CCNA 3 – Tema 2 : Escalamiento de VLAN

El protocolo VTP (VLAN Trunking Protocol, protocolo de enlaces troncales de VLAN) reduce la administración en una red conmutada.

El uso de redes VLAN para segmentar una red conmutada proporciona más rendimiento, seguridad y capacidad de administración. Se utilizan enlaces troncales para transportar información de varias VLAN entre dispositivos. El protocolo DTP (Dynamic Trunking Protocol, protocolo de enlace troncal dinámico) permite que los puertos negocien automáticamente los enlaces troncales entre los switches.

Dado que las VLAN segmentan la red y se encuentran cada una en su propia red o subred, se requiere un proceso de capa 3 para permitir que el tráfico se desplace de una VLAN a otra.

# VTP, VLAN extendidas y DTP

VTP permite que un administrador de redes maneje las VLAN en un switch configurado como servidor VTP. El servidor distribuye y sincroniza la información de la VLAN en los enlaces troncales a los switches habilitados por el VTP en toda la red conmutada. Esto elimina la necesidad de configurar la VLAN nueva en cada switch.

*VTP solo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005).*

*El protocolo VTP guarda configuraciones de VLAN en vlan.dat*

## Conceptos y funcionamiento de VTP

Un switch puede configurarse en uno de los tres modos de VTP.

|  |  |
| --- | --- |
| Nombre | Definición |
| Servidor VTP | * Anuncia la información de VLAN del dominio de VTP a otros switches habilitados para VTP en el mismo dominio VTP. * Almacena la información de VLAN para todo el dominio en la NVRAM. * Crea, elimina o cambia los nombres de las VLAN para el dominio. * Modo predeterminado del protocolo VTP. |
| Cliente VTP | * Un switch en este modo no puede crear, cambiar o eliminar las VLAN. * Almacena la información de VLAN para todo el dominio en la RAM. * Debe configurarse como cliente VTP. |
| VTP transparente | * Un switch en este modo no participa en VTP, excepto para enviar publicaciones del VTP a los clientes y servidores. * Las VLAN de estos switches son locales. * Debe configurarse como VTP transparente. |

**Nota**: Un switch que está en modo servidor o modo cliente con un número de revisión de configuración más alto que el servidor VTP existente actualiza toda la información de la VLAN en el dominio VTP. Cisco recomienda, como mejor práctica, implementar VTP en modo transparente para tener más control de VLAN, seguridad y capacidad de administración.

### Publicaciones del VTP

El VTP emite tres tipos de publicaciones:

* Publicaciones de resumen. Informan a los switches adyacentes el nombre de dominio de VTP y el número de revisión de configuración. Cada 5 minutos predeterminado.
* Solicitud de publicación. Responde a un mensaje de publicación de resumen cuando la publicación de resumen contiene un número de revisión de configuración más alto que el valor actual.
* Publicaciones de subgrupos. Contienen información de VLAN, incluido cualquier cambio.

Cuando un switch recibe un paquete de publicación de resumen, compara el nombre de dominio de VTP con su propio nombre de dominio de VTP. Si el nombre es diferente, el switch simplemente ignora el paquete. Si el nombre es el mismo, el switch compara la revisión de configuración con su propia revisión. Si el número de revisión de la configuración es mayor o igual al número de revisión de configuración del paquete, se ignora el paquete. Si el número de revisión de la configuración es más bajo, se envía una solicitud de publicación que solicita para el mensaje de publicación del subgrupo.

El mensaje de publicación de subgrupo contiene información de la VLAN con cualquier cambio. Al agregar, eliminar o cambiar una VLAN en el servidor VTP, el servidor del VTP aumenta la revisión de configuración y emite una publicación de resumen. Una o varias publicaciones de subgrupos siguen la publicación de resumen que incluye la información de VLAN que incluye cualquier cambio. Este proceso se muestra en la figura.

### Configuración predeterminada del protocolo VTP

Para ver el estado del protocolo VTP en el switch:

**S1# show vtp status**

Información que ofrece:

* Versión de VTP. Predeterminado 1.
* Nombre de dominio del VTP. Predeterminado null
* Modo de depuración del VTP. Muestra si la depuración está activada. De manera prederminada no lo está.
* Generación de traps del VTP. Muestra si se envían traps hacia la estación de administración de red.
* Identificador del dispositivo (MAC del switch).
* Modo operativo del VTP.
* Cantidad de VLAN permitidas y existentes.
* Revisión de la configuración.

