



PRÁCTICA 17. CONFIGURACIÓN DE VLAN. ENLACES TRONCALES.

Eric Serrano Marín

CONTENIDO

Topología	2
Tabla de asignación de direcciones	2
Objetivos.....	2
Aspectos básicos/situación	2
Instrucciones.....	3
Parte 1: Arme la red y configure los ajustes básicos de los dispositivos.....	3
Paso 1: Construya la red como se muestra en la topología.....	3
Paso 2: Configure los parámetros básicos para cada switch.....	4
Paso 3: Configurar los equipos host	7
Paso 4: Probar la conectividad	9
Parte 2: Crear redes VLAN y asignar puertos de switch.....	10
Paso 1: Crear las VLAN en los switches	10
Paso 2: Asignar las VLAN a las interfaces del switch correctas.....	12
Parte 3: Mantener las asignaciones de puertos de VLAN y la base de datos de VLAN.....	14
Paso 1: Asignar una VLAN a varias interfaces.....	14
Paso 2: Eliminar una asignación de VLAN de una interfaz	16
Paso 3: Eliminar una ID de VLAN de la base de datos de VLAN.....	16
Parte 4: Configurar un enlace troncal 802.1Q entre los switches.....	19
Paso 1: Usar DTP para iniciar el enlace troncal en F0/1	19
Paso 2: Configurar manualmente la interfaz de enlace troncal F0/1	22
Parte 5: Eliminar la base de datos de VLAN.....	24
Paso 1: Determinar si existe la base de datos de VLAN	24
Paso 2: Eliminar la base de datos de VLAN	25
Preguntas de reflexión	26

PACKET TRACER — CONFIGURAR VLAN Y ENLACES TRONCALES — MODO FÍSICO

TOPOLOGÍA

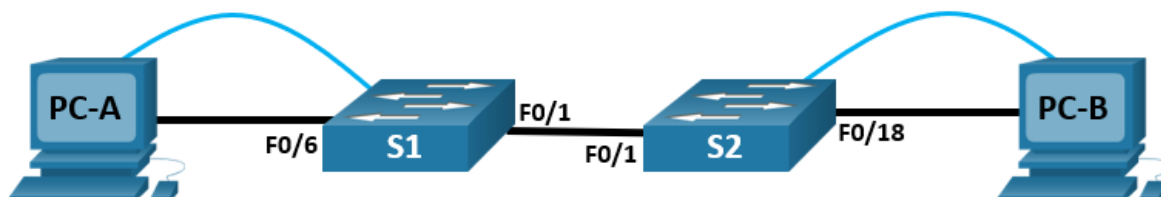


TABLA DE ASIGNACIÓN DE DIRECCIONES

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace predeterminada
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
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

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 actividad Packet Tracer Modo Físico (PTPM), creará VLAN en ambos switches de la topología, asignará VLAN a los puertos de acceso del switch, y verificará que las VLAN funcionan como se esperaba. A continuación, creará un troncal VLAN entre los dos conmutadores para permitir que los hosts de la misma VLAN se comuniquen a través del troncal, independientemente del conmutador al que esté conectado el host.

INSTRUCCIONES

PARTE 1: ARME LA RED Y CONFIGURE 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.

PASO 1: CONSTRUYA LA RED COMO SE MUESTRA EN LA TOPOLOGÍA.

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

- a. Haga clic y arrastre los conmutadores **S1** y **S2** al **Rack**.

Nota: Esta actividad se abrirá con un 37% de finalización porque los puertos del conmutador están todos apagados. Cuando instale los conmutadores en el rack, los puertos se activarán automáticamente. Después de aproximadamente un minuto, el puntaje caerá al 1%. Más adelante en la actividad, apagará los puertos no utilizados.

- b. Haga clic y arrastre tanto **PC-A** como **PC-B** a la **Mesa** y utilice el botón de encendido para encenderlos.
- c. Proporcione conectividad de red **conectando cables straight-through** (directos), como se muestra en la topología.
- d. Conecte el **cable de consola** del dispositivo **PC-A** a **S1** y del dispositivo **PC-B** a **S2**.



