Práctica de laboratorio: Configuración de VLAN y enlaces troncales (Versión para el instructor)

**Nota para el instructor**: Los elementos con color de fuente rojo o resaltados en gris indican texto que aparece solo en la copia del instructor.

# 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.

**Nota para el instructor**: Consulte el Manual de Laboratorio del Instructor para conocer los procedimientos para inicializar y recargar dispositivos.

# 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

switch> **enable**

* + - 1. Ingrese al modo de configuración.

switch# **config terminal**

* + - 1. Asigne un nombre de dispositivo al switch.

switch(config)# **hostname S1**

switch(config)# **hostname S2**

* + - 1. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

S1(config)# **no ip domain-lookup**

S2(config)# **no ip domain-lookup**

* + - 1. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

S1(config)# **enable secret class**

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

* + - 1. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

S1(config)# **line console 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S2(config)# **line console 0**

S2(config-line)# **password cisco**

S2(config-line)# **login**

* + - 1. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

S1 (config) # **línea vty 0 4**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S2 (config) # **línea vty 0 4**

S2(config-line)# **password cisco**

S2(config-line)# **login**

* + - 1. Cifre las contraseñas de texto sin formato.

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

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

* + - 1. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

S1(config)# **banner motd $ Authorized Users Only! $**

S2(config)# **banner motd $ Authorized Users Only! $**

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

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

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

S1(config-if)# **no shutdown**

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

S2(config)# **interface vlan 1**

S2(config-if)# **ip address 192.168.1.12 255.255.255.0**

S2(config-if)# **no shutdown**

S2(config-if)# **exit**

* + - 1. Apague todas las interfaces que no se utilizarán.

S1 (config) # **interface range f0/2-5, f0/7-24, g0/1-2**

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

S2 (config) # **interface range f0/2-17, f0/18-24, g0/1-2**

S2(config-if-range)# **shutdown**

* + - 1. Ajuste el reloj en el interruptor.

S1# **clock set 15:30:00 19 September 2019**

S2# **clock set 15:30:00 19 September 2019**

* + - 1. Guardar la configuración en ejecución en el archivo de configuración de inicio

S1# **copy running-config startup-config**

S2# **copy running-config startup-config**

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?

Escriba sus respuestas aquí.

Sí

¿Se puede hacer ping de la PC-A al S1?

Escriba sus respuestas aquí.

No

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

Escriba sus respuestas aquí.

No

Abrir la ventana de configuración

¿Se puede hacer ping del S1 al S2?

Escriba sus respuestas aquí.

Sí

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

Escriba sus respuestas aquí.

Los pings fallaron cuando se intentó hacer ping a un dispositivo en una subred diferente. Para que esos pings se realicen correctamente, debe existir un gateway predeterminado para enrutar el tráfico de una subred a otra.

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?

Escriba sus respuestas aquí.

VLAN 1

¿Qué puertos se asignan a la VLAN predeterminada?

Escriba sus respuestas aquí.

Todos los puertos del switch se asignan a la VLAN 1 de manera predeterminada.

### 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.

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 Operations 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

* + - 1. Emita el comando **show ip interface brief**.

S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Vlan1 unassigned YES unset up up

Vlan99 192.168.1.11 YES manual up down

FastEthernet0/1 unassigned YES unset up up

FastEthernet0/2 unassigned YES unset administratively down down

FastEthernet0/3 unassigned YES unset administratively down down

FastEthernet0/4 unassigned YES unset administratively down down

FastEthernet0/5 unassigned YES unset administratively down down

FastEthernet0/6 unassigned YES unset up up

FastEthernet0/7 unassigned YES unset administratively down down

<output omitted>

#### Pregunta:

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

Escriba sus respuestas aquí.

El estado de la VLAN 99 es arriba / abajo, arriba porque la VLAN existe en la base de datos, pero abajo porque la VLAN aún no se ha asignado a un puerto activo.

* + - 1. Asigne PC-B a la VLAN de Operaciones en S2.

S2(config)# **interface f0/18**

S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 10**

* + - 1. Elimine la dirección IP para la VLAN 1 en el S2.

S2(config)# **interface vlan 1**

S2 (config-if) # **no ip address**

* + - 1. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.

