

Packet Tracer — Configurar VLAN y enlaces troncales — Modo físico

Topología

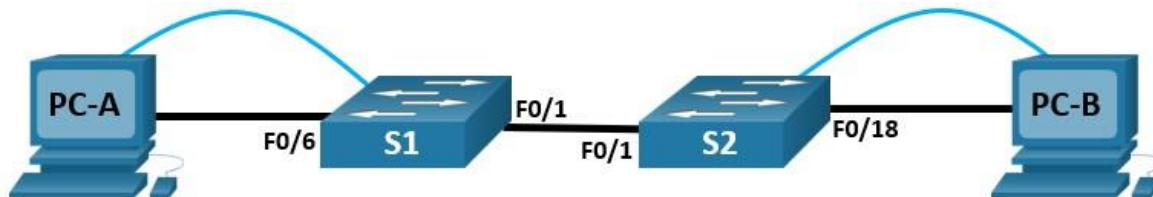


Tabla de asignación de direcciones

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

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

- a. 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.
- b. Ingrese al modo de configuración.
- c. Asigne un nombre de dispositivo al switch.
- d. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- e. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
- f. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
- g. Encripte las contraseñas de texto sin formato.
- h. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- 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 avalúa porque la eliminará más adelante en la actividad. Sin embargo, necesitará VLAN 1 para probar la conectividad más adelante en esta parte.
- j. Apague todas las interfaces que no se utilizarán.
- k. Ajuste el reloj en cada conmutador.
Nota: La configuración del reloj no se puede clasificar en Packet Tracer.
- l. Guarde la configuración en ejecución en el archivo de configuración de inicio

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.

Paso 4: Probar la conectividad

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

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

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

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

¿Se puede hacer ping de **S1** a **S2**? **SI**

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

Los ping no tuvieron éxito al intentar hacer ping a un dispositivo en una subred diferente.

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.

- 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
```

- Cree las mismas VLAN en el S2.

- Ejecute el comando **show vlan brief** para ver la lista de VLANs 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_Lot active
```

```
99 Management active
```

```
1000 Native active
```

```
1002 fddi-default active
```

```
1003 token-ring-default active
```

```
1004 fddinet-default active
```

```
1005 trnet-default active
```

¿Cuál es la VLAN predeterminada?

VLAN 1

¿Qué puertos se asignan a la VLAN predeterminada?

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

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 f0/6
```

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

```
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)# 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.

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

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

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

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

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

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

¿Puede **S1** hacer ping a **S2**? Explique.

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

¿Puede **PC-A** hacer ping a **PC-B**? Explique.

No. La interfaz F0/1 no está asignada a la VLAN 10, por lo que el tráfico de la VLAN 10 no se enviará a través de ella.

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)# switchport mode access
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.
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.

¿Con qué VLAN está asociado F0/24 ahora?

VLAN 1, la VLAN predeterminada.

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
```

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.

¿Cuál es el nombre predeterminado de la VLAN 30?

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.

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?

Cuando elimina una VLAN, todos los puertos asignados a esa VLAN se vuelven inactivos.

- e. Ejecute el comando **no switchport access vlan** en la interfaz F0/24.
f. Ejecute el comando **show vlan brief** para determinar la asignación de VLAN para F0/24.

¿A qué VLAN se asignó F0/24?

La VLAN predeterminada, VLAN 1

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?

Las interfaces asignadas a una VLAN que se elimina de la base de datos de VLAN se vuelven inactivas y no están disponibles para su uso hasta que se reasignan a otra VLAN.

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)# 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
```

- 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.
- 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**

S2# **show interfaces trunk**

Nota: de manera predeterminada, todas las VLAN se permiten en un enlace troncal. El comando **switchport trunk** le permite controlar qué VLAN tienen acceso al enlace troncal. Para esta 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.

¿Puede S1 hacer ping a **S2**? SI

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

¿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, justifíquela a continuación.

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

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.

- a. 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
```

- 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
```

- 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
```

- 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
```

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

No todos los equipos utilizan DTP.

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

El uso de la VLAN 1, la VLAN predeterminada, como VLAN nativa es un riesgo de seguridad

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?

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

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

Las respuestas variarán, pero los beneficios de VLAN incluyen: mejor seguridad, ahorro de costos