PASO 2: CONFIGURE LOS PARÁMETROS BÁSICOS PARA CADA SWITCH

- Desde la pestaña **Desktop** (Escritorio) de cada PC, utilice el **Terminal** para conectarse a la consola en cada conmutador y habilite el modo EXEC privilegiado.
- Ingresa al modo de configuración.
- Asigne un nombre de dispositivo al switch.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostna
Switch(config)#hostname S2
S2(config)#
```

```
S1(config)#hostname S1
S1(config)#
```

- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

```
S2(config)#enable secret class
S2(config)#
```

```
S1(config)#enable secret class
S1(config)#line console 0
```

- Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

```
S2(config)#line console 0
S2(config-line)#pass
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#
```

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

- Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

```
S2(config)#line vty 0 15
S2(config-line)#pass
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#
```

```
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
```

- g. Encripte las contraseñas de texto sin formato.

```
S2(config)#service password-encryption
S2(config)#

S1(config)#service password-encryption
S1(config)#
```

- h. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
S2(config)#banner motd $ Acceso no autorizado! $
S2(config)#

S1(config)#banner motd #Prohibido Acceso no Autorizado#
S1(config)#
```

- i. Configure la dirección IP que figura en la tabla de direcciones para VLAN 1 en el switch.

Nota: La dirección VLAN 1 no se evalúa porque la eliminará más adelante en la actividad. Sin embargo, necesitará VLAN 1 para probar la conectividad más adelante en esta parte.

```
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.12 255.255.255.0
S2(config-if)#no shu
S2(config-if)#no shutdown
S2(config-if)#
*Mar 1 00:51:24.558: %LINK-3-UPDOWN: Interface Vlan
*Mar 1 00:51:25.564: %LINEPROTO-5-UPDOWN: Line prot
d state to up
S2(config-if)#exit
S2(config)#

S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

- j. Apague todas las interfaces que no se utilizarán.

```
S2(config)#interface range f0/2-17, f0/19-24
S2(config-if-range)#shut
S2(config-if-range)#shutdown
S2(config-if-range)#
*Mar 1 00:55:05.698: %LINK-5-CHANGED: Interface FastEthernet0/2,
administratively down
*Mar 1 00:55:05.715: %LINK-5-CHANGED: Interface FastEthernet0/3,
administratively down
*Mar 1 00:55:06.009: %LINK-5-CHANGED: Interface FastEthernet0/24,
administratively down
S2(config-if-range)#exit
S2(config)#
```

```

S1(config)#interface range f0/2-5, f0/7-24
S1(config-if-range)#shutdown
S1(config-if-range)#
*Mar  1 00:14:35.795: %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down
*Mar  1 00:14:35.804: %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
administratively down
*Mar  1 00:14:35.804: %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to
administratively down
*Mar  1 00:14:35.812: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down
*Mar  1 00:14:35.812: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down
*Mar  1 00:14:35.820: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down
*Mar  1 00:14:35.820: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down
*Mar  1 00:14:35.829: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down
*Mar  1 00:14:35.829: %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down
*Mar  1 00:14:35.829: %LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down
*Mar  1 00:14:35.837: %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
*Mar  1 00:14:35.837: %LINK-5-CHANGED: Interface FastEthernet0/14, changed state to

```

```

S1(config)#interface range g0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#exit
S1(config)#

```

- k. Ajuste el reloj en cada conmutador.

Nota: La configuración del reloj no se puede clasificar en Packet Tracer.

```

S2#clock set 12:11:00 Jan 23 2023
S2#
*Jan 23 12:11:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:58:
31 UTC Mon Mar 1 1993 to 12:11:00 UTC Mon Jan 23 2023, configured from console by c
onsole.
S2#

```

```

S1#clock set 12:08:00 JAN 23 2023
S1#
*Jan 23 12:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:17
:36 UTC Mon Mar 1 1993 to 12:08:00 UTC Mon Jan 23 2023, configured from console by
console.

```

- I. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
0 bytes copied in 0.772 secs (0 bytes/sec)
S2#
```

En el S1 se ha repetido el mismo procedimiento

PASO 3: CONFIGURAR LOS EQUIPOS HOST

En la pestaña **Desktop** (Escritorio) de cada **PC**, haga clic en Configuración IP e introduzca la información de direccionamiento tal como se muestra en la tabla de direcciones.

