Práctica de laboratorio 4.4.1: Configuración básica del VTP

Diagrama de topología

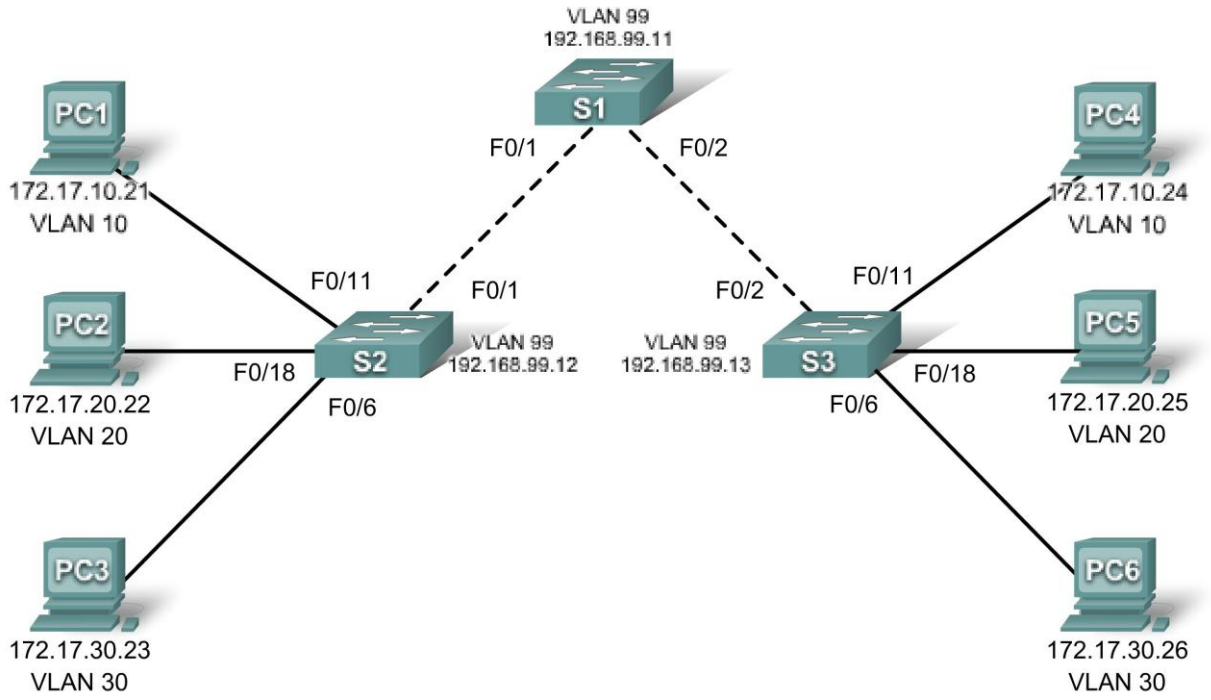

Tabla de direccionamiento

Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	172.17.99.11	255.255.255.0	No aplicable
S2	**VLAN 99**	172.17.99.12	255.255.255.0	No aplicable
S3	**VLAN 99**	172.17.99.13	255.255.255.0	No aplicable
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Asignaciones de puertos (Switches 2 y 3)

Puertos	Asignación	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30: Guest (predeterminada)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración inicial y volver a cargar un switch al estado predeterminado
- Realizar las tareas de configuración básicas en un switch
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches
- Habilitar el enlace troncal en conexiones entre switches
- Verificar la configuración de enlace troncal
- Modificar los modos VTP y observar el impacto.
- Crear las VLAN en el servidor VTP y distribuir la información de estas VLAN a los switches en la red.
- Explicar las diferencias en operación entre el modo VTP transparente, el modo servidor y el modo cliente.
- Asignar puertos de switch a las VLAN.
- Guardar la configuración de la VLAN
- Permitir depuraciones de VTP en la red
- Explicar de qué modo la depuración reduce el tráfico de broadcast innecesario en la LAN.

Tarea 1: Preparar la red

Paso 1: Cablear una red de manera similar al diagrama de topología.

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en la topología. El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960. El uso de cualquier otro tipo de switch puede producir resultados distintos. Si va a usar switches más antiguos, algunos comandos pueden ser diferentes o no estar disponibles.

Observe en la Tabla de direccionamiento que las PC se han configurado con una dirección de IP predeterminada de la gateway. Ésta sería la dirección IP del router local que no se incluye en este escenario de práctica de laboratorio. La gateway predeterminada, el router sería necesario para las PC en diferentes VLAN para poder comunicarse. Esto se analiza más adelante, en otro capítulo.

