

Configuración de VLAN y Troncales

Un switch divide los dominios de colisión y es un dominio de difusión único. Entonces, ¿cómo romper un dominio individual de difusión en múltiples dominios de difusión? **VLAN (Virtual LAN)** lo hace posible y en un solo switch podemos tener múltiples dominios de difusión. Pero una vez que crea múltiples VLAN en un switch, resulta tedioso replicar la misma configuración en todos los demás switches. Aquí es donde entra en juego **VTP (VLAN Trunking Protocol)**. Por lo tanto, tenemos múltiples switches con diferentes VLAN y VTP, lo que facilita la administración. Pero, ¿cómo hacemos que un dispositivo en una VLAN se comunique con un dispositivo en otra VLAN? Cubriremos esto en el enrutamiento InterVLAN.

Creación de VLAN y dominios VTP

VLAN es una tecnología utilizada para dividir una red única de capa 2 en múltiples dominios de difusión. Esto se hace para restringir la comunicación entre dispositivos que comparten el mismo medio de difusión. Sin embargo, estos dispositivos se pueden comunicar entre sí a través de un dispositivo de capa 3, como un enrutador o router. Esto es similar a conectar dispositivos a diferentes switches y luego conectarlos a un enrutador para separar el tráfico de difusión.

A medida que se crean más y más VLAN, resulta tedioso replicar la configuración en todos los switches, razón por la cual se creó VTP.

Primero aprenderemos sobre la creación de VLAN y la asignación de puertos a ella. La VLAN 1 se crea de manera predeterminada en todos los switches, y todos los puertos residen en ella. Esta VLAN se llama **VLAN de administración**.

Para crear una VLAN, use el siguiente comando:

```
Sw1(config)#vlan 2
```

La VLAN ID puede estar entre 1 y 1001. Los ID 1002, 1003, 1004 y 1005 están reservados. Una vez que se ha ingresado este comando, va al modo de subconfiguración de VLAN. Este es el lugar donde podemos asignar un nombre a la VLAN.

```
Sw1(config-vlan)#name finance
```

Asignar un nombre a una VLAN es opcional; de forma predeterminada, el nombre es VLAN0002. A continuación, asignaremos algunos puertos a esta VLAN. Para asignar muchos puertos a una sola VLAN, se puede usar el comando de rango, que luego selecciona múltiples interfaces.

```
Sw1(config)#interface range f0/10-20
```

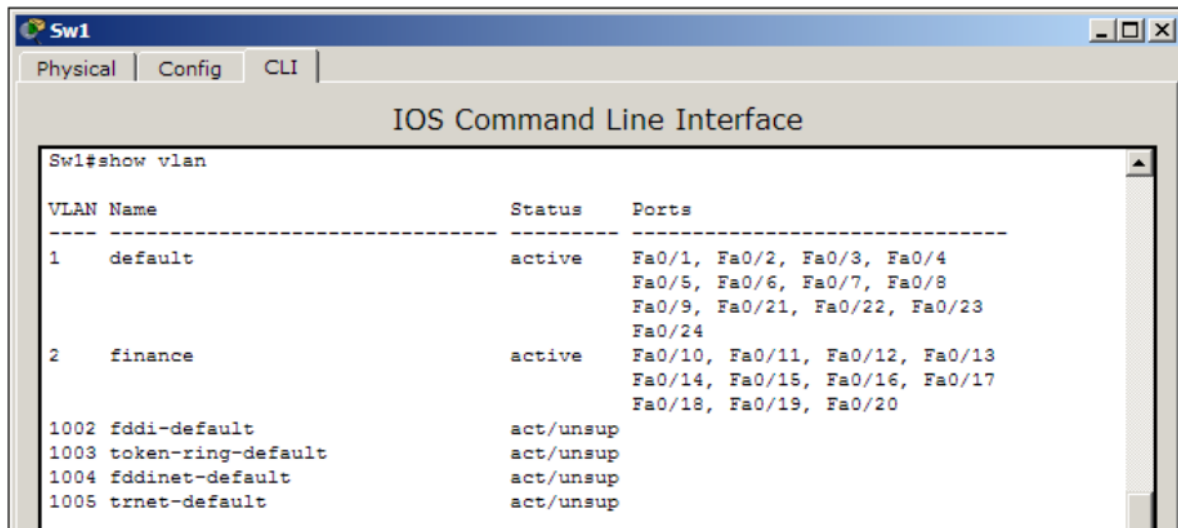
Para asignar estos puertos a la VLAN 2, use el siguiente comando:

¹ Traducción libre realizada por Wilfredo Cruz Yarlequé (Universidad Nacional de Piura, Perú), del Chapter 10: *Border Configuring VLAN and Trunks* del libro de **Jesin A**, «**Packet Tracer Network Simulator**», editado por Packt Publishing Ltd., año 2014. Licencia [Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/).

```
Sw1(config-if-range)#switchport access vlan 2
```

Verifiquemos si los puertos fueron asignados a la VLAN correcta.

```
Sw1#show vlan
```

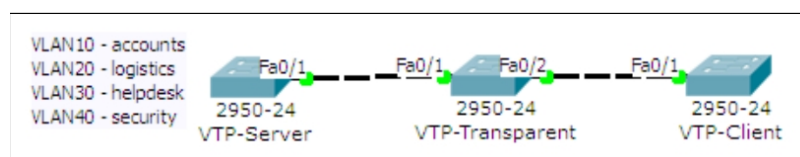


Tenga en cuenta que en el ejemplo anterior, parte de la salida se ha omitido por brevedad.

Ahora crearemos una topología con tres switches para demostrar VTP. VTP tiene tres modos: servidor, cliente y transparente.

- **Server** / Servidor: este es el modo predeterminado de VTP; en este modo, los switches pueden modificar sus VLAN y enviar anuncios VTP.
- **Client** / Cliente: en este modo, los switches escuchan los anuncios de VTP desde otros switches de servidor. Los switches de cliente no pueden modificar su base de datos de VLAN localmente.
- **Transparent** / Transparente: este modo funciona de forma independiente de otros switches. En este modo, el switch solo reenvía los anuncios de VTP que recibe y no genera ninguno, ni modifica sus propias VLAN basadas en los anuncios de VTP.

La siguiente topología se usará para la demostración:



1. En el primer switch (Servidor VTP), tendremos cuatro VLAN con diferentes nombres. Luego, estableceremos todos los puertos del switch de conmutación en trunking.

```
VTP-Server(config)#interface Fa0/1
VTP-Server(config-if)#switchport mode trunk
```

```
VTP-Transparent(config)#interface range Fa0/1-2
VTP-Transparent(config-if-range)#switchport mode trunk
```

```
VTP-Client(config)#interface Fa0/1
VTP-Client(config-if)#switchport mode trunk
```

2. Como VTP ya está en modo servidor, simplemente cambiaremos el nombre de dominio VTP y estableceremos una contraseña.

```
VTP-Server(config)#vtp domain My-Office
```

Cambiar el nombre de dominio VTP de NULL a My-Office

```
VTP-Server(config)#vtp password secreta
```

Establecer la contraseña de la base de datos de VLAN del dispositivo a **secreta**

3. Avance al segundo switch (**VTP-Transparent**) y hágalo transparente.

```
VTP-Transparent(config)#vtp mode transparent
```

4. La tarea final es mover el tercer switch (VTP-Client) al modo cliente.

```
VTP-Client(config)#vtp mode client
```

5. Cambiar el dominio, lo que hará que el cliente recoja el nombre de dominio del servidor. Es necesario configurar la contraseña de VTP.

```
VTP-Client(config)#vtp domain My-Office
```

```
VTP-Client(config)#vtp password secreta
```

La configuración está hecha; ahora, use el comando show vlan en el switch **VTP-Client** para ver las nuevas VLAN. Este ejemplo es solo para demostrar VTP. Esta topología no permitirá la comunicación normal entre **VTP-Server** y el **VTP-Client**, ya que el switch en el medio (**VTP-Transparent**) no tiene ninguna de las VLAN que configuramos.

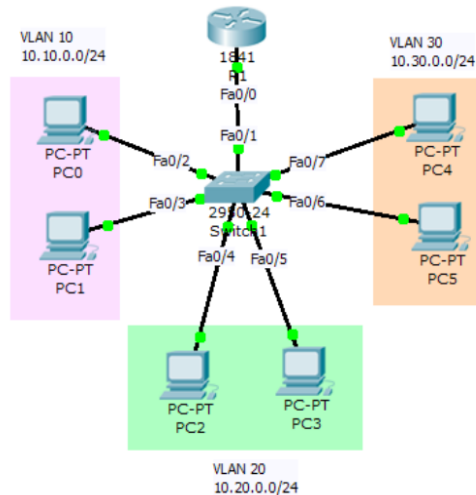
Enrutamiento InterVLAN con enrutadores y switches capa 3

Aunque la VLAN se usa para dividir el dominio de difusión, es necesario habilitar la comunicación entre dos o más VLAN en la capa 3 mediante el enrutamiento IP. Esto se denomina enrutamiento InterVLAN y se puede configurar usando enrutadores y switches de capa 3. Esto requiere asignar una subred IP diferente para dispositivos en cada VLAN.