### Advertencias del VTP

Agregar un switch con VTP habilitado a un dominio de VTP existente borrará las configuraciones de la VLAN existente en el dominio si el nuevo switch se configura con distintas VLAN y tiene un número de revisión de configuración más alto que el servidor VTP existente. El nuevo switch puede ser servidor VTP o switch de cliente. Esta propagación puede ser difícil de corregir. Por lo tanto, cuando un switch se agrega a una red, asegúrese de que tenga la configuración predeterminada del VTP.

El número de revisión de configuración del VTP se almacena en la NVRAM (o Flash en algunas plataformas) y no se restablece si borra la configuración del switch y lo vuelve a cargar. Para restablecer el número de revisión de configuración del VTP en cero tiene dos opciones:

* Cambie el dominio VTP del switch a un dominio VTP inexistente y luego vuelva a cambiar el dominio al nombre original.
* Cambie al modo VTP del switch al modo transparente y luego vuelva al modo anterior del VTP.

## Configuración del VTP

Pasos para la configuración general:

1. Configurar el servidor VTP

**S1(config)#vtp mode {server|off|server|transparent}**

Para confirmar:

**S1#show vtp status**

*El número de revisión será aún 0.*

1. Configurar el nombre de dominio y la contraseña del VTP

**S1(config)#vtp domain *nombre-dominio***

**S1(config)#vtp password *contraseña-dominio***

Para confirmar:

**S1#show vtp password**

1. Configurar los clientes VTP

**S2(config)#vtp mode client**

**S2(config)#vtp domain *nombre-dominio***

**S2(config)#vtp password *contraseña-dominio***

1. Configurar la VLAN en el servidor VTP

**S1(config)#vlan *número***

**S1(config-vlan)#name *NOMBRE***

Para confirmar:

**S1#show vlan brief**

**S1#show vtp status** -> “Configuration revision” = Cada cambio (agregar vlan, darle nombre… aumenta en uno el número)

1. Verificar que los clientes VTP han recibido la nueva información.

**S2#show vlan brief** -> se han añadido las vlan de S1

**S2#show vtp status** -> “Configuration revision”

## VLAN extendidas

Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar las ID de las VLAN de rango extendido.

Se identifican mediante una ID de VLAN entre 1006 y 4094.

Las configuraciones no se escriben en el archivo vlan.dat. Se guardan en el archivo de configuración en ejecución de manera predeterminada.

**VTP no aprende las VLAN de rango extendido.**

Para configurar una VLAN extendida en un switch 2960, se debe establecer en el modo VTP transparente.

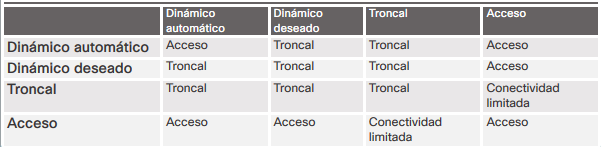
**S1(config)#vtp mode transparent**

**S1(config)#vlan 2000**

## Protocolo de enlace troncal dinámico (DTP)

La negociación de enlaces troncales entre dispositivos de red la maneja el protocolo de enlace troncal dinámico (DTP), que solo funciona de punto a punto. DTP maneja la negociación de enlaces troncales solo si el puerto del switch vecino está configurado en un modo de enlace troncal que admite DTP.

Para habilitar los enlaces troncales desde un switch Cisco hacia un dispositivo que no admite DTP, utilice los comandos **switchport mode trunk** y **switchport nonegotiate** del modo de configuración de interfaz. Esto hace que la interfaz se convierta en un enlace troncal, pero sin que genere tramas DTP.



* **Switchport mode access**. Coloca la interfaz (puerto de acceso) en modo de enlace no troncal permanente y negocia para convertir el enlace en uno no troncal. La interfaz se convierte en una interfaz no troncal, independientemente de si la interfaz vecina es una interfaz troncal.
* **Switchport mode Dynamic desirable**. Hace que la interfaz intente convertir el enlace en un enlace troncal de forma activa. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en modo de enlace troncal, deseado o dinámico automático.
* **Switchport mode trunk.** Coloca la interfaz en modo de enlace troncal permanente y negocia para convertir el enlace en un enlace troncal. La interfaz se convierte en una interfaz de enlace troncal, incluso si la interfaz vecina no es una interfaz de enlace troncal.
* **Switchport nonegotiate**. Evita que la interfaz genere tramas DTP. Puede utilizar este comando solo cuando el modo de switchport de la interfaz es **access** o **trunk**. Para establecer un enlace troncal, debe configurar manualmente la interfaz vecina como interfaz troncal.