S2(config-if)# **interface vlan 99**

S2(config-if)# **ip address 192.168.1.12 255.255.255.0**

* + - 1. 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

#### Preguntas:

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

Escriba sus respuestas aquí.

No. Las direcciones IP de los switches ahora residen en la VLAN 99. El tráfico de la VLAN 99 no se envía a través de la interfaz F0/1.

Cerrar la ventana de configuración

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

Escriba sus respuestas aquí.

No. La interfaz F0/1 no se asignó a la VLAN 10, de modo que el tráfico de la VLAN 10 no se envía a través de esta interfaz.

## 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.

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 Operaciones activas Fa0/6

20 Parking\_Lot active

99 Management active 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

1000 Native active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

* + - 1. Reasigne F0/11 y F0/21 a la VLAN 20.

S1(config)# **interface range f0/11, f0/21**

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

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

* + - 1. 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, Gi0/1, Gi0/2

10 Operations active Fa0/6, Fa0/11, Fa0/21

20 Parking\_Lot active

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

### 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?

Escriba sus respuestas aquí.

VLAN 1, la VLAN predeterminada.

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, Fa0/11, Fa0/21

20 Parking\_Lot active

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

### 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.

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 Operaciones activas Fa0/6, Fa0/11, Fa0/21

20 Parking\_Lot active

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?

Escriba sus respuestas aquí.

VLAN0030

* + - 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?

Escriba sus respuestas aquí.

Cuando elimina una VLAN, cualquier puerto asignado a esa VLAN queda inactivo. Por lo tanto, el puerto F0/24 sigue estando asociado a la VLAN 30. Sin embargo, la VLAN 30 está inactiva porque no existe en la base de datos de VLAN. Además, el puerto no transferirá ningún tráfico.

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, Fa0/11, Fa0/21

20 Parking\_Lot active

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

* + - 1. Ejecute el comando **no switchport access vlan** en la interfaz F0/24.

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

S1 (config-if) # **sin acceso a puerto de conmutación 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?

Escriba sus respuestas aquí.

VLAN 1, la VLAN predeterminada.

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, Fa0/11, Fa0/21

20 Parking\_Lot active

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?

Escriba sus respuestas aquí.

Las interfaces asignadas a una VLAN que se eliminó de la base de datos de VLAN no están disponibles para usar hasta que se reasignen a otra VLAN. Este problema puede ser difícil de resolver, ya que las interfaces de enlace troncal tampoco aparecen en la lista de puertos (en la parte 4, se incluye más información sobre las interfaces de enlace troncal).

Cerrar la ventana de configuración

## 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.

S1# **show vlan brief**

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, Fa0/11, Fa0/21

20 Parking\_Lot active

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

* + - 1. 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**

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**

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

**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?

Escriba sus respuestas aquí.

Sí

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

Escriba sus respuestas aquí.

Sí

¿Se puede hacer ping de la PC-A al S1?

Escriba sus respuestas aquí.

No

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

Escriba sus respuestas aquí.

No

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

Escriba sus respuestas aquí.

Los switches están en la VLAN 99 y las PC están en la VLAN 10; por lo tanto, los pings entre VLAN no tuvieron éxito.

### 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**

S2(config)# **interface f0/1**

S2(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**

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

* + - 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**

S2(config)# **interface f0/1**

S2(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**

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 1,10,20,99,1000

#### Preguntas:

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

Escriba sus respuestas aquí.

No todos los equipos usan DTP. Con el comando switchport mode trunk, se garantiza que el puerto se convierta en un enlace troncal, independientemente del tipo de equipo conectado al otro extremo del enlace.

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

Escriba sus respuestas aquí.

El uso de VLAN 1, la VLAN predeterminada, ya que la VLAN nativa es un riesgo para la seguridad. Todos los diferentes protocolos de control que se intercambian entre switches se intercambian a través de la VLAN 1 nativa sin etiquetar, y esa información podría verse expuesta si se utiliza la configuración predeterminada en los puertos a los que se conectan los usuarios.

