

Práctica de laboratorio: configuración de VTP, DTP y VLAN extendidas

Topología

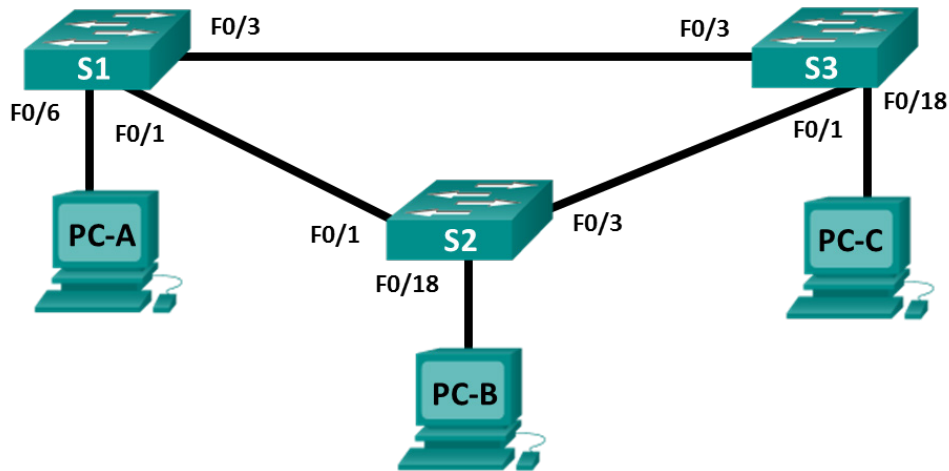


Tabla de direccionamiento

Encabezado de la tabla	Interfaz	Dirección IP	Máscara de subred
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
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.20.1	255.255.255.0
PC-C	NIC	192.168.10.2	255.255.255.0

Objetivos

- Parte 1. Configurar VTP
- Parte 2. Configurar DTP
- Parte 3. Agregar redes VLAN y asignar puertos
- Parte 4. Configurar VLAN extendidas

Aspectos básicos/situación

A medida que la cantidad de switches aumenta, la administración de VLAN y enlaces troncales en una red puede convertirse en un desafío. 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 automatizada entre los dispositivos de red. El protocolo DTP se encuentra habilitado de manera predeterminada en los switches Catalyst 2960 y Catalyst 3560.

En esta práctica de laboratorio, configurará enlaces troncales entre los switches. También configurará un servidor VTP y clientes VTP en el mismo dominio VTP. Además, configurará una VLAN extendida en uno de los switches, asignará puertos a las VLAN y comprobará la conectividad completa dentro de la misma VLAN.

Nota: Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros 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.

Nota: Asegúrese de que los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 3 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 3 PC (Windows 7 u 8 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

Parte 1: Configurar el VTP

Todos los switches se configurarán de modo que usen VTP para las actualizaciones de VLAN. S2 se configurará como el servidor. Los switches S1 y S3 se configurarán como clientes. Estarán en el dominio VTP **CCNA** y usarán la contraseña **cisco**.

- a. Configure S2 como servidor VTP en el dominio VTP **CCNA** y utilice **cisco** como contraseña VTP.

```
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S2(config)#
*Mar  1 00:03:44.193: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
S2(config)# vtp mode server
Device mode already VTP Server for VLANS.
S2(config)# vtp password cisco
Setting device VTP password to cisco
```

- b. Configure S1 y S3 como clientes VTP en el dominio VTP **CCNA** y utilice **cisco** como contraseña VTP. A continuación, se muestran las configuraciones de VTP.

```
S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
*Mar  1 00:03:44.193: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
S1(config)# vtp mode client
Device mode VTP client for VLANS.
S1(config)# vtp password cisco
Setting device VTP password to cisco
```

- c. Introduzca el comando **show vtp status** en todos los switches para comprobar las configuraciones de VTP. A continuación, se muestra el estado de VTP para S3.

```
S3# show vtp status
VTP Version capable           : 1 to 3
VTP version running           : 1
```

```
VTP Domain Name           : CCNA
VTP Pruning Mode          : Disabled
VTP Traps Generation      : Disabled
Device ID                  : 0cd9.96d2.3580
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Feature VLAN:

```
VTP Operating Mode        : Client
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
Configuration Revision     : 0
MD5 digest                 : 0x8B 0x58 0x3D 0x9D 0x64 0xBE 0xD5 0xF6
                           0x62 0xCB 0x4B 0x50 0xE5 0x9C 0x6F 0xF6
```

Parte 2: Configurar DTP

Paso 1: Configurar enlaces troncales dinámicos entre S1 y S2.

- a. Introduzca el comando **show interfaces f0/1 switchport** en S1 y S2.
¿Cuáles son los modos administrativo y operativo del puerto de switch f0/1?

-
- b. En el modo de configuración de interfaz, configure un enlace troncal dinámico entre S1 y S2. Debido a que el modo predeterminado es `dynamic auto`, solo un extremo del enlace debe configurarse como `dynamic desirable`.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
S1(config-if)#
*Mar 1 00:30:45.082: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar 1 00:30:48.102: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

- c. Con el comando **show interfaces trunk**, compruebe el enlace troncal entre el S1 y el S2.

```
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
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none
```

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

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1

Paso 2: Configurar un enlace troncal estático entre S1 y S3.

- a. Entre S1 y S3, configure un enlace troncal estático con el comando **switchport mode trunk** en el modo de configuración de interfaz para el puerto F0/3.