Para ver el modo DTP actual:

**Show dtp interface**

**Nota:** por lo general, se recomienda que la interfaz se establezca en **trunk** y **nonegotiate** cuando se requiere un enlace troncal. Se debe inhabilitar DTP en los enlaces cuando no se deben usar enlaces troncales.

# Conmutación en capa 3

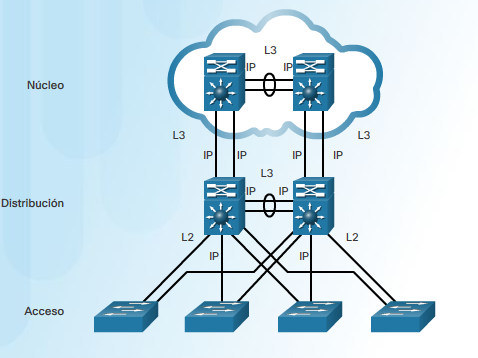
Los router multicapa admiten los tipos de interfaces de capa 3:

* **Puerto enrutado.** Puramente capa 3, similar a la interfaz de un router.
* **Interfaz virtual del switch (SVI)**. Una interfaz VLAN virtual para enrutamiento de VLAN.

## Funcionamiento y configuración

El routing se puede transferir a las capas de núcleo y de distribución (y, en ocasiones, incluso a la capa de acceso) sin afectar el rendimiento de la red.

Muchos usuarios están en VLAN separadas, y cada VLAN suele ser una subred distinta. Por lo tanto, resulta lógico configurar los switches de distribución como gateways de capa 3 para los usuarios de la VLAN de cada switch de acceso.



Los puertos de capa 3 (enrutados) se suelen implementar entre la capa de distribución y la capa de núcleo.

Motivos para configurar SVI:

* Proporcionar Gateway a VLAN para poder enrutar tráfico dentro/fuera de la VLAN
* Proporcionar conectividad IP de capa 3 al switch
* Admitir configruar de puente y protocolo de routing

Ventajas:

* Mucho más veloz que router-on-a-stick porque el switching y routing se hacen por hardware.
* No requiere enlaces externos del switch al router
* Se pueden realizar etherchannels de capa 2 entre los switches
* Latencia mucho más baja: los datos no salen del switch para ir a otra red

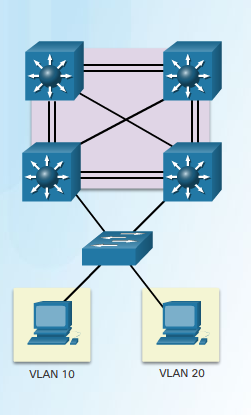
Desventaja: el switch multicapa es más caro.

## Routing entre VLAN con puertos enrutados

Un puerto enrutado es un puerto físico que funciona de manera similar a una interfaz en un router. A diferencia de los puertos de acceso, los puertos enrutados no se asocian a una VLAN determinada.

Los protocolos de capa 2 (tales como STP), no funcionan en interfaces enrutadas. Sin embargo, algunos protocolos, como LACP y EtherChannel, funcionan en la capa 3. Tampoco admiten subinterfaces.

Los puertos enrutados se utilizan para enlaces punto a punto. Las conexiones de routers WAN y dispositivos de seguridad son ejemplos del uso de puertos enrutados. En una red conmutada, los puertos enrutados se suelen configurar entre los switches de las capas de núcleo y de distribución.



Para configurar los puertos enrutados, utilice el comando **no switchport** del modo de configuración de interfaz en los puertos adecuados. Además, asigne una dirección IP y otros parámetros de capa 3, según sea necesario. Después de asignar la dirección IP, verifique que el routing IP esté habilitado de manera global y que los protocolos de routing aplicables estén configurados.

**Nota:** los switches de la serie Catalyst 2960 no admiten puertos enrutados.