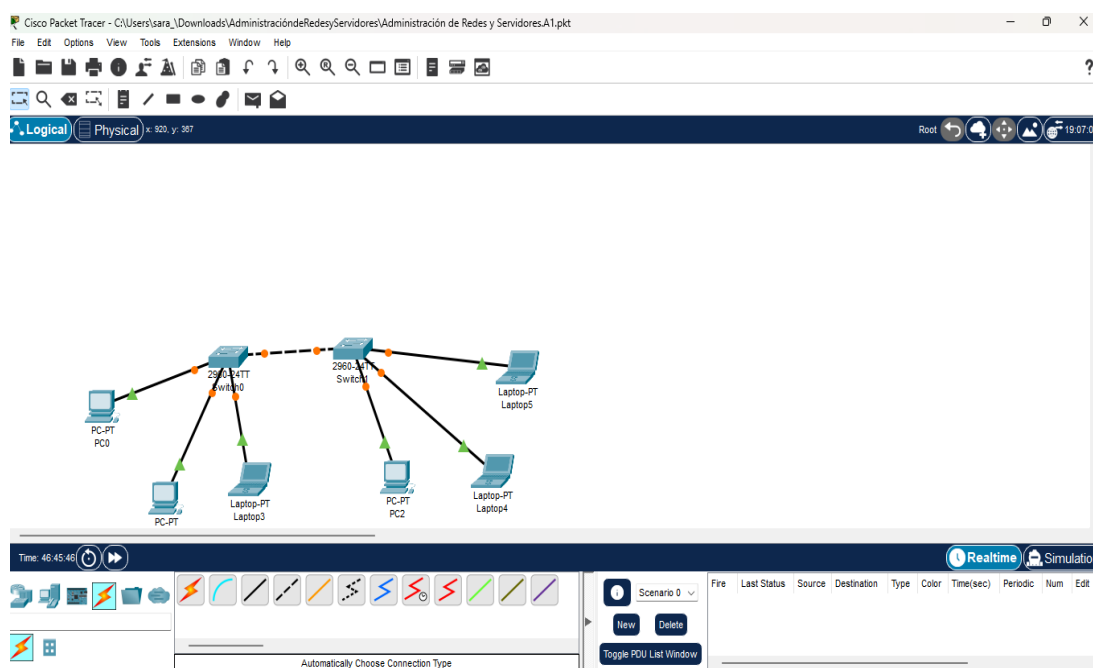
departamentos. Es esencial para prever futuras conexiones y configurar adecuadamente las VLANs.

### **Implicaciones a futuro:**

La correcta disposición de los dispositivos asegura una segmentación lógica eficiente en fases posteriores, mejorando la administración y seguridad de la red.

### **Figura 3**

#### ***Conexiones Físicas Establecidas entre Dispositivos***



*Notas:* En esta fase del proyecto, se han completado las conexiones físicas entre todos los dispositivos integrados en la red.

### **Descripción física y cableado:**

PCs y laptops conectadas a sus respectivos switches mediante cables directos (verdes), siguiendo el estándar de conexión entre dispositivos de distinto tipo.

Interconexión entre Switch0 y Switch1 mediante cable cruzado (negro), conforme a los

estándares para comunicación entre dispositivos del mismo tipo.

### **Función principal:**

Establecer un entorno de comunicación jerárquica mediante la correcta disposición de los switches como nodos centrales de conmutación.

### **Relevancia técnica:**

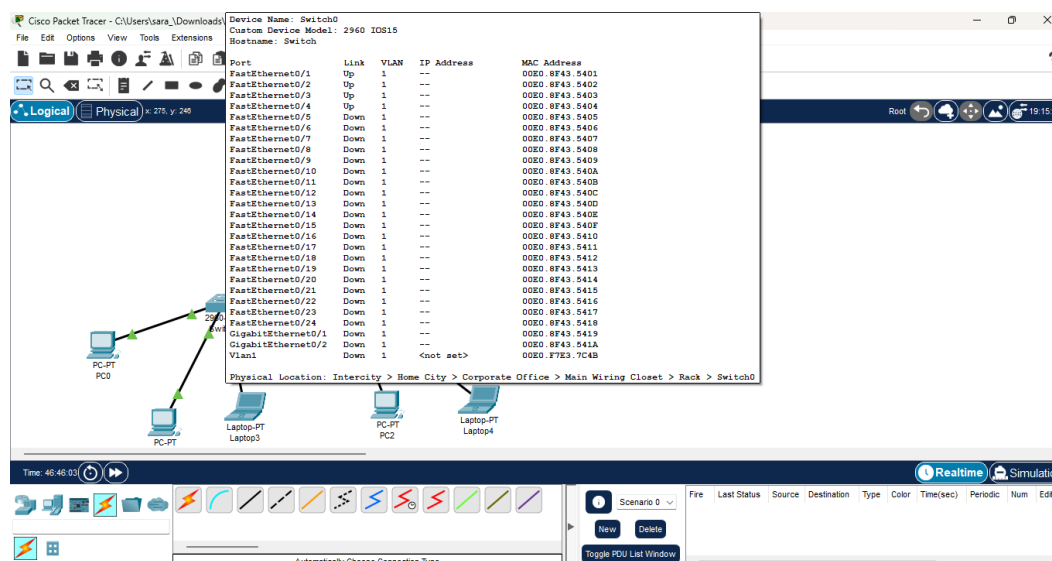
Esta fase consolida la infraestructura física base para configuraciones lógicas como VLANs, el tipo de cableado utilizado asegura una comunicación eficiente y evita conflictos de señal.

### **Implicaciones a futuro:**

Permite la segmentación futura por departamentos y la implementación efectiva de políticas de red según la estructura organizacional.

### **Figura 4**

*Estado de puertos en Switch0 (antes de asignar VLANs):*



*Nota:* Esta figura muestra el estado de las interfaces del Switch0 después de haber establecido las conexiones físicas con los dispositivos finales, a través de la vista de estado en Cisco Packet Tracer, se observan las interfaces activas (estado "Up"), lo que indica que han



detectado correctamente la presencia de señal eléctrica proveniente de los dispositivos conectados, como PCs o laptops.

