Capítulo 6: VLAN

El rendimiento de la red es un factor importante en la productividad de una organización. Una de las tecnologías que contribuyen a mejorar el rendimiento de la red es la división de los grandes dominios de difusión en dominios más pequeños. Por una cuestión de diseño, los routers bloquean el tráfico de difusión en una interfaz. Sin embargo, los routers generalmente tienen una cantidad limitada de interfaces LAN. La función principal de un router es trasladar información entre las redes, no proporcionar acceso a la red a las terminales.

La función de proporcionar acceso a una LAN suele reservarse para los switches de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red dé soporte a los objetivos de una organización. Si bien las VLAN se utilizan principalmente dentro de las redes de área local conmutadas, las implementaciones modernas de las VLAN les permiten abarcar redes MAN y WAN.

Debido a que las VLAN segmentan la red, es necesario un proceso de capa 3 para permitir que el tráfico pase de un segmento de red a otro.

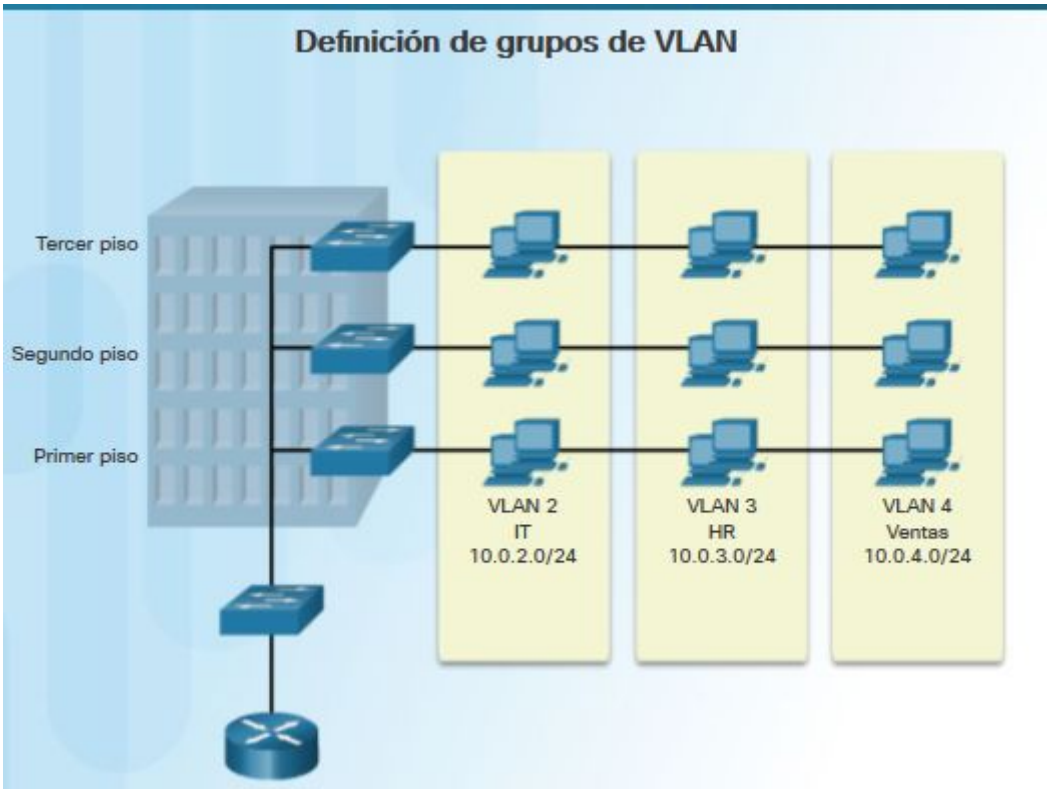
Definiciones de VLAN

Dentro de una red conmutada, las VLAN proporcionan la segmentación y la flexibilidad organizativa. Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN. Un grupo de dispositivos dentro de una VLAN se comunica como si cada dispositivo estuviera conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.

Las VLAN permiten que el administrador divida las redes en segmentos según factores como la función, el equipo del proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo. Cada VLAN se considera una red lógica diferente. Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN

Varias subredes IP pueden existir en una red conmutada, sin el uso de varias VLAN. Sin embargo, los dispositivos estarán en el mismo dominio de difusión de capa 2. Esto significa que todas las difusiones de capa 2, tales como una solicitud de ARP, serán recibidas por todos los dispositivos de la red conmutada, incluso por aquellos que no se quiere que reciban la difusión.

Las VLAN habilitan la implementación de las políticas de acceso y de seguridad según grupos específicos de usuarios. Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch).



Beneficios de las redes VLAN

Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial

Reducción de costos: el ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.

Mejor rendimiento: la división de las redes planas de capa 2 en varios grupos de trabajo lógicos (dominios de difusión) reduce el tráfico innecesario en la red y mejora el rendimiento.

Reducción del tamaño de los dominios de difusión: la división de una red en redes VLAN reduce la cantidad de dispositivos en el dominio de difusión.

Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando se dispone de un switch nuevo, se implementan todas las políticas y los procedimientos que ya se configuraron para la VLAN específica cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre.

Administración más simple de aplicaciones y proyectos: las VLAN agregan dispositivos de red y usuarios para admitir los requisitos geográficos o comerciales.

Tipos de VLAN

VLAN de datos

Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios. Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. A veces a una VLAN de datos se la denomina VLAN de usuario. Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.