Establezca conexiones de consola en los tres switches.

Paso 2: Borrar toda configuración existente en los switches.

De ser necesario, consulte la Práctica de laboratorio 2.5.1, Apéndice 1 para leer sobre el procedimiento para borrar las configuraciones del switch y las VLAN. Utilice el comando **show vlan** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.

```
S1#show vlan

Nombre de la VLAN                     Estado    Puertos
---- -------------------------------- --------- -------------------------------
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
```

Paso 3: Deshabilitar todos los puertos con el comando shutdown.

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown
```

```
S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown
```

```
S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Paso 4: Volver a habilitar los puertos de usuario en S2 y S3.

Configure los puertos de usuario en modo de acceso. Consulte el diagrama de topología para determinar cuáles puertos están conectados a dispositivos de usuario final.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

```
S3(config)#interface fa0/6
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/11
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
```

Tarea 2: Realizar las configuraciones básicas del switch

Configure los switches S1, S2 y S3 según las siguientes pautas y guarde todas sus configuraciones:

- Configure el nombre de host del switch según lo indicado en la topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **class**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

(Se muestran los resultados para S1)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. Finalice con CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configurado desde la consola por la consola
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Tarea 3: Configurar las interfaces Ethernet en las PC Host

Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP y las gateways predeterminadas indicadas en la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Verifique que la PC1 pueda hacer ping a PC4; que la PC2 pueda hacer ping a la PC5 y que la PC3 pueda hacer ping a la PC6.

Tarea 4: Configurar VTP en los switches

VTP permite al administrador de redes controlar las instancias de las VLAN en la red creando dominios VTP. Dentro de cada dominio VTP se configuran uno o más switches con servidores VTP. Las VLAN se crean en el servidor VTP y se informan a los otros switches en el dominio. Las tareas comunes de configuración VTP son la configuración del modo operativo, del dominio y de la contraseña. En esta práctica de laboratorio se utilizará a S1 como el servidor VTP, con S2 y S3 configurados como clientes o en el modo transparente de VTP.

Paso 1: Verificar las configuraciones VTP actuales en los tres switches.

```
S1#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S2#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S3#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que los tres switches se encuentran en modo servidor. El modo servidor es el modo VTP predeterminado para la mayoría de los switches Catalyst.

Paso 2: Configurar el modo operativo, el nombre de dominio y la contraseña de VTP en los tres switches.

Establezca **Lab4** como nombre de dominio VTP y **cisco** como contraseña en los tres switches. Configure S1 en modo servidor, S2 en modo cliente, y S3 en modo transparente.

```
S1(config)#vtp mode server
Modo dispositivo ya es SERVIDOR VTP.
S1(config)#vtp domain Lab4
Cambiar el nombre del dominio VTP de NULL a Lab4
S1(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S1(config)#end

S2(config)#vtp mode client
Configurar el dispositivo en modo CLIENTE VTP
S2(config)#vtp domain Lab4
Cambiar el nombre del dominio VTP de NULL a Lab4
S2(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S2(config)#end

S3(config)#vtp mode transparent
Configurar el dispositivo en modo TRANPARENT VTP.
S3(config)#vtp domain Lab4
Cambiar el nombre del dominio VTP de NULL a Lab4
S3(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S3(config)#end
```

Nota: El nombre del dominio VTP puede ser aprendido por un switch de cliente desde un switch de servidor pero solamente si el dominio del switch de cliente se encuentra en estado nulo. No puede aprender un nombre nuevo si un nombre fue establecido anteriormente. Por esta razón, es una buena práctica configurar el nombre de dominio manualmente en todos los switches para asegurar que el nombre del dominio sea configurado correctamente. Los switches en diferentes dominios VTP no intercambian información de VLAN.

Paso 3: Configurar los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en los tres switches.

Simplifique esta tarea con el comando **interface range** en el modo de configuración global.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Paso 4: Configurar la seguridad de Puerto en los switches de capa de acceso S2 y S3.

Configure los puertos fa0/6, fa0/11 y fa0/18 de modo tal que sólo permitan un solo host y aprendan la dirección MAC del host de manera dinámica.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end

S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Paso 5: Configurar las VLAN en el servidor VTP.

Hay cuatro VLAN adicionales que se requieren en esta práctica de laboratorio:

- VLAN 99 (administración)
- VLAN 10 (cuerpo docente/personal)
- VLAN 20 (estudiantes)
- VLAN 30 (guest)

Configúrelas en el servidor VTP.

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
```

Verifique que se hayan creado las VLAN en S1 con el comando **show vlan brief**.