PC-B

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

☐ Obtener una dirección IP automáticamente

☒ Usar la siguiente dirección IP:

Dirección IP:	192 . 168 . 10 . 4
Máscara de subred:	255 . 255 . 255 . 0
Puerta de enlace predeterminada:	192 . 168 . 10 . 1

☐ Obtener la dirección del servidor DNS automáticamente

☒ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:	. . .
Servidor DNS alternativo:	. . .

☐ Validar configuración al salir

Opciones avanzadas...

PC-A

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4) X

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

☐ Obtener una dirección IP automáticamente

☒ Usar la siguiente dirección IP:

Dirección IP: 192 . 168 . 10 . 3

Máscara de subred: 255 . 255 . 255 . 0

Puerta de enlace predeterminada: 192 . 168 . 10 . 1

☐ Obtener la dirección del servidor DNS automáticamente

☒ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: . . .

Servidor DNS alternativo: . . .

☒ Validar configuración al salir: Opciones avanzadas...

Aceptar Cancelar

PASO 4: PROBAR LA CONECTIVIDAD

Pruebe la conectividad de red intentando hacer ping entre cada uno de los dispositivos cableados.

PREGUNTAS:

¿Se puede hacer ping de la **PC-A** a la **PC-B**? Sí.

```
C:\Users\cire7>ping 192.168.10.4

Haciendo ping a 192.168.10.4 con 32 bytes de datos:
Respuesta desde 192.168.10.4: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.4: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.4: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.4: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.10.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

¿Se puede hacer ping de la **PC-A** a **S1**? No.

```
C:\Users\cire7>ping 192.168.1.11

Haciendo ping a 192.168.1.11 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.1.11:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

¿Se puede hacer ping de la **PC-B** a **S2**? No.

```
C:\Users\Raúl Campos>ping 192.168.1.12

Haciendo ping a 192.168.1.12 con 32 bytes de datos:
Respuesta desde 192.168.10.4: Host de destino inaccesible.
Respuesta desde 192.168.10.4: Host de destino inaccesible.
Respuesta desde 192.168.10.4: Host de destino inaccesible.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.1.12:
    Paquetes: enviados = 4, recibidos = 3, perdidos = 1
    (25% perdidos),

C:\Users\Raúl Campos>
```

¿Se puede hacer ping de S1 a S2?

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms  
S1#ping 192.168.1.11
```

S2 a S1

```
S2#ping 192.168.1.11  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms  
S2#
```

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

Los pings nos han fallado cuando hemos intentado hacer ping entre PC y Switch por el simple hecho de que estamos haciendo ping a una red diferente, si quisiésemos que estos pings funcionasen deberíamos poner una puerta de enlace predeterminada para enlazar el tráfico de una red a otra.

PARTE 2: CREAR REDES VLAN Y ASIGNAR PUERTOS DE SWITCH

En la parte 2, creará las VLANs **Management**, **Operations**, **Parking_Lot**, and **Native** en ambos conmutadores. A continuación, asignará las VLAN a la interfaz correspondiente. El comando **show VLAN** se usa para verificar las opciones de configuración.

PASO 1: CREAR LAS VLAN EN LOS SWITCHES

En la pestaña **Escritorio** de cada **PC**, utilice Terminal para continuar configurando ambos conmutadores de red.

a. Cree las VLAN en S1.

```
S1(config)#vlan 10  
S1(config-vlan)#name Operations  
S1(config-vlan)#exit  
S1(config)#vlan 20  
S1(config-vlan)#name Parking_Lot  
S1(config-vlan)#exit  
S1(config)#vlan 99  
S1(config-vlan)#name Management  
S1(config-vlan)#exit  
S1(config)#vlan 1000  
S1(config-vlan)#name Native  
S1(config-vlan)#end
```

- b. Cree las mismas VLAN en el S2.