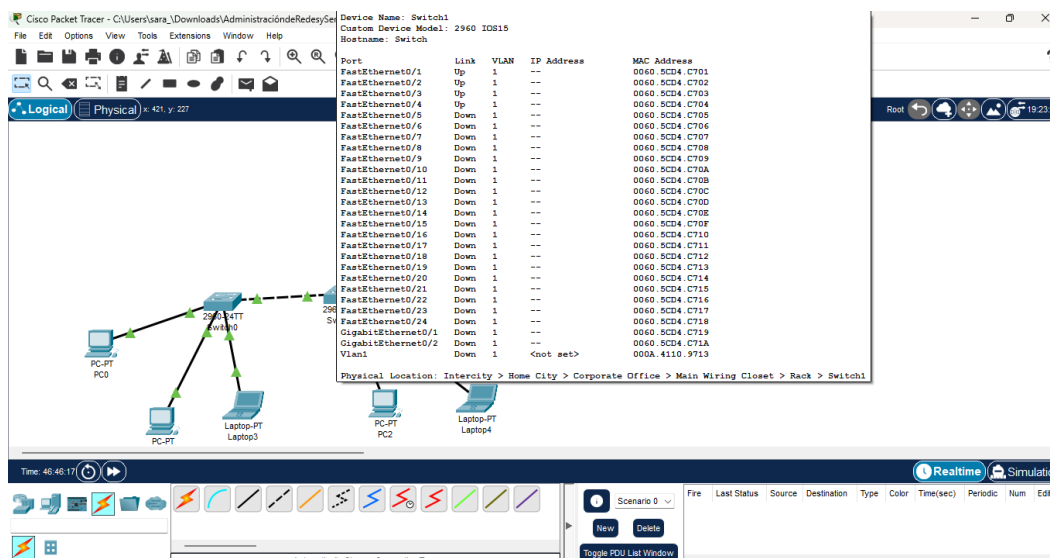
Este tipo de verificación es crucial para confirmar que la capa física de red está funcionando adecuadamente. Las interfaces FastEthernet en estado activo representan conexiones que están listas para recibir configuraciones lógicas como la asignación a VLANs. Por otro lado, aquellas en estado "Down" indican puertos sin dispositivos conectados o con problemas físicos.

La función principal de esta etapa es diagnosticar de forma visual y rápida el estado de cada puerto, permitiendo al administrador de red tomar decisiones informadas sobre a qué VLAN debe pertenecer cada puerto según el dispositivo conectado.

En términos técnicos, este diagnóstico previo reduce errores durante la asignación lógica de puertos, ya que permite validar qué interfaces están siendo utilizadas y cuáles están disponibles. Asimismo, proporciona evidencia de que la red responde correctamente a nivel físico, lo que es indispensable antes de aplicar configuraciones que afectan la capa 2 o superior.

**Figura 5**

*Estado de puertos en Switch1 (antes de configurar VLANs):*



*Nota:* En esta imagen se visualiza el estado operativo de las interfaces del Switch1, similar a la verificación realizada en Switch0, esta revisión busca confirmar que los dispositivos finales del segundo piso o segunda zona estén correctamente conectados y reconocidos por el switch.

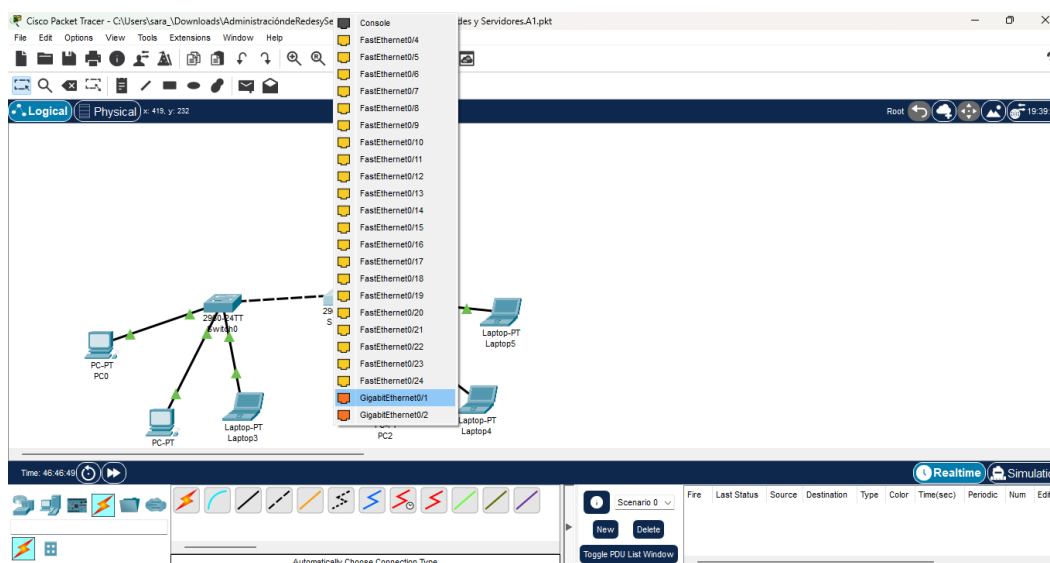
Se puede apreciar que algunas interfaces están en estado "Up", lo cual implica que hay conectividad física con laptops o PCs, esta validación es necesaria antes de aplicar cualquier configuración lógica, como la asignación de puertos a VLANs específicas.

Técnicamente, este tipo de análisis permite asegurar que el hardware de red está funcionando como se espera, la correcta detección de enlaces activos es una condición esencial para asegurar que las futuras configuraciones (como VLANs o enlaces troncales) se apliquen de forma efectiva.

Esta revisión también permite prevenir conflictos durante la segmentación, ya que ayuda a identificar y separar adecuadamente los puertos utilizados por cada grupo de trabajo o departamento.

**Figura 6**

***Selección de interfaz GigabitEthernet0/1 en Switch1:***



*Nota:* Esta figura muestra la selección de la interfaz GigabitEthernet0/1 del Switch1, una acción previa necesaria para configurar el enlace troncal que permitirá la comunicación entre múltiples VLANs a través de Switch0 y Switch1.

