Packet Tracer: configuración de VLAN, VTP y DTP

Topología

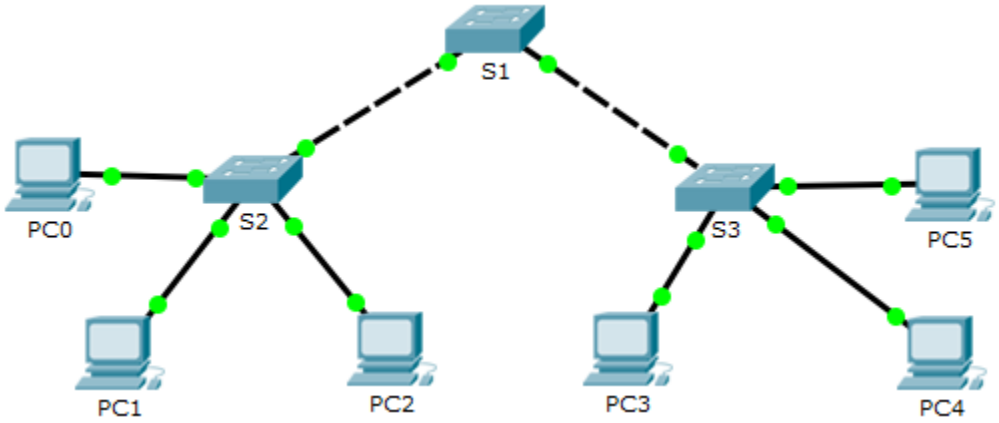

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
PC0	NIC	192.168.10.1	255.255.255.0
PC1	NIC	192.168.20.1	255.255.255.0
PC2	NIC	192.168.30.1	255.255.255.0
PC3	NIC	192.168.30.2	255.255.255.0
PC4	NIC	192.168.20.2	255.255.255.0
PC5	NIC	192.168.10.2	255.255.255.0
S1	VLAN 99	192.168.99.1	255.255.255.0
S2	VLAN 99	192.168.99.2	255.255.255.0
S3	VLAN 99	192.168.99.3	255.255.255.0

Objetivos

Parte 1. Configurar y comprobar DTP

Parte 2. Configurar y comprobar VTP

Aspectos básicos/situación

A medida que la cantidad de switches en una red aumenta, el control que se necesita para administrar las VLAN y los enlaces troncales puede plantear un desafío. Para facilitar algunas de las configuraciones de VLAN y de enlaces troncales, el protocolo VTP (VLAN Trunking Protocol, protocolo de enlace troncal de VLAN) permite que un administrador de redes automatice la administración de VLAN. El protocolo DTP (Dynamic Trunking Protocol, protocolo de enlace troncal dinámico) administra la negociación de enlaces troncales entre los dispositivos de red y se encuentra habilitado de manera automática en los switches Catalyst 2960 y Catalyst 3560.

En esta actividad, configurará enlaces troncales entre los switches. Configurará un servidor VTP y clientes VTP en el mismo dominio VTP. También observará el comportamiento de VTP cuando un switch está en modo VTP transparente. Asignará puertos a las VLAN y comprobará la conectividad completa con la misma VLAN.

Parte 1: Configurar y comprobar DTP

En la parte 1, configurará enlaces troncales entre los switches y establecerá la VLAN 999 como VLAN nativa.

Paso 1: Verificar la configuración de la VLAN.

Compruebe las VLAN configuradas en los switches.

a. En S1, haga clic en **CLI**. En el símbolo del sistema, introduzca **enable** y el comando **show vlan brief** para comprobar las VLAN configuradas 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
                                                 Gig0/1, Gig0/2
99   Management                        active
999  VLAN0999                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

b. Repita el paso A en los switches S2 y S3. ¿Qué VLAN están configuradas en los switches?

Paso 2: Configurar enlaces troncales en S1, S2 y S3.

El protocolo DTP (Dynamic Trunking Protocol, protocolo de enlace troncal dinámico) administra los enlaces troncales entre switches de Cisco. En este momento, todos los puertos de switch están en el modo de enlace troncal predeterminado, que es dynamic auto. En este paso, cambiará el modo de enlace troncal a dynamic desirable para el enlace entre los switches S1 y S2. Para el enlace entre los switches S1 y S3, establecerá el enlace como enlace troncal estático. En esta topología, utilice la red VLAN 999 como VLAN nativa.

a. En S1, establezca el enlace troncal en modo dynamic desirable en la interfaz GigabitEthernet 0/1.

```
S1(config)# interface g0/1
S1(config-if)# switchport mode dynamic desirable
```

b. Para el enlace troncal entre S1 y S3, configure un enlace troncal estático en la interfaz GigabitEthernet 0/2.

```
S1(config)# interface g0/2
S1(config-if)# switchport mode trunk
S3(config)# interface g0/2
S3(config-if)# switchport mode trunk
```


c. Compruebe que los enlaces troncales estén habilitados en todos los switches mediante el comando **show interfaces trunk**.

```
S1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      desirable    n-802.1q       trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,99,999
Gig0/2      1,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      none
Gig0/2      none
```

¿Cuál es, en este momento, la VLAN nativa para estos enlaces troncales?

d. Configure la VLAN 999 como VLAN nativa para los enlaces troncales en S1.

```
S1(config)# interface range g0/1 - 2
S1(config-if-range)# switchport trunk native vlan 999
```

¿Qué mensajes recibió en S1? ¿Cómo lo corregiría?

e. Configure la VLAN 999 como VLAN nativa en S2 y S3.

f. Compruebe que los enlaces troncales se hayan configurado correctamente en todos los switches. Debe poder hacer ping en un switch desde otro switch en la topología mediante el uso de las direcciones IP configuradas en la SVI.

