UNIVERSIDAD CATÓLICA DE SANTA MARÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SESIÓN 03:

Configuración de VLAN

I
OBJETIVOS

- Configurar VLAN en un switch
- Configurar un enlace troncal entre los switches
- Verificar la configuración de VLAN y enlaces troncales
- Implementar seguridad de VLAN

II
TEMAS A TRATAR

- VLAN
- Beneficios de las redes VLAN
- Rangos de VLAN
- Tipos de VLAN
- VLAN de Voz
- Enlaces troncales de la VLAN
- Configuración de VLAN
- Eliminación de una VLAN
- Configuración de enlaces troncales
- Verificación de configuración de VLAN

III
MARCO TEORICO

Los switches LAN se pueden dividir en grupos de puertos llamados “VLAN” para mejorar el rendimiento, la administración y seguridad de la red.

Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red dé soporte a los objetivos de una organización.

VLAN

Una VLAN permite que un administrador de red cree grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN.

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. En el switch deben darse de alta las VLANs y cada puerto asignarse a la VLAN correspondiente. Un puerto de switch con una VLAN singular configurada en el mismo se denomina puerto de acceso.

Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch).

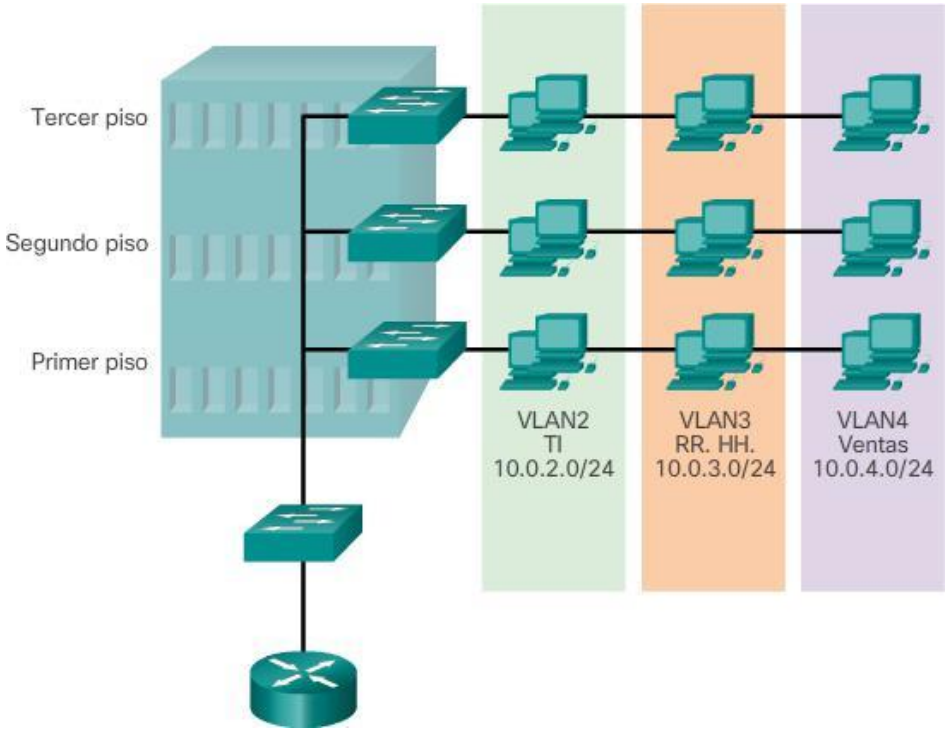


Figura 1: VLAN

BENEFICIOS DE LAS REDES VLAN

Los principales beneficios de las VLAN son:

Seguridad: Los grupos que tienen datos sensibles se separan del resto de la red, lo que disminuye las posibilidades de que ocurran violaciones de información confidencial.

Reducción de costos: El ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.

Mejor rendimiento: La división de las redes planas de capa 2 en varios grupos de trabajo lógicos (dominios de difusión) reduce el tráfico innecesario en la red y mejora el rendimiento.
Dominios de difusión reducidos: La división de una red en redes VLAN reduce la cantidad de dispositivos en el dominio de difusión.