Paso 6: Verificar que las VLAN creadas en S1 se hayan distribuido a S2 y S3.

Utilice el comando **show vlan brief** en S2 y S3 para determinar si el servidor VTP ha pulsado su configuración VLAN a todos los switches.

```
S2#show vlan brief

Nombre de VLAN                          Estado    Puerto
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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   faculty/staff                    active
20   students                         active
30   guest                            active
99   management                       active

S3#show vlan brief

Nombre de la VLAN                       Estado    Puertos
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

¿Están configuradas las mismas VLAN en todos los switches? _____

Explique por qué S2 y S3 tienen diferentes configuraciones de VLAN en este momento. _____

_____

_____

Paso 7: Crear una nueva VLAN en switches 2 y 3.

```
S2(config)#vlan 88
%VTP VLAN configuration not allowed when device is in CLIENT mode.

S3(config)#vlan 88
S3(config-vlan)#name test
S3(config-vlan)#
```

¿Por qué no se le permite crear una nueva VLAN en S2 pero sí en S3? _____

_____

Borre la VLAN 88 de S3.

```
S3(config)#no vlan 88
```

Paso 8: Configurar las VLAN en forma manual.

Configure las cuatro VLAN identificadas en el Paso 5 en el switch S3.

```
S3(config)#vlan 99
S3(config-vlan)#name management
S3(config-vlan)#exit
S3(config)#vlan 10
S3(config-vlan)#name faculty/staff
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name students
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name guest
S3(config-vlan)#exit
```

Aquí se aprecia una de las ventajas del VTP. La configuración manual es tediosa y puede suscitar errores y cualquier error introducido aquí puede evitar la comunicación entre VLAN. Además, puede resultar difícil diagnosticar este tipo de errores.

Paso 9: Configurar la dirección de la interfaz de administración en los tres switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
```

```
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
```

```
S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Verifique que todos los switches estén correctamente configurados haciendo ping entre ellos. Desde S1, haga ping a la interfaz de administración en S2 y S3. Desde S2, haga ping a la interfaz de administración en S3.

¿Los pings son exitosos? _____

En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.

Paso 10: Asignar puertos de switch a las VLAN.

Consulte la tabla de asignación de puertos al principio de la práctica de laboratorio para asignar puertos a las VLAN. Simplifique esta tarea con el comando **interface range**. Las asignaciones de puertos no se configuran a través del VTP. Las asignaciones de puerto deben ser configurado en cada switch manualmente o dinámicamente utilizando un servidor VMPS. Los comandos se muestran para S3 solamente, pero los switches S2 y S1 deben ser configurados de manera similar. Cuando termine, guarde la configuración.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [intro]
Building configuration...
[OK]
S3#
```

Tarea 5: Configurar la depuración VTP en los switches

La depuración VTP permite a un servidor VTP suprimir tráfico de broadcast IP para VLAN específicas a switches que no tienen ningún puerto en esa VLAN. De manera predeterminada, todos los multicasts y broadcasts en una VLAN se saturan en toda la VLAN. Todos los switches en la red reciben todos los broadcasts, incluso en situaciones en las que unos pocos usuarios están conectados a esa VLAN. La depuración del VTP se utiliza para eliminar o depurar este tráfico innecesario. La depuración ahorra banda ancha LAN porque los broadcasts no tienen que ser enviados a los switches que no los necesitan.

La depuración se configura en el switch del servidor mediante el comando **vtp pruning** en modo de configuración global. La configuración se pulsa a los switches de clientes. Sin embargo, puesto que S3 está en modo transparente, la depuración de VTP debe configurarse localmente en ese switch.

Confirme la configuración de depuración VTP en cada switch utilizando el commando **show vtp status**. El modo de depuración VTP debe estar activado en cada switch.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 17
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Servidor
VTP Domain Name                 : Lab4
VTP Pruning Mode                : Habilitado
<resultado omitido>
```

Tarea 6: Limpieza

Borre las configuraciones y vuelva a cargar los switches. Desconecte y guarde el cableado. En caso de PC hosts que están normalmente conectadas a otras redes (tales como la LAN de la escuela o de Internet) vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.