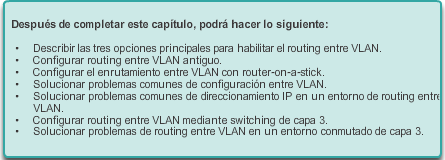
# Enrutamiento entre VLAN

## Introducción

Hemos visto que el uso de redes VLAN para segmentar una red conmutada proporciona mayor rendimiento, seguridad y capacidad de administración. Se utilizan enlaces troncales para transportar información de varias VLAN entre dispositivos. Sin embargo, debido a que estas VLAN segmentan la red, es necesario un proceso de capa 3 para permitir que el tráfico pase de un segmento de red a otro.

Este proceso de routing de capa 3 puede implementarse utilizando un router o una interfaz de switch de capa 3. El uso de un dispositivo de capa 3 proporciona un método para controlar el flujo de tráfico entre segmentos de red, incluidos los segmentos de red creados por las VLAN.

En este capítulo, se analizan los métodos utilizados para la implementación del routing entre VLAN. Se incluye configuraciones para el uso de un router y un switch de capa 3 y también se describen los problemas que se encuentran al implementar routing entre VLAN y técnicas estándar de resolución de problemas.



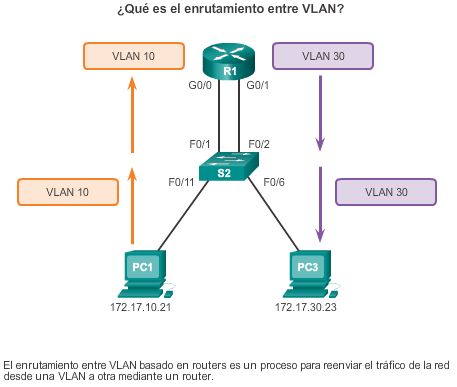


## Configuración del routing entre VLAN

### Funcionamiento del routing entre VLAN

Las VLAN se utilizan para segmentar redes conmutadas. Un profesional de redes puede configurar switches de capa 2, tales como los de la serie Catalyst 2960, con más de 4000 VLAN. Sin embargo, los switches de capa 2 tienen una funcionalidad muy limitada en cuanto a IPv4 e IPv6, y no pueden realizar las funciones de routing de los routers. Mientras que los switches de capa 2 adquieren cada vez una mayor funcionalidad de IP, como la capacidad de realizar routing estático, no admiten routing dinámico. La gran cantidad de VLAN posibles en estos switches hace que el routing estático sea insuficiente.

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. 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”.



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.

**Nota:** la topología utiliza enlaces paralelos para establecer los enlaces troncales entre los switches a fin de obtener agregación de enlaces y redundancia. Sin embargo, los enlaces redundantes hacen que la topología sea más compleja y pueden introducir problemas de conectividad si no se administran de la manera adecuada. Deben implementarse protocolos y técnicas, tales como árbol de expansión y EtherChannel, para administrar los enlaces redundantes. Estas técnicas exceden el ámbito de este capítulo.

Haga clic en el botón Reproducir de la ilustración para ver una animación del routing entre VLAN antiguo.

Tal como se observa en la animación:

1. La PC1 en la VLAN 10 se comunica con la PC3 en la VLAN 30 a través del router R1.

2. PC1 y PC3 están en VLAN diferentes y tienen direcciones IP en subredes diferentes.

3. El router R1 tiene una interfaz separada configurada para cada una de las VLAN.

4. La PC1 envía el tráfico de unidifusión destinado a la PC3 al switch S2 en la VLAN 10, desde el cual luego se reenvía por la interfaz troncal al switch S1.

5. Después, el switch S1 reenvía el tráfico de unidifusión al router R1 en la interfaz G0/0.

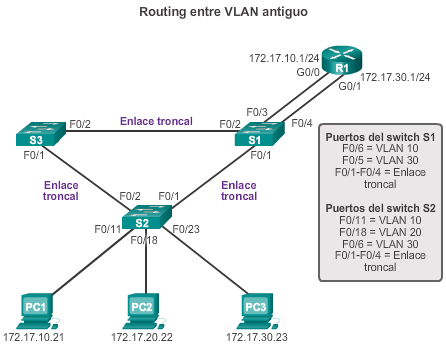
6. El router enruta el tráfico de unidifusión a través de la interfaz G0/1, que está conectada a la VLAN 30.

7. El router reenvía el tráfico unicast al switch S1 en la VLAN 30.

8. El switch S1 luego reenvía el tráfico de unidifusión al switch S2 a través del enlace troncal activo, tras lo cual el switch S2 puede reenviar el tráfico de unidifusión a la PC3 en la VLAN 30.

En este ejemplo el router se configuró con dos interfaces físicas separadas para interactuar con las distintas VLAN y realizar el enrutamiento.