Mayor eficiencia del personal de TI: Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando se dispone de un switch nuevo, se implementan todas las políticas y los procedimientos que ya se configuraron para la VLAN específica cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre.

Administración más simple de aplicaciones y proyectos: Las VLAN agregan dispositivos de red y usuarios para admitir los requisitos geográficos o comerciales. Al tener características diferentes, se facilita la administración de un proyecto o el trabajo

con una aplicación especializada; un ejemplo de este tipo de aplicación es una plataforma de desarrollo de aprendizaje por medios electrónicos para el cuerpo docente.

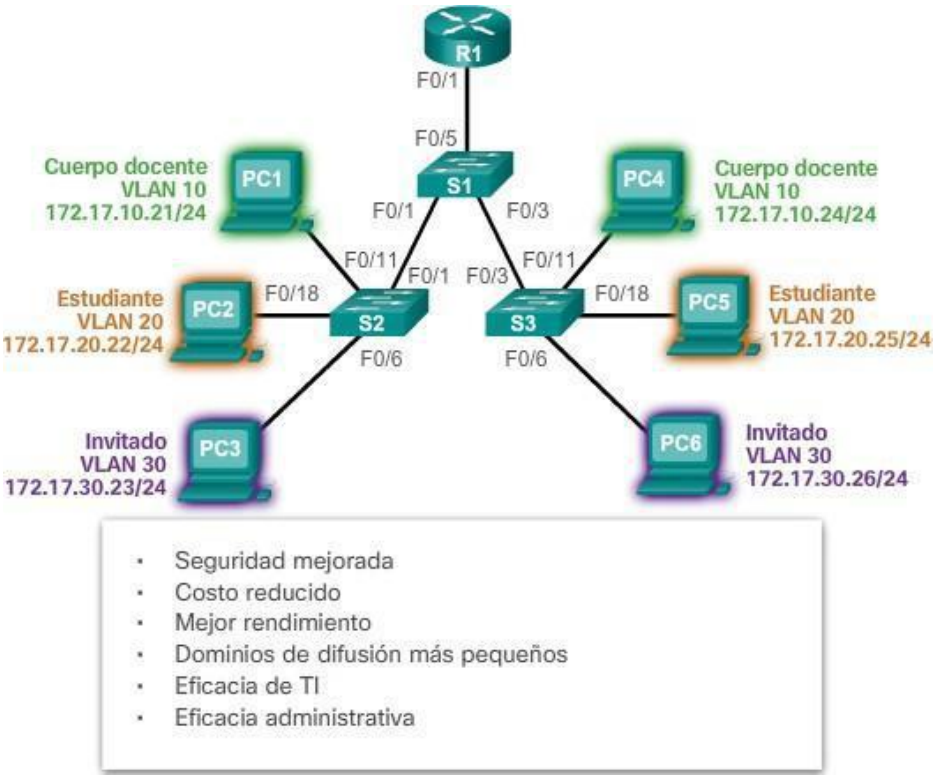


Figura 2: Beneficios de las redes VLAN

RANGOS DE VLAN

Los rangos de VLAN normal son:

Se identifica mediante un ID de VLAN entre 1 y 1005.
Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI
Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar.

Las configuraciones se almacenan dentro de un archivo de datos de la VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.
El protocolo de enlace troncal de la VLAN (VTP), que ayuda a gestionar las configuraciones de la VLAN entre los switches, sólo puede asimilar las VLAN de rango normal y las almacena en el archivo de base de datos de la VLAN

TIPOS DE VLAN

VLAN de datos

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos.

VLAN predeterminadas

Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast.

La VLAN predeterminada para los switches Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

VLAN Nativa

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa.

El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN. De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio conmutado.

VLAN administración

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada. Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP. Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.

En el pasado, la VLAN de administración para los switches 2960 era la única SVI activa. En las versiones 15.x de IOS de Cisco para los switches de la serie Catalyst 2960, es posible tener más de una SVI activa. Con IOS de Cisco 15.x, se debe registrar la SVI activa específica asignada para la administración remota. Si bien, en teoría, un switch puede tener más de una VLAN de administración, esto aumenta la exposición a los ataques de red.

