Práctica de laboratorio: Configuración de VLAN y enlaces troncales

.JULIO ANTHONY ENGELS RUIZ COTO - 1284719

# Topología



# Tabla de asignación de direcciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | N/D |
| S2 | VLAN 1 | 192.168.1.12 | 255.255.255.0 | N/D |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-B | NIC | 192.168.10.4 | 255.255.255.0 | 192.168.10.1 |

# Objetivos

Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: Crear redes VLAN y asignar puertos de switch

Parte 3: Mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

Parte 4: Configurar un enlace troncal 802.1Q entre los switches

Parte 5: Eliminar la base de datos de VLAN

# Aspectos básicos/situación

Los switches modernos usan redes de área local virtuales (VLAN) para mejorar el rendimiento de la red mediante la división de grandes dominios de difusión de capa 2 en otros más pequeños. Las VLAN también se pueden usar como medida de seguridad al controlar qué hosts se pueden comunicar. Por lo general, las redes VLAN facilitan el diseño de una red para respaldar los objetivos de una organización.

Los enlaces troncales de VLAN se usan para abarcar redes VLAN a través de varios dispositivos. Los enlaces troncales permiten transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN.

En esta práctica de laboratorio, creará redes VLAN en los dos switches de la topología, asignará las VLAN a los puertos de acceso de los switches, verificará que las VLAN funcionen como se espera y, a continuación, creará un enlace troncal de VLAN entre los dos switches para permitir que los hosts en la misma VLAN se comuniquen a través del enlace troncal, independientemente del switch al que está conectado el host.

**Nota**: Los switches que se usan en este laboratorio de CCNA son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota**: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

# Recursos necesarios

* 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
* 2 PC (Windows con un programa de emulación de terminal, como Tera Term)
* Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
* Cables Ethernet, como se muestra en la topología

# Instrucciones

## Armar la red y configurar los ajustes básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

### Realizar el cableado de red como se muestra en la topología

Conecte los dispositivos como se muestra en la topología y realizar el cableado necesario.

### Configurar los parámetros básicos para cada switch

* + - 1. Acceda al switch mediante el puerto de consola y habilite al modo EXEC con privilegios.

Abrir la ventana de configuración

* + - 1. Ingrese al modo de configuración.
      2. Asigne un nombre de dispositivo al switch.
      3. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.
      4. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
      5. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
      6. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
      7. Cifre las contraseñas de texto sin formato.
      8. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
      9. Configure la dirección IP que figura en la tabla de direcciones para VLAN 1 en el switch.
      10. Apague todas las interfaces que no se utilizarán.
      11. Ajuste el reloj en el interruptor.

Cerrar la ventana de configuración

### Configurar los equipos host

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

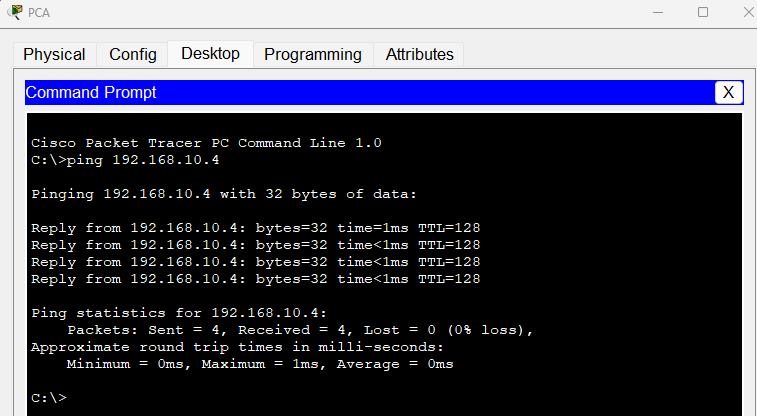
### Probar la conectividad

Verifique que los equipos host puedan hacer ping entre sí.