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:**

Directory of flash:/

2 -rwx 59416 1 de mar de 1993 01:20:12 + 00:00 multiple-fs

3 -rwx 15186645 Mar 1 1993 00:19:23 + 00:00 C2960-Lanbasek9-mz.152-4.E8.bin

5 -rwx 796 19 sep 2019 02:48:04 + 00:00 vlan.dat

61028352 bytes total (33762304 bytes free)

**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:**

Directory of flash:/

2 -rwx 59416 1 de mar de 1993 01:20:12 + 00:00 multiple-fs

3 -rwx 15186645 Mar 1 1993 00:19:23 + 00:00 C2960-Lanbasek9-mz.152-4.E8.bin

61028352 bytes total (33763840 bytes free)

#### Pregunta:

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

Escriba sus respuestas aquí.

Para que un switch vuelva a la configuración predeterminada, se deben emitir los comandos erase startup-config y reload después de emitir el comando delete vlan.dat.

Cerrar la ventana de configuración

# 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?

Escriba sus respuestas aquí.

Las respuestas variarán, pero para permitir el enrutamiento entre VLAN se requiere un dispositivo de capa 3 para enrutar el tráfico entre las VLAN.

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

Escriba sus respuestas aquí.

Las respuestas varían, pero algunos de los beneficios de las VLAN incluyen lo siguiente: aumento de la seguridad, ahorro de costos (uso eficaz del ancho de banda y los uplinks), aumento del rendimiento (dominios de difusión más pequeños), mitigación de las tormentas de difusión, aumento de la eficiencia del personal de TI, simplificación de la administración de proyectos y aplicaciones.

Fin del documento

# Configuración de dispositivo: Final

# Switch S1

Building configuration...

Current configuration : 2571 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 5 $1$GCQG$N33u/asvJfEWsnrIHRWjM1

!

no aaa new-model

system mtu routing 1500

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

switchport trunk native vlan 1000

switchport mode trunk

!

interface FastEthernet0/2

shutdown

!

interface FastEthernet0/3

shutdown

!

interface FastEthernet0/4

shutdown

!

interface FastEthernet0/5

shutdown

!

interface FastEthernet0/6

switchport access vlan 10

switchport mode access

!

interface FastEthernet0/7

shutdown

!

interface FastEthernet0/8

shutdown

!

interface FastEthernet0/9

shutdown

!

interface FastEthernet0/10

shutdown

!

interface FastEthernet0/11

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/12

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/14

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/19

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/21

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/22

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/23

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/24

switchport mode access

shutdown

!

interface GigabitEthernet0/1

shutdown

!

interface GigabitEthernet0/2

shutdown

!

interface Vlan1

no ip address

!

interface Vlan99

ip address 192.168.1.11 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password cisco

logging synchronous

login

line vty 0 4

password cisco

login

line vty 5 15

password cisco

login

!

end

# Switch S2

Building configuration...

Current configuration : 1875 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S2

!

boot-start-marker

boot-end-marker

!

enable secret 5 $1$jTd.$1rhSHu68akU70GYYyc4Dy1

!

no aaa new-model

system mtu routing 1500

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

switchport trunk native vlan 1000

switchport mode trunk

!

interface FastEthernet0/2

shutdown

!

interface FastEthernet0/3

shutdown

!

interface FastEthernet0/4

shutdown

!

interface FastEthernet0/5

shutdown

!

interface FastEthernet0/6

shutdown

!

interface FastEthernet0/7

shutdown

!

interface FastEthernet0/8

shutdown

!

interface FastEthernet0/9

shutdown

!

interface FastEthernet0/10

shutdown

!

interface FastEthernet0/11

shutdown

!

interface FastEthernet0/12

shutdown

!

interface FastEthernet0/13

shutdown

!

interface FastEthernet0/14

shutdown

!

interface FastEthernet0/15

shutdown

!

interface FastEthernet0/16

shutdown

!

interface FastEthernet0/17

shutdown

!

interface FastEthernet0/18

switchport access vlan 10

switchport mode access

!

interface FastEthernet0/19

shutdown

!

interface FastEthernet0/20

shutdown

!

interface FastEthernet0/21

shutdown

!

interface FastEthernet0/22

shutdown

!

interface FastEthernet0/23

shutdown

!

interface FastEthernet0/24

shutdown

!

interface GigabitEthernet0/1

shutdown

!

Interface GigabitEthernet0/2

shutdown

!

interface Vlan1

no ip address

!

interface Vlan99

ip address 192.168.1.12 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password cisco

logging synchronous

login

line vty 0 4

password cisco

login

line vty 5 15

password cisco

login

!

end