```
S2(config)#vlan 10
S2(config-vlan)#name Operations
S2(config-vlan)#exit
S2(config)#vlan 20
S2(config-vlan)#name Parking_Lot
S2(config-vlan)#exit
S2(config)#vlan 99
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#vlan 1000
S2(config-vlan)#name Native
S2(config-vlan)#end
S2#
```

- c. Ejecute el comando **show VLAN brief** para ver la lista de VLANs en S1.

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Gi0/1, Gi0/2
10	Operations	active	Fa0/6
20	Parking_Lot	active	Fa0/11, Fa0/21
99	Management	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23, Fa0/24
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?

La VLAN predeterminada es la 1

¿Qué puertos se asignan a la VLAN predeterminada?

Se le asignan todos los puertos que no han sido cambiados a otra VLAN manualmente.

PASO 2: ASIGNAR LAS VLAN A LAS INTERFACES DEL SWITCH CORRECTAS

- a. Asigne las VLAN a las interfaces en **S1**.

- 1) Asigne la PC-A a la VLAN Operation.

```
S1(config)#interface vlan 1
S1(config-if)#exit
S1(config)#interface f0/6
S1(config-if)#sw
S1(config-if)#switchport mode
S1(config-if)#switchport mode acc
S1(config-if)#switchport mode access
S1(config-if)#sw
S1(config-if)#switchport acce
S1(config-if)#switchport access vlan 10
```

- 2) Desde la VLAN 1, quite la dirección IP de administración y configúrela en VLAN 99.

```
S1(config)#interface vlan 1
S1(config-if)#no ip address
S1(config-if)#inter
S1(config-if)#exit
S1(config)#inter
S1(config)#interface vlan 99
S1(config-if)#ip address
Jan 23 12:39:30.590: %LINEPROTO-5-UPDOWN: Line protocol is down
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#end
```

- b. Emita el comando **show VLAN brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/24, Gi0/1, Gi0/2
10	Operations	active	Fa0/6
20	Parking_Lot	active	Fa0/11, Fa0/21
99	Management	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
1000	Native	active	
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdiinet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Emita el comando **show ip interface brief**.

```
S1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	manual	up	up
Vlan99	192.168.1.11	YES	manual	up	down
FastEthernet0/1	unassigned	YES	unset	up	up

PREGUNTA:

¿Cuál es el estado de la VLAN 99?

Tal y como podemos observar el Status está up (porque existe en la base de datos), pero el protocolo down, ya que todavía no le hemos asignado ningún puerto activo.

- d. Asigne **PC-B** a la VLAN **Operations** en **S2**.

```
S2(config)#interface f0/18
S2(config-if)#swi
S2(config-if)#switchport mode ac
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#
```

- e. Desde la VLAN 1, quite la dirección IP de administración y configúrela en la VLAN 99 de acuerdo con la tabla de direcciones.

```
S2(config)#interface vlan 99
S2(config-if)#ip add
S2(config-if)#ip address 192.168.1.12 255.255.255.0
S2(config-if)#exit
S2(config)#
```

- f. Use el comando **show VLAN brief** para verificar que las VLAN se hayan asignado a las interfaces correctas.

```
S2#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, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10	Operations	active	Fa0/18
20	Parking_Lot	active	
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	

```
S2#
```

PREGUNTAS:

¿Puede S1 hacer ping a S2? Sí, ya que ambos están en la misma VLAN.

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
S1#ping 192.168.1.11
```

¿Puede PC-A hacer ping a PC-B? No, ya que PC1 está en la F0/6 que está en VLAN1 y PC2 está en F0/18 que está en VLAN 10.

```
C:\Users\cire7>ping 192.168.10.4

Haciendo ping a 192.168.10.4 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.10.3: Host de destino inaccesible.
Respuesta desde 192.168.10.3: Host de destino inaccesible.

Estadísticas de ping para 192.168.10.4:
    Paquetes: enviados = 4, recibidos = 2, perdidos = 2
              (50% perdidos),
```

PARTE 3: 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.

PASO 1: ASIGNAR UNA VLAN A VARIAS INTERFACES

En la pestaña **Escritorio** de cada **PC**, utilice **Terminal** para continuar configurando ambos conmutadores de red.

