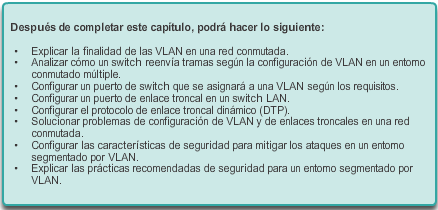
# VLAN

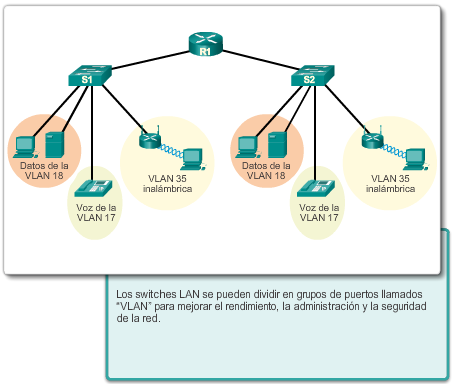
## Introducción

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.

En este capítulo, se describe cómo configurar y administrar VLAN y enlaces troncales de VLAN, así como resolver problemas relacionados. También se analizan cuestiones y estrategias de seguridad relacionadas con las VLAN y los enlaces troncales, así como las prácticas recomendadas para el diseño de VLAN.





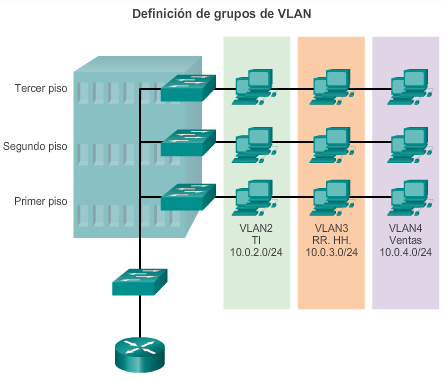
## Segmentación de VLAN

Dentro de un entorno de internetwork 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 estuvieran 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. Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN. Cualquier puerto de switch puede pertenecer a una VLAN, y los paquetes de unidifusión, difusión y multidifusión se reenvían y saturan solo las estaciones terminales dentro de la VLAN donde se originan los paquetes. Cada VLAN se considera una red lógica independiente, y los paquetes destinados a las estaciones que no pertenecen a la VLAN se deben reenviar a través de un dispositivo que admita el routing.

Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños. Si un dispositivo en una VLAN envía una trama de Ethernet de difusión, todos los dispositivos en la VLAN reciben la trama, pero los dispositivos en otras VLAN no la reciben.

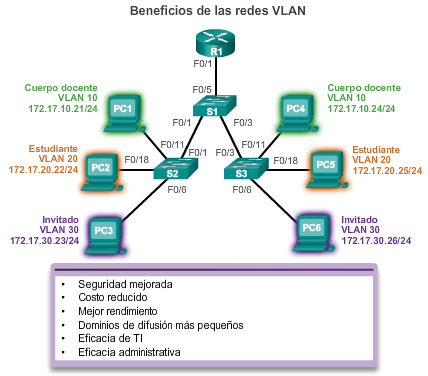
Las VLAN habilitan la implementación de las políticas de acceso y de seguridad según grupos específicos de usuarios. Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch).



La productividad de los usuarios y la adaptabilidad de la red son importantes para el crecimiento y el éxito de las empresas. Las redes VLAN facilitan el diseño de una red para dar soporte a los objetivos de una organización. Los principales beneficios de utilizar las VLAN son los siguientes:

* **Seguridad**: los grupos que tienen datos sensibles se separan del resto de la red, lo que disminuye las posibilidades de que ocurran violaciones de información confidencial. Como se muestra en la ilustración, las computadoras del cuerpo docente están en la VLAN 10 y separadas por completo del tráfico de datos de los estudiantes y los Invitados.
* **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.
* **Dominios de difusión reducidos:** la división de una red en redes VLAN reduce la cantidad de dispositivos en el dominio de difusión. Como se muestra en la ilustración, existen seis computadoras en esta red, pero hay tres dominios de difusión: Cuerpo docente, Estudiantes e Invitados.
* **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. En la ilustración, para facilitar la identificación, se denominó “Cuerpo Docente” a la VLAN 10, “Estudiantes” a la VLAN 20 e “Invitados” a la VLAN 30.
* **Administración más simple de aplicaciones y proyectos:** las VLAN agregan dispositivos de red y usuarios para admitir los requisitos geográficos o comerciales. Al tener características diferentes, se facilita la administración de un proyecto o el trabajo con una aplicación especializada; un ejemplo de este tipo de aplicación es una plataforma de desarrollo de aprendizaje por medios electrónicos para el cuerpo docente.

Cada VLAN en una red conmutada corresponde a una red IP; por lo tanto, al diseñar la VLAN, se debe tener en cuenta la implementación de un esquema de direccionamiento de red jerárquico. El direccionamiento jerárquico de la red significa que los números de red IP se aplican a los segmentos de red o a las VLAN de manera ordenada, lo que permite que la red se tome en cuenta como conjunto. Los bloques de direcciones de red contiguas se reservan para los dispositivos en un área específica de la red y se configuran en estos, como se muestra en la ilustración.



Existen diferentes tipos de redes VLAN, los cuales se utilizan en las redes modernas. Algunos tipos de VLAN se definen según las clases de tráfico. Otros tipos de VLAN se definen según la función específica que cumplen.

**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. En la ilustración, se emitió el comando **show vlan brief** en un switch que ejecuta la configuración predeterminada. Observe que todos los puertos se asignan a la VLAN 1 de manera predeterminada.

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 nativa**

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El tráfico con etiquetas hace referencia al tráfico que tiene 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. El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

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.

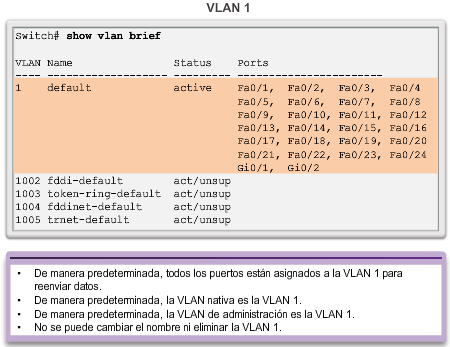
Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN. De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio conmutado.

**VLAN de 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.

En el pasado, la VLAN de administración para los switches 2960 era la única SVI activa. En las versiones 15.x de IOS de Cisco para los switches de la serie Catalyst 2960, es posible tener más de una SVI activa. Con IOS de Cisco 15.x, se debe registrar la SVI activa específica asignada para la administración remota. Si bien, en teoría, un switch puede tener más de una VLAN de administración, esto aumenta la exposición a los ataques de red.

En la ilustración, actualmente todos los puertos están asignados a la VLAN 1 predeterminada. No hay ninguna VLAN nativa asignada explícitamente ni otras VLAN activas; por lo tanto, la VLAN nativa de la red que se diseñó es la VLAN de administración. Esto se considera un riesgo de seguridad.

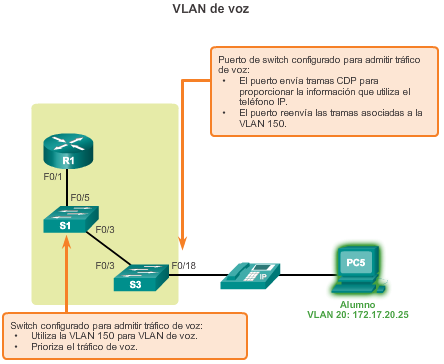


Se necesita una VLAN separada para admitir la tecnología de voz sobre IP (VoIP). El tráfico de VoIP requiere:

* 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. Los detalles sobre cómo configurar una red para que admita VoIP exceden el ámbito de este curso, pero es útil resumir cómo funciona una VLAN de voz entre un switch, un teléfono IP Cisco y una computadora.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes.



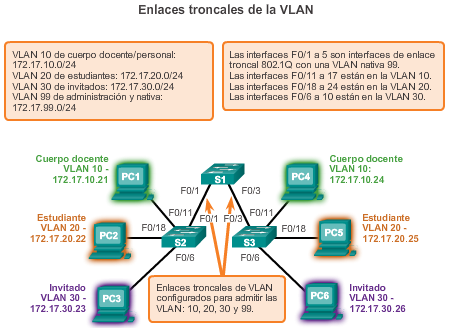
### Redes VLAN en un entorno conmutado múltiple

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.