**Note**: Puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

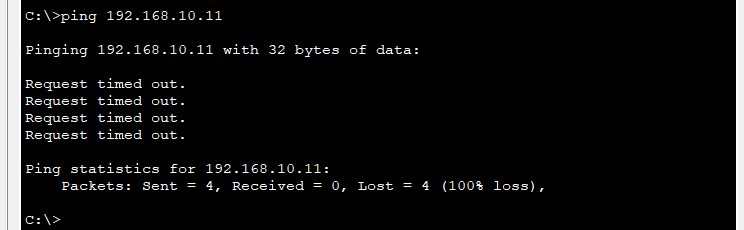
#### Preguntas:

¿Se puede hacer ping de la PC-A a la PC-B? R// SI

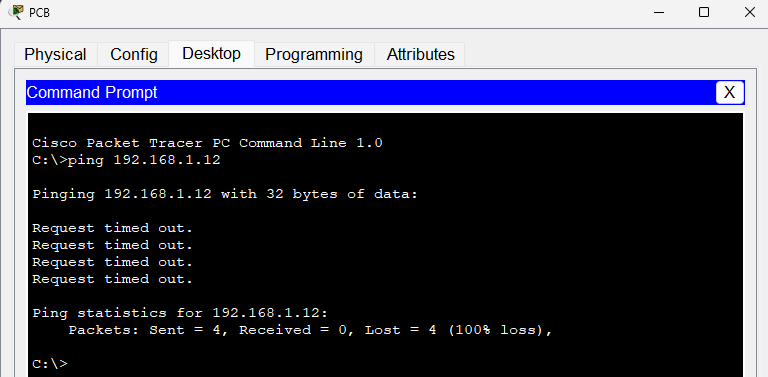


Escriba sus respuestas aquí.

¿Se puede hacer ping de la PC-A al S1? R// NO

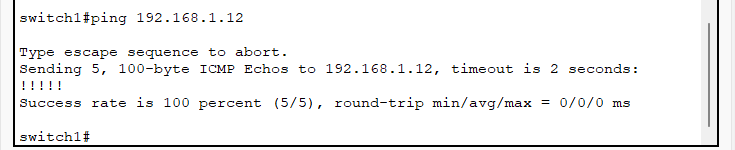
uí. 

¿Se puede hacer ping de la PC-B al S2? R// NO



Abrir la ventana de configuración

¿Se puede hacer ping del S1 al S2? R// SI



Si la respuesta a cualquiera de las preguntas anteriores es no, ¿por qué fallaron los pings?

Los pings fallaron ya que PC-A y PC-B están configuradas para usar una dirección ip en la subred 192.168.10.0 /24 mientras que los switche S1 y S2 en la subred 192.168.1.0/24 no hay comunicaciones directas entre estas subredes sin un router.

Escriba sus respuestas aquí.

Cerrar la ventana de configuración

## Crear redes VLAN y asignar puertos de switch

En la parte 2, creará VLAN para los estudiantes, el cuerpo docente y la administración en ambos switches. A continuación, asignará las VLAN a la interfaz correspondiente. El comando **show vlan** se usa para verificar las opciones de configuración.

### Crear las VLAN en los switches

Abrir la ventana de configuración

* + - 1. Cree las VLAN en S1.

S1(config)# **vlan 10**

S1 (config-vlan) # **name Operations**

S1(config-vlan)# **vlan 20**

S1(config-vlan)# **name Parking\_Lot**

S1(config-vlan)# **vlan 99**

S1(config-vlan)# **name Management**

S1 (config-vlan) # **vlan 1000**

S1(config-vlan)# **name Native**

S1(config-vlan)# **end**

* + - 1. Cree las mismas VLAN en el S2.
      2. **Ejecute el comando show vlan brief** paraver la lista de VLAN en S1.