VLAN de voz

Se necesita una VLAN separada para admitir la tecnología de voz sobre IP (VoIP). El tráfico de VoIP requiere:

Ancho de banda garantizado para asegurar la calidad de la voz Prioridad de la transmisión sobre los tipos de tráfico de la red Capacidad para ser enrutado en áreas congestionadas de la red Una demora inferior a 150 ms a través de la red

ENLACES TRONCALES DE LA VLAN

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red, no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

Las VLAN no serían muy útiles sin los enlaces troncales de VLAN. Los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router.

En la Figura 3, los enlaces entre los switches S1 y S2, y S1 y S3 se configuraron para transmitir el tráfico proveniente de las VLAN 10, 20, 30 y 99 a través de la red. Esta red no podría funcionar sin los enlaces troncales de VLAN.

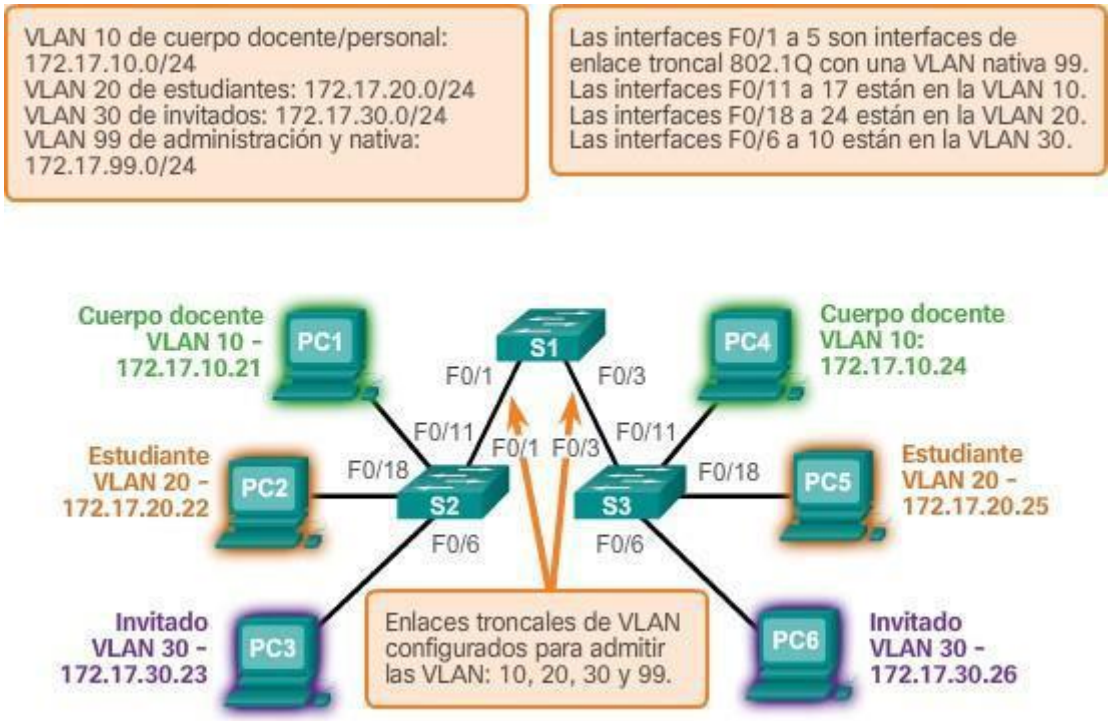


Figura 3: Enlaces troncales de la VLAN

CONFIGURACION DE VLAN

Al configurar redes VLAN de rango normal, los detalles de configuración se almacenan en la memoria flash del switch en un archivo denominado vlan.dat. La memoria flash es persistente y no requiere el comando **copy running-config startup-config**. Sin embargo, debido a que en los switches Cisco se suelen configurar otros detalles al mismo tiempo que se crean las VLAN, es aconsejable guardar los cambios a la configuración en ejecución en la configuración de inicio.