```
S1(config)# interface f0/3  
S1(config-if)# switchport mode trunk
```

- b. Compruebe los enlaces troncales con el comando **show interfaces trunk** en el S1.

S1# **show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1
Fa0/3	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/3	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1
Fa0/3	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	none
Fa0/3	none

- c. Configure un enlace troncal permanente entre S2 y S3.
- d. Registre los comandos que utilizó para crear el enlace troncal estático.

Parte 3: Agregar redes VLAN y asignar puertos

Paso 1: Agregar VLAN en los switches.

- a. En S1, agregue la VLAN 10.

```
S1(config)# vlan 10
```

¿Pudo crear la VLAN 10 en S1? Explique.

- b. En S2, agregue las siguientes VLAN.

VLAN	Nombre
10	Rojo
20	Azul
30	Amarillo
99	Administración

```
S2(config)# vlan 10
S2(config-vlan)# name Red
S2(config-vlan)# vlan 20
S2(config-vlan)# name Blue
S2(config-vlan)# vlan 30
S2(config-vlan)# name Yellow
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# end
```

```
S2# show vlan brief
```

```
VLAN Name                Status      Ports
-----
1    default                active     Fa0/2, 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   Red                    active
20   Blue                   active
30   Yellow                 active
99   Management             active
<resultado omitido>
```

Paso 2: Comprobar las actualizaciones de VTP en el S1 y el S3.

Debido a que S2 está configurado como servidor VTP, y S1 y S3 están configurados como clientes VTP, S1 y S3 deben obtener y implementar la información de VLAN de S2.

¿Qué comandos **show** utilizó para comprobar las actualizaciones de VTP en S1 y S3?

Paso 3: Asignar puertos a las VLAN.

En este paso, asociará puertos a las VLAN y configurará direcciones IP de acuerdo con la tabla a continuación.

Asignación de puertos	VLAN	Dirección IP y prefijo de la PC asociada
S1 F0/6	VLAN 10	PC-A: 192.168.10.1 / 24
S2 F0/18	VLAN 20	PC-B: 192.168.20.1 /24
S3 F0/18	VLAN 10	PC-C: 192.168.10.2 /24

- En S1, configure F0/6 en modo de acceso y asigne F0/6 a la VLAN 10.

```
S1(config)# interface f0/6  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 10
```
- Repita el procedimiento para el puerto de switch F0/18 en S2 y S3. Asigne la VLAN según la tabla anterior.
- Asigne las direcciones IP a las computadoras según la tabla anterior.

Paso 4: Configurar direcciones IP en switches.

- En S1, asigne la dirección IP a la SVI para VLAN 99 según la tabla de direcciones y active la interfaz.

```
S1(config)# interface vlan 99  
S1(config-if)# ip address 192.168.99.1 255.255.255.0  
S1(config-fi)# no shutdown
```
- Repita el paso A para los switches S2 y S3.

Paso 5: Verificar la conectividad de extremo a extremo.

- Desde la PC-B, haga ping en la PC-A. ¿Tuvo éxito? Explique.

- Desde la PC-C, haga ping en la PC-A. ¿Tuvo éxito? Explique.

- Desde el S1, haga ping en la PC-A. ¿Tuvo éxito? Explique.

- Desde el S2, haga ping en el S1. ¿Tuvo éxito? Explique.

Parte 4: Configurar una VLAN extendida

Una VLAN extendida es una VLAN entre 1025 y 4096. Como las VLAN extendidas no pueden administrarse con VTP, VTP debe configurarse en modo transparente. En esta parte, cambiará el modo VTP del S1 a transparente y creará una VLAN extendida en el S1.

Paso 1: Configurar el modo de VTP en transparente en el S1.

- a. En el switch S1, establezca el modo VTP en transparente.

```
S1(config)# vtp mode transparent
Setting device to VTP Transparent mode for VLANs.
S1(config)# exit
```

- b. Compruebe el modo de VTP en el S1.

```
S1# show vtp status
VTP Version capable          : 1 to 3
VTP version running         : 1
VTP Domain Name              : CCNA
VTP Pruning Mode             : Disabled
VTP Traps Generation        : Disabled
Device ID                    : 0cd9.96e2.3d00
Configuration last modified by 0.0.0.0 at 3-1-93 02:36:11

Feature VLAN:
-----
VTP Operating Mode           : Transparent
Maximum VLANs supported locally : 255
Number of existing VLANs     : 9
Configuration Revision       : 0
MD5 digest                   : 0xB2 0x9A 0x11 0x5B 0xBF 0x2E 0xBF 0xAA
                               0x31 0x18 0xFF 0x2C 0x5E 0x54 0x0A 0xB7
```

Paso 2: Configurar una VLAN extendida en S1.

- a. Visualice las configuraciones actuales de VLAN en S1.
b. Cree la VLAN extendida 2000.

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# vlan 2000
S1(config-vlan)# end
```

- c. Compruebe la creación de la VLAN.

```
S1# show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, 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 Red	active	Fa0/6
20 Blue	active	
30 Yellow	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
2000 VLAN2000 active
```

Reflexión

¿Cuáles son las ventajas y desventajas de usar VTP?

Tabla de resumen de interfaces del router

Resumen de la interfaz del router				
Modelo de router	Interfaz Ethernet 1	Interfaz Ethernet 2	Interfaz serial 1	Interfaz serial 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: Para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.