- a. En **S1**, asigne las interfaces F0/11 – 24 a VLAN99.

```
S1(config)#interface range f0/11-24
S1(config-if-range)#sw
S1(config-if-range)#switchport mode
S1(config-if-range)#switchport mode a
S1(config-if-range)#switchport mode access
S1(config-if-range)#sw
S1(config-if-range)#switchport ac
S1(config-if-range)#switchport access vlan 99
S1(config-if-range)#end
```

- b. Ejecute el comando **show VLAN brief** para verificar las asignaciones de VLAN.

```
S1#show vlan
Jan 23 13:12:52.683: %SYS-5-CONFIG_I: Configured from console by cons

VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/24, Gi0/1, Gi0/2
10   Operations              active    Fa0/6
20   Parking_Lot             active    Fa0/11, Fa0/21
99   Management               active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/22, Fa0/23
1000 Native                active
1002 fddi-default           act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Transl Trans2
-----
1    enet     100001    1500  -      -      -      -      -      0      0
10   enet     100010    1500  -      -      -      -      -      0      0
20   enet     100020    1500  -      -      -      -      -      0      0
99   enet     100099    1500  -      -      -      -      -      0      0
1000 enet     101000    1500  -      -      -      -      -      0      0
```

- c. Reasigne F0/11 y F0/21 a la VLAN 20.

```
S1(config)#interface f0/11
S1(config-if)#sw
S1(config-if)#switchport acc
S1(config-if)#switchport access vlan 20
S1(config-if)#exit
S1(config)#exit
```

```
S1(config)#interface f0/21
S1(config-if)#sw
S1(config-if)#switchport acc
S1(config-if)#switchport access 20
```

- d. Verifique que las asignaciones de VLAN sean las correctas.

```
S1#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/24, Gi0/1, Gi0/2
10   Operations              active    Fa0/6
20   Parking_Lot             active    Fa0/11, Fa0/21
99   Management               active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/22, Fa0/23
1000 Native                active
1002 fddi-default           act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup
```


PASO 2: ELIMINAR UNA ASIGNACIÓN DE VLAN DE UNA INTERFAZ

- a. 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 sw
S1(config-if)#no switchport acc
S1(config-if)#no switchport access vlan
S1(config-if)#end
```

- b. Verifique que se haya realizado el cambio de VLAN.

```
S1#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/24, Gi0/1, Gi0/2
10   Operations              active    Fa0/6
20   Parking_Lot             active    Fa0/11, Fa0/21
99   Management               active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/22, Fa0/23
1000 Native                active
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup
```

PREGUNTA:

¿Con qué VLAN está asociado F0/24 ahora?

Con la VLAN 1, que es la VLAN default.

PASO 3: ELIMINAR UNA ID DE VLAN DE LA BASE DE DATOS DE VLAN

- a. 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
```

```
S1(config)#interface f0/24
S1(config-if)#sw
S1(config-if)#switchport acc
S1(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
S1(config-if)#exit
```

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.

- b. Verifique que la nueva VLAN se muestre en la tabla de VLAN.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Gi0/1, Gi0/2
10	Operations	active	Fa0/6
20	Parking_Lot	active	Fa0/11, Fa0/21
30	VLAN0030	active	Fa0/24
99	Management	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
1000	Native	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

PREGUNTA:

¿Cuál es el nombre predeterminado de la VLAN 30?

Se llama VLAN0030.

- c. 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
```

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

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Gi0/1, Gi0/2
10	Operations	active	Fa0/6
20	Parking_Lot	active	Fa0/11, Fa0/21
99	Management	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
1000	Native	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Int 0/24 no aparece

PREGUNTA:

Después de eliminar la VLAN 30 de la base de datos VLAN, ¿por qué F0/24 ya no se muestra en la salida del comando `show VLAN brief`? ¿A qué VLAN está asignado el puerto F0/24 ahora? ¿Qué sucede con el tráfico destinado al host que está conectado a F0/24?

F0/24 ya no se muestra porque hemos eliminado la VLAN a la que pertenecía y esto hace que quede inactiva. Lo que pasa es que la interfaz sigue estando enlazada con esa VLAN, pero esta está inactiva porque ya no existe en la base de datos.

- e. Ejecute el comando **no switchport access VLAN** en la interfaz F0/24.