VLAN predeterminada

Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches Cisco es la VLAN 1

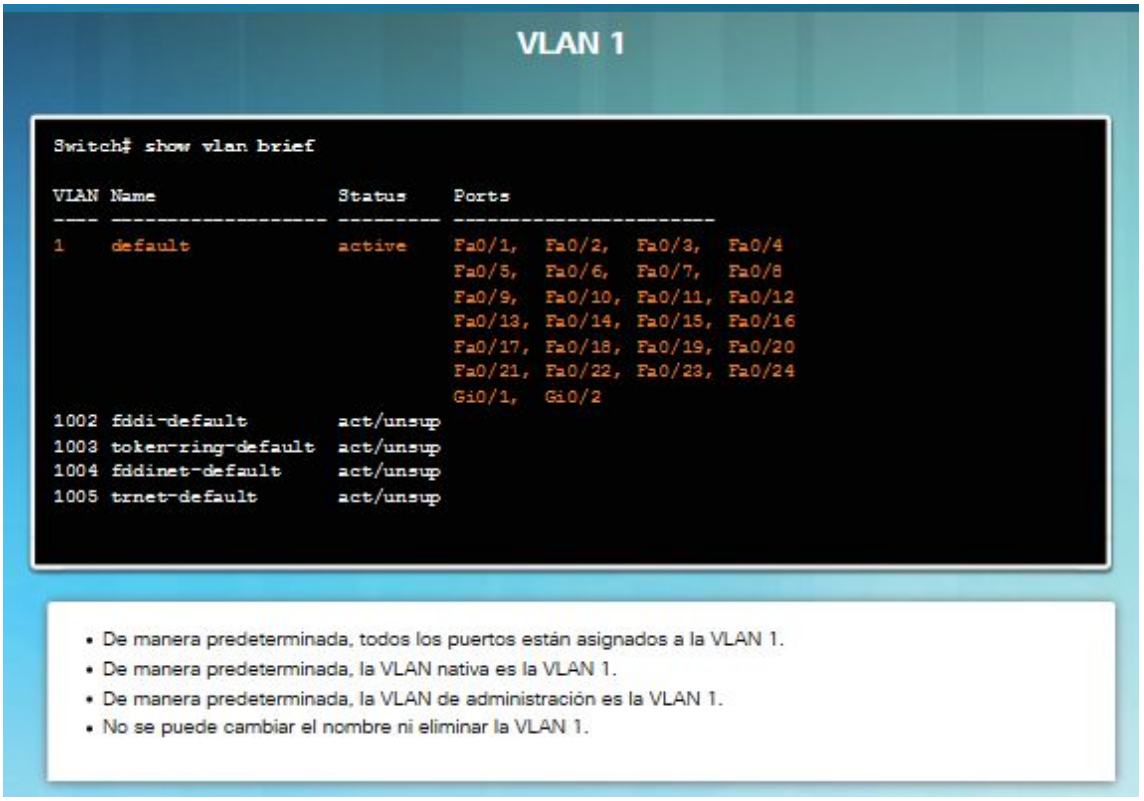
La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

VLAN de administración

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada. Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP. Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.

Las VLAN nativas se definen en la especificación IEEE 802.1Q a fin de mantener la compatibilidad con el tráfico sin etiquetar de modelos anteriores común a las situaciones de LAN antiguas. Una VLAN nativa funciona como identificador común en extremos opuestos de un enlace troncal.

Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN. De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio conmutado.



VLAN de voz

Se necesita una VLAN separada para admitir la tecnología de voz sobre IP (VoIP). El tráfico de VoIP requiere:

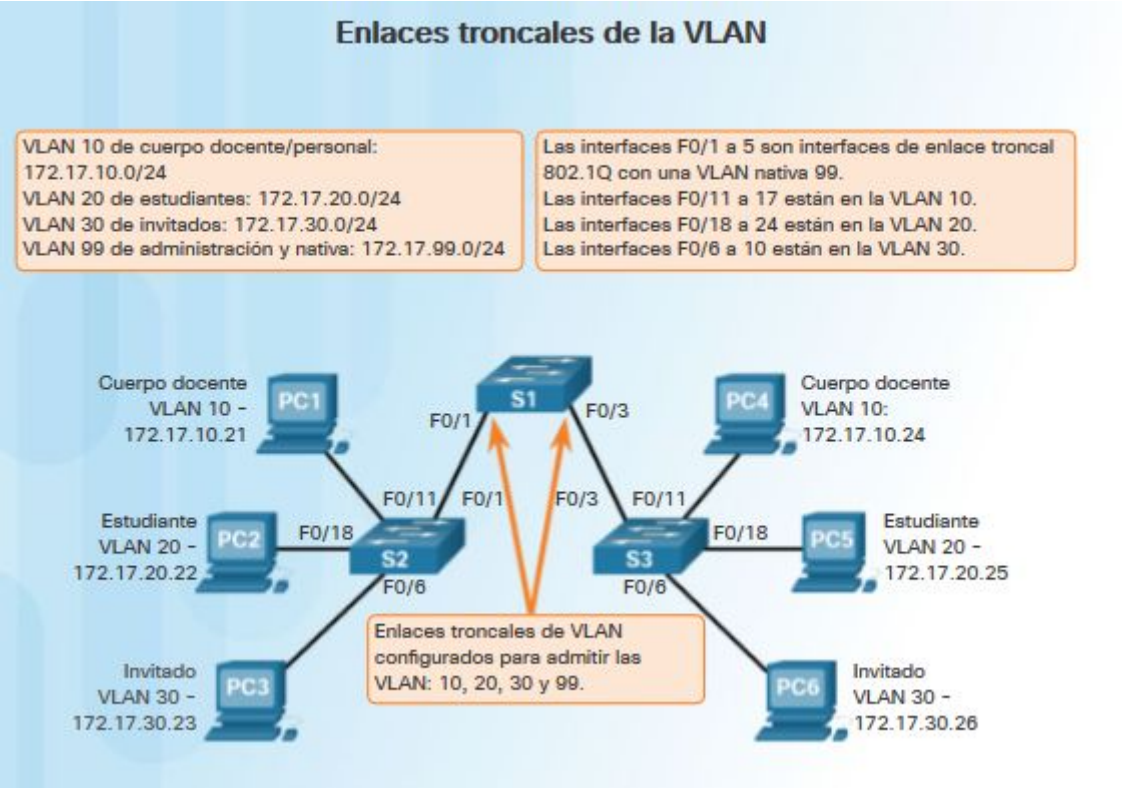
- Ancho de banda garantizado para asegurar la calidad de la voz
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Una demora inferior a 150 ms a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP.

Enlaces troncales de la VLAN

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.
.
Las VLAN no serían muy útiles sin los enlaces troncales de VLAN. Los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para varias VLAN entre switches y routers. También se puede utilizar un enlace troncal entre un dispositivo de red y un servidor u otro dispositivo que cuente con una NIC con capacidad 802.1Q. En los switches Cisco Catalyst, se admiten todas las VLAN en un puerto de enlace troncal de manera predeterminada.



Control de los dominios de broadcast con las VLAN

Redes sin VLAN

En condiciones normales de funcionamiento, cuando un switch recibe una trama de difusión en uno de sus puertos, reenvía la trama por todos los demás puertos, excepto el puerto por donde recibió la difusión.

