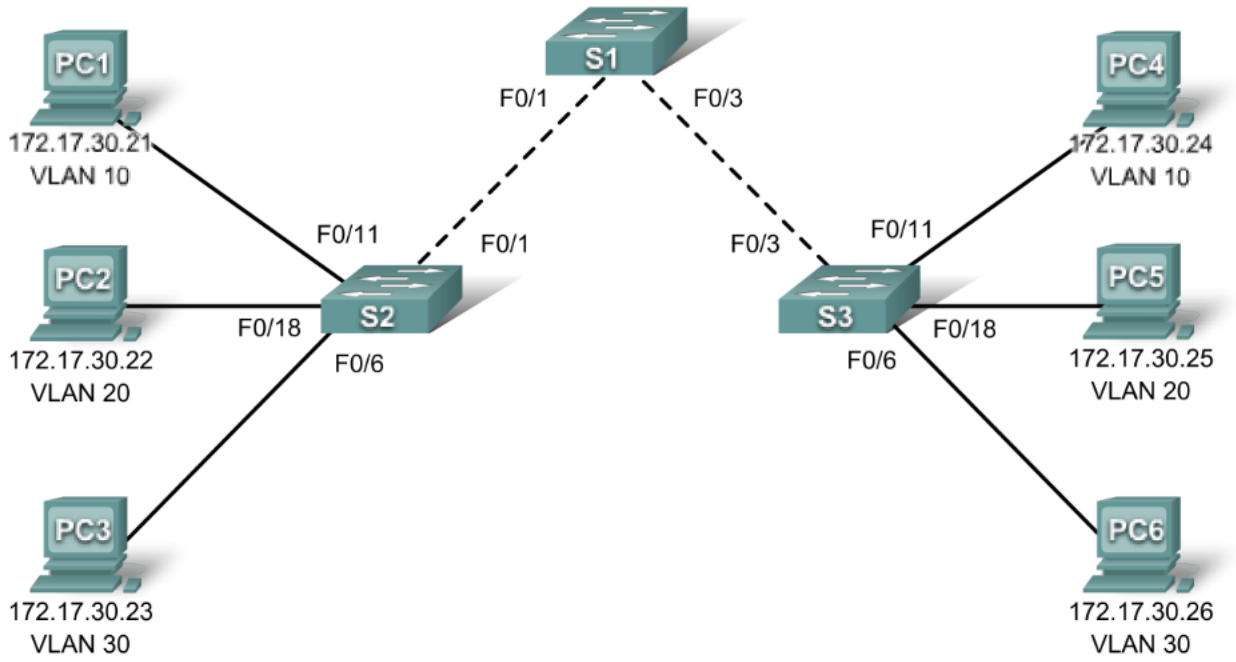
Actividad de Packet Tracer 4.3.3: Configuración del VTP

Diagrama de topología



Objetivos de aprendizaje

- Investigar la configuración actual.
- Configurar S1 como servidor VTP.
- Configurar S2 y S3 como clientes VTP.
- Configurar las VLAN en S1.
- Configurar enlaces troncales en S1, S2 y S3.
- Verificar el estado del VTP en S1, S2 y S3.
- Asignar VLAN a puertos en S2 y S3.
- Verificar la implementación de VLAN y probar la conectividad.

Introducción

En esta actividad, se podrá practicar la configuración de VTP. Cuando Packet Tracer se abre por primera vez, los switches ya contienen una configuración parcial. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiado es **class**.

Tarea 1: Investigar la configuración actual

Paso 1: Verifique la configuración en ejecución actual de los switches.

¿Qué configuraciones ya están presentes en los switches?

_____

_____

_____

Paso 2: Muestre las VLAN actuales de cada switch.

¿Hay VLAN presentes? ¿Las VLAN presentes son VLAN predeterminadas o creadas por el usuario?

_____

```
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
                                              Gig1/1, Gig1/2
1002 fddi-default                  active
1003 token-ring-default            active
1004 fddinet-default               active
1005 trnet-default                 active
```

El porcentaje final debe ser de 0% al finalizar esta tarea.