```
S1(config)#interface f0/24
S1(config-if)#no sw
S1(config-if)#no switchport acc
S1(config-if)#no switchport access vlan
S1(config-if)#end
```

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

```
S1#show vlan
Jan 23 13:12:52.683: %SYS-5-CONFIG_I: Configured from console by cons
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/24, Gi0/1, Gi0/2
10 Operations	active	Fa0/6
20 Parking_Lot	active	Fa0/11, Fa0/21
99 Management	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
1000 Native	active	

PREGUNTAS:

¿A qué VLAN se asignó F0/24?

Se asignó automáticamente a la VLAN 1.

```
S1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/14, Gi0/1, Gi0/2
10 Operations	active	Fa0/6
20 Parking_Lot	active	Fa0/11, Fa0/21
99 Management	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
1000 Native	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

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?

Es básicamente por lo mismo que hemos experimentado en la práctica con la F0/24. Cuando asignas una interfaz a una VLAN y esta se elimina de la base de datos, la interfaz no va a estar disponible para usar hasta que se vuelva a asignar a otra VLAN. Y como hemos visto también en la práctica, cuando hemos eliminado la VLAN 30 no nos aparecía la interfaz en el listado de puertos lo que puede complicar las cosas.

PARTE 4: 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.

PASO 1: 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.

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

```
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport mod
S1(config-if)#switchport mode dy
S1(config-if)#switchport mode dynamic de
S1(config-if)#switchport mode dynamic desirable
S1(config-if)#
Jan 23 13:11:40.574: %LINEPROTO-5-UPDOWN: Line p
ed state to down
Jan 23 13:11:41.564: %LINEPROTO-5-UPDOWN: Line p
0/1, changed state to down
Jan 23 13:11:44.592: %LINEPROTO-5-UPDOWN: Line p
0/1, changed state to up
```

- b. En **S1** y **S2**, emita el comando **show VLAN brief**. 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.

```
S2#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, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10	Operations	active	Fa0/18
20	Parking_Lot	active	
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	

```
S2#
```

```
S1#show vlan
```

```
Jan 23 13:12:52.683: %SYS-5-CONFIG_I: Configured from console by cons
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/24, Gi0/1, Gi0/2
10	Operations	active	Fa0/6
20	Parking_Lot	active	Fa0/11, Fa0/21
99	Management	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23

- c. 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

```
S1#show interfaces trunk

Port        Mode           Encapsulation  Status        Native vlan
Fa0/1       desirable      802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99,1000

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99,1000
```

S2# show interfaces trunk

```
S2#show interfaces trunk

Port        Mode           Encapsulation  Status        Native vlan
Fa0/1       auto           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99,1000

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99,1000
S2#
```

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 actividad, mantenga la configuración predeterminada. Esto permite que todas las VLAN atraviesen F0/1.

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

PREGUNTAS:

¿Puede S1 hacer ping a S2? Sí

```
S1#ping 192.168.1.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

¿Se puede hacer ping de la PC-A a la PC-B? Sí

```
C:\Users\cire7>ping 192.168.10.4

Haciendo ping a 192.168.10.4 con 32 bytes de datos:
Respuesta desde 192.168.10.4: bytes=32 tiempo=488ms TTL=128
Respuesta desde 192.168.10.4: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.10.4: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.4: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.10.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 488ms, Media = 122ms
```

¿Puede PC-A ping S1?

No.

¿Se puede hacer ping de la PC-B ping S2?

No.

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

No podemos hacer ping entre PC y Switches porque están en distinta VLAN. En este caso práctico nuestros PCs están en la VLAN 10, y los switches en la VLAN 99

PASO 2: 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.

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

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

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

```
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport mode trunk
```

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

S1# **show interfaces trunk**

```
S1#show interfaces trunk

Port      Mode           Encapsulation  Status        Native vlan
Fa0/1     on             802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-4094

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,99,1000

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,99,1000

S1#delete vlan.dat
```

- c. 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**

```
S2(config)#interface f0/1
S2(config-if)#swi
S2(config-if)#switchport trunk
Jan 23 13:32:02.867: %CDP-4-NATIVE_VLAN_MISMATCH
% Incomplete command.

S2(config-if)#switchport trunk native vlan 1000
S2(config-if)#end
```

```
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport trunk
S1(config-if)#switchport trunk native
S1(config-if)#switchport trunk native vlan 1000
```


- d. 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

```
S2#show interfaces trunk

Port        Mode           Encapsulation  Status        Native vlan
Fa0/1       on             802.1q         trunking      1000

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99,1000

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,99
S2#
```

PREGUNTAS:

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

Porque no todos los equipos tienen DTP y usándolo sabemos que el puerto se va a convertir en un enlace troncal aunque uno de los dos equipos no tenga DTP.