Configuraremos el enrutamiento de InterVLAN conectando el enrutador a un switch utilizando un solo enlace. Todo el tráfico a otras VLAN pasa a través de este enlace, al enrutador y viceversa a través de este enlace. Este método de configuración también se denomina **router-on-a-stick**, ya que un único enlace al enrutador maneja todo el tráfico.

InterVLAN con un enrutador

Utilizaremos la siguiente topología para esta configuración:



Como se indicó anteriormente, cada VLAN tendrá direcciones IP de diferentes rangos de red y la interfaz del enrutador tendrá tres direcciones IP, cada una perteneciente a una red diferente.

1. Después de que se hayan asignado las direcciones IP a todas las PC, cree las VLAN necesarias en el switch y asigne los puertos.

```
Sw1(config)#int range f0/2-3
Sw1(config-if-range)#switchport access vlan 10
Sw1(config-if-range)#int range f0/4-5
Sw1(config-if-range)#switchport access vlan 20
Sw1(config-if-range)#int range f0/6-7
Sw1(config-if-range)#switchport access vlan 30
```

2. Configure el puerto del switch que se conecta al enrutador como un enlace troncal. Más sobre esto en la sección de Enlaces Troncales Switch-to-switch.

```
Sw1(config)#int f0/1
Sw1(config-if)#switchport mode trunk
```

3. Ahora, pasando a la parte del enrutador de la configuración, levante la interfaz.

```
R1(config)#int f0/0
R1(config-if)#no shutdown
```

4. Ahora crearemos las subinterfaces. Cada uno tendrá su propia dirección IP en una red diferente.

```
R1(config-subif)#int f0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 10.10.0.1 255.255.255.0
R1(config-subif)#int f0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.20.0.1 255.255.255.0
R1(config-subif)#int f0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.30.0.1 255.255.255.0
```

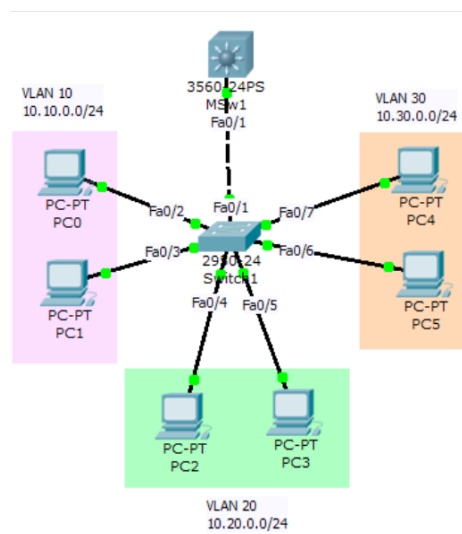
5. Observe el comando **encapsulation**. Especifica la ID de VLAN que manejará la interfaz.

6. Eso es todo, ahora prueba la conectividad entre hosts en diferentes VLAN usando PDU simples o un **ping**. El primer paquete siempre caducará ya que el ARP (Protocolo de Resolución de Direcciones) tarda un poco en completarse.

Intenta usar **tracert** para ver la ruta que toma el paquete.

InterVLAN en un switch de capa 3

El único switch de capa 3 presente en Packet Tracer es **3560-24PS**. Utilizaremos la misma topología reemplazando solo el enrutador con el switch de capa 3, como se muestra en la siguiente captura de pantalla:



La creación y configuración de VLAN es la misma en el switch de capa 2, por lo que no se repetirá aquí. Entonces, nos moveremos al switch de capa 3 inmediatamente.

1. Como el enlace switch-switch en el switch de la capa 2 se configuró en el modo troncalizado con el comando `switchport mode trunk`, el mismo puerto en el switch de la capa 3 también estará en el modo troncal. Esto se puede verificar de la siguiente manera:

```
MSw1#sh interface trunk
```

```
MSw1
Physical Config CLI
IOS Command Line Interface
MSw1#sh interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

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

El estado **trunking** lo indica. Más información sobre cómo este puerto se movió automáticamente a la troncal se discutirá en la siguiente sección (Enlaces Troncales Switch-a-switch).

2. Configuraremos lo que se llama **SVI (Switch Virtual Interface)**, que actuará como interfaces de capa 3 para cada VLAN.