Etiquetado de tramas de Ethernet para la identificación de VLAN

Los switches de la serie Catalyst 2960 son dispositivos de capa 2. Estos utilizan la información del encabezado de la trama de Ethernet para reenviar paquetes. No poseen tablas de routing. El encabezado de las tramas de Ethernet estándar no contiene información sobre la VLAN a la que pertenece la trama; por lo tanto, cuando las tramas de Ethernet se colocan en un enlace troncal, se debe agregar la información sobre las VLAN a las que pertenecen. Este proceso, denominado "etiquetado", se logra mediante el uso del encabezado IEEE 802.1Q, especificado en el estándar IEEE 802.1Q. El encabezado 802.1Q incluye una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original que especifica la VLAN a la que pertenece la trama.

Cuando el switch recibe una trama en un puerto configurado en modo de acceso y asignado a una VLAN, el switch coloca una etiqueta VLAN en el encabezado de la trama, vuelve a calcular la secuencia de verificación de tramas (FCS) y envía la trama etiquetada por un puerto de enlace troncal.

Detalles del campo de etiqueta de la VLAN

El campo de etiqueta de la VLAN consta de un campo de tipo, un campo de prioridad, un campo de identificador de formato canónico y un campo de ID de la VLAN:

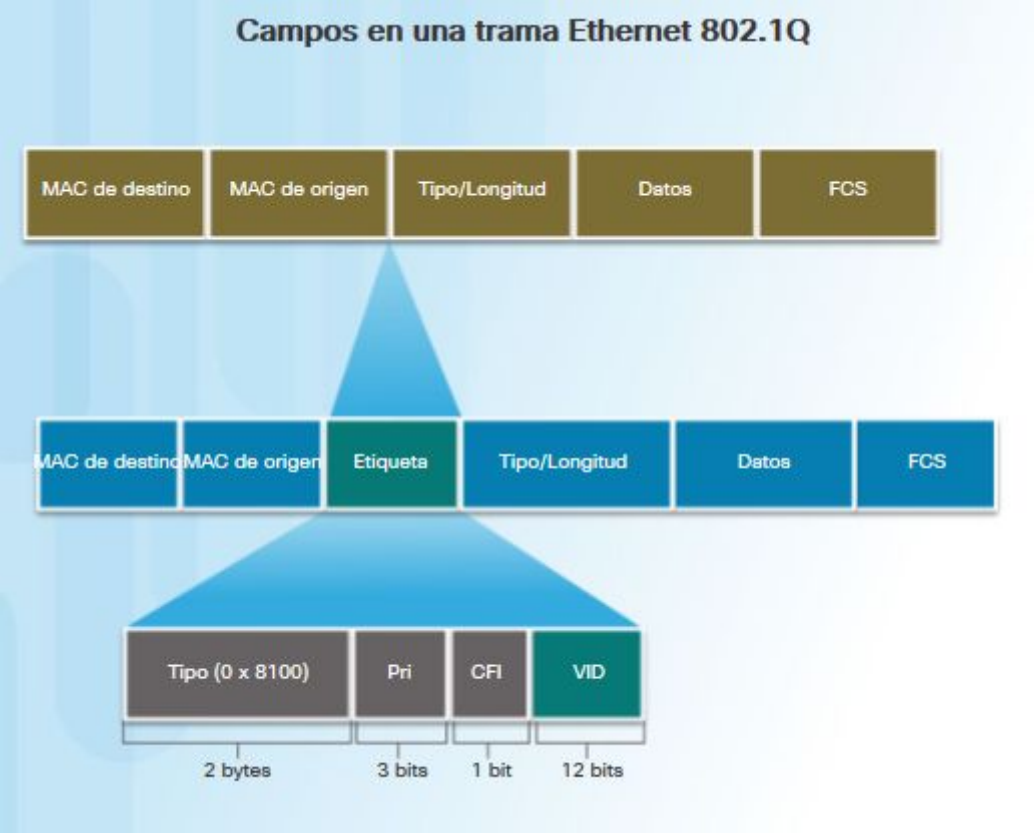
- **Tipo:** es un valor de 2 bytes denominado “ID de protocolo de etiqueta” (TPID). Para Ethernet, este valor se establece en 0x8100 hexadecimal.

- **Prioridad de usuario:** es un valor de 3 bits que admite la implementación de nivel o de servicio.

- **Identificador de formato canónico (CFI):** es un identificador de 1 bit que habilita las tramas Token Ring que se van a transportar a través de los enlaces Ethernet.

- **ID de VLAN (VID):** es un número de identificación de VLAN de 12 bits que admite hasta 4096 ID de VLAN.

Una vez que el switch introduce los campos Tipo y de información de control de etiquetas, vuelve a calcular los valores de la FCS e inserta la nueva FCS en la trama.



VLAN nativas y etiquetado de 802.1Q

Tramas etiquetadas en la VLAN nativa

Algunos dispositivos que admiten los enlaces troncales agregan una etiqueta VLAN al tráfico de las VLAN nativas. El tráfico de control que se envía por la VLAN nativa no se debe etiquetar. Si un puerto de enlace troncal 802.1Q recibe una trama etiquetada con la misma ID de VLAN que la VLAN nativa, descarta la trama. Por consiguiente, al configurar un puerto de un switch Cisco, configure los dispositivos de modo que no envíen tramas etiquetadas por la VLAN nativa. Los dispositivos de otros