**Nota:** este método de routing entre VLAN no es eficaz y, por lo general, ya no se implementa en las redes conmutadas. Se muestra en este curso solo con fines explicativos.



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.

Haga clic en el botón Reproducir de la ilustración para ver una animación de la forma en que un router-on-a-stick desempeña su función de routing.

Tal como se observa en la animación:

1. La PC1 en la VLAN 10 se comunica con la PC3 en la VLAN 30 a través del router R1 mediante una única interfaz física del router.

2. PC1 envía el tráfico unicast al switch S2.

3. Luego, el switch S2 etiqueta el tráfico de unidifusión como originado en la VLAN 10 y lo reenvía por el enlace troncal al switch S1.

4. El switch S1 reenvía el tráfico etiquetado por la otra interfaz troncal en el puerto F0/5 a la interfaz en el router R1.

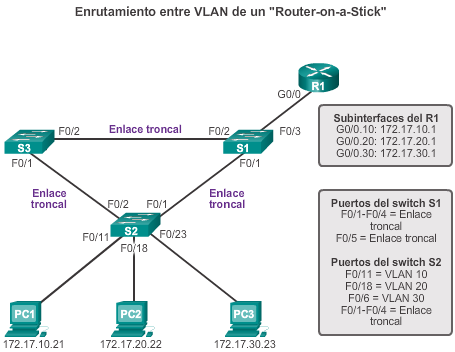
5. El router R1 acepta el tráfico de unidifusión etiquetado en la VLAN 10 y lo enruta a la VLAN 30 mediante sus subinterfaces configuradas.

6. El tráfico de unidifusión se etiqueta con la VLAN 30 mientras se envía por la interfaz del router al switch S1.

7. El switch S1 reenvía el tráfico unicast etiquetado por el otro enlace troncal al switch S2.

8. El switch S2 elimina la etiqueta de la VLAN de la trama de unicast y reenvía la trama a PC3 en el puerto F0/6.

**Nota:** el método de routing entre VLAN de router-on-a-stick no es escalable más allá de las 50 VLAN.



La implementación de routing entre VLAN de router-on-a-stick requiere solamente una interfaz física en un router y una interfaz en un switch, lo que simplifica el cableado del router. Sin embargo, en otras implementaciones de routing entre VLAN, no se necesita un router dedicado.

Los switches multicapa pueden realizar funciones de capa 2 y de capa 3, lo que remplaza la necesidad de utilizar routers dedicados para realizar tareas de routing básico en una red. Los switches multicapa admiten routing dinámico y routing entre VLAN.

Haga clic en el botón Reproducir de la ilustración para ver una animación de la forma en que se realiza el routing entre VLAN basado en switch.

Tal como se observa en la animación:

1. La PC1 en la VLAN 10 se comunica con la PC3 en la VLAN 30 a través del switch S1 mediante las interfaces VLAN configuradas para cada VLAN.

2. PC1 envía el tráfico unicast al switch S2.

3. El switch S2 etiqueta el tráfico de unidifusión como originado en la VLAN 10 a medida que lo reenvía por el enlace troncal al switch S1.

4. El switch S1 elimina la etiqueta de VLAN y reenvía el tráfico de unidifusión a la interfaz de la VLAN 10.

5. El switch S1 enruta el tráfico de unidifusión a su interfaz de la VLAN 30.

6. El switch S1 luego vuelve a etiquetar el tráfico de unidifusión con la VLAN 30 y lo reenvía por el enlace troncal al switch S2.

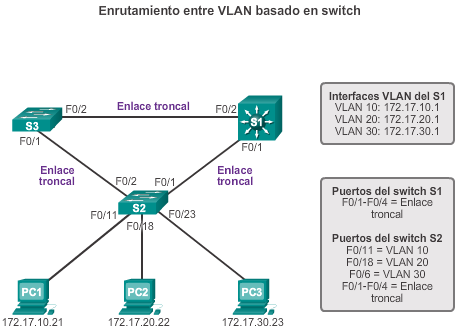
7. El switch S2 elimina la etiqueta de la VLAN de la trama de unicast y reenvía la trama a PC3 en el puerto F0/6.

Para habilitar un switch multicapa para que realice funciones de routing, debe tener routing IP habilitado.

El switching de multicapa es más escalable que cualquier otra implementación de routing entre VLAN. Esto se debe a que los routers tienen una cantidad limitada de puertos disponibles para conectarse a las redes. Además, en el caso de las interfaces que se configuran como una línea troncal, se puede admitir una cantidad limitada de tráfico en la línea al mismo tiempo.

Con un switch multicapa, el tráfico se enruta internamente al dispositivo de switch, lo que significa que los paquetes no se filtran por una única línea troncal para obtener nueva información de etiquetado de VLAN. Sin embargo, un switch multicapa no reemplaza totalmente la funcionalidad de un router. Los routers admiten una cantidad considerable de características adicionales, como la capacidad de implementar mayores controles de seguridad. En cambio, un switch multicapa se puede pensar como un dispositivo de capa 2 actualizado para tener algunas capacidades de routing.