Creación de una VLAN

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	`S1# configure terminal`
Cree una VLAN con un número de ID válido.	`S1(config)#vlan id-vlan`
Especifique un nombre único para identificar la VLAN.	`S1(config-vlan)#name nombre-vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-vlan)# end`

Ejemplo:

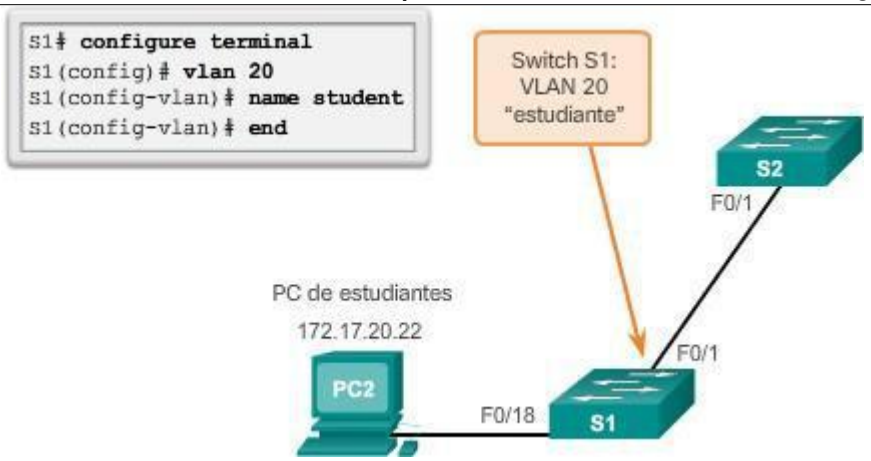


Figura 4: Ejemplo de Configuración

Utilice el comando **show vlan brief** para mostrar el contenido del archivo vlan.dat.
Se puede introducir una serie de ID de VLAN separadas por comas o un rango de ID de VLAN separado por guiones con el comando **vlan** *id-vlan*.

S1(config)# **vlan 100,102,105-107**

Asignación de puertos a las redes VLAN

Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. Un puerto de acceso puede pertenecer a una sola VLAN por vez; una excepción a esta regla es un puerto conectado a un teléfono IP, en cuyo caso, hay dos VLAN asociadas al puerto: una para voz y otra para datos.

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	S1# configure terminal
Ingrese al modo de configuración de interfaz para la SVI.	S1(config)# interface *id_interfaz*
Establezca el puerto en modo de acceso.	S1(config-if)# switchport mode access
Asigne el puerto a una VLAN.	S1(config-if)# switchport access vlan *id_vlan*
Vuelva al modo EXEC privilegiado.	S1(config-if)# end

Ejemplo:

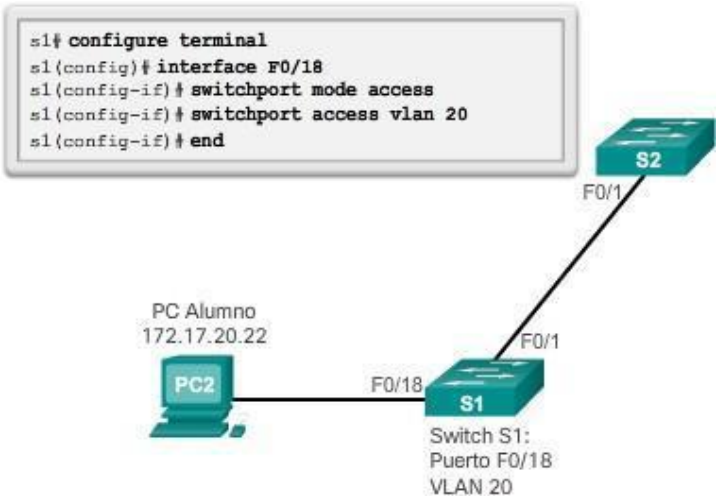


Figura 5: Asignación de puertos a las redes VLAN

- Asignación de un rango de puertos: Ej. Los puertos FastEthernet 0/1 al FastEthernet 0/5 los asignamos a la VLAN 3