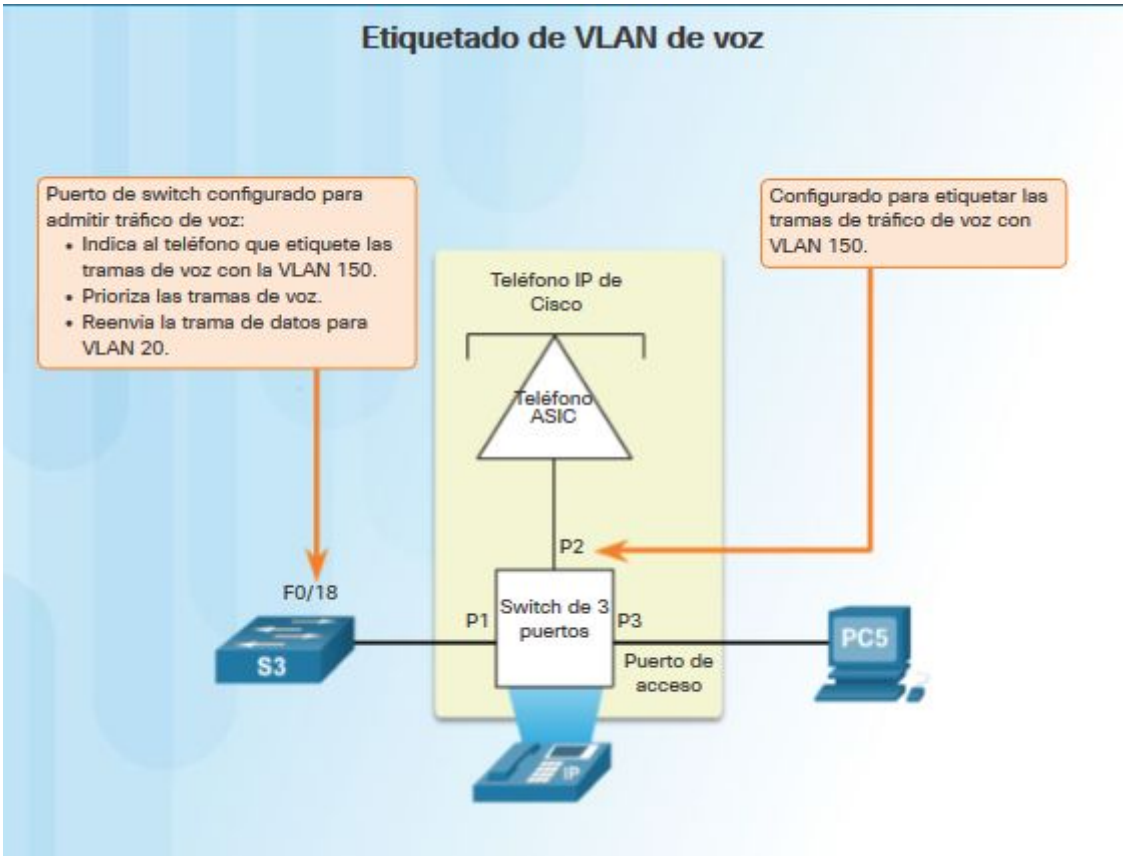
proveedores que admiten tramas etiquetadas en la VLAN nativa incluyen: teléfonos IP, servidores, routers y switches que no pertenecen a Cisco.

Tramas sin etiquetar en la VLAN nativa

Cuando un puerto de enlace troncal de un switch Cisco recibe tramas sin etiquetar (poco usuales en las redes bien diseñadas), envía esas tramas a la VLAN nativa. Si no hay dispositivos asociados a la VLAN nativa (lo que es usual) y no existen otros puertos de enlace troncal (es usual), se descarta la trama. La VLAN nativa predeterminada es la VLAN 1. Al configurar un puerto de enlace troncal 802.1Q, se asigna el valor de la ID de VLAN nativa a la ID de VLAN de puerto (PVID) predeterminada. Todo el tráfico sin etiquetar entrante o saliente del puerto 802.1Q se reenvía según el valor de la PVID. Por ejemplo, si se configura la VLAN 99 como VLAN nativa, la PVID es 99, y todo el tráfico sin etiquetar se reenvía a la VLAN 99. Si no se volvió a configurar la VLAN nativa, el valor de la PVID se establece en VLAN 1.

Etiquetado de VLAN de voz

Se necesita una red VLAN de voz separada para admitir VoIP.
Un puerto de acceso que se usa para conectar un teléfono IP de Cisco se puede configurar para usar dos VLAN separadas: una VLAN para el tráfico de voz y otra VLAN para el tráfico de datos desde un dispositivo conectado al teléfono. El enlace entre el switch y el teléfono IP funciona como un enlace troncal para transportar tanto el tráfico de la VLAN de voz como el tráfico de la VLAN de datos.



Rangos de VLAN en los switches Catalyst

Los distintos switches Cisco Catalyst admiten diversas cantidades de VLAN. La cantidad de VLAN que admiten es suficiente para satisfacer las necesidades de la mayoría de las organizaciones. Por ejemplo, los switches de las series Catalyst 2960 y 3560 admiten más de 4000 VLAN. Las VLAN de rango normal en estos switches se numeran del 1 al 1005, y las VLAN de rango extendido se numeran del 1006 al 4094.

VLAN de rango normal

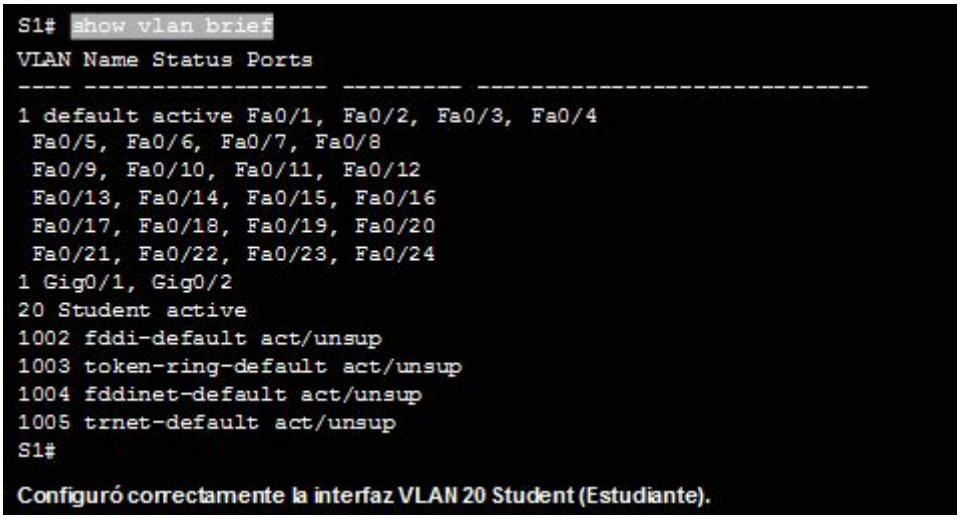
- Se utiliza en redes de pequeños y medianos negocios y empresas.
- Se identifica mediante una ID de VLAN entre 1 y 1005.
- Las ID de 1002 a 1005 se reservan para las VLAN de Token Ring e interfaz de datos distribuidos por fibra óptica (FDDI).
- Las ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar.
- Las configuraciones se almacenan en un archivo de base de datos de VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.
- El protocolo de enlace troncal de VLAN (VTP), que permite administrar la configuración de VLAN entre los switches, solo puede detectar y almacenar redes VLAN de rango normal.