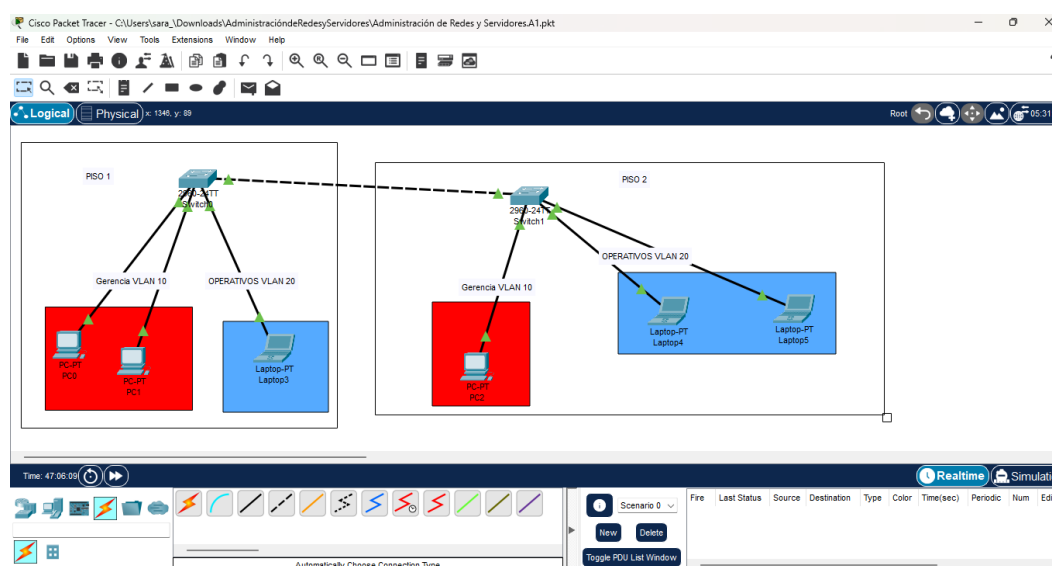
Comando utilizado: `interface gigabitEthernet 0/1`, este comando coloca al administrador dentro del modo de configuración específica para la interfaz mencionada, permitiendo modificar parámetros de la interfaz, como su modo de operación (access o trunk), velocidad, encapsulación y asignación a VLANs.

A partir de este punto, cualquier comando ingresado se aplicará únicamente a dicha interfaz, este paso es esencial para permitir que la VLAN 10 y la VLAN 20 se propaguen de forma simultánea entre ambos switches, si no se configura correctamente esta interfaz como trunk, el tráfico de

VLANs diferentes no podrá cruzar entre switches, afectando la conectividad de la red, esta acción es parte fundamental de la configuración de redes jerárquicas con segmentación lógica, ya que el trunk actúa como una carretera principal por donde viajan paquetes etiquetados pertenecientes a diversas VLANs.

**Figura 7**

***Segmentación por Pisos y VLANs con Enlace Troncal:***



*Nota:* En esta imagen se presenta la topología lógica completa de la red, estructurada en dos segmentos físicos equivalentes a diferentes pisos o departamentos, la red incluye dos switches (Switch0 y Switch1), cada uno conectado a varios dispositivos finales que han sido organizados en dos VLANs: VLAN 10 (Gerencia) y VLAN 20 (Operativos).

Se observa la conexión entre switches mediante un cable de mayor grosor (generalmente negro), que representa un enlace troncal, este trunk es configurado para transportar tráfico de múltiples VLANs, asegurando así la segmentación lógica a través de la infraestructura física.

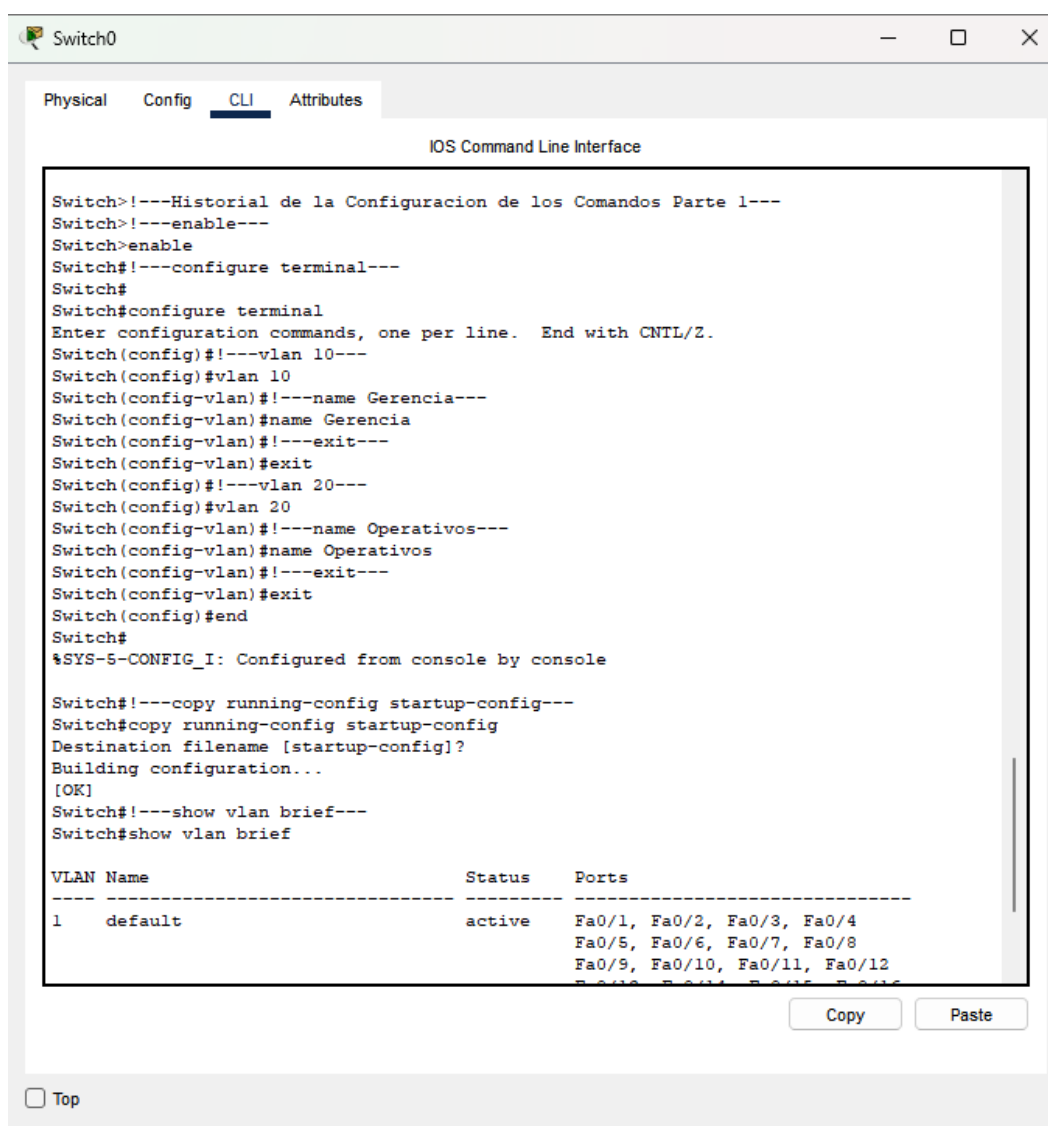
Esta disposición facilita la administración del tráfico de red al aislar dominios de broadcast, mejorar la seguridad entre departamentos, y optimizar el rendimiento, la conexión troncal es un