S1# **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

Gi0/1, Gi0/2

10 Operations active

20 Parking\_Lote activo

99 Management active

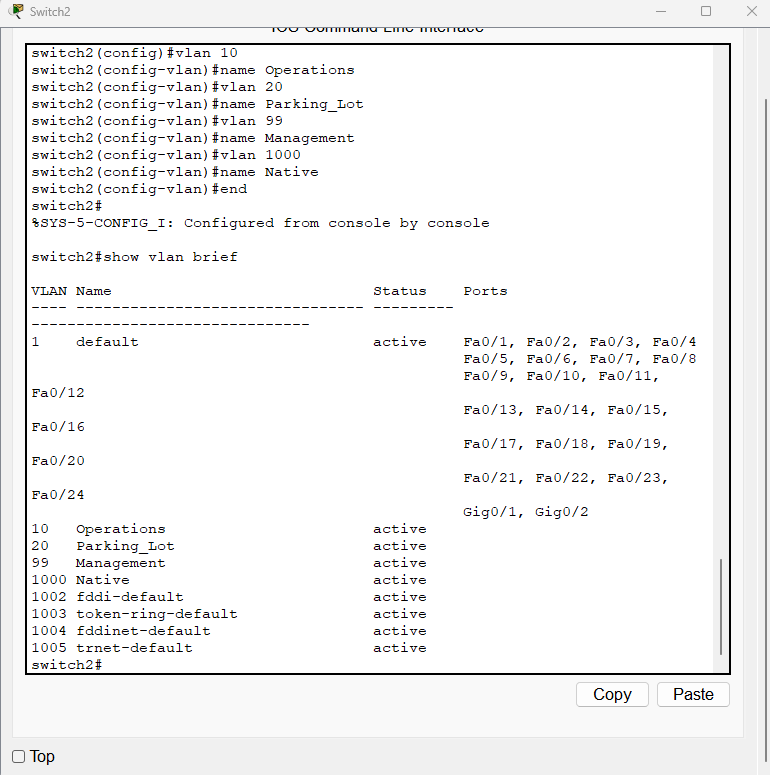
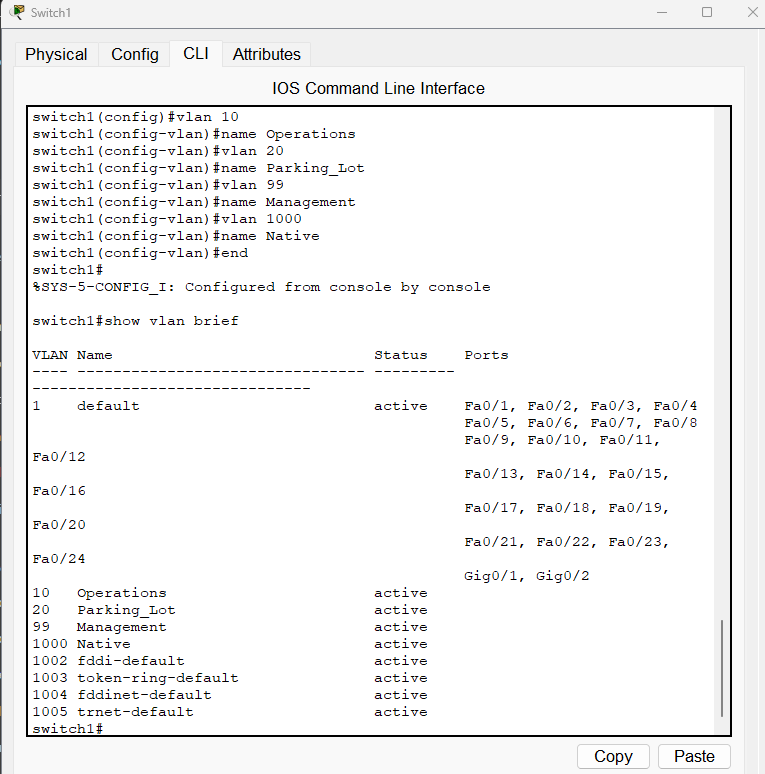
1000 Native active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup



#### Preguntas:

¿Cuál es la VLAN predeterminada? R// VLAN1

Escriba sus respuestas aquí.

¿Qué puertos se asignan a la VLAN predeterminada? R// Fa0/1 hasta Fa0/24 , Gig0/1 y Gig0/2

Escriba sus respuestas aquí.

### Asignar las VLAN a las interfaces del switch correctas

* + - 1. Asigne las VLAN a las interfaces en el S1.
         1. Asigne la PC-A a la VLAN Operation.

S1(config)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 10**

* + - * 1. Transfiera la dirección IP del switch a la VLAN 99.

S1(config)# **interface vlan 1**

S1(config-if)# **no ip address**

S1(config-if)# **interface vlan 99**

S1(config-if)# **ip address 192.168.1.11 255.255.255.0**

S1(config-if)# **end**

* + - 1. Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.
      2. Emita el comando **show ip interface brief**.