Tarea 2: Configurar S1 como servidor VTP

Paso 1: Configure el comando del modo VTP.

S1 será el servidor para VTP. Establezca S1 en el modo de servidor.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#
```

Observe que el switch ya está establecido en el modo de servidor predeterminado. No obstante, es importante que configure explícitamente este comando para asegurarse de que el switch esté en el modo de servidor.

Paso 2: Configure el nombre del dominio VTP.

Configure S1 con **CCNA** como el nombre de dominio VTP. Recuerde que los nombres de dominio VTP distinguen entre mayúsculas y minúsculas.

```
S1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
```


Paso 3: Configure la contraseña de dominio VTP.

Configure S1 con **cisco** como la contraseña de dominio VTP. Recuerde que las contraseñas de dominio VTP distinguen mayúsculas de minúsculas.

```
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#
```

Paso 4: Confirme los cambios de configuración.

Use el comando **show vtp status** en S1 para confirmar que el modo VTP y el dominio están configurados correctamente.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Para verificar la contraseña de VTP, use el comando **show vtp password**.

```
S1#show vtp password
VTP Password: cisco
S1#
```

Paso 5: Verifique los resultados.

Su porcentaje de finalización debe ser del 8%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar S2 y S3 como clientes VTP

Paso 1: Configure el comando del modo VTP.

S2 y S3 serán clientes VTP. Establezca estos dos switches en modo de cliente.

Paso 2: Configure el nombre del dominio VTP.

Antes de que S2 y S3 acepten publicaciones VTP de S1, deben pertenecer al mismo dominio VTP. Configure S2 y S3 con **CCNA** como el nombre de dominio VTP. Recuerde que los nombres de dominio VTP distinguen entre mayúsculas y minúsculas.

Paso 3: Configure la contraseña de dominio VTP.

S2 y S3 también deben usar la misma contraseña antes de aceptar publicaciones VTP del servidor VTP. Configure S2 y S3 con **cisco** como la contraseña de dominio VTP. Recuerde que las contraseñas de dominio VTP distinguen mayúsculas de minúsculas.

Paso 4: Confirme los cambios de configuración.

Use el comando **show vtp status** en cada switch para confirmar que el modo VTP y el dominio están configurados correctamente. Aquí se muestra el resultado para el S3.

```
S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que el número de revisión de la configuración es 0 en los tres switches. ¿Por qué?

_____

_____

_____

Para verificar la contraseña de VTP, use el comando **show vtp password**.

```
S3#show vtp password
VTP Password: cisco
S3#
```

Paso 5: Verifique los resultados.

Su porcentaje de finalización debe ser del 31%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Configurar las VLAN en S1.

Las VLAN se pueden crear en el servidor VTP y distribuir a otros switches en el dominio VTP. En esta tarea, usted crea 4 VLAN nuevas en el servidor VTP del S1. Estas VLAN se distribuirán a S2 y S3 a través de VTP.

Paso 1: Cree las VLAN.

Para efectos de calificación en Packet Tracer, los nombres de las VLAN distinguen mayúsculas de minúsculas.

- VLAN 10 con el nombre **Faculty/Staff**
- VLAN 20 con el nombre **Students**
- VLAN 30 con el nombre **Guest(Default)**
- VLAN 99 con el nombre **Management&Native**

Paso 2: Verifique las VLAN.