VLAN de rango extendido

- 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.
- Admiten menos características de VLAN que las VLAN de rango normal.
- Se guardan, de manera predeterminada, en el archivo de configuración en ejecución.
- VTP no aprende las VLAN de rango extendido.

Creación de una VLAN

Al configurar redes VLAN de rango normal, los detalles de configuración se almacenan en la memoria flash del switch en un archivo denominado vlan.dat. La memoria flash es persistente y no requiere el comando **copy running-config startup-config**. Sin embargo, debido a que en los switches Cisco se suelen configurar otros detalles al mismo tiempo que se crean las VLAN, es aconsejable guardar los cambios a la configuración en ejecución en la configuración de inicio.



Asignación de puertos a las redes VLAN

Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN.
Es importante tener en cuenta que las VLAN se configuran en el puerto del switch y no en el terminal.El comando **switchport mode access** es optativo, pero se aconseja como práctica recomendada de seguridad. Con este comando, la interfaz cambia al modo de acceso permanente.

Las redes LAN que admiten tráfico de voz por lo general también tienen la Calidad de servicio (QoS) habilitada. El tráfico de voz debe etiquetarse como confiable ni bien ingresa en la red. Use el comando de configuración de interfaces **mls qos trust[cos | device cisco-phone | dscp | ip-precedence]** para establecer el estado confiable de una interfaz, y para indicar qué campos del paquete se usan para clasificar el tráfico.
Nota: El comando **switchport access vlan** fuerza la creación de una VLAN si es que aún no existe en el switch.

Cambio de pertenencia de puertos de una VLAN

Existen varias maneras de cambiar la pertenencia de puertos de una VLAN.

Comandos de IOS de un switch Cisco	
Ingresa al modo de configuración global.	`S1# configure terminal`
Ingrese el modo de configuración de interfaz.	`S1(config)# interface F0/18`
Elimine la asignación de la VLAN del puerto.	`S1(config-if)# no switchport access vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

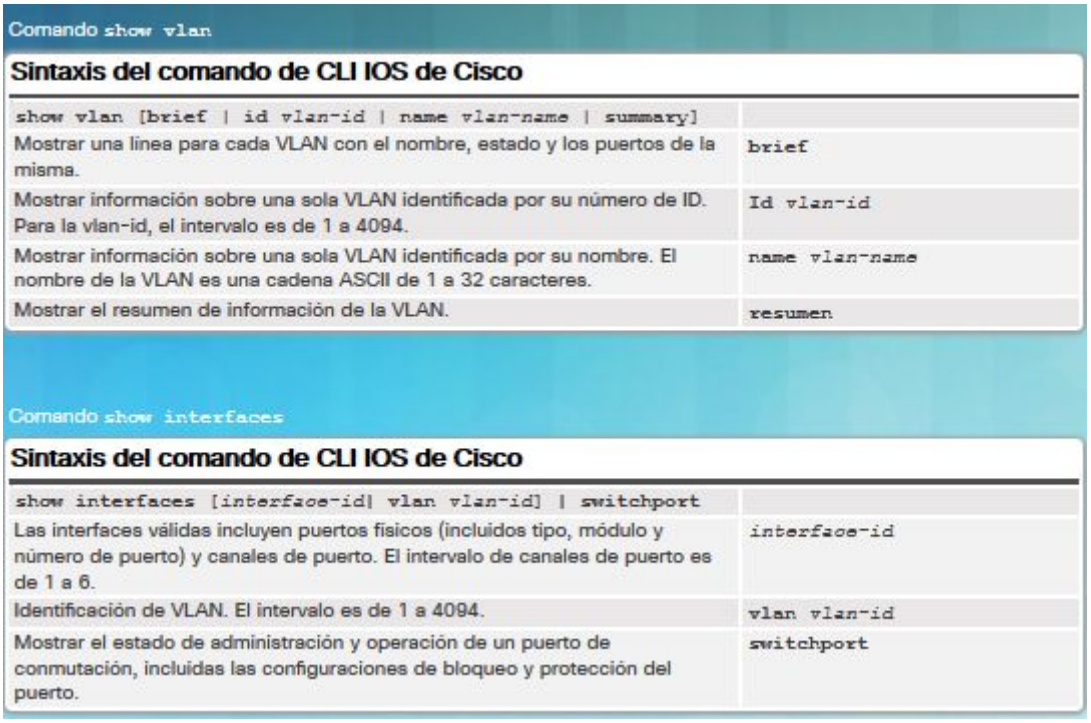
Eliminación de VLAN

el comando del modo de configuración global **no vlan** *vlan-id* se utiliza para eliminar una vlan del switch El comando **show vlan brief** verifica que las vlan eliminada ya no esté presente en el archivo vlan.dat después de utilizar el comando.

Precaución: Antes de borrar una VLAN, reasigne todos los puertos miembros a una VLAN distinta. Los puertos que no se trasladen a una VLAN activa no se podrán comunicar con otros hosts una vez que se elimine la VLAN y hasta que se asignen a una VLAN activa.

Alternativamente, se puede eliminar el archivo vlan.dat completo con el comando **delete flash:vlan.dat** del modo EXEC privilegiado. Se puede utilizar la versión abreviada del comando (**delete vlan.dat**) si no se trasladó el archivo vlan.dat de su ubicación predeterminada. Después de emitir este comando y de volver a cargar el switch, las VLAN configuradas anteriormente ya no están presentes. Esto vuelve al switch a la condición predeterminada de fábrica con respecto a la configuración de VLAN.

Nota: para los switches Catalyst, el comando **erase startup-config** debe acompañar al comando **delete vlan.dat** antes de la recarga para restaurar el switch a la condición predeterminada de fábrica.