#### Pregunta:

¿Cuál es el estado de la VLAN 99? Explique.

R// La interfaz VLAN 99 está configurada con la dirección IP 192.168.1.11. El estado de la interfaz es "up", lo que significa que está activa desde el punto de vista de la capa 2 (enlace de datos). Sin embargo, el protocolo está "down", lo que indica que la capa 3 (red) no está operativa. Este estado "up/down" es común en interfaces VLAN y puede ocurrir por varias razones, No hay puertos activos asignados a esta VLAN. La VLAN 99 está configurada y activa (up) a nivel de switch, pero no está completamente operativa (down) a nivel de red.

riba susspuestas aquí.

* + - 1. Asigne PC-B a la VLAN de Operaciones en S2.
      2. Elimine la dirección IP para la VLAN 1 en el S2.
      3. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.
      4. Use el comando **show vlan brief** para verificar que las VLAN se hayan asignado a las interfaces correctas.

#### Preguntas:

¿Es posible hacer ping del S1 al S2? Explique.

R// no ya que ambos switches tienen configuradas direcciones IP en la VLAN 99 no hay una conexión física entre los switches que este configurada para llevar el tráfico de la VLAN99

¿Es posible hacer ping de la PC-A a la PC-B? Explique

R// no, aunque PC-A y PC-B están en la misma VLAN están conectadas a switches diferentes, no hay una conexión configurada entre los switches que permita que el trafico de la VLAN de operaciones pase entre ellos.

## Mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

En la parte 3, cambiará las asignaciones de VLAN a los puertos y eliminará las VLAN de la base de datos de VLAN.

### Asignar una VLAN a varias interfaces

Abrir la ventana de configuración

* + - 1. En el S1, asigne las interfaces F0/11 a 24 a la VLAN 99.

S1(config)# **interface range f0/11-24**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 99**

S1(config-if-range)# **end**

* + - 1. Ejecute el comando **show vlan brief** para verificar las asignaciones de VLAN.
      2. Reasigne F0/11 y F0/21 a la VLAN 20.
      3. Verifique que las asignaciones de VLAN sean las correctas.

### Eliminar una asignación de VLAN de una interfaz

* + - 1. Use el comando **no switchport access vlan** para eliminar la asignación de la VLAN 10 a F0/24.

S1(config)# **interface f0/24**

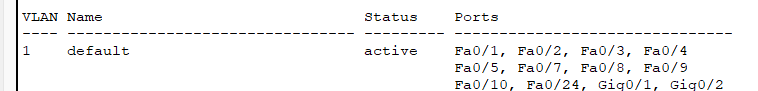
S1(config-if)# **no switchport access vlan**

S1(config-if)# **end**

* + - 1. Verifique que se haya realizado el cambio de VLAN.

#### Pregunta:

¿Con qué VLAN está asociado F0/24 ahora? R// default



### Eliminar una ID de VLAN de la base de datos de VLAN

* + - 1. Add VLAN 30 to interface F0/24 without issuing the global VLAN command.

S1(config)# **interface f0/24**

S1(config-if)# **switchport access vlan 30**

% Access VLAN does not exist. Creating vlan 30

**Nota**: La tecnología de switches actual ya no requiere la emisión del comando **vlan** para agregar una VLAN a la base de datos. Al asignar una VLAN desconocida a un puerto, la VLAN se agrega a la base de datos de VLAN.

* + - 1. Verifique que la nueva VLAN se muestre en la tabla de VLAN.

#### Pregunta:

¿Cuál es el nombre predeterminado de la VLAN 30?



* + - 1. Use el comando **no vlan 30** para eliminar la VLAN 30 de la base de datos de VLAN.

S1(config)# **no vlan 30**

S1(config)# **end**

* + - 1. Emita el comando **show vlan brief**. F0/24 se asignó a la VLAN 30.

#### Pregunta:

Una vez que se elimina la VLAN 30, ¿a qué VLAN se asigna el puerto F0/24? ¿Qué sucede con el tráfico destinado al host conectado a F0/24?