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

Por motivos de seguridad, ya que todo el tráfico pasaría por la VLAN 1, ya que es la predeterminada. Y al ser la configuración predeterminada la información podría verse expuesta.

PARTE 5: 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.

PASO 1: DETERMINAR SI EXISTE LA BASE DE DATOS DE VLAN

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

S1# show flash:

```
COM5 - PuTTY
anged state to up
*Mar 1 00:01:15.732: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, ch
anged state to upProhibido Acceso no Autorizado

User Access Verification

Password:
S1>ena
Password:
S1#show flash

Directory of flash:/

 2  -rwx    796  Jan 23 2023 13:00:20 +00:00  vlan.dat
 4  -rwx    2311  Mar 1 1993 00:00:39 +00:00  config.text
 5  -rwx    3096  Mar 1 1993 00:00:56 +00:00  multiple-fs
 6  -rwx   11660773  Mar 25 2014 15:34:23 +00:00  c2960-lanbasek9-mz.122-58.
SE2.bin
 7  drwx     192  Mar 1 1993 00:07:15 +00:00  c2960-lanbasek9-mz.122-50.
SE5
562  -rwx    1919  Mar 1 1993 00:00:59 +00:00  private-config.text

32514048 bytes total (9290752 bytes free)
S1#
```

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

PASO 2: ELIMINAR LA BASE DE DATOS DE VLAN

- 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

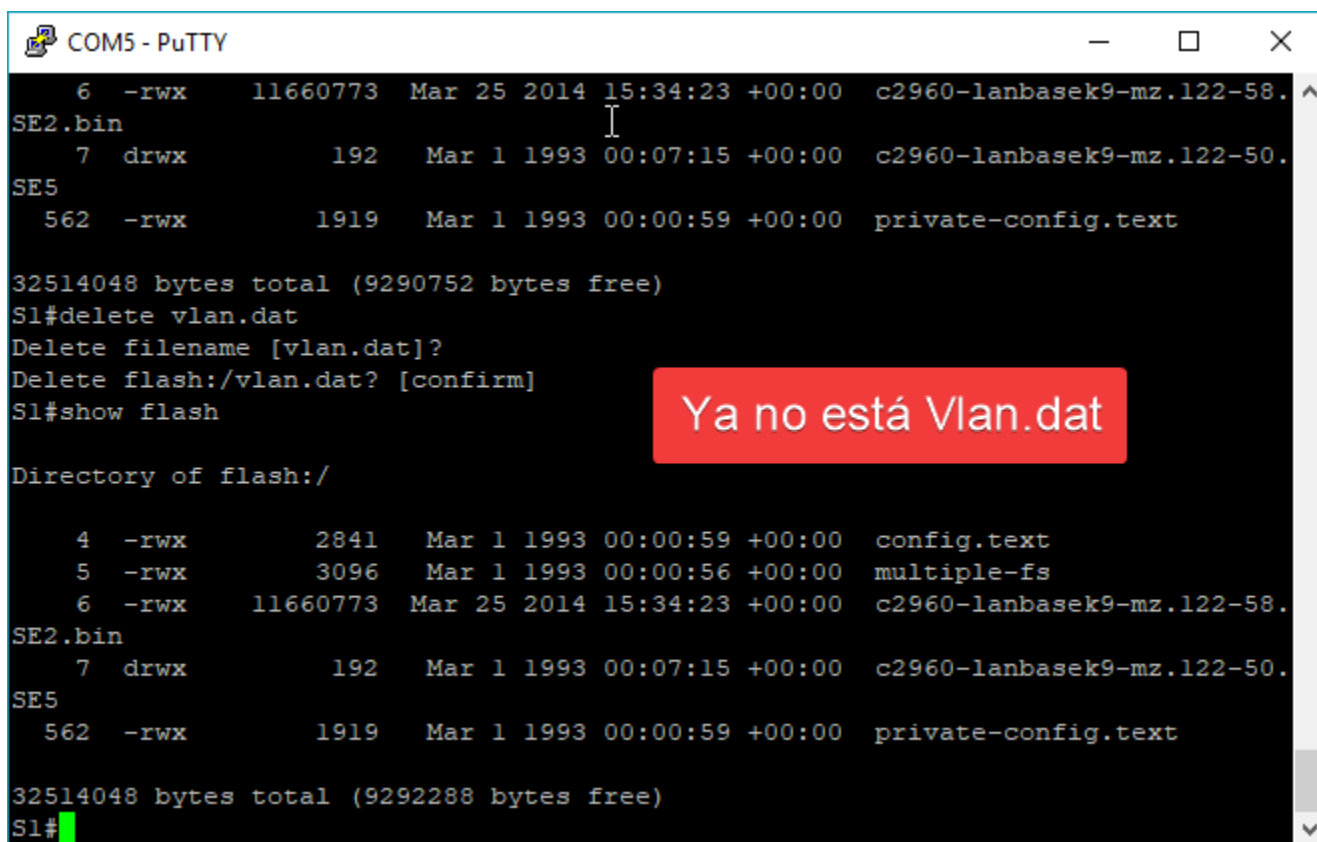
Delete filename [VLAN.dat]?