canal compartido que debe configurarse adecuadamente (con comandos como `switchport mode trunk`) para que los paquetes etiquetados lleguen a su destino correcto.

Comando `switchport mode trunk`: Configura un puerto para permitir tráfico de múltiples VLANs (trunking), es esencial para comunicación entre switches en entornos segmentados.

**Figura 8**

*Configuración de VLANs en Switch0 (Parte I):*



```
Switch0
Physical Config CLI Attributes
IOS Command Line Interface

Switch>!--Historial de la Configuracion de los Comandos Parte 1--
Switch>!--enable--
Switch>enable
Switch>!--configure terminal--
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#!--vlan 10--
Switch(config)#vlan 10
Switch(config-vlan)#!--name Gerencia--
Switch(config-vlan)#name Gerencia
Switch(config-vlan)#!--exit--
Switch(config-vlan)#exit
Switch(config)#!--vlan 20--
Switch(config)#vlan 20
Switch(config-vlan)#!--name Operativos--
Switch(config-vlan)#name Operativos
Switch(config-vlan)#!--exit--
Switch(config-vlan)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#!---copy running-config startup-config---
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#!---show vlan brief---
Switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

*Nota:* Esta imagen muestra la consola del Switch0 durante la creación de VLANs.

**Comandos utilizados:**

- ``vlan 10``: Crea una nueva VLAN con ID 10.
- ``name Gerencia``: Asigna el nombre “Gerencia” a la VLAN 10.
- ``vlan 20``: Crea la VLAN 20.
- ``name Operativos``: Asigna el nombre “Operativos” a la VLAN 20.
- ``copy running-config startup-config``: Guarda la configuración en la memoria NVRAM.

Los comandos ``vlan`` permiten definir segmentos lógicos dentro de la red, el comando ``copy`` asegura que la configuración persista tras un reinicio.

Si no se guardan los cambios con ``copy running-config startup-config``, la configuración se perderá al apagar el dispositivo, este paso es clave para evitar la reconfiguración futura y consolidar la segmentación.

*Comando ``vlan 10``*: Crea una VLAN con ID 10, esto permite definir un dominio de broadcast independiente para dispositivos asociados, facilitando la segmentación lógica de la red, si no se configura correctamente, los dispositivos asignados no podrán comunicarse.

*Comando ``vlan 20``*: Similar al anterior, este comando crea la VLAN 20, normalmente usada para otro departamento o grupo de trabajo, su ausencia puede generar falta de conectividad dentro del grupo esperado.

*Comando ``name Gerencia``*: Asigna un nombre descriptivo a la VLAN 10, esto ayuda en la gestión y documentación, aunque no tiene efecto funcional en el tráfico de red.

*Comando ``name Operativos``*: Asigna un nombre identificador a la VLAN 20, al igual que el anterior, es útil para la claridad organizativa.

*Comando ``copy running-config startup-config``*: Guarda la configuración en memoria permanente (NVRAM). Si se omite, la configuración se pierde tras un reinicio.

Figura 9

*Verificación de VLANs en Switch0*

```

Switch0
Physical Config CLI Attributes
IOS Command Line Interface
Switch(config-vlan)#name Gerencia
Switch(config-vlan)#!---exit---
Switch(config-vlan)#exit
Switch(config)#!---vlan 20---
Switch(config)#vlan 20
Switch(config-vlan)#!---name Operativos---
Switch(config-vlan)#name Operativos
Switch(config-vlan)#!---exit---
Switch(config-vlan)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#!---copy running-config startup-config---
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#!---show vlan brief---
Switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2