R// El puerto F0/24 se ha movido a un estado inactivo o suspendido, ya que no se reasigno automáticamente a otra VLAN. En cuanto al trafico destinado al host conectado a F0/24 este tráfico será descartado el switch no enviara ni recibirá tráfico a través de este puerto hasta que se la asigne una nueva VLAN valida.

Ejecute el comando **no switchport access vlan** en la interfaz F0/24.

S1(config)# **interface f0/24**

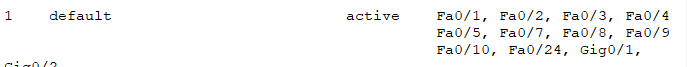
S1 (config-if) # **no switchport access vlan**

S1(config-if)# **end**

* + - 1. Ejecute el comando **show vlan brief** para determinar la asignación de VLAN para F0/24.

#### Preguntas:

¿A qué VLAN se asignó F0/24?



aquí.

**Nota**: Antes de eliminar una VLAN de la base de datos, se recomienda reasignar todos los puertos asignados a esa VLAN.

¿Por qué debe reasignar un puerto a otra VLAN antes de eliminar la VLAN de la base de datos de VLAN?

R// según referencias bibliográficas hacen mención que es una buena practica ya que las VLANs a menudo se utilizan para separar el trafico de diferentes grupos de usuarios o tipos de trafico por razones de seguridad, ya que si se elimina una VLAN sin primero reasignar sus puertos se podría accidentalmente exponer datos sensibles al permitir que el trafico se mezcle en una VLAN no segura o diferente.

## Configurar un enlace troncal 802.1Q entre los switches

En la parte 4, configurará la interfaz F0/1 para que use el protocolo de enlace troncal dinámico (DTP) y permitir que negocie el modo de enlace troncal. Después de lograr y verificar esto, desactivará DTP en la interfaz F0/1 y la configurará manualmente como enlace troncal.

### Usar DTP para iniciar el enlace troncal en F0/1

El modo de DTP predeterminado de un puerto en un switch 2960 es dinámico automático. Esto permite que la interfaz convierta el enlace en un enlace troncal si la interfaz vecina se establece en modo de enlace troncal o dinámico deseado.

Abrir la ventana de configuración

* + - 1. Establezca F0/1 en el S1 en modo de enlace troncal.

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode dynamic desirable**

Sep 19 02:51:47.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Sep 19 02:51:47.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

También debe recibir mensajes de estado de enlace en el S2.

S2#

Sep 19 02:42:19.424: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

Sep 19 02:42:21.454: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Sep 19 02:42:22.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

* + - 1. Emita el comando **show vlan brief** en el S1 y el S2. La interfaz F0/1 ya no está asignada a la VLAN 1. Las interfaces de enlace troncal no se incluyen en la tabla de VLAN.
      2. Emita el comando **show interfaces trunk** para ver las interfaces de enlace troncal. Observe que el modo en el S1 está establecido en deseado, y el modo en el S2 en automático.

S1# **show interfaces trunk**

S2# **show interfaces trunk**

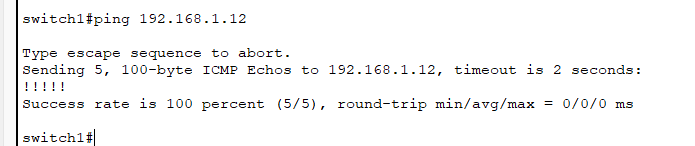
**Nota**: de manera predeterminada, todas las VLAN se permiten en un enlace troncal. El comando**switchport trunk** le permite controlar qué VLAN tienen acceso al enlace troncal. Para esta práctica de laboratorio, mantenga la configuración predeterminada que permite que todas las VLAN atraviesen F0/1.

Cerrar la ventana de configuración

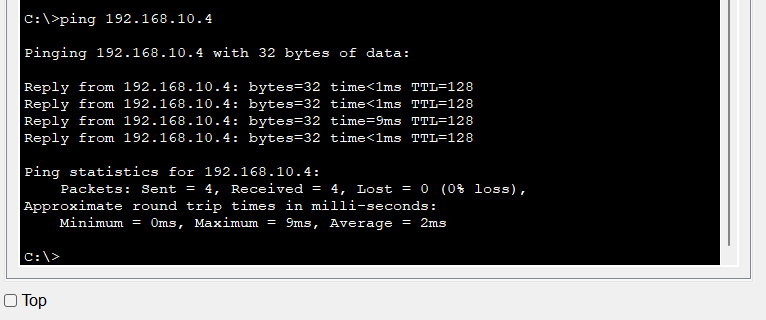
* + - 1. Verifique que el tráfico de VLAN se transfiera a través de la interfaz de enlace troncal F0/1.