  Switch (config) #interface range fastEthernet 0/1 - 5
  Switch (config-if-range) #switchport mode access
  Switch (config-if-range) #switchport access vlan 3

- Asignación de rangos no contiguos. Ej Los puertos FastEthernet 0/2, FastEthernet 0/6 y FastEthernet 0/18 lo asignamos a la VLAN 3

  Switch (config) #interface range fastEthernet 0/2, fastEthernet 0/6, fastEthernet 0/18
  Switch (config-if-range) #switchport mode access
  Switch (config-if-range) #switchport access vlan 3

Cambio de pertenencia de puertos de una VLAN

Eliminación de la asignación de la VLAN:

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	`S1# configure terminal`
Elimine la asignación de la VLAN del puerto.	`S1(config-if)# no switchport access vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

El comando **show vlan brief** muestra una línea para cada VLAN. El resultado para cada VLAN incluye el nombre, el estado y los puertos de switch de la VLAN.

```
S1(config)# int F0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
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
20   student            active
1002 fddi-default       act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default    act/unsup
1005 trnet-default      act/unsup
S1#
```

Figura 6: Cambio de pertenencia de puertos de VLAN

La VLAN 20 sigue activa, aunque no tenga puertos asignados. En la figura 7, se muestra que el resultado del comando **show interfaces f0/18 switchport** verifica que la VLAN de acceso para la interfaz F0/18 se haya restablecido a la VLAN 1.

```
S1# sh interfaces F0/18 switchport
Name: F0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

<resultado omitido>
```

Figura 7: Verificación de la asignación de VLAN

La pertenencia de VLAN de un puerto se puede cambiar fácilmente. No es necesario eliminar primero un puerto de una VLAN para cambiar su pertenencia de VLAN. Cuando se vuelve a asignar la pertenencia de VLAN de un puerto de acceso a otra VLAN existente, la nueva pertenencia de VLAN simplemente reemplaza la pertenencia de VLAN anterior. En la figura 8, el puerto F0/11 se asignó a la VLAN 20.

```
S1# config t
S1(config)# int F0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
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, Fa0/12, 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
20   student              active     F0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Figura 8: Asignación de un puerto a una VLAN

ELIMINACIÓN DE UNA VLAN

Switch#configure terminal
Switch(vlan)#no vlan 3

En algunos modelos de Switches es necesario eliminar el archivo de información de la base de datos de la VLAN que está almacenado en la memoria flash

Switch#delete flash:vlan.dat

Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm][Intro]

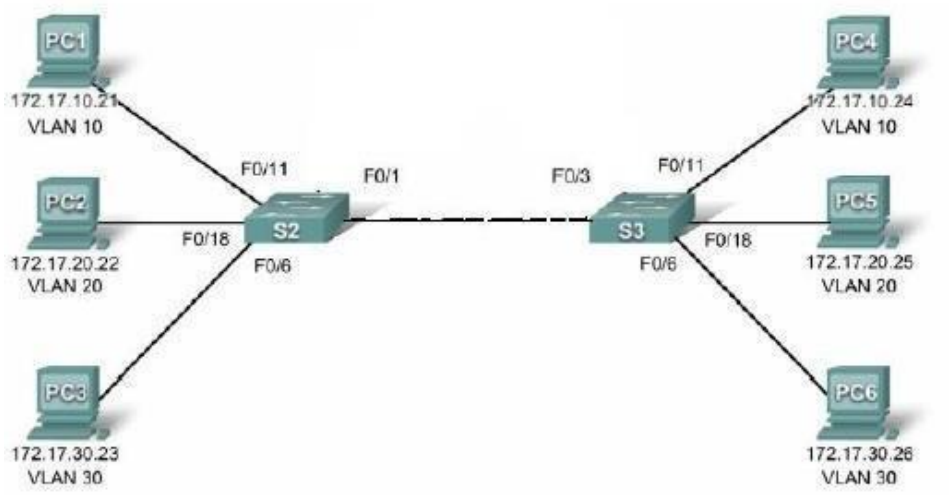
Se puede utilizar la versión abreviada del comando (delete vlan.dat)

CONFIGURACIÓN DE ENLACES TRONCALES

Para configurar un puerto de switch en un extremo de un enlace troncal, utilice el comando **switchport mode trunk**.

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese al modo de configuración de interfaz para la SVI.	`S1(config)# interface` *id_interfaz*
Haga que el enlace sea un enlace troncal.	`S1(config-if)# switchport mode trunk`
Especifique una VLAN nativa para enlaces troncales 802.1Q sin etiquetar.	`S1(config-if)# switchport trunk native vlan` *id_vlan*
Especifique la lista de VLAN que se permitirán en el enlace troncal.	`S1(config-if)# switchport trunk allowed vlan` *lista-vlan*
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

Ejemplo:



Se ha configurado los puertos para cada una de las VLANs existentes, para levantar el enlace troncal, realizamos lo siguiente:

```
S2(config)#interface fastethernet 0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#switchport trunk allowed vlan 10, 20, 30, 99

S3(config)#interface fastethernet 0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#switchport trunk allowed vlan 10, 20, 30, 99
```

Para el restablecimiento del enlace troncal al estado predeterminado, use los siguientes comandos:

Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese al modo de configuración de interfaz para la SVI.	`S1(config)# interface id_intrfaz`
Establezca el enlace troncal para permitir todas las VLAN.	`S1(config-if)# no switchport trunk allowed vlan`
Restablezca la VLAN nativa al valor predeterminado.	`S1(config-if)# no switchport trunk native vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

Para el restablecimiento del puerto al modo de acceso use el comando **switchport mode Access**

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

VERIFICACIÓN DE CONFIGURACIÓN DE VLAN

Opciones del comando **show vlan**

Sintaxis del comando de CLI IOS de Cisco

`show vlan [brief | id id-vlan | name nombre-vlan | summary ].`	
Mostrar una línea para cada VLAN con el nombre, estado y los puertos de la misma.	`brief`
Mostrar información sobre una sola VLAN identificada por su número de ID. Para la vlan-id, el intervalo es de 1 a 4094.	`id` *id de la VLAN*
Mostrar información sobre una sola VLAN identificada por su nombre. El nombre de la VLAN es una cadena ASCII de 1 a 32 caracteres.	`name` *nombre de la VLAN*
Mostrar el resumen de información de la VLAN.	`resumen`

Ejemplo de uso del comando **show vlan**

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0
```

Opciones del comando **show interfaces**

Sintaxis del comando de CLI IOS de Cisco	
show interfaces [*id-interfaz* | **vlan** *id-vlan*] | **switchport**	
Las interfaces válidas incluyen puertos físicos (incluidos tipo, módulo y número de puerto) y canales de puerto. El intervalo de canales de puerto es de 1 a 6.	*id de la interfaz*
Identificación de VLAN. El intervalo es de 1 a 4094.	**vlan** *id de la VLAN*
Mostrar el estado de administración y operación de un puerto de conmutación, incluidas las configuraciones de bloqueo y protección del puerto.	**switchport**

Ejemplo de uso del comando **show interfaces**

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

La configuración del enlace troncal se verifica con el comando **show interfaces** *ID-interfaz* **switchport**.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<resultado omitido>
```

IV

ACTIVIDADES

(La práctica tiene una duración de 2 horas)

1. Realice la configuración de VLAN y enlaces troncales

TOPOLOGÍA

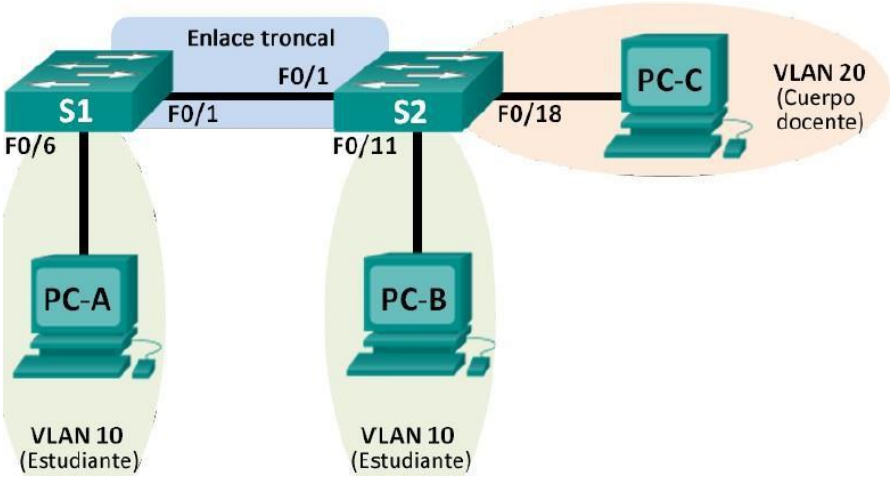


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
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
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

PARTE 1. Armar la red y configurar los parámetros básicos de los dispositivos

Paso 1. Configurar los parámetros básicos para cada switch

Configure el nombre del dispositivo como se muestra en la topología. Asigne **class** como la contraseña del modo EXEC privilegiado.

Asigne **cisco** como la contraseña de vty y la contraseña de consola.
Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.

Paso 2. Configurar los equipos host

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

Paso 3. Probar la conectividad.

Verifique que los equipos host puedan hacer ping entre sí.

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.
¿Se puede hacer ping de la PC-A a la PC-B? _____
¿Se puede hacer ping de la PC-A a la PC-C? _____
¿Se puede hacer ping de la PC-A al S1? _____
¿Se puede hacer ping de la PC-B a la PC-C? _____
¿Se puede hacer ping de la PC-B al S2? _____
¿Se puede hacer ping de la PC-C al S2? _____
¿Se puede hacer ping del S1 al S2? _____

PARTE 2. Crear redes VLAN y asignar puertos de switch

En la parte 2, creará redes 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.

Paso 1. Crear las VLAN en los switches.

a. Cree las VLAN en S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

b. Cree las mismas VLAN en el S2.

c. Emita el comando **show vlan** para ver la lista de VLAN en el S1.

S1# **show vlan**

```
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   Student                           active
20   Faculty                           active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

¿Cuál es la VLAN predeterminada? _____
¿Qué puertos se asignan a la VLAN predeterminada?

Paso 2. Asignar las VLAN a las interfaces del switch correctas.

a. Asigne las VLAN a las interfaces en el S1.

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

S1(config)# **interface f0/6** S1(config-if)# **switchport mode access**

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

3) Transfiera la dirección IP del switch a la VLAN 99.

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

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

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

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, Fa0/11, 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   Student                           active    Fa0/6
20   Faculty                           active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

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

¿Cuál es el estado de la VLAN 99? ¿Por qué?

_____

d. Use la topología para asignar las VLAN a los puertos correspondientes en el S2.

e. Elimine la dirección IP para la VLAN 1 en el S2.

f. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.

g. 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, Fa0/12, 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   Student                           active    Fa0/11
20   Faculty                           active    Fa0/18
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

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

_____

¿Es posible hacer ping del S1 al S2? ¿Por qué?

_____

PARTE 3. Mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

En esta parte, 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.

a. En el S1, asigne las interfaces F0/11 a 24 a la VLAN 10.

S1(config)# **interface range f0/11-24**
S1(config-if-range)# **switchport mode access**
S1(config-if-range)# **switchport access vlan 10**
S1(config-if-range)# **end**

b. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN.

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

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

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

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

¿A qué VLAN está asociada ahora F0/24?

Paso 3. Eliminar una ID de VLAN de la base de datos de VLAN.
a. Agregue la VLAN 30 a la interfaz F0/24 sin emitir el comando VLAN.

```
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.

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, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
30   VLAN0030                          active    Fa0/24
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

¿Cuál es el nombre predeterminado de la VLAN 30?

_____

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.

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?

_____

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, Gi0/1, Gi0/2
10   Student                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/22, Fa0/23
```

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

f. Emita el comando **show vlan brief** para determinar la asignación de VLAN para F0/24. ¿A qué VLAN se asignó F0/24?

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?

Parte 4. Configurar un enlace troncal 802.1Q entre los switches implementando seguridad de VLAN

Paso 1. 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.

a. Configure el puerto F0/1 en el **S1** como puerto de enlace troncal.

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

b. Configure el puerto F0/1 en el **S2** como puerto de enlace troncal.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c. Verifique los enlaces troncales en el S1 y el S2. Emita el comando **show interface trunk** en los dos switches.

```
S1# show interface trunk
```

Paso 2. Cambiar la VLAN nativa para los puertos de enlace troncal en el S1 y el S2. Es aconsejable para la seguridad cambiar la VLAN nativa para los puertos de enlace troncal de la VLAN 1 a otra VLAN.

a. ¿Cuál es la VLAN nativa actual para las interfaces F0/1 del S1 y el S2?

……..

b. Configure la VLAN nativa de la interfaz de enlace troncal F0/1 del S1 en la VLAN 99

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Configure la VLAN 99 como VLAN nativa de la interfaz de enlace troncal F0/1 del S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

d. Verifique que ahora la VLAN nativa sea la 99 en ambos switches.

```
S1# show interface trunk
```

Paso 3. Verificar que el tráfico se pueda transmitir correctamente a través del enlace troncal.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?

---

b. En la sesión de consola del S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

---

c. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-B. ¿Los pings se realizaron correctamente? ¿Por qué?

---

d. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A. ¿Tuvo éxito? ¿Por qué?

Paso 4. Impedir el uso de DTP en el S1 y el S2.

Cisco utiliza un protocolo exclusivo conocido como "protocolo de enlace troncal dinámico" (DTP) en los switches. Algunos puertos negocian el enlace troncal de manera automática. Se recomienda desactivar la negociación. Puede ver este comportamiento predeterminado mediante la emisión del siguiente comando:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

a. Desactive la negociación en el S1.

S1(config)# **interface f0/1**
S1(config-if)# **switchport nonegotiate**

b. Desactive la negociación en el S2.

S2(config)# **interface f0/1**
S2(config-if)# **switchport nonegotiate**

c. Verifique que la negociación esté desactivada mediante la emisión del comando **show interface f0/1 switchport** en el S1 y el S2.

De manera predeterminada, se permite transportar todas las VLAN en los puertos de enlace troncal. Por motivos de seguridad, se recomienda permitir que solo se transmitan las VLAN deseadas y específicas a través de los enlaces troncales en la red.

d. Restrinja el puerto de enlace troncal F0/1 en el S1 para permitir solo las VLAN 10, 20 y 99.

S1(config)# **interface f0/1**
S1(config-if)# **switchport trunk allowed vlan 10,20,99**

e. Restrinja el puerto de enlace troncal F0/1 en el S2 para permitir solo las VLAN 10, 20 y 99.

f. Verifique las VLAN permitidas. Emita el comando

show interface trunk en el modo EXEC privilegiado en el S1 y el S2

S1# **show interface trunk**

Nota: Presentar al docente para la revisión antes de proceder a la eliminación de la VLAN

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**

```
Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         736   Mar 1 1993 00:19:41 +00:00  vlan.dat

32514048 bytes total (20858880 bytes free)
```

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.

a. 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#
```

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

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

V

CUESTIONARIO

1. ¿Cuáles son algunos de los beneficios principales que una organización puede obtener mediante el uso eficaz de las VLAN?
2. ¿Qué problemas de seguridad, si los hubiera, tiene la configuración predeterminada de un switch Cisco?

VI

BIBLIOGRAFIA Y REFERENCIAS

- CISCO SYSTEMS. “Switching, Routing, y Wireless Essentials v7.0 (SRWE)”, Currícula CISCO CCNA v7.0 en Español. Módulo 2. Portable Multiplataforma, 2021
- ARIGANELLO, ERNESTO, “Redes Cisco guía de estudio para la certificación CCNA Routing y Switching” Edición 4 2016.
- ROSAS, LAURA, “Matemática de Redes”, Universidad Católica de Santa María, 2017