Use el comando **show vlan brief** para verificar las VLAN y sus nombres.

```
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
                                            Gig1/1, Gig1/2
10   Faculty/Staff                active
20   Students                     active
30   Guest(Default)               active
99   Management&Native            active
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

Si se introduce el mismo comando en S2 y S3, se observa que las VLAN no están en su base de datos de VLAN. ¿Por qué no?

_____

_____

Paso 3: Verifique los resultados.

Su porcentaje de finalización debe ser del 46%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 5: Configurar enlaces troncales en S1, S2 y S3.

Use el comando **switchport mode trunk** para establecer el modo de enlace troncal para cada uno de los enlaces troncales. Use el comando **switchport trunk native vlan 99** para establecer la VLAN 99 como la VLAN nativa.

Paso 1: Configure FastEthernet 0/1 y FastEthernet 0/3 en el S1 para el enlace troncal.

Ingrese los comandos apropiados para configurar el enlace troncal y establecer la VLAN 99 como VLAN nativa.

Una vez configurada, el protocolo de enlace troncal dinámico (DTP) activará los enlaces troncales. Puede verificar que S2 y S3 sean ahora enlaces troncales si introduce el comando **show interface fa0/1 switchport** en S2 y el comando **show interface fa0/3 switchport** en S3.

Si espera algunos minutos a que Packet Tracer simule todos los procesos, S1 publicará la configuración de VLAN a S2 y S3. Esta verificación puede ejecutarse en S2 o S3 mediante los comandos **show vlan brief** o **show vtp status**.

No obstante, se recomienda configurar ambos extremos de los enlaces troncales en el modo **on**.

Paso 2: Configure Fast Ehternet 0/1 en el S2 para el enlace troncal.

Ingrese los comandos apropiados para configurar el enlace troncal y establecer la VLAN 99 como VLAN nativa.

Paso 3: Configure Fast Ethernet 0/3 en el S3 para el enlace troncal.

Ingrese los comandos apropiados para configurar el enlace troncal y establecer la VLAN 99 como VLAN nativa.

Paso 4: Verifique los resultados.

Su porcentaje de finalización debe ser del 77%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 6: Verificar el estado del VTP

Use los comandos **show vtp status** y **show vlan brief** para verificar lo siguiente.

- S1 debe mostrar el estado del servidor.
- S2 y S3 deben mostrar el estado de cliente.
- S2 y S3 deben tener VLAN de S1.

Nota: Las publicaciones de VTP se envían a través del dominio de administración cada cinco minutos o siempre que se efectúe una modificación en las configuraciones de la VLAN. Para acelerar este proceso, puede alternar entre el modo de tiempo real y el modo de simulación hasta la próxima vuelta de actualizaciones. Sin embargo, es posible que deba hacerlo varias veces, ya que esto sólo adelanta el reloj de Packet Tracer 10 segundos cada vez. Otra opción es cambiar uno de los switches cliente al modo transparente y luego volverlo al modo de cliente. (Es posible que la numeración de la revisión de la configuración difiera de los routers reales frente a los routers del Packet Tracer. Esta actividad no califica los números de revisión de la configuración).

¿Cuál es el número de revisión de la configuración? _____

¿Es el número de revisión de la configuración mayor que la cantidad de VLAN que creó?

_____

_____

¿Cuál es el número actual de las VLAN existentes? _____

¿Por qué existen más VLAN que las cuatro que usted creó?

_____

Al final de esta tarea, el porcentaje de finalización aún debe ser del 77%.

Tarea 7: Asignar VLAN a puertos

Use el comando **switchport mode access** para establecer el modo de acceso de los enlaces de acceso. Use el comando **switchport access vlan** *id de la VLAN* para asignar una VLAN a un puerto de acceso.

Paso 1: Asigne VLAN a los puertos de S2.

- Fa0/11 en VLAN 10
- Fa0/18 en VLAN 20
- Fa0/6 en VLAN 30

Paso 2: Asigne VLAN a los puertos en S3.

- Fa0/11 en VLAN 10
- Fa0/18 en VLAN 20
- Fa0/6 en VLAN 30

Paso 3: Verifique los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 8: Verificar la implementación de VLAN y probar la conectividad

Paso 1: Verifique la configuración de la VLAN y las asignaciones de puertos.

Use el comando **show vlan brief** para verificar la configuración de la VLAN y las asignaciones de puertos en cada switch. Compare la información obtenida con la topología.

Paso 2: Pruebe la conectividad entre las PC.

Los pings entre las PC de la misma VLAN deben tener éxito, mientras que los pings entre PC de diferentes VLAN deben fallar.

Desde PC1, haga ping a PC4.

Desde PC2, haga ping a PC5.

Desde la PC3, haga ping a PC6.