#### Preguntas:

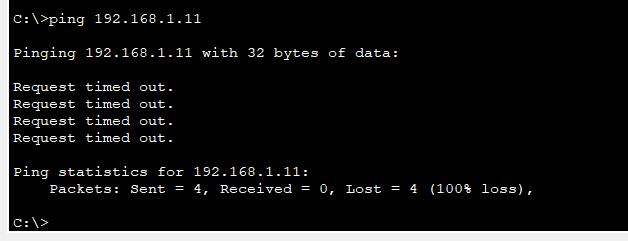
¿Se puede hacer ping del S1 al S2? R// SI



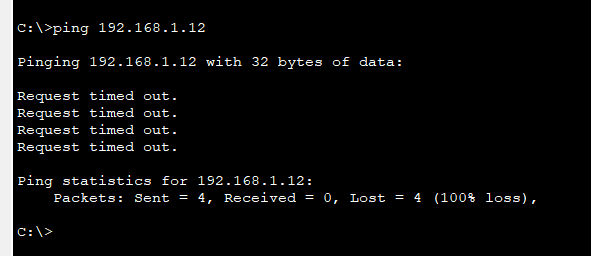
¿Se puede hacer ping de la PC-A a la PC-B? R// SI



¿Se puede hacer ping de la PC-A al S1? R// NO



¿Se puede hacer ping de la PC-B al S2? R// NO



Si la respuesta a cualquiera de las preguntas anteriores es no, justifíquela a continuación.

R// para las PC-A , PC-B a S1 y S2 las PC están en una VLAN que no tiene acceso a la VLAN de gestión de S1 o no hay un enrutamiento inter-VLAN para permitir la comunicación.

### Configurar manualmente la interfaz de enlace troncal F0/1

El comando **switchport mode trunk** se usa para configurar un puerto manualmente como enlace troncal. Este comando se debe emitir en ambos extremos del enlace.

* + - 1. Cambie el modo de switchport en la interfaz F0/1 para forzar el enlace troncal. Haga esto en ambos switches.

Abrir la ventana de configuración

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode trunk**

* + - 1. Ejecute el comando **show interfaces trunk** para ver el modo de enlace troncal. Observe que el modo cambió de **desirable** a **on**.

S2# **show interfaces trunk**

* + - 1. Modifique la configuración troncal en ambos switches cambiando la VLAN nativa de VLAN 1 a VLAN 1000.

S1(config)# **interface f0/1**

S1(config-if)# **switchport trunk native vlan 1000**

* + - 1. Use el comando show interfaces trunk para verificar la configuración de los enlaces troncales. Observe que se actualiza la información de VLAN nativa.

S2# **show interfaces trunk**

#### Preguntas:

¿Por qué desearía configurar una interfaz en modo de enlace troncal de forma manual en lugar de usar DTP?

R// por rendimiento DTP genera trafico adicional en la red. Aunque es mínimo, en entornos de alto rendimiento, eliminar este trafico puede ser beneficioso, también no todos los dispositivos soportan DTP, en cambio la configuración manual asegura un comportamiento consistente y predecible, especialmente en entornos de red complejos.

¿Por qué podría querer cambiar la VLAN nativa en un tronco?

R// la VLAN1 es la VLAN nativa por defecto y es bien conocida cambiarla puede dificultar ataques de VLAN hopping, también en diseños de red complejos, cambiar la VLAN nativa puede ayudar a cumplir con requisitos específicos de segmentación o diseño. En ciertas topologías, cambiar la VLAN nativa puede ayudar a prevenir loops de capa 2.

Cerrar la ventana de configuración

## Eliminar la base de datos de VLAN

En la parte 5, eliminará la base de datos de VLAN del switch. Es necesario hacer esto al inicializar un switch para que vuelva a la configuración predeterminada.

### Determinar si existe la base de datos de VLAN

Abrir la ventana de configuración

Emita el comando **show flash** para determinar si existe el archivo **vlan.dat** en la memoria flash.

S1# **show flash:**

**Nota**: Si hay un archivo **vlan.dat** en la memoria flash, la base de datos de VLAN no contiene la configuración predeterminada.

### Eliminar la base de datos de VLAN

* + - 1. Emita el comando **delete vlan.dat** para eliminar el archivo vlan.dat de la memoria flash y restablecer la base de datos de VLAN a la configuración predeterminada. Se le solicitará dos veces que confirme que desea eliminar el archivo vlan.dat. Presione Enter ambas veces.

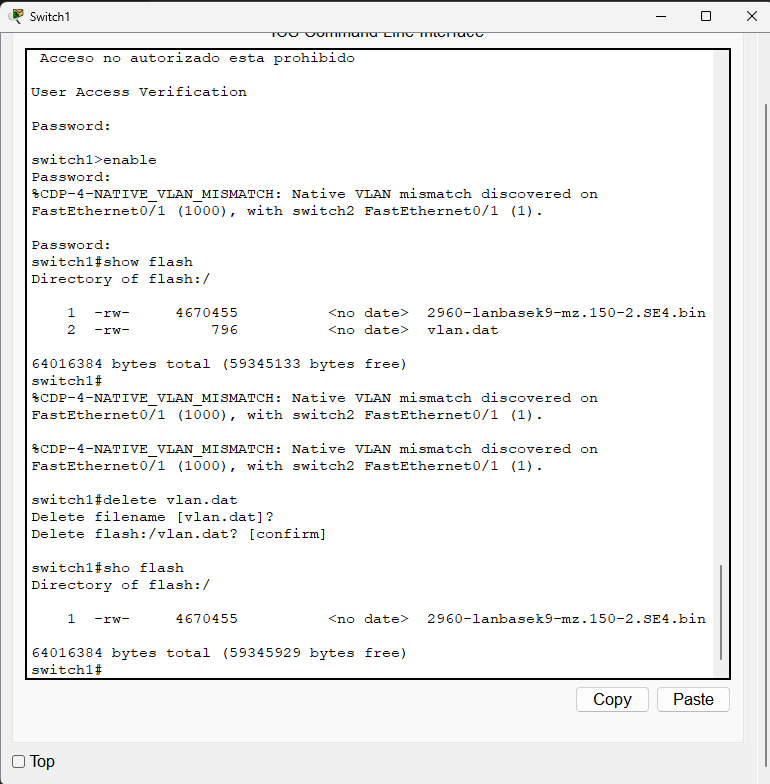
S1# **delete vlan.dat**

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

* + - 1. Emita el comando **show flash** para verificar que se haya eliminado el archivo vlan.dat.

S1# **show flash:**



#### Pregunta:

Para inicializar un switch para que vuelva a la configuración predeterminada, ¿cuáles son los otros comandos que se necesitan?

Switch# erase startup-config

Switch# delete vlan.dat

Switch# reload

# Preguntas de reflexión

* 1. ¿Qué se necesita para permitir que los hosts en la VLAN 10 se comuniquen con los hosts en la VLAN 99?

R// configurar rutas estáticas o un protocolo de enrutamiento dinámico para permitir la comunicación entre las subredes de las diferentes VLANs. Asegurarse de que los puertos troncales entre switches permitan el tráfico de ambas VLANs.

* 1. ¿Cuáles son algunos de los beneficios principales que una organización puede obtener mediante el uso eficaz de las VLAN?

R// las VLAN permiten agrupar lógicamente a los usuarios por función, departamento o uso de aplicación, independientemente de su ubicación física en la red. Esto simplifica las tareas administrativas como la configuración de la red y la solución de problemas. Limita el dominio de broadcast a la VLAN, mejorando el rendimiento de la red. Soporte para aplicaciones multimedia y sensibles a la latencia, permite la creación de VLANs dedicadas para voz o video. Ayuda a cumplir con regulaciones que requieren la separación de ciertos tipos de tráfico.