10   Gerencia                active
20   Operativos              active
1002 fddi-default           active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active
Switch#
Copy Paste
Top

```

*Nota:* En esta etapa se verifica la creación de VLANs con el comando:

***show vlan brief***: Muestra un resumen de todas las VLANs configuradas, incluyendo sus

nombres, estados y puertos asociados, permite validar visualmente que las VLANs 10 y 20 están registradas y activas.

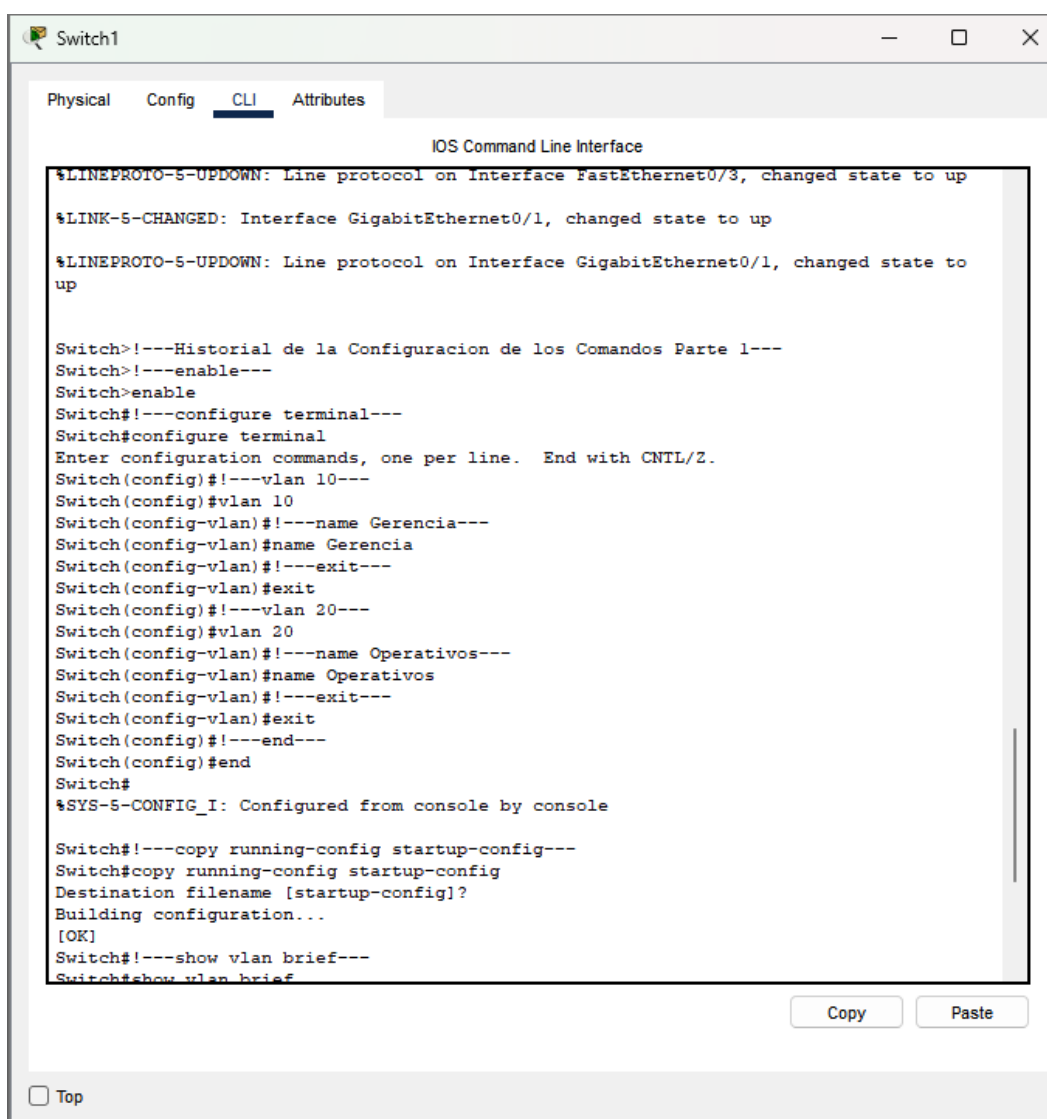
Esta verificación evita errores en etapas posteriores, como la asignación incorrecta de puertos. Si

una VLAN no aparece en este resumen, no funcionará como se espera, y los dispositivos asignados a ella no podrán comunicarse.

Comando ``show vlan brief``: Muestra todas las VLANs configuradas, con sus estados y puertos asociados, es útil para validar que la configuración se aplicó correctamente.

**Figura 10**

### *Configuración de VLANs en Switch1:*



```

Switch1
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch>!--Historial de la Configuracion de los Comandos Parte 1--
Switch>!--enable--
Switch>enable
Switch#!---configure terminal---
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#!---vlan 10---
Switch(config)#vlan 10
Switch(config-vlan)#!---name Gerencia---
Switch(config-vlan)#name Gerencia
Switch(config-vlan)#!---exit---
Switch(config-vlan)#exit
Switch(config)#!---vlan 20---
Switch(config)#vlan 20
Switch(config-vlan)#!---name Operativos---
Switch(config-vlan)#name Operativos
Switch(config-vlan)#!---exit---
Switch(config-vlan)#exit
Switch(config)#!---end---
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#!---copy running-config startup-config---
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#!---show vlan brief---
Switch#show vlan brief
  
```

*Nota:* Se repite el proceso de creación de VLANs en Switch1.



**Comandos utilizados:**

- ``vlan 10``
- ``name Gerencia``
- ``vlan 20``
- ``name Operativos``
- ``copy running-config startup-config``

Estos pasos aseguran que ambos switches compartan la misma segmentación lógica, esta homogeneidad es obligatoria para permitir que el tráfico entre VLANs pueda propagarse correctamente a través del enlace troncal, ya que si un switch desconoce una VLAN, descartará los paquetes etiquetados con esa ID.

Comando ``vlan 10``: Crea una VLAN con ID 10, esto permite definir un dominio de broadcast independiente para dispositivos asociados, facilitando la segmentación lógica de la red, si no se configura correctamente, los dispositivos asignados no podrán comunicarse.

Comando ``vlan 20``: Similar al anterior, este comando crea la VLAN 20, normalmente usada para otro departamento o grupo de trabajo, su ausencia puede generar falta de conectividad dentro del grupo esperado.

Comando ``name Gerencia``: Asigna un nombre descriptivo a la VLAN 10, esto ayuda en la gestión y documentación, aunque no tiene efecto funcional en el tráfico de red.

Comando ``name Operativos``: Asigna un nombre identificador a la VLAN 20, al igual que el anterior, es útil para la claridad organizativa.

Comando ``copy running-config startup-config``: Guarda la configuración en memoria permanente (NVRAM), si se omite, la configuración se pierde tras un reinicio.

Figura 11

*Verificación de VLANs en Switch1:*

```

Switch1
Physical Config CLI Attributes
IOS Command Line Interface

Switch(config-vlan)#!---exit---
Switch(config-vlan)#exit
Switch(config)#!---vlan 20---
Switch(config)#vlan 20
Switch(config-vlan)#!---name Operativos---
Switch(config-vlan)#name Operativos
Switch(config-vlan)#!---exit---
Switch(config-vlan)#exit
Switch(config)#!---end---
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#!---copy running-config startup-config---
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#!---show vlan brief---
Switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2