```
MSw1(config)#int vlan 10
MSw1(config-if)#ip add 10.10.0.1 255.255.255.0
MSw1(config-if)#int vlan 20
MSw1(config-if)#ip add 10.20.0.1 255.255.255.0
MSw1(config-if)#int vlan 30
MSw1(config-if)#ip add 10.30.0.1 255.255.255.0
```

3. Estas interfaces permanecerán inactivas, ya que este switch de capa 3 no tiene VLAN 10, 20 ni 30. Entonces los crearemos de la siguiente manera:

```
MSw1(config)#vlan 10
MSw1(config-vlan)#vlan 20
MSw1(config-vlan)#vlan 30
```

4. A medida que se ingresa cada comando, aparecerá el SVI asociado. El enrutamiento IP debe estar habilitado.

```
MSw1(config)#ip routing
```

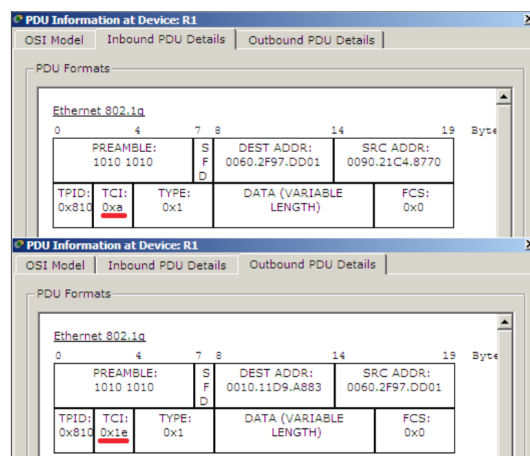
5. Use la herramienta PDU simple para probar la conectividad.

Aquí, también, el primer paquete siempre tendrá un tiempo de espera ya que el proceso ARP toma algo de tiempo.

Enlaces Troncales Switch-a-switch

Cuando dos switches se conectan entre sí, debe haber un mecanismo para identificar la VLAN a la que pertenece una trama. No estamos hablando de la capa física sino de la capa de enlace de datos. Cuando dos switches se conectan entre sí, cada uno necesita saber a qué red VLAN está destinado el tráfico. Aquí es donde entra el etiquetado VLAN; cuando una trama se mueve sobre un enlace switch-a-switch, el switch de origen etiqueta la trama con la ID de VLAN, y este enlace de switch-a-switch se conoce como enlace troncal.

A continuación se muestra una captura de pantalla de una PDU entrante y saliente, capturada en modo de simulación, cuando una PC en VLAN 10 conectó una PC en la VLAN 30:



Observe el campo **TCI (Tag Control Information / Información de Control de Etiquetas)** que contiene un valor hexadecimal; denota la ID de VLAN. Entonces, la PDU de entrada tiene **0xa**, que es un origen de VLAN 10, y la PDU de salida tiene **0x1e**, que es un destino de VLAN 30.

Analizando broadcast en el modo de simulación

El concepto de VLAN es dividir el dominio de difusión: por lo tanto, en esta sección, veremos cómo se manejan las transmisiones en un entorno de VLAN utilizando el modo de simulación. Use la misma topología InterVLAN que utilizamos anteriormente. Desde **PC0** haga **ping** a **255.255.255.255**, establece la dirección MAC de destino en **FFFF.FFFF.FFFF**, que es la dirección de difusión de la capa 2. Cambie al modo de simulación y vea qué sucede. El switch recibe un paquete ICMP de **PC0** y envía dos copias: una al enrutador y otra a la PC1. Si esta red no estuviera dividida en VLAN, el paquete ICMP se habría enviado a todas y cada una de las PC conectadas al switch.

Resumen

En este capítulo, aprendimos cómo usar los dispositivos en Packet Tracer para crear VLAN y configurar VTP para facilitar su administración. También configuramos el enrutamiento InterVLAN con enrutadores y switches de capa 3. Entonces, ya estarías familiarizado con los SVI de estos switches de capa 3. Finalmente, aprendimos sobre las diferencias entre los enlaces switch-PC normales y los enlaces switch-a-switch, que también se denominan troncales. El modo de simulación de Packet Tracer es de gran ayuda aquí, ya que permite visualizar el flujo de paquetes en un entorno de VLAN.