En la ilustración, los enlaces entre los switches S1 y S2, y S1 y S3 se configuraron para transmitir el tráfico proveniente de las VLAN 10, 20, 30 y 99 a través de la red. Esta red no podría funcionar sin los enlaces troncales de 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. En la animación de la figura 1, se configuró toda la red en la misma subred (172.17.40.0/24), y no se configuró ninguna VLAN. Como consecuencia, cuando la computadora del cuerpo docente (PC1) envía una trama de difusión, el switch S2 envía dicha trama de difusión por todos sus puertos. Finalmente, toda la red recibe la difusión porque la red es un dominio de difusión.

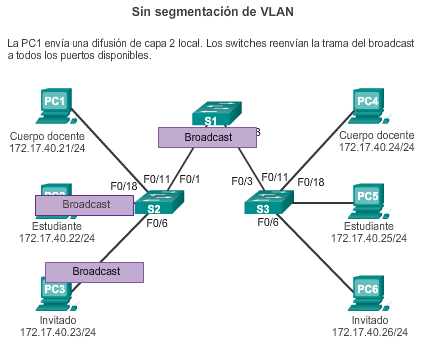
**Red con VLAN**

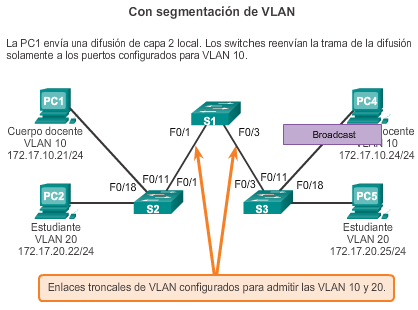
Como se muestra en la animación de la figura 2, la red se segmentó mediante dos VLAN. Los dispositivos del cuerpo docente se asignaron a la VLAN 10, y los dispositivos de los estudiantes se asignaron a la VLAN 20. Cuando se envía una trama de difusión desde la computadora del cuerpo docente, la PC1, al switch S2, el switch reenvía esa trama de difusión solo a los puertos de switch configurados para admitir la VLAN 10.

Los puertos que componen la conexión entre los switches S2 y S1 (puertos F0/1), y entre el S1 y el S3 (puertos F0/3) son enlaces troncales y se configuraron para admitir todas las VLAN en la red.

Cuando el S1 recibe la trama de difusión en el puerto F0/1, reenvía la trama de difusión por el único puerto configurado para admitir la VLAN 10, que es el puerto F0/3. Cuando el S3 recibe la trama de difusión en el puerto F0/3, reenvía la trama de difusión por el único puerto configurado para admitir la VLAN 10, que es el puerto F0/11. La trama de difusión llega a la única otra computadora de la red configurada en la VLAN 10, que es la computadora PC4 del cuerpo docente.

Cuando se implementan las VLAN en un switch, la transmisión del tráfico de unidifusión, multidifusión y difusión desde un host en una VLAN en particular se limita a los dispositivos presentes en esa 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.

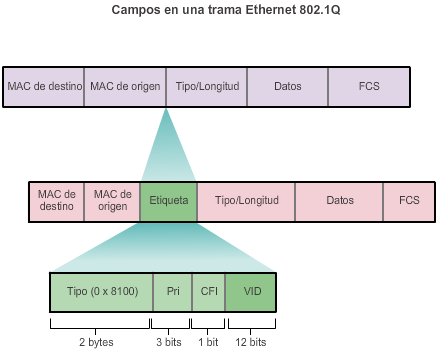
Cuando el switch recibe una trama en un puerto configurado en modo de acceso y asignado a una VLAN, el switch coloca una etiqueta VLAN en el encabezado de la trama, vuelve a calcular la FCS y envía la trama etiquetada por un puerto de enlace troncal.

**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.



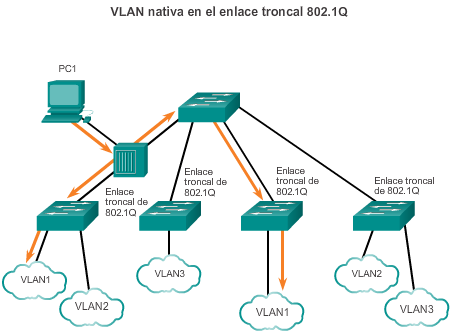
**Tramas etiquetadas en la VLAN nativa**

Algunos dispositivos que admiten 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 no es poco usual) y no existen otros puertos de enlace troncal (lo que no es poco 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.

En la ilustración, la PC1 está conectada a un enlace troncal 802.1Q mediante un hub. La PC1 envía el tráfico sin etiquetar que los switches asocian a la VLAN nativa configurada en los puertos de enlace troncal y que reenvían según corresponda. El tráfico etiquetado del enlace troncal que recibe la PC1 se descarta. Esta situación refleja un diseño de red deficiente por varios motivos: utiliza un hub, tiene un host conectado a un enlace troncal y esto implica que los switches tengan puertos de acceso asignados a la VLAN nativa. Sin embargo, ilustra la motivación de la especificación IEEE 802.1Q para que las VLAN nativas sean un medio de manejo de entornos antiguos.



Recuerde que, para admitir VoIP, se requiere una VLAN de voz separada.

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.

El teléfono IP Cisco contiene un switch integrado 10/100 de tres puertos. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

* El puerto 1 se conecta al switch o a otro dispositivo VoIP.
* El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.
* El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

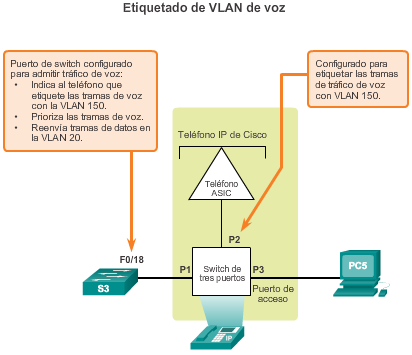
En el switch, el acceso está configurado para enviar paquetes del protocolo de descubrimiento de Cisco (CDP) que instruyen a un teléfono IP conectado para que envíe el tráfico de voz al switch en una de tres formas posibles, según el tipo de tráfico:

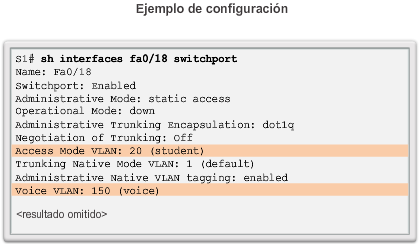
* En una VLAN de voz con una etiqueta de valor de prioridad de clase de servicio (CoS) de capa 2.
* En una VLAN de acceso con una etiqueta de valor de prioridad de CoS de capa 2.
* En una VLAN de acceso sin etiqueta (sin valor de prioridad de CoS de capa 2).

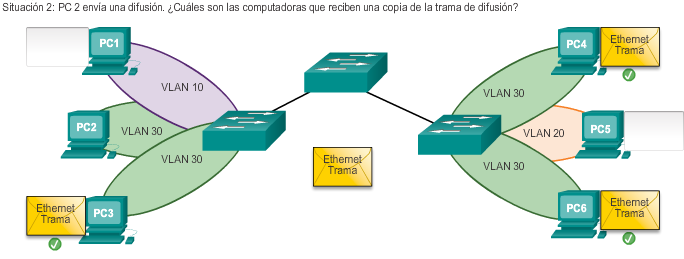
En la figura 1, la computadora del estudiante PC5 está conectada a un teléfono IP de Cisco, y el teléfono está conectado al switch S3. La VLAN 150 está diseñada para transportar tráfico de voz, mientras que la PC5 está en la VLAN 20, que se usa para los datos de los estudiantes.

**Ejemplo de configuración**

En la figura 2, se muestra un resultado de ejemplo. El análisis de los comandos de voz de IOS de Cisco exceden el ámbito de este curso, pero las áreas resaltadas en el resultado de ejemplo muestran que la interfaz F0/18 se configuró con una VLAN configurada para datos (VLAN 20) y una VLAN configurada para voz (VLAN 150).







## Implementaciones de VLAN

### Asignación de red VLAN

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. En la ilustración, se muestran las VLAN disponibles en un switch Catalyst 2960 que ejecuta IOS de Cisco, versión 15.x.