10   Gerencia                active
20   Operativos              active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
Switch#

```

Copy Paste

☐ Top

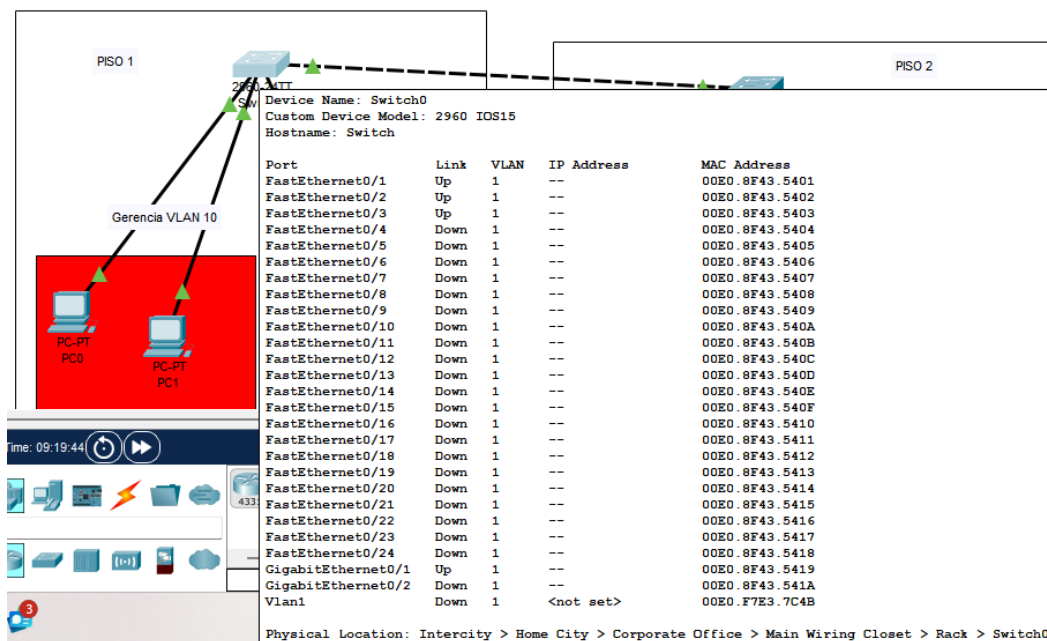
*Nota:* Se utiliza nuevamente el comando `show vlan brief` en Switch1 para validar que las VLANs han sido creadas correctamente, este paso refleja buenas prácticas de administración, ya que permite corregir errores antes de proceder con la asignación de puertos. Confirmar la presencia de VLANs evita fallos de conectividad y asegura que todos los

dispositivos asociados funcionen correctamente en sus respectivos segmentos.

Comando ``show vlan brief``: Muestra todas las VLANs configuradas, con sus estados y puertos asociados, es útil para validar que la configuración se aplicó correctamente.

**Figura 12**

*Estado de Puertos Switch0 – VLAN 10 (Gerencia):*



*Nota:* La figura muestra qué interfaces físicas del Switch0 están en uso por la VLAN 10.

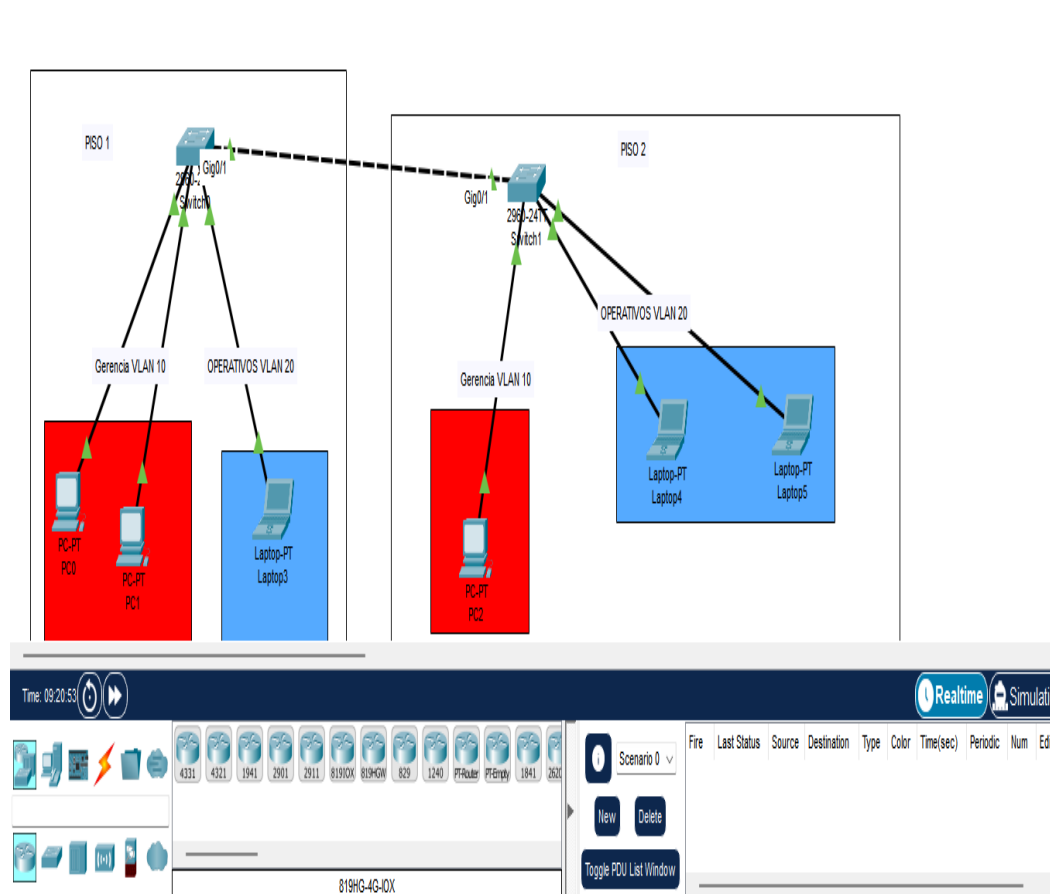
Aunque no se visualiza un comando específico, puede derivarse de la interfaz gráfica o del uso del comando ``show interface status``.

Permite verificar qué puertos están conectados activamente a dispositivos y asociarlos manualmente a la VLAN 10.

Esta verificación asegura que solo los dispositivos pertenecientes al departamento de Gerencia compartan el mismo dominio de broadcast, mejorando la seguridad y control de tráfico.

**Figura 13**

***Red Final con Conexión Troncal y Segmentación Aplicada:***



*Nota:* En esta imagen se confirma que todos los dispositivos han sido segmentados correctamente por VLAN y que la comunicación entre switches se realiza a través de un enlace troncal activo.

Función de la topología: Permite mantener separados los dominios de broadcast sin necesidad de switches adicionales, promoviendo una red escalable y eficiente, esta estructura permite que dispositivos de la misma VLAN, aunque estén en switches distintos, se comuniquen sin conflictos.

Figura 14

**Switch1 con PC2 (Gerencia) y Trunk Activado:**

The screenshot displays the configuration of a switch named 'Switch1'. The main configuration pane shows the following details:

- Device Name: Switch1
- Custom Device Model: 2960 IOS15
- Hostname: Switch

Below this, a table lists the status of various ports:

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	1	--	0060.5CD4.C701
FastEthernet0/2	Up	1	--	0060.5CD4.C702
FastEthernet0/3	Up	1	--	0060.5CD4.C703
FastEthernet0/4	Down	1	--	0060.5CD4.C704
FastEthernet0/5	Down	1	--	0060.5CD4.C705
FastEthernet0/6	Down	1	--	0060.5CD4.C706
FastEthernet0/7	Down	1	--	0060.5CD4.C707
FastEthernet0/8	Down	1	--	0060.5CD4.C708
FastEthernet0/9	Down	1	--	0060.5CD4.C709
FastEthernet0/10	Down	1	--	0060.5CD4.C70A
FastEthernet0/11	Down	1	--	0060.5CD4.C70B
FastEthernet0/12	Down	1	--	0060.5CD4.C70C
FastEthernet0/13	Down	1	--	0060.5CD4.C70D
FastEthernet0/14	Down	1	--	0060.5CD4.C70E
FastEthernet0/15	Down	1	--	0060.5CD4.C70F
FastEthernet0/16	Down	1	--	0060.5CD4.C710
FastEthernet0/17	Down	1	--	0060.5CD4.C711
FastEthernet0/18	Down	1	--	0060.5CD4.C712
FastEthernet0/19	Down	1	--	0060.5CD4.C713
FastEthernet0/20	Down	1	--	0060.5CD4.C714
FastEthernet0/21	Down	1	--	0060.5CD4.C715
FastEthernet0/22	Down	1	--	0060.5CD4.C716
FastEthernet0/23	Down	1	--	0060.5CD4.C717
FastEthernet0/24	Down	1	--	0060.5CD4.C718
GigabitEthernet0/1	Up	1	--	0060.5CD4.C719
GigabitEthernet0/2	Down	1	--	0060.5CD4.C71A
Vlan1	Down	1	<not set>	000A.4110.9713

The physical location is listed as: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch1.

At the bottom, there is a 'Realtime' and 'Simulation' toggle, and a table for monitoring traffic:

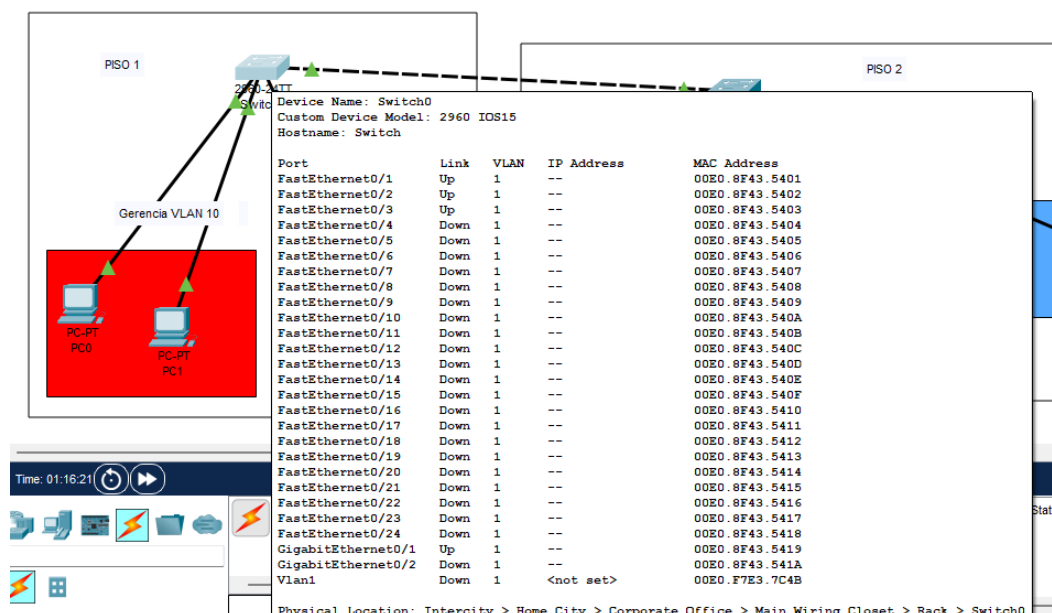
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit

*Nota:* Se observa a PC2 conectada al Switch1 dentro de la VLAN 10, y el trunk activo entre Switch0 y Switch1, esta configuración permite que PC2 se comuniquen con dispositivos de la misma VLAN ubicados en Switch0.

Esta visualización verifica que tanto la asignación de puertos como la troncalización están funcionando correctamente, asegurando la continuidad lógica de la VLAN a través de varios switches.

**Figura 15**

***Activación de Puertos VLAN Gerencia y Trunk en Switch0:***

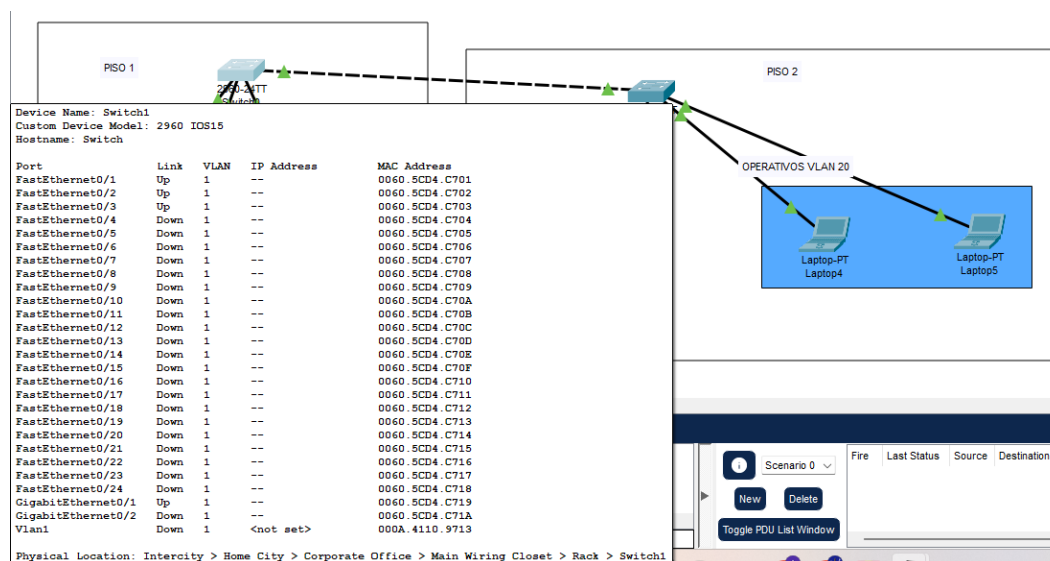


*Nota:* Se visualiza el estado activo ('up') tanto en los puertos asignados a la VLAN 10 como en el trunk.

El correcto estado operativo de estas interfaces indica que la red está funcionando conforme a la segmentación planificada. Cualquier error de configuración (como puerto mal asignado o trunk mal definido) podría haber provocado la desconexión entre segmentos.

**Figura 16**

***Switch1 – VLAN 20 (Operativos) Funcionando:***



*Nota:* Muestra los puertos del Switch1 operando bajo la VLAN 20.

Confirma que los dispositivos operativos están correctamente aislados y que su tráfico se mantiene dentro de su dominio lógico, la separación funcional facilita tareas administrativas, aumenta la seguridad, y reduce interferencias de tráfico.

***Enlace para visualizar el Archivo .pkt de Cisco en GitHub:***

[Administraci-n-de-Redes-y-Servidores/Sarahi Jaqueline Gomez Juarez\\_Escenario LAN A1.pkt at main · SarahiJaquelineGomezJuarez/Administraci-n-de-Redes-y-Servidores](https://github.com/SarahiJaquelineGomezJuarez/Administraci-n-de-Redes-y-Servidores/blob/main/LAN_A1.pkt)

## **Conclusión**

La creación del escenario de red empresarial, basado en la segmentación lógica mediante VLANs, representa un paso esencial dentro del proceso de diseño de infraestructuras tecnológicas modernas, en esta etapa inicial del proyecto, se ha logrado establecer la topología física y lógica de la red, incluyendo la organización jerárquica de los dispositivos, la conexión estructurada de switches y terminales, así como la planificación de la segmentación por departamentos a través de VLANs específicas.

Si bien aún no se ha iniciado la fase de configuración técnica, esta etapa de diseño constituye la base estratégica sobre la cual se construirá una red funcional, segura y escalable, la preparación adecuada de los elementos físicos y la previsión de aspectos como el direccionamiento IP, los enlaces troncales y la asignación de puertos permiten anticipar una implementación eficiente, alineada con los principios fundamentales de la Administración de Redes y Servidores.

Más allá del plano académico, la adquisición de estos conocimientos tiene una gran relevancia tanto en la vida diaria como en el entorno profesional. En el contexto actual, donde la conectividad es esencial en prácticamente todas las actividades humanas, comprender cómo funciona una red local, cómo se organiza la infraestructura de comunicación digital y cómo se aplican medidas de seguridad y eficiencia, es una competencia indispensable.

En el ámbito laboral, estos saberes se traducen en ventajas competitivas claras: permiten desempeñarse con solvencia en áreas de soporte técnico, administración de sistemas, ciberseguridad, desarrollo de infraestructura TI, entre otros campos con alta demanda.



En definitiva, este proyecto no solo fortalece las habilidades técnicas necesarias para futuras configuraciones, sino que también promueve una visión integral y estratégica del diseño de redes, representa una base sólida para el crecimiento académico y profesional, al tiempo que aporta herramientas prácticas para comprender y desenvolverse con mayor seguridad en un mundo cada vez más interconectado.

### Referencias:

AnirbanPaul. (s. f.). *Networking documentation*. Microsoft Learn.

<https://learn.microsoft.com/es-es/windows-server/networking/>

*Aprendizaje gratuito basado en competencias impartido por expertos en tecnología / IBM SkillsBuild*. (s. f.). IBM SkillsBuild. <https://skillsbuild.org/es>

iOSMart Academy by Marco Alonso. (2022, 20 octubre). *Configurar 2 VLAN en dos switches de una red LAN (Parte 1)* [Vídeo]. YouTube.

<https://www.youtube.com/watch?v=iKfZlPxrmzY>

Lorenzo, J. A. (2025, 18 julio). Aprende a navegar por la Deep Web con estos buscadores. *RedesZone*. <https://www.redeszone.net/tutoriales/seguridad/buscadores-navegar-deep-web/>

*Video conferencing, web conferencing, webinars, screen sharing*. (s. f.). Zoom.  
[https://academiaglobal-mx.zoom.us/rec/play/0FHKjIzmNSOMhlmN-i73gikMhSBE6taretej\\_l\\_W8HbleHbwX-K1BKnxph1X8OrzVAxfvP\\_ATl4m6xyL.kdo\\_tqegQeumk4Qq?eagerLoadZvaPages=sidemenu.billing.plan\\_management&accessLevel=meeting&canPlayFromShare=true&from=share\\_recording\\_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2F0fWyVFATxAcyKmWNBwgNhr8zW00H7oHP3qLI7jNRPxZuFAA5tXInShyeBQGDx55O.uGjJXKuqAs7Hf7uu](https://academiaglobal-mx.zoom.us/rec/play/0FHKjIzmNSOMhlmN-i73gikMhSBE6taretej_l_W8HbleHbwX-K1BKnxph1X8OrzVAxfvP_ATl4m6xyL.kdo_tqegQeumk4Qq?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2F0fWyVFATxAcyKmWNBwgNhr8zW00H7oHP3qLI7jNRPxZuFAA5tXInShyeBQGDx55O.uGjJXKuqAs7Hf7uu)