Parte 2: Configurar y comprobar el protocolo VTP

S1 se configura como servidor VTP y S2 se configura como cliente VTP. Todos los switches se configuran de modo que se encuentren en el dominio VTP **CCNA** y usen la contraseña VTP **cisco**.

Las VLAN se pueden crear en el servidor VTP y distribuir a otros switches en el dominio VTP. En esta parte, usted crea 3 VLAN nuevas en el servidor VTP de S1. Estas VLAN se distribuyen al S2 por medio del VTP. Observe el comportamiento del modo VTP transparente.

Paso 1: Configurar S1 como servidor VTP.

Configure S1 como servidor VTP en el dominio **CCNA** con la contraseña **cisco**.

a. Configure S1 como servidor VTP.

```
S1(config)# vtp mode server
Setting device to VTP SERVER mode.
```

b. Configure **CCNA** como el nombre de dominio VTP.

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


c. Utilice **cisco** como contraseña VTP.

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

Paso 2: Comprobar VTP en S1.

a. Utilice el comando **show vtp status** en los switches para confirmar que el modo y el dominio VTP se hayan configurado correctamente.

```
S1# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLAN supported locally  : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
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 0x17
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 192.168.99.1 on interface Vl99 (lowest numbered VLAN interface
found)
```

b. Para verificar la contraseña VTP, utilice el comando **show vtp password**.

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

Paso 3: Agregar S2 y S3 al dominio VTP.

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

a. Configure S2 como cliente VTP en el dominio VTP **CCNA** con la contraseña VTP **cisco**.

```
S2(config)# vtp mode client
Setting device to VTP CLIENT mode.
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S2(config)# vtp password cisco
Setting device VLAN database password to cisco
```

b. Para verificar la contraseña VTP, utilice el comando **show vtp password**.

```
S2# show vtp password
VTP Password: cisco
```

c. Configure S3 en el dominio VTP **CCNA** con la contraseña VTP **cisco**. El switch S3 permanecerá en el modo VTP transparente.

```
S3(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S3(config)# vtp password cisco
Setting device VLAN database password to cisco
```


d. Introduzca el comando **show vtp status** en todos los switches para responder la siguiente pregunta.

Observe que el número de revisión de la configuración es 0 en los tres switches. Explique.

Paso 4: Crear más VLAN en S1.

a. En S1, cree la VLAN 10 y asígnele el nombre Red.

```
S1(config)# vlan 10
S1(config-vlan)# name Red
```

b. Cree la VLAN 20 y la VLAN 30 de acuerdo con la siguiente tabla.

Número de VLAN	Nombre de la VLAN
10	Rojo
20	Azul
30	Amarillo

c. Compruebe la incorporación de las VLAN nuevas. Introduzca **show vlan brief** en el modo EXEC privilegiado.

¿Qué VLAN están configuradas en S1?

d. Confirme los cambios en la configuración; para ello, utilice el comando **show vtp status** en los switches S1 y S2 para corroborar que el modo y el dominio VTP se hayan configurado correctamente. Aquí se muestra el resultado para el S2:

```
S2# show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLAN supported locally  : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE6 0x56 0x05 0xE0 0x7A 0x63 0xFB 0x33
Configuration last modified by 192.168.99.1 at 3-1-93 00:21:07
```

¿Cuántas VLAN están configuradas en S2? ¿El switch S2 tiene las mismas VLAN que el switch S1? Explique.

Paso 5: Observar el modo transparente VTP.

S3 está configurado actualmente como modo VTP transparente.

a. Use el comando **show vtp status** para responder la siguiente pregunta.

¿Cuántas VLAN están configuradas actualmente en S3? ¿Cuál es el número de revisión de la configuración? Explique su respuesta.

¿Cómo cambiaría la cantidad de VLAN en S3?

b. Cambie el modo VTP a cliente en S3.

Utilice los comandos show para comprobar los cambios en modo VTP. ¿Cuántas VLAN existen ahora en S3?

Nota: Las notificaciones VTP se saturan en todo el dominio de administración cada cinco minutos o cada vez que ocurre un cambio en las configuraciones de 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 solo adelanta el reloj de Packet Tracer 10 segundos cada vez. De forma alternativa, se puede cambiar uno de los switches clientes al modo transparente y luego regresar al modo cliente.

Paso 6: Asignar VLAN a los puertos.

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

Puertos	Asignaciones	Red
S1 F0/1 – 8 S2 F0/1 – 8	VLAN 10 (Red)	192.168.10.0 /24
S1 F0/9 – 16 S2 F0/9 – 16	VLAN 20 (Blue)	192.168.20.0 /24
S1 F0/17 – 24 S2 F0/17 – 24	VLAN 30 (Yellow)	192.168.30.0 /24

a. Asigne VLAN a los puertos de S2 usando asignaciones de la tabla anterior.

```
S2(config-if)# interface range f0/1 - 8
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 10
S2(config-if-range)# interface range f0/9 -16
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 20
S2(config-if-range)# interface range f0/17 - 24
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 30
```

b. Asigne VLAN a los puertos de S3 usando asignaciones de la tabla anterior.

Paso 7: Verificar la conectividad completa.

a. Desde la PC0 haga ping en la PC5.

b. Desde la PC1 haga ping en la PC4.

c. Desde la PC2 haga ping en la PC3.