**Nota:** en este curso, la configuración de routing entre VLAN en un switch se restringe a configurar rutas estáticas en un switch 2960, que es la única funcionalidad de routing admitida en los switches 2960. Los switches 2960 admiten hasta 16 rutas estáticas (entre las que se incluyen las rutas configuradas por el usuario y la ruta predeterminada) y todas las rutas conectadas directamente y las rutas predeterminadas para la interfaz de administración. Los switches 2960 pueden tener una dirección IP asignada a cada interfaz virtual de switch (SVI). En cuanto a switches multicapa relativamente económicos con todas las características, los switches de la serie Cisco Catalyst 3560 admiten los protocolos de routing EIGRP, OSPF y BGP.



### Configuración de routing entre VLAN antiguo

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 IP para la subred asociada con la VLAN específica a la cual está conectada. Al configurar las direcciones IP 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.

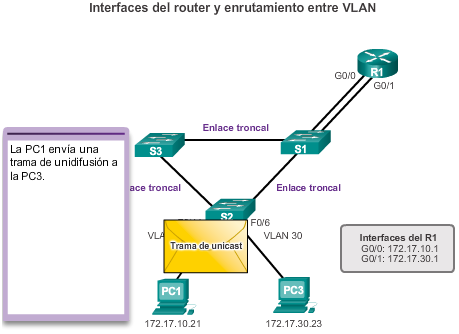
El proceso de enrutamiento requiere del dispositivo de origen para determinar si el dispositivo de destino es local o remoto con respecto a la subred local. El dispositivo de origen realiza esta determinación al comparar las direcciones IP de origen y de destino con la máscara de subred. Una vez que se determina que la dirección IP 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 IP de la interfaz del router en la subred local actúa como gateway predeterminado para el dispositivo emisor.

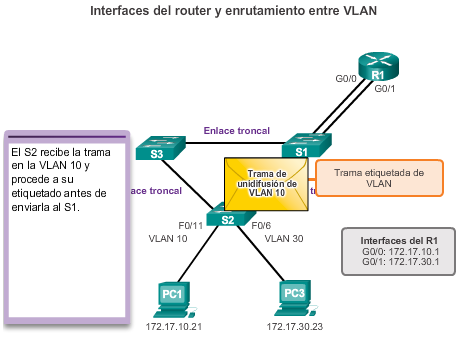
Una vez que el dispositivo de origen determina que el paquete debe viajar a través de la interfaz del router local en la VLAN conectada, envía una solicitud de ARP para determinar la dirección MAC de la interfaz del router local. Una vez que el router envía su respuesta de ARP al dispositivo de origen, este puede utilizar la dirección MAC para finalizar el entramado del paquete antes de enviarlo a la red como tráfico de unidifusión.

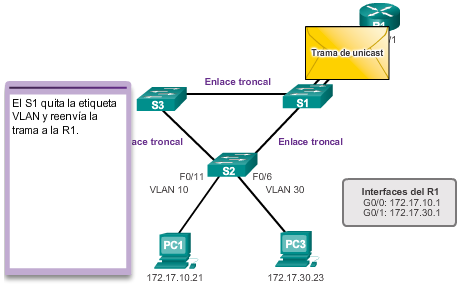
Dado que la trama de Ethernet tiene la dirección MAC de destino de la interfaz del router, el switch sabe exactamente a qué puerto del switch reenviar el tráfico de unidifusión para llegar a la interfaz del router de dicha VLAN. Cuando la trama llega al router, el router elimina la información de la dirección MAC de origen y destino para examinar la dirección IP de destino del paquete. El router compara la dirección de destino con las entradas en la tabla de enrutamiento para determinar dónde es necesario reenviar los datos para alcanzar el destino final. Si el router determina que la red de destino es una red conectada en forma local, como sería el caso del routing entre VLAN, envía una solicitud de ARP por la interfaz conectada físicamente a la VLAN de destino. El dispositivo de destino responde al router con la dirección MAC, la cual luego utiliza el router para entramar el paquete. El router envía el tráfico unicast al switch, que lo reenvía por el puerto donde se encuentra conectado el dispositivo de destino.

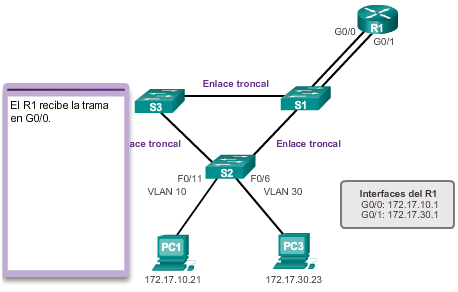
Haga clic en el botón Reproducir de la ilustración para ver cómo se realiza el routing entre VLAN antiguo.