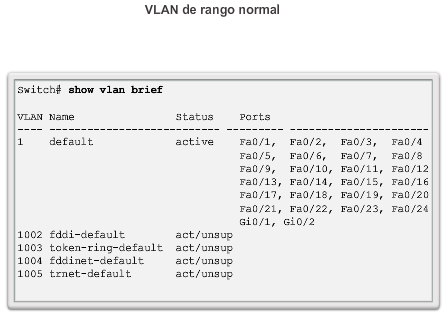
**VLAN de rango normal**

* Se utiliza en redes de pequeños y medianos negocios y empresas.
* Se identifica mediante un ID de VLAN entre 1 y 1005.
* Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.
* Los 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 descubrir 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 los ID de las VLAN de rango extendido.
* Se identifican mediante un 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 en el archivo de configuración en ejecución de manera predeterminada.
* VTP no aprende las VLAN de rango extendido.

**Nota:** la cantidad máxima de VLAN disponibles en los switches Catalyst es 4096, ya que el campo ID de VLAN tiene 12 bits en el encabezado IEEE 802.1Q.



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.

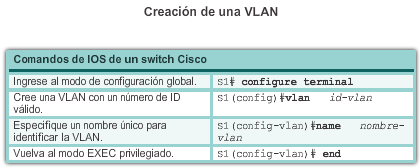
En la figura 1, se muestra la sintaxis del comando de IOS de Cisco que se utiliza para agregar una VLAN a un switch y asignarle un nombre. Se recomienda asignarle un nombre a cada VLAN en la configuración de un switch.

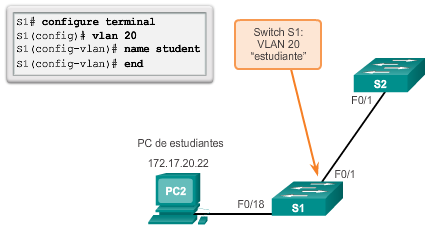
En la figura 2, se muestra cómo se configura la VLAN para estudiantes (VLAN 20) en el switch S1. En el ejemplo de topología, la computadora del estudiante (PC2) todavía no se asoció a ninguna VLAN, pero tiene la dirección IP 172.17.20.22.

Utilice el verificador de sintaxis de la figura 3 para crear una VLAN y utilice el comando**show vlan brief** para mostrar el contenido del archivo vlan.dat.

Además de introducir una única ID de VLAN, se puede introducir una serie de ID de VLAN separadas por comas o un rango de ID de VLAN separado por guiones con el comando **vlan***id-vlan*. Por ejemplo, utilice el siguiente comando para crear las VLAN 100, 102, 105, 106 y 107:

S1(config)# **vlan 100,102,105-107**





Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. Un puerto de acceso puede pertenecer a una sola VLAN por vez; una excepción a esta regla es un puerto conectado a un teléfono IP, en cuyo caso, hay dos VLAN asociadas al puerto: una para voz y otra para datos.

En la figura 1, se muestra la sintaxis para definir un puerto como puerto de acceso y asignarlo a una VLAN. 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.

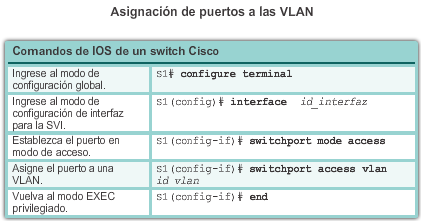
**Nota:** utilice el comando **interface range** para configurar varias interfaces simultáneamente.

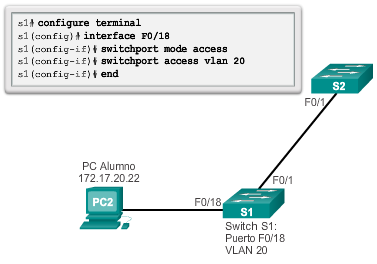
En el ejemplo de la figura 2, la VLAN 20 se asigna al puerto F0/18 del switch S1; por lo tanto, la computadora de estudiantes (PC2) está en la VLAN 20. Cuando se configura la VLAN 20 en otros switches, el administrador de red sabe que debe configurar las otras computadoras de estudiantes para que estén en la misma subred que la PC2 (172.17.20.0/24).

Utilice el verificador de sintaxis de la figura 3 para asignar una VLAN y utilice el comando**show vlan brief** para mostrar el contenido del archivo vlan.dat.

El comando **switchport access vlan**fuerza la creación de una VLAN si es que aún no existe en el switch. Por ejemplo, la VLAN 30 no está presente en el resultado del comando **show vlan brief** del switch. Si se introduce el comando**switchport access vlan 30** en cualquier interfaz sin configuración previa, el switch muestra lo siguiente:

% Access VLAN does not exist. Creating vlan 30





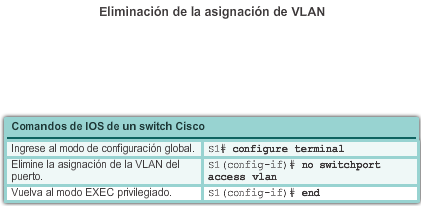
Existen varias maneras de cambiar la pertenencia de puertos de una VLAN. En la figura 1, se muestra la sintaxis para cambiar la pertenencia de un puerto de switch de la VLAN 1 con el comando **no switchport access vlan** del modo de configuración de interfaz.

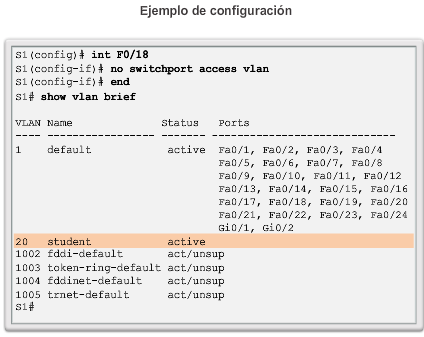
La interfaz F0/18 se asignó anteriormente a la VLAN 20. Se introduce el comando **no switchport access vlan** para la interfaz F0/18. Examine el resultado del comando **show vlan brief** que le sigue inmediatamente, como se muestra en la figura 2. El comando **show vlan brief**muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. El comando **show vlan brief** muestra una línea para cada VLAN. El resultado para cada VLAN incluye el nombre, el estado y los puertos de switch de la VLAN.

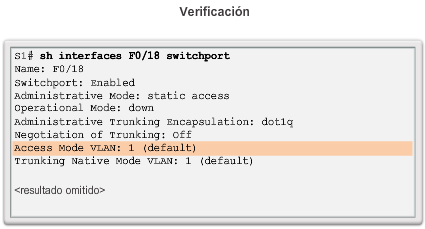
La VLAN 20 sigue activa, aunque no tenga puertos asignados. En la figura 3, se muestra que el resultado del comando**show interfaces f0/18 switchport**verifica que la VLAN de acceso para la interfaz F0/18 se haya restablecido a la VLAN 1.

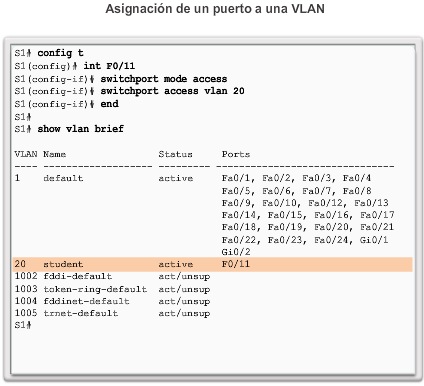
La pertenencia de VLAN de un puerto se puede cambiar fácilmente. No es necesario eliminar primero un puerto de una VLAN para cambiar su pertenencia de VLAN. Cuando se vuelve a asignar la pertenencia de VLAN de un puerto de acceso a otra VLAN existente, la nueva pertenencia de VLAN simplemente reemplaza la pertenencia de VLAN anterior. En la figura 4, el puerto F0/11 se asignó a la VLAN 20.

Utilice el verificador de sintaxis de la figura 5 para cambiar la pertenencia de puertos de una VLAN.







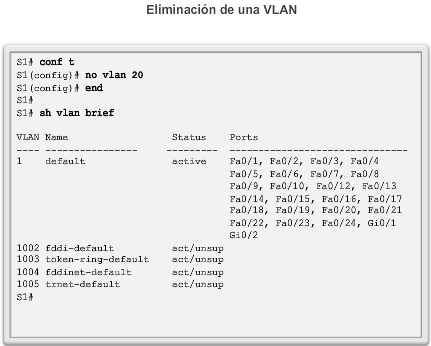


En la ilustración, se utiliza el comando **no vlan***id-vlan* del modo de configuración global para eliminar la VLAN 20 del switch. El switch S1 tenía una configuración mínima con todos los puertos en la VLAN 1 y una VLAN 20 sin usar en la base de datos de VLAN. El comando **show vlan brief**verifica que la VLAN 20 ya no esté presente en el archivo vlan.dat después de utilizar el comando **no vlan 20**.