Delete flash:/VLAN.dat? [confirm]

```
S1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

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

S1# show flash:



The screenshot shows a PuTTY terminal window titled 'COM5 - PuTTY'. The terminal output is as follows:

```

6 -rwx 11660773 Mar 25 2014 15:34:23 +00:00 c2960-lanbasek9-mz.122-58.
SE2.bin
7 drwx 192 Mar 1 1993 00:07:15 +00:00 c2960-lanbasek9-mz.122-50.
SE5
562 -rwx 1919 Mar 1 1993 00:00:59 +00:00 private-config.text

32514048 bytes total (9290752 bytes free)
S1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#show flash

Directory of flash:/

4 -rwx 2841 Mar 1 1993 00:00:59 +00:00 config.text
5 -rwx 3096 Mar 1 1993 00:00:56 +00:00 multiple-fs
6 -rwx 11660773 Mar 25 2014 15:34:23 +00:00 c2960-lanbasek9-mz.122-58.
SE2.bin
7 drwx 192 Mar 1 1993 00:07:15 +00:00 c2960-lanbasek9-mz.122-50.
SE5
562 -rwx 1919 Mar 1 1993 00:00:59 +00:00 private-config.text

32514048 bytes total (9292288 bytes free)
S1#
```

A red callout box with the text "Ya no está Vlan.dat" is overlaid on the terminal output, indicating that the file has been successfully deleted.

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

Para ello se reiniciaría el router usando -> erase startup-config y después reiniciando usando 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?

Con la utilización de un router podríamos comunicar ambas VLAN. Simplemente usaríamos los conocimientos de enrutamiento, lo cual ya hemos aprendido.

2. ¿Cuáles son algunos de los beneficios principales que una organización puede obtener mediante el uso eficaz de las VLAN?
 - ✓ **Mayor seguridad**, ya que permiten segmentar la red, lo que ayuda a limitar el acceso no autorizado y a reducir el riesgo de propagación de ataques informáticos.
 - ✓ **Mayor rendimiento**: Al segmentar la red, se reduce el tráfico no deseado.
 - ✓ **Mayor flexibilidad**: Facilita la agregación de nuevos dispositivos y la modificación de las configuraciones de red.
 - ✓ **Mayor escalabilidad**: Al segmentar la red se pueden agregar nuevos dispositivos sin afectar al rendimiento de la red y se pueden crear nuevas VLAN para adaptarse a las necesidades en caso de que cambien.
 - ✓ **Mayor eficiencia**: Las VLAN permiten una mejor utilización de los recursos de red, ya que se pueden asignar diferentes prioridades a diferentes tipos de tráfico.