Comando `show vlan`

Sintaxis del comando de CLI IOS de Cisco

`show vlan [brief | id vlan-id | name vlan-name | summary]`	
Mostrar una línea para cada VLAN con el nombre, estado y los puertos de la misma.	`brief`
Mostrar información sobre una sola VLAN identificada por su número de ID. Para la vlan-id, el intervalo es de 1 a 4094.	`Id vlan-id`
Mostrar información sobre una sola VLAN identificada por su nombre. El nombre de la VLAN es una cadena ASCII de 1 a 32 caracteres.	`name vlan-name`
Mostrar el resumen de información de la VLAN.	`resumen`

Comando `show interfaces`

Sintaxis del comando de CLI IOS de Cisco

`show interfaces [interface-id| vlan vlan-id] | switchport`	
Las interfaces válidas incluyen puertos físicos (incluidos tipo, módulo y número de puerto) y canales de puerto. El intervalo de canales de puerto es de 1 a 6.	*`interface-id`*
Identificación de VLAN. El intervalo es de 1 a 4094.	`vlan vlan-id`
Mostrar el estado de administración y operación de un puerto de conmutación, incluidas las configuraciones de bloqueo y protección del puerto.	`switchport`

Configuración de enlaces troncales IEEE 802.1Q

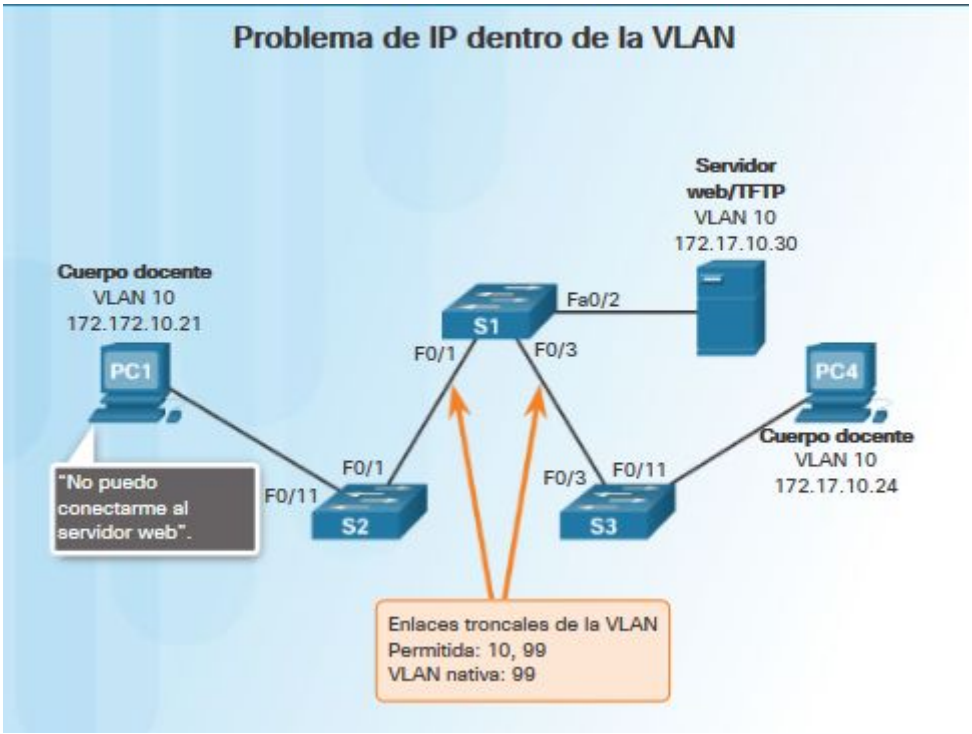
Un enlace troncal de VLAN es un enlace de capa 2 del modelo OSI entre dos switches que transporta el tráfico para todas las VLAN (a menos que se restrinja la lista de VLAN permitidas de manera manual o dinámica). Para habilitar los enlaces troncales, configure los puertos en cualquier extremo del enlace físico con conjuntos de comandos paralelos.

Para configurar un puerto de switch en un extremo de un enlace troncal, utilice el comando **switchport mode trunk**. Con este comando, la interfaz cambia al modo de enlace troncal permanente. El puerto establece una negociación de protocolo de enlace troncal dinámico (DTP) para convertir el enlace en un enlace troncal, incluso si la interfaz conectada a este no acepta el cambio. En este curso, el comando **switchport mode trunk** es el único método que se implementa para la configuración de enlaces troncales.

Restablecimiento del enlace troncal al estado predeterminado

Problemas de direccionamiento IP de VLAN

Cada VLAN debe corresponder a una subred IP única. Si dos dispositivos en la misma VLAN tienen direcciones de subred diferentes, no se pueden comunicar. Este es un problema frecuente y se resuelve fácilmente mediante la identificación de la configuración incorrecta y el cambio de la dirección de la subred por una dirección correcta.



Introducción a la resolución de problemas de enlaces troncales

Una de las tareas frecuentes de los administradores de red es resolver problemas de formación de enlaces troncales o de puertos que se comportan incorrectamente como puertos de enlace troncal. En ocasiones, un puerto de switch se puede comportar como puerto de enlace troncal, incluso si no se configuró como tal. Por ejemplo, un puerto de acceso puede aceptar tramas de redes VLAN distintas de la VLAN a la cual se asignó. Esto se conoce como "filtración de VLAN".

Problemas comunes con enlaces troncales

En general, los problemas de enlaces troncales se deben a una configuración incorrecta. Al configurar las VLAN y los enlaces troncales en una infraestructura conmutada, los errores de configuración más frecuentes son los siguientes:

- **Incompatibilidad de VLAN nativa:** los puertos de enlace troncal se configuraron con VLAN nativas diferentes. Este error de configuración genera notificaciones de consola y puede causar problemas de routing entre VLAN, entre otros inconvenientes. Esto representa un riesgo de seguridad.

- **Incompatibilidades de modo de enlace troncal:** un puerto de enlace troncal está configurado en un modo que no es compatible para enlaces troncales en el puerto par correspondiente. Estos errores de configuración hacen que el vínculo de enlace troncal deje de funcionar. Asegúrese de que se configuren ambos lados del enlace troncal con el comando **switchport mode trunk**. Los demás comandos de configuración de enlace troncal superan el alcance de este curso.

- **VLAN permitidas en enlaces troncales:** no se actualizó la lista de VLAN permitidas en un enlace troncal con los requisitos de enlace troncal de VLAN actuales. En este caso, se envía tráfico inesperado o ningún tráfico al enlace troncal.

¿Qué es el routing entre VLAN?

Las VLAN se utilizan para segmentar redes conmutadas. Los switches de capa 2, tales como los de la serie Catalyst 2960, se pueden configurar con más de 4000 VLAN. Una VLAN es un dominio de difusión, por lo que las computadoras en VLAN separadas no pueden comunicarse sin la intervención de un dispositivo de routing. Los switches de capa 2 tienen una funcionalidad muy limitada en cuanto a IPv4 e IPv6, y no pueden realizar las funciones de routing dinámico de los routers. Si bien los switches de capa 2 adquieren cada vez más funcionalidad de IP, como la capacidad de realizar routing estático, esto no es suficiente para abordar esta gran cantidad de VLAN.
Se puede usar cualquier dispositivo que admita routing de capa 3, como un router o un switch multicapa, para lograr la funcionalidad de routing necesaria. Independientemente del dispositivo empleado, el proceso de reenvío del tráfico de la red de una VLAN a otra mediante routing se conoce como “routing entre VLAN”.

Hay tres opciones para el routing entre redes VLAN:

- Routing entre VLAN antiguo
- Router-on-a-stick
- Switching de capa 3 mediante las SVI

Routing entre VLAN antiguo

Históricamente, la primera solución para el routing entre VLAN se valía de routers con varias interfaces físicas. Era necesario conectar cada interfaz a una red separada y configurarla para una subred diferente.
En este enfoque antiguo, el routing entre VLAN se realiza mediante la conexión de diferentes interfaces físicas del router a diferentes puertos físicos de switch. Los puertos de switch conectados al router se colocan en modo de acceso, y cada interfaz física se asigna a una VLAN diferente. Cada interfaz del router puede entonces aceptar el tráfico desde la VLAN asociada a la interfaz del switch que se encuentra conectada y el tráfico puede enrutarse a otras VLAN conectadas a otras interfaces.

Routing entre VLAN con router-on-a-stick

A diferencia del routing entre VLAN antiguo, que requiere varias interfaces físicas, tanto en el router como en el switch, las implementaciones más comunes y actuales de routing entre VLAN no tienen esos requisitos. En cambio, algunos softwares de router permiten configurar una interfaz del router como enlace troncal, lo que significa que solo es necesaria una interfaz física en el router y en el switch para enrutar paquetes entre varias VLAN.

‘Router-on-a-stick” es un tipo de configuración de router en la cual una única interfaz física enruta el tráfico entre varias VLAN en una red. Como puede verse en la ilustración, el router está conectado al switch S1 mediante una única conexión de red física (un enlace troncal).

La interfaz del router se configura para funcionar como enlace troncal y se conecta a un puerto del switch configurado en modo de enlace troncal. Para realizar el routing entre VLAN, el router acepta en la interfaz troncal el tráfico con etiquetas de VLAN proveniente del switch adyacente y luego lo enruta en forma interna entre las VLAN, mediante subinterfaces. El router reenvía el tráfico enrutado con etiquetas de VLAN para la VLAN de destino a través de la misma interfaz física utilizada para recibir el tráfico.

Las subinterfaces son interfaces virtuales basadas en software, asociadas con una única interfaz física. Las subinterfaces se configuran en software en un router, y cada subinterfaz se configura de manera independiente con una dirección IP y una asignación de VLAN. Las subinterfaces se configuran para

subredes diferentes que corresponden a su asignación de VLAN para facilitar el routing lógico. Después de que se toma una decisión de routing según la VLAN de destino, las tramas de datos reciben etiquetas de VLAN y se envían de vuelta por la interfaz física.

Configuración del routing entre VLAN antiguo: preparación

El routing entre VLAN antiguo requiere que los routers tengan varias interfaces físicas. El router realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz se configura con una dirección IPv4 para la subred asociada con la VLAN específica a la cual está conectada. Al configurar las direcciones IPv4 en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN pueden comunicarse con el router mediante la interfaz física conectada a la misma VLAN. En esta configuración los dispositivos de red pueden utilizar el router como un gateway para acceder a los dispositivos conectados a las otras VLAN.

El proceso de enrutamiento requiere del dispositivo de origen para determinar si el dispositivo de destino es local o remoto con respecto a la subred local. El dispositivo de origen realiza esta determinación al comparar las direcciones IPv4 de origen y de destino con la máscara de subred. Una vez que se determina que la dirección IPv4 de destino está en una red remota, el dispositivo de origen debe identificar adónde necesita reenviar el paquete para llegar al dispositivo de destino. El dispositivo de origen examina la tabla de enrutamiento local para determinar dónde es necesario enviar los datos. Los dispositivos utilizan sus gateways predeterminados como destino de capa 2 para todo el tráfico que debe abandonar la subred local. El gateway predeterminado es la ruta que el dispositivo utiliza cuando no tiene otra ruta explícitamente definida hacia la red de destino. La dirección IPv4 de la interfaz del router en la subred local actúa como gateway predeterminado para el dispositivo emisor.

Configuración de router-on-a-stick: preparación

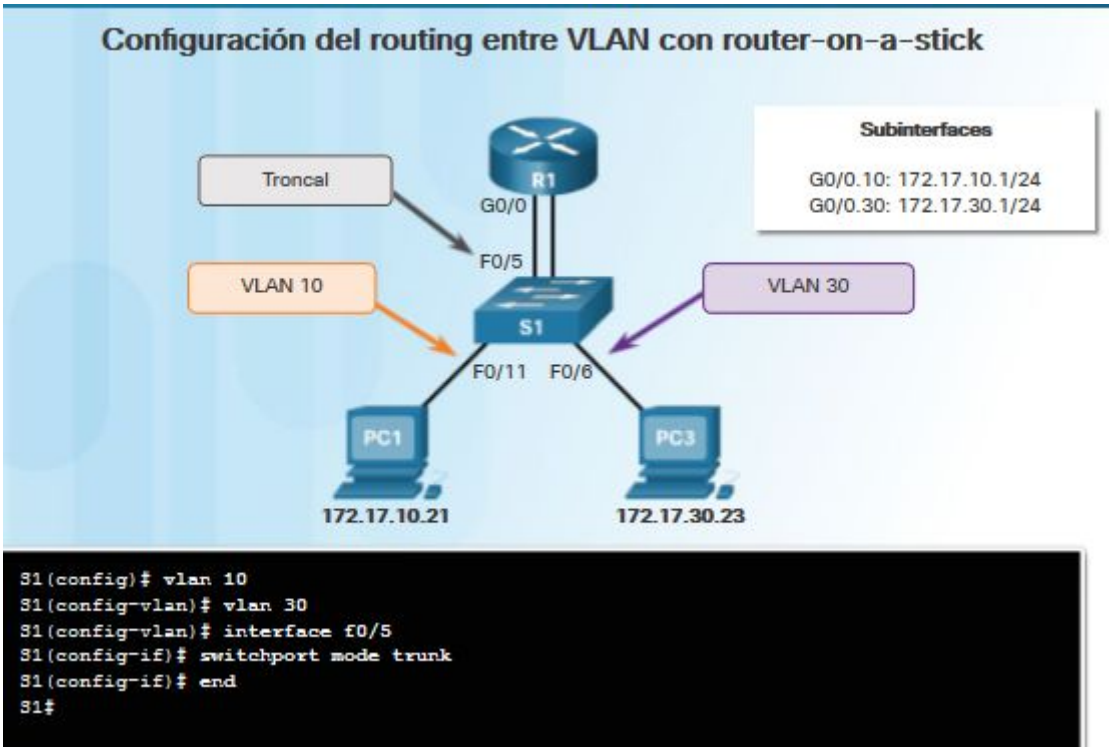
El routing entre VLAN antiguo con interfaces físicas tiene una limitación importante. Los routers tienen una cantidad limitada de interfaces físicas para conectarse a diferentes VLAN. A medida que aumenta la cantidad de VLAN en una red, el hecho de tener una interfaz física del router por VLAN agota rápidamente la capacidad de interfaces físicas de un router. Una alternativa en redes más grandes es utilizar subinterfaces y enlaces troncales de VLAN. Los enlaces troncales de VLAN permiten que una única interfaz física del router enrute el tráfico de varias VLAN. Esta técnica se denomina “router-on-a-stick” y utiliza subinterfaces virtuales en el router para superar las limitaciones de interfaces físicas del hardware.

Al configurar el enrutamiento inter VLAN mediante el modelo router-on-a-stick, la interfaz física del router debe estar conectada al enlace troncal en el switch adyacente. En el router, se crean subinterfaces para cada VLAN única en la red. A cada subinterfaz se le asigna una dirección IP específica para su subred/VLAN y también se configura para etiquetar las tramas para esa VLAN. De esa manera, el router puede mantener separado el tráfico de cada subinterfaz a medida que atraviesa el enlace troncal hacia el switch.

En términos de funcionamiento, utilizar el modelo router-on-a-stick es lo mismo que utilizar el modelo de routing entre VLAN antiguo, pero en lugar de utilizar las interfaces físicas para realizar el routing, se utilizan las subinterfaces de una única interfaz física.

Configuración de router-on-a-stick: configuración del switch

Para habilitar el routing entre VLAN utilizando el método router-on-a stick, comience por habilitar el enlace troncal en el puerto del switch que está conectado al router.



Configuración de router-on-a-stick: configuración de subinterfaces del router

Cuando se utiliza una configuración de router-on-a-stick, la configuración del router es diferente en comparación con el routing entre VLAN antiguo.

Cada subinterfaz se crea con el comando**interfaz** *id_interfaz id_subinterfaz* comando global configuration mode. La sintaxis para la subinterfaz es la interfaz física, en este caso g0/0, seguida de un punto y un número de subinterfaz. Como se muestra en la figura, la subinterfaz GigabitEthernet0/0.10 se crea con el comando de modo de configuración global **interface g0/0.10**. El número de subinterfaz normalmente se configura para reflejar el número de VLAN.

Antes de asignar una dirección IP a una subinterfaz, es necesario configurar la subinterfaz para que funcione en una VLAN específica mediante el comando**encapsulation dot1q** *id_de_vlan* .

A continuación, asigne la dirección IPv4 para la subinterfaz mediante el comando de modo de configuración de interfaz**dirección ip** *dirección_ip máscara_subred* .
Este proceso se repite para todas las subinterfaces del router necesarias para el enrutamiento entre las VLAN configuradas en la red. Es necesario asignar una dirección IP a cada subinterfaz del router en una subred única para que se produzca el routing.

Después de habilitar una interfaz física, las subinterfaces se habilitarán automáticamente con la configuración. No es necesario habilitar las subinterfaces con el comando**no shutdown**a nivel del modo de configuración de subinterfaz del software Cisco IOS.

Configuración de router-on-a-stick: verificación de subinterfaces

Los routers Cisco están configurados de manera predeterminada para enrutar el tráfico entre subinterfaces locales. Por lo tanto, no es necesario que esté habilitado el enrutamiento.

Resumen

En este capítulo, se presentaron las redes VLAN. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas. Las VLAN son un mecanismo para permitir que los administradores de red creen dominios de difusión lógicos que puedan extenderse a través de un único switch o varios switches, independientemente de la cercanía física.
Existen varios tipos de VLAN:

- VLAN predeterminada
- VLAN de administración
- VLAN nativa
- VLAN de datos/de usuarios
- VLAN de voz

El comando**switchport access vlan**se utiliza para crear una VLAN en un switch. Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. El comando**show vlan brief**muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. Cada VLAN debe corresponder a una subred IP única.

Utililce el comando**show vlan**para verificar si el puerto pertenece a la VLAN esperada. Si el puerto está asignado a la VLAN incorrecta, utilice el comando**switchport access vlan**para corregir la pertenencia de VLAN. Utililce elcomando **show mac address-table** para revisar qué direcciones se obtuvieron en un puerto determinado del switch y a qué VLAN se asignó ese puerto.

Un puerto de un switch es un puerto de acceso o un puerto de enlace troncal. Los puertos de acceso transportan el tráfico de una VLAN específica asignada al puerto. Un puerto de enlace troncal pertenece a todas las VLAN de manera predeterminada; por lo tanto, transporta el tráfico para todas las VLAN.

Los enlaces troncales de VLAN facilitan la comunicación entre switches mediante el transporte de tráfico relacionado con varias VLAN. El etiquetado de tramas IEEE 802.1Q permite diferenciar tramas de Ethernet asociadas a distintas VLAN a medida que atraviesan enlaces troncales en común. Para habilitar los enlaces troncales, utilice el comando**switchport mode trunk**. Utililce el comando**show interfaces trunk**para verificar si se estableció un enlace troncal entre los switches.

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 es un protocolo exclusivo de Cisco que se habilita de manera automática en los switches de las series Catalyst 2960 y Catalyst 3560.

Para volver un switch a la configuración predeterminada de fábrica con una VLAN predeterminada, utilice los comandos **delete flash:vlan.dat**y**erase startup-config.**
En este capítulo también se examinó la configuración, verificación y resolución de problemas de las VLAN y los enlaces troncales mediante la utilización de la CLI de Cisco IOS.