**Precaución:** antes de eliminar una VLAN, asegúrese de reasignar primero todos los puertos miembro de una VLAN a otra. 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.



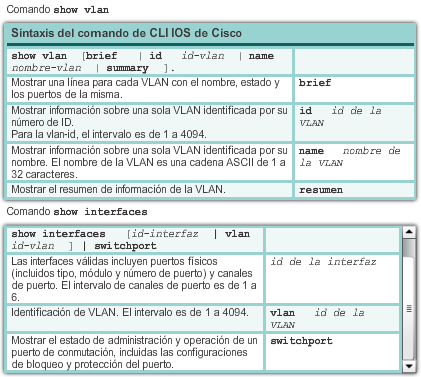
Una vez que se configura una VLAN, se puede validar la configuración con los comandos **show** de IOS de Cisco.

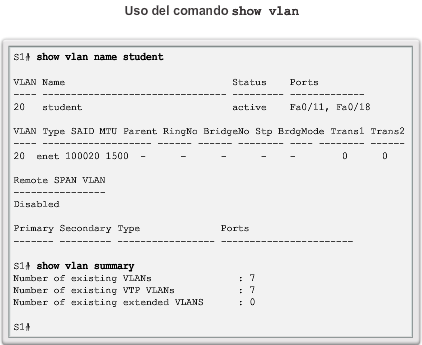
En la figura 1, se muestran las opciones de los comandos **show vlan** y **show interfaces**.

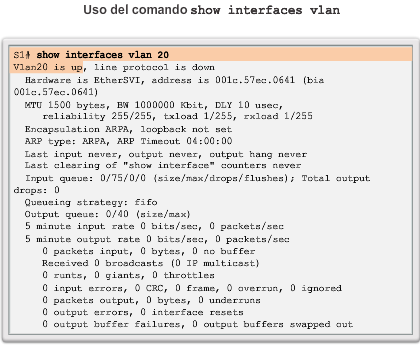
En el ejemplo de la figura 2, el comando**show vlan name student** produce un resultado que no se interpreta fácilmente. Es preferible usar el comando **show vlan brief**. El comando **show vlan summary** muestra el conteo de todas las VLAN configuradas. El resultado de la figura 2 muestra siete VLAN.

El comando **show interfaces vlan***id-vlan* muestra detalles que exceden el ámbito de este curso. La información importante aparece en la segunda línea de la figura 3, que indica que la VLAN 20 está activa.

Utilice el verificador de sintaxis de la figura 4 para mostrar la información de VLAN y de puertos del switch, así como para verificar el modo y las asignaciones de VLAN.







### Enlaces troncales de la VLAN

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. El protocolo DTP se describe en el tema siguiente. En este curso, el comando**switchport mode trunk** es el único método que se implementa para la configuración de enlaces troncales.

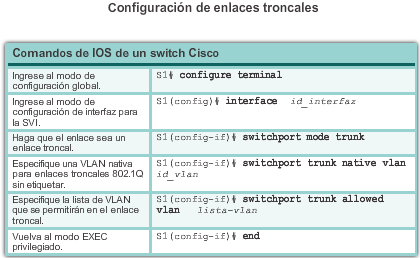
En la figura 1, se muestra la sintaxis del comando de IOS de Cisco para especificar una VLAN nativa (distinta de la VLAN 1).

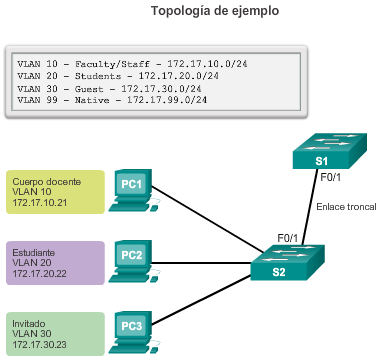
Utilice el comando **switchport trunk allowed vlan***lista-vlan* de IOS de Cisco para especificar la lista de VLAN que se permiten en el enlace troncal.

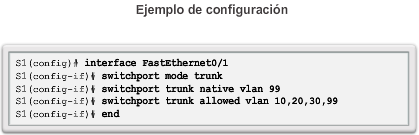
En la figura 2, las VLAN 10, 20 y 30 admiten las computadoras de Cuerpo docente, Estudiante e Invitado (PC1, PC2 y PC3). La VLAN nativa también se debe cambiar de la VLAN 1 a otra VLAN, como la VLAN 99. De manera predeterminada, se permiten todas las VLAN a lo largo de un enlace troncal. Para limitar las VLAN permitidas, se puede usar el comando**switchport trunk allowed vlan**.

En la figura 3, el puerto F0/1 en el switch S1está configurado como puerto de enlace troncal, asigna la VLAN nativa a la VLAN 99 y especifica el enlace troncal para que solo reenvíe tráfico para las VLAN 10, 20, 30 y 99.

**Nota:** esta configuración supone el uso de los switches Cisco Catalyst 2960 que utilizan de manera automática la encapsulación 802.1Q en los enlaces troncales. Es posible que otros switches requieran la configuración manual de la encapsulación. Siempre configure ambos extremos de un enlace troncal con la misma VLAN nativa. Si la configuración de enlace troncal 802.1Q no es la misma en ambos extremos, el software IOS de Cisco registra errores.



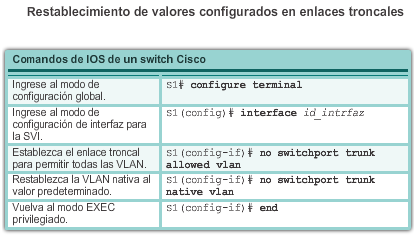


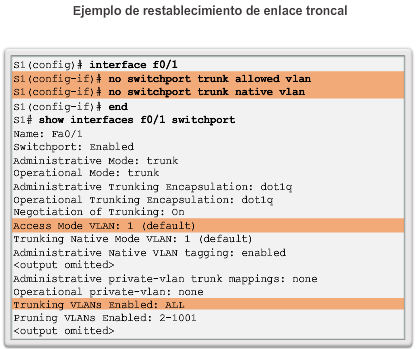


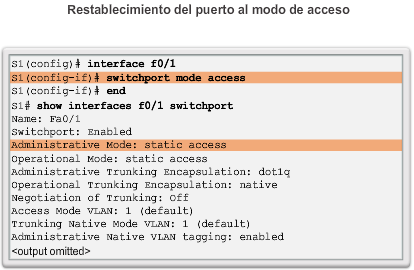
En la figura 1, se muestran los comandos para eliminar las VLAN permitidas y restablecer la VLAN nativa del enlace troncal. Cuando se restablece al estado predeterminado, el enlace troncal permite todas las VLAN y utiliza la VLAN 1 como VLAN nativa.

En la figura 2, se muestran los comandos utilizados para restablecer todas las características de enlace troncal de una interfaz troncal a la configuración predeterminada. El comando **show interfaces f0/1 switchport** revela que el enlace troncal se volvió a configurar en un estado predeterminado.

En la figura 3, el resultado de ejemplo muestra los comandos utilizados para eliminar la característica de enlace troncal del puerto F0/1 del switch S1. El comando**show interfaces f0/1 switchport**revela que la interfaz F0/1 ahora está en modo de acceso estático.



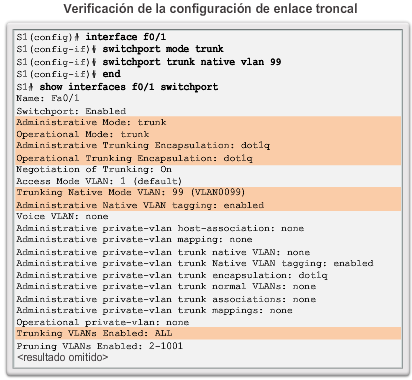




En la figura 1, se muestra la configuración del puerto F0/1 del switch S1. La configuración se verifica con el comando**show interfaces***ID-interfaz***switchport**.

En el área superior resaltada, se muestra que el modo administrativo del puerto F0/1 se estableció en **trunk**. El puerto está en modo de enlace troncal. En la siguiente área resaltada, se verifica que la VLAN nativa es la VLAN 99. Más abajo en el resultado, en el área inferior resaltada, se muestra que todas las VLAN están habilitadas en el enlace troncal.

Utilice el verificador de sintaxis de la figura 2 para configurar un enlace troncal que admita todas las VLAN en la interfaz F0/1 con la VLAN 99 como VLAN nativa. Verifique la configuración de enlace troncal con el comando **show interfaces f0/1 switchport**.



### Protocolo de enlace troncal dinámico

Las interfaces troncales Ethernet admiten diferentes modos de enlace troncal. Una interfaz se puede establecer como troncal o no troncal, o esta puede negociar el enlace troncal con la interfaz vecina. 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.

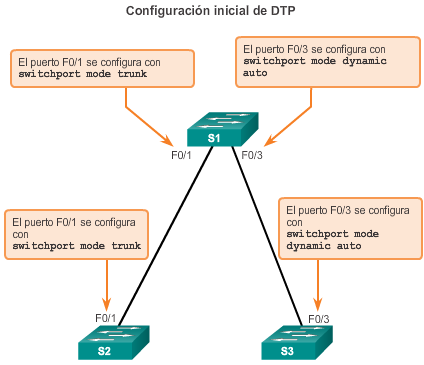
DTP es un protocolo exclusivo de Cisco que se habilita de manera automática en los switches de las series Catalyst 2960 y Catalyst 3560. Los switches de otros proveedores no admiten el DTP. DTP maneja la negociación de enlaces troncales solo si el puerto del switch vecino está configurado en un modo de enlace troncal que admite DTP.

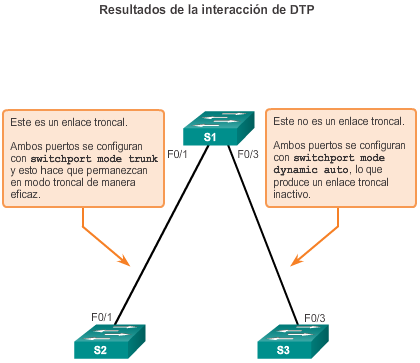
**Precaución:** algunos dispositivos de internetworking pueden reenviar tramas DTP de manera incorrecta, lo que puede causar errores de configuración. Para evitar esto, desactive DTP en las interfaces de los switches Cisco conectadas a dispositivos que no admiten DTP.

La configuración predeterminada de DTP para los switches Cisco Catalyst 2960 y 3560 es dynamic auto (dinámico automático), como se muestra en la figura 1, en la interfaz F0/3 de los switches S1 y S3.

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.

En la figura 2, el enlace entre los switches S1 y S2 se convierte en un enlace troncal porque los puertos F0/1 de los switches S1 y S2 se configuraron para omitir todos los anuncios de DTP, así como para aparecer y permanecer en modo de puerto de enlace troncal. Los puertos F0/3 de los switches S1 y S3 se establecieron en modo dinámico automático, de modo que el resultado de la negociación es el estado de modo de acceso. Esto genera un enlace troncal inactivo. Al configurar un puerto para que esté en modo de enlace troncal mediante el comando **switchport mode trunk**, no existe ambigüedad sobre el estado en que se encuentra el enlace troncal: este se encuentra siempre activo. Con esta configuración, es fácil recordar en qué estado están los puertos de enlace troncal: si se supone que el puerto es un enlace troncal, el modo se establece en enlace troncal.





Las interfaces Ethernet de los switches de las series Catalyst 2960 y Catalyst 3560 admiten diversos modos de enlace troncal con la ayuda de DTP:

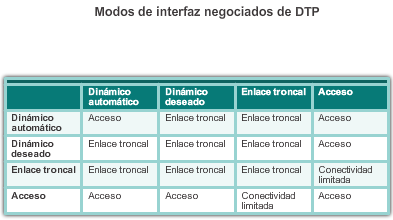
* **switchport mode access**: coloca la interfaz (puerto de acceso) en modo de enlace no troncal permanente y negocia para convertir el enlace en uno no troncal. La interfaz se convierte en una interfaz no troncal, independientemente de si la interfaz vecina es una interfaz troncal.
* **switchport mode dynamic auto**: hace que la interfaz pueda convertir el enlace en un enlace troncal. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en modo de enlace troncal o deseado. El modo de switchport predeterminado para todas las interfaces Ethernet es**dynamic auto**.
* **switchport mode dynamic desirable**: hace que la interfaz intente convertir el enlace en un enlace troncal de manera activa. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en modo de enlace troncal, deseado o automático. Este es el modo de switchport predeterminado en los switches antiguos, como los switches de las series Catalyst 2950 y 3550.
* **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.

En la figura 1, se muestran los resultados de las opciones de configuración de DTP en extremos opuestos de un enlace troncal conectado a los puertos de un switch Catalyst 2960.

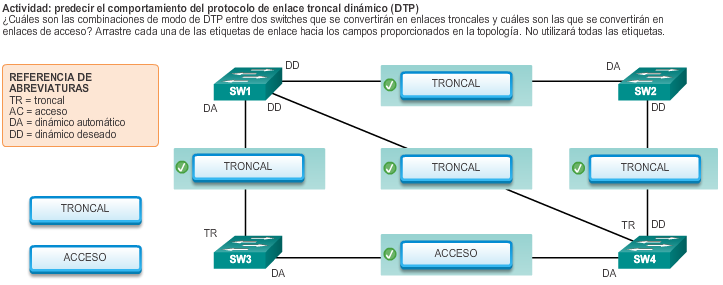
Configure los enlaces troncales estáticamente siempre que sea posible. El modo de DTP predeterminado depende de la versión del software IOS de Cisco y de la plataforma. Para determinar el modo de DTP actual, emita el comando **show dtp interface**, como se muestra en la figura 2.

Utilice el verificador de sintaxis de la figura 3 para determinar el modo de DTP en la interfaz F0/1.

**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.







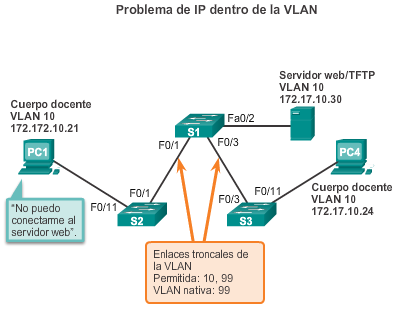
### Resolución de problemas de VLAN y enlaces troncales

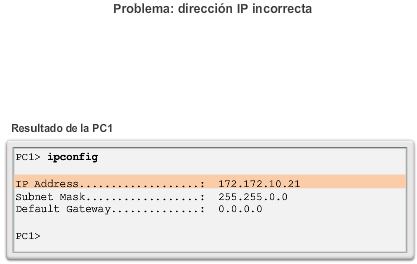
Cada VLAN debe corresponder a una subred IP única. Si dos dispositivos en la misma VLAN tienen direcciones de subred diferentes, no se pueden comunicar. Este es un problema frecuente y se resuelve fácilmente mediante la identificación de la configuración incorrecta y el cambio de la dirección de la subred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

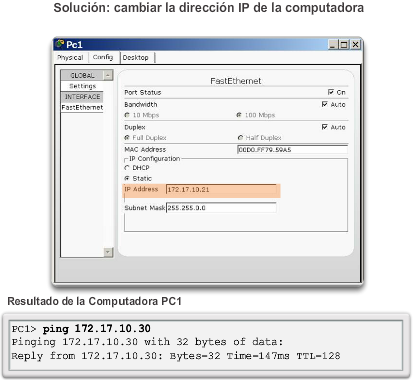
En la figura 1, la PC1 no se puede conectar al servidor Web/TFTP que se muestra.

La verificación de las opciones de configuración IP de la PC1, que se muestra en la figura 2, revela el error más frecuente en la configuración de redes VLAN: una dirección IP mal configurada. La PC1 se configuró con la dirección IP 172.172.10.21, pero debería haberse configurado con la dirección 172.17.10.21.

El cuadro de diálogo de la configuración de Fast Ethernet de la PC1 muestra la dirección IP actualizada, 172.17.10.21. En la figura 3, el resultado que se muestra en la parte inferior indica que la PC1 recuperó la conectividad al servidor Web/TFTP que se encuentra en la dirección IP 172.17.10.30.







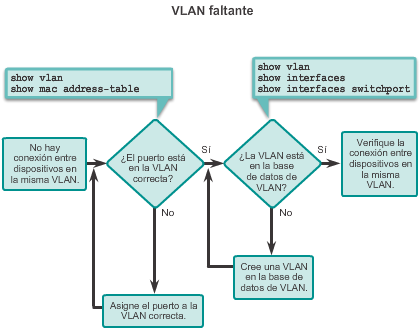
Si todavía no hay conexión entre los dispositivos en una VLAN pero se descartaron los problemas de direccionamiento IP, consulte el diagrama de flujo de la figura 1 para llevar a cabo la resolución de problemas:

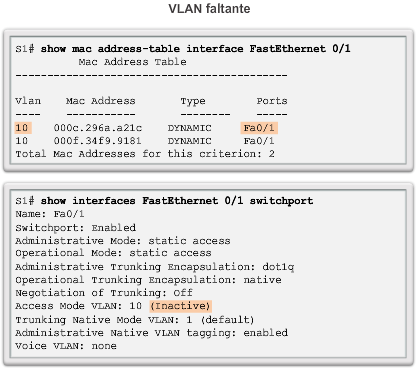
**Paso 1.**Utilice el comando **show vlan**para verificar si el puerto pertenece a la VLAN esperada. Si el puerto se asignó a una VLAN incorrecta, utilice el comando**switchport access vlan** para corregir la pertenencia de VLAN. Utilice el comando**show mac address-table** para revisar qué direcciones se obtuvieron en un puerto determinado del switch y a qué VLAN se asignó ese puerto.

**Paso 2.**Si se elimina la VLAN a la que se asignó el puerto, el puerto pasa a estar inactivo. Utilice los comandos **show vlan**o **show interfaces switchport**.

Para ver la tabla de direcciones MAC, utilice el comando **show mac-address-table**. En el ejemplo de la figura 2, se muestran las direcciones MAC que se obtuvieron en la interfaz F0/1. Se puede observar que en la interfaz F0/1 de la VLAN 10 se obtuvo la dirección MAC 000c.296a.a21c. Si este no es el número de VLAN previsto, cambie la pertenencia de puerto de VLAN con el comando **switchport access vlan**.

Cada puerto de un switch pertenece a una VLAN. Si se elimina la VLAN a la que pertenece el puerto, este pasa a estar inactivo. Ninguno de los puertos que pertenecen a la VLAN que se eliminó puede comunicarse con el resto de la red. Utilice el comando **show interface f0/1 switchport** para verificar si el puerto está inactivo. Si el puerto está inactivo, no funciona hasta que se cree la VLAN con el comando **vlan***id\_vlan*.





Una de las tareas frecuentes de los administradores de red es resolver problemas de formación de enlaces troncales o de enlaces que se comportan incorrectamente como enlaces troncales. 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”.

En la figura 1, se muestra un diagrama de flujo de las pautas generales de resolución de problemas de enlaces troncales.

Para resolver problemas de enlaces troncales que no se forman o de filtración de VLAN, proceda de la siguiente manera:

**Paso 1.**Utilice el comando **show interfaces trunk** para verificar si hay coincidencia entre la VLAN nativa local y peer. Si la VLAN nativa no coincide en ambos extremos, hay una filtración de VLAN.

**Paso 2.**Utilice el comando **show interfaces trunk** para verificar si se estableció un enlace troncal entre los switches. Configure estáticamente los enlaces troncales siempre que sea posible. Los puertos de los switches Cisco Catalyst utilizan DTP de manera predeterminada e intentan negociar un enlace troncal.

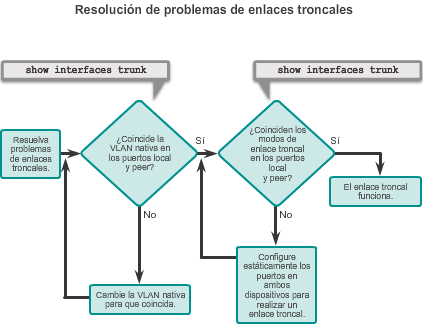
Para mostrar el estado del enlace troncal, la VLAN nativa utilizada en ese enlace troncal y verificar el establecimiento del enlace troncal, utilice el comando **show interfaces trunk**. En el ejemplo de la figura 2, se muestra que la VLAN nativa en un extremo del enlace troncal se cambió a la VLAN 2. Si un extremo del enlace troncal se configura como VLAN 99 nativa y el otro extremo como VLAN 2 nativa, las tramas que se envían desde la VLAN 99 en un extremo se reciben en la VLAN 2 en el otro extremo. La VLAN 99 se filtra en el segmento VLAN 2.

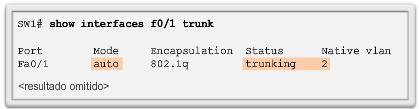
CDP muestra un aviso de incompatibilidad de VLAN nativa en un enlace troncal con este mensaje:

\*Mar 1 06:45:26.232: %CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).

Si existe una incompatibilidad de VLAN nativa, se producen problemas de conectividad en la red. El tráfico de datos para las VLAN distintas de las dos VLAN nativas configuradas se propaga correctamente a través del enlace troncal, pero los datos relacionados con cualquiera de las VLAN nativas no se propagan correctamente a través del enlace troncal.

Como se muestra en la figura 2, los problemas de incompatibilidad de la VLAN nativa no impiden que se forme el enlace troncal. Para resolver una incompatibilidad de VLAN nativa, configure la VLAN nativa para que sea la misma VLAN en ambos lados del enlace.

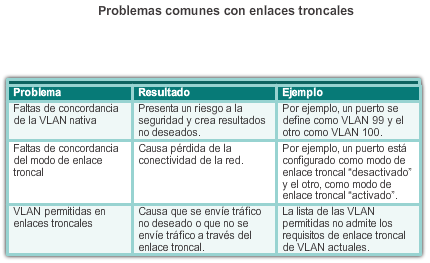




En general, los problemas de enlaces troncales se deben a una configuración incorrecta. Al configurar las VLAN y los enlaces troncales en una infraestructura conmutada, los errores de configuración más frecuentes son los siguientes:

* **Incompatibilidad de VLAN nativa:**los puertos de enlace troncal se configuraron con VLAN nativas diferentes. Este error de configuración genera notificaciones de consola y provoca que el tráfico de control y administración se dirija erróneamente. 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 peer correspondiente. Estos errores de configuración hacen que el vínculo de enlace troncal deje de funcionar.
* **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.

Si se detecta un problema con un enlace troncal y se desconoce la causa, comience la resolución de problemas con un examen de los enlaces troncales para determinar si hay una incompatibilidad de VLAN nativa. Si esa no es la causa, verifique si hay una incompatibilidad de modo de enlace troncal y, por último, revise la lista de VLAN permitidas en el enlace troncal. En las dos páginas siguientes, se analiza cómo solucionar problemas frecuentes de los enlaces troncales.

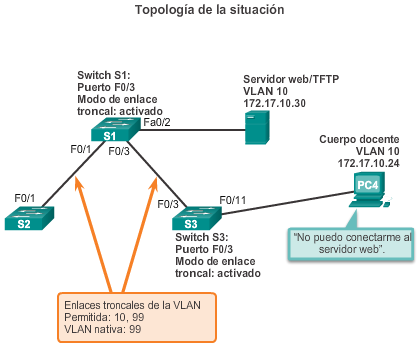


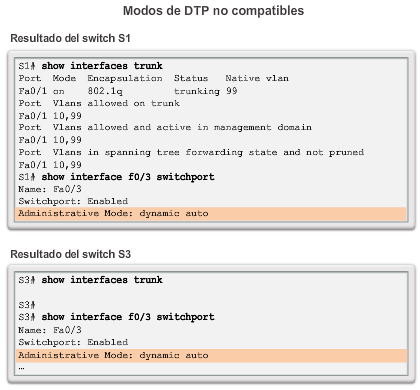
Por lo general, los enlaces troncales se configuran estáticamente con el comando**switchport mode trunk**. Los puertos de enlace troncal de los switches Cisco Catalyst utilizan DTP para negociar el estado del enlace. Cuando un puerto en un enlace troncal se configura con un modo de enlace troncal que no es compatible con el puerto de enlace troncal vecino, no se puede formar un enlace troncal entre los dos switches.

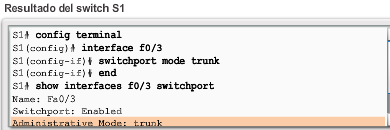
En la situación que se describe en la figura 1, la PC4 no puede conectarse al servidor web interno. La topología indica una configuración válida. ¿Por qué hay un problema?

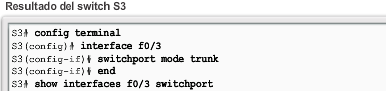
Verifique el estado de los puertos de enlace troncal del switch S1 con el comando **show interfaces trunk**. El resultado que se muestra en la figura 2 indica que la interfaz Fa0/3 del switch S1 actualmente no es un enlace troncal. Si se examina la interfaz F0/3, se descubre que el puerto del switch está en modo dinámico automático. Si se examinan los enlaces troncales del switch S3, se descubre que no hay puertos de enlace troncal activos. Si se sigue examinando, se descubre que la interfaz Fa0/3 también está en modo dinámico automático. Esto explica la inactividad del enlace troncal.

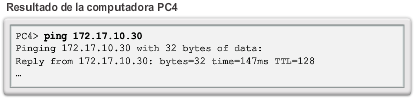
Para resolver el problema, vuelva a configurar el modo de enlace troncal de los puertos F0/3 de los switches S1 y S3, como se muestra en la figura 3. Después del cambio de configuración, el resultado del comando **show interfaces** indica que el puerto del switch S1 ahora está en modo de enlace troncal. El resultado de la PC4 indica que esta recuperó la conectividad al servidor Web/TFTP que se encuentra en la dirección IP 172.17.10.30.









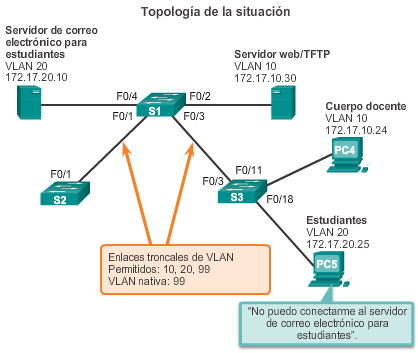


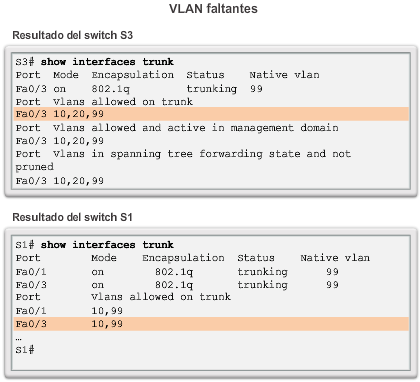
Para que el tráfico de una VLAN se transmita a través de un enlace troncal, debe estar permitido en dicho enlace. Para hacerlo, utilice el comando **switchport trunk allowed vlan***id-vlan*.

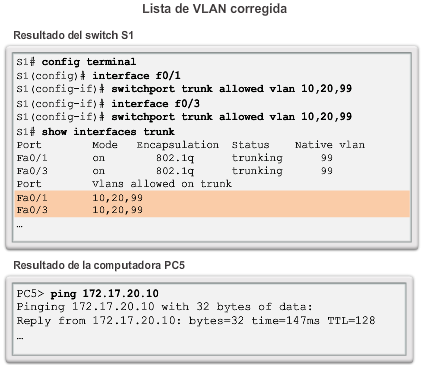
En la figura 1, se agregaron la VLAN 20 (Estudiantes) y la PC5 a la red. La documentación se ha actualizado para mostrar que las VLAN permitidas en el enlace troncal son las 10, 20 y 99. En esta situación, la PC5 no puede conectarse al servidor de correo electrónico para estudiantes.

Verifique los puertos de enlace troncal del switch S1 con el comando **show interfaces trunk**, como se muestra en la figura 2. El comando revela que la interfaz F0/3 del switch S3 se configuró correctamente para permitir las VLAN 10, 20 y 99. Si se examina la interfaz F0/3 del switch S1, se descubre que las interfaces F0/1 y F0/3 permiten solo las VLAN 10 y 99. Alguien actualizó el registro pero olvidó volver a configurar los puertos del switch S1.

Vuelva a configurar los puertos F0/1 y F0/3 del switch S1 con el comando**switchport trunk allowed vlan 10,20,99**, como se muestra en la figura 3. El resultado muestra que ya se agregaron las VLAN 10, 20 y 99 a los puertos F0/1 y F0/3 del switch S1. El comando **show interfaces trunk** es una excelente herramienta para revelar problemas frecuentes de enlace troncal. La PC5 recuperó la conectividad al servidor de correo electrónico para estudiantes que se encuentra en la dirección IP 172.17.20.10.







## Seguridad y diseño de redes VLAN

### Ataques a redes VLAN

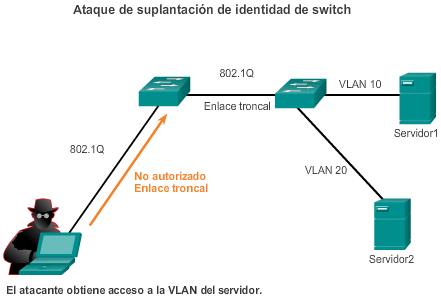
Existen diferentes tipos de ataques a VLAN en las redes conmutadas modernas. La arquitectura VLAN simplifica el mantenimiento de la red y mejora el rendimiento, pero también posibilita el uso indebido. Es importante comprender la metodología general detrás de estos ataques y los métodos principales para mitigarlos.

Los saltos de VLAN permiten que una VLAN pueda ver el tráfico de otra VLAN. La suplantación de identidad de switch es un tipo de ataque con salto de VLAN que funciona mediante el aprovechamiento de un puerto de enlace troncal mal configurado. De manera predeterminada, los puertos de enlace troncal tienen acceso a todas las VLAN y pasan el tráfico para varias VLAN a través del mismo enlace físico, generalmente entre switches.

Haga clic en el botón Play (Reproducir) de la ilustración para ver una animación del ataque de suplantación de identidad de switch.

En un ataque de suplantación de identidad de switch básico, el atacante aprovecha el hecho de que la configuración predeterminada del puerto del switch sea dinámica automática. El atacante de la red configura un sistema para suplantar su propia identidad y hacerse pasar por un switch. Esta suplantación de identidad requiere que el atacante de la red pueda emular mensajes 802.1Q y DTP. Al hacerle creer al switch que otro switch intenta crear un enlace troncal, el atacante puede acceder a todas las VLAN permitidas en el puerto de enlace troncal.

La mejor manera de prevenir un ataque de suplantación de identidad de switch básico es inhabilitar los enlaces troncales en todos los puertos, excepto en los que específicamente requieren enlaces troncales. En los puertos de enlace troncal requeridos, inhabilite DTP y habilite los enlaces troncales manualmente.



Otro tipo de ataque VLAN es el ataque con salto de VLAN de etiquetado doble (o de encapsulado doble). Este tipo de ataque aprovecha la forma en que funciona el hardware en la mayoría de los switches. La mayoría de los switches realizan solo un nivel de desencapsulación 802.1Q, lo que permite que un atacante incorpore una etiqueta 802.1Q oculta en la trama. Esta etiqueta permite que la trama se reenvíe a una VLAN que la etiqueta 802.1Q original no especificó. Una característica importante del ataque con salto de VLAN de encapsulado doble es que funciona incluso si se inhabilitan los puertos de enlace troncal, ya que, generalmente, un host envía una trama por un segmento que no es un enlace troncal.

Los ataques con salto de VLAN de etiquetado doble implican los siguientes tres pasos:

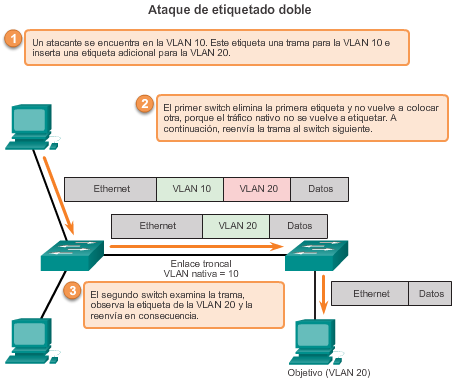
1. El atacante envía una trama 802.1Q con doble etiqueta al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN nativa del puerto de enlace troncal. Se supone que el switch procesa la trama que recibe del atacante como si estuviera en un puerto de enlace troncal o un puerto con una VLAN de voz (un switch no debe recibir una trama de Ethernet etiquetada en un puerto de acceso). A los fines de este ejemplo, suponga que la VLAN nativa es la VLAN 10. La etiqueta interna es la VLAN víctima; en este caso, la VLAN 20.

2. La trama llega al switch, que observa la primera etiqueta 802.1Q de 4 bytes. El switch observa que la trama está destinada a la VLAN 10, que es la VLAN nativa. El switch reenvía el paquete por todos los puertos de la VLAN 10 después de eliminar la etiqueta de VLAN 10. En el puerto de enlace troncal, se elimina la etiqueta de VLAN 10, y no se vuelve a etiquetar el paquete porque esta forma parte de la VLAN nativa. En este punto, la etiqueta de VLAN 20 sigue intacta, y el primer switch no la inspeccionó.

3. El segundo switch observa solo la etiqueta 802.1Q interna que envió el atacante y ve que la trama está destinada a la VLAN 20, el objetivo. El segundo switch envía la trama al puerto víctima o lo satura, según si existe una entrada en la tabla de direcciones MAC para el host víctima.

Este tipo de ataque es unidireccional y solo funciona cuando el atacante se conecta a un puerto que reside en la misma VLAN que la VLAN nativa del puerto de enlace troncal. Frustrar este tipo de ataque no es tan fácil como detener ataques de salto de VLAN básicos.

El mejor método para mitigar los ataques de etiquetado doble es asegurar que la VLAN nativa de los puertos de enlace troncal sea distinta de la VLAN de cualquier puerto de usuario. De hecho, se considera una práctica recomendada de seguridad la utilización de una VLAN fija distinta de todas las VLAN de usuario como VLAN nativa para todos los enlaces troncales 802.1Q en la red conmutada.



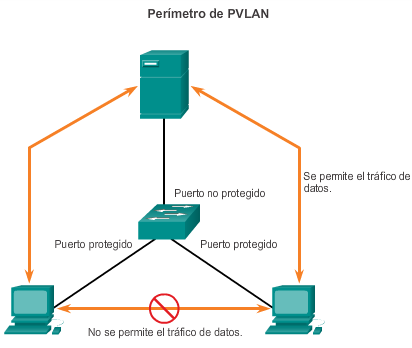
Algunas aplicaciones requieren que no se reenvíe tráfico en la capa 2 entre los puertos del mismo switch, de modo que un vecino no vea el tráfico generado por otro vecino. En ese entorno, el uso de la característica de perímetro de VLAN privada (PVLAN), también conocida como “puertos protegidos”, asegura que no se intercambie tráfico de unidifusión, difusión o multidifusión entre estos puertos del switch (figura 1).

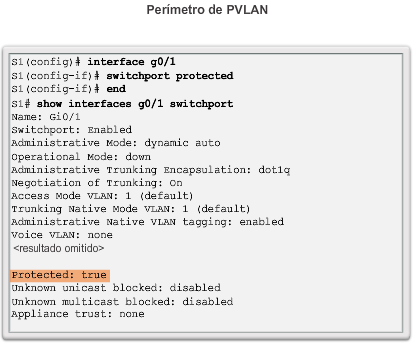
Las características de la función de perímetro de PVLAN son las siguientes:

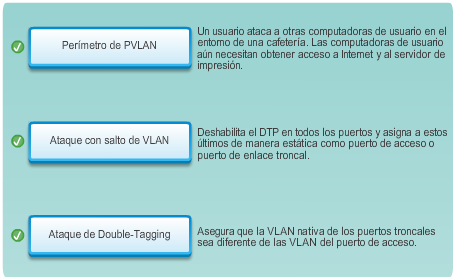
* Los puertos protegidos no reenvían tráfico (de unidifusión, difusión o multidifusión) a ningún otro puerto que también sea un puerto protegido, excepto el tráfico de control. El tráfico de datos no se puede reenviar entre los puertos protegidos en la capa 2.
* El comportamiento de reenvío entre un puerto protegido y un puerto no protegido continúa normalmente.
* Los puertos protegidos se deben configurar manualmente.

Para configurar la característica de perímetro de PVLAN, introduzca el comando **switchport protected** en el modo de configuración de interfaz (figura 2). Para inhabilitar los puertos protegidos, utilice el comando **no switchport protected** del modo de configuración de interfaz. Para verificar la configuración de la característica de perímetro de PVLAN, utilice el comando **show interfaces***id-interfaz***switchport** del modo de configuración global.

Utilice el verificador de sintaxis de la figura 3 para configurar la característica de perímetro de PVLAN en la interfaz G0/1 y verificar la configuración.







## Prácticas recomendadas de diseño para las VLAN

Los switches Cisco tienen una configuración de fábrica en la cual las VLAN predeterminadas se preconfiguran para admitir diversos tipos de medios y protocolos. La VLAN Ethernet predeterminada es la VLAN 1. Por seguridad, se recomienda configurar todos los puertos de todos los switches para que se asocien a VLAN distintas de la VLAN 1. Generalmente, esto se logra configurando todos los puertos sin utilizar en una VLAN de agujero negro que no se use para nada en la red. Todos los puertos utilizados se asocian a VLAN independientes de la VLAN 1 y de la VLAN de agujero negro. También se recomienda desactivar los puertos de switch sin utilizar para evitar el acceso no autorizado.

Una buena práctica de seguridad es separar el tráfico de administración y de datos de usuario. La VLAN de administración, que es la VLAN 1 de manera predeterminada, se debe cambiar a una VLAN diferente e independiente. Para comunicarse de manera remota con un switch Cisco con fines de administración, el switch debe tener una dirección IP configurada en la VLAN de administración. Los usuarios en otras VLAN no pueden establecer sesiones de acceso remoto al switch, a menos que se los enrute a la VLAN de administración, lo que proporciona una capa de seguridad adicional. Además, se debe configurar el switch para que solo acepte sesiones SSH cifradas para la administración remota.

Todo el tráfico de control se envía por la VLAN 1. Por lo tanto, cuando se cambia la VLAN nativa a una opción distinta de la VLAN 1, todo el tráfico de control se etiqueta en los enlaces troncales de VLAN IEEE 802.1Q (se etiqueta con la ID de VLAN 1). Por seguridad, se recomienda cambiar la VLAN nativa a una VLAN distinta de la VLAN 1. La VLAN nativa también debe ser distinta de todas las VLAN de usuarios. Asegúrese de que la VLAN nativa para un enlace troncal 802.1Q sea la misma en ambos extremos del enlace troncal.

DTP ofrece cuatro modos de puerto de switch: acceso, enlace troncal, dinámico automático y dinámico deseado. Una pauta general es inhabilitar la autonegociación. Una práctica recomendada de seguridad de puertos es no utilizar los modos de puerto de switch dinámico automático o dinámico deseado.

Por último, el tráfico de voz tiene requisitos de QoS estrictos. Si las computadoras y los teléfonos IP de los usuarios están en la misma VLAN, cada uno intenta usar el ancho de banda disponible sin tener en cuenta al otro dispositivo. Para evitar este conflicto, es aconsejable utilizar VLAN separadas para la telefonía IP y para el tráfico de datos.

## 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. Esta función es útil para reducir el tamaño de los dominios de difusión o para permitir la agrupación lógica de grupos o usuarios sin la necesidad de que estén ubicados físicamente en el mismo lugar.

Existen varios tipos de VLAN:

* VLAN predeterminada
* VLAN de administración
* VLAN nativa
* VLAN de datos/de usuarios
* VLAN de agujero negro
* VLAN de voz

En los switches Cisco, la VLAN 1 es la VLAN Ethernet predeterminada, la VLAN nativa predeterminada y la VLAN de administración predeterminada. Las prácticas recomendadas sugieren que la VLAN nativa y la de administración se cambien a una VLAN distinta, y que los puertos de switch sin utilizar se trasladen a una VLAN de “agujero negro” para mayor seguridad.

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.

Utilice el comando **show vlan** para verificar si el puerto pertenece a la VLAN esperada. Si el puerto se asignó a una VLAN incorrecta, utilice el comando**switchport access vlan** para corregir la pertenencia de VLAN. Utilice el comando**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**. Utilice 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 su condición predeterminada de fábrica con una VLAN predeterminada, use el comando **delete flash:vlan.dat** y **erase startup-config**.

En este capítulo, también se analizó la configuración y la verificación de redes VLAN y de enlaces troncales, así como la resolución de problemas relacionados mediante la CLI de IOS de Cisco, y se exploraron las consideraciones básicas de seguridad y de diseño en el contexto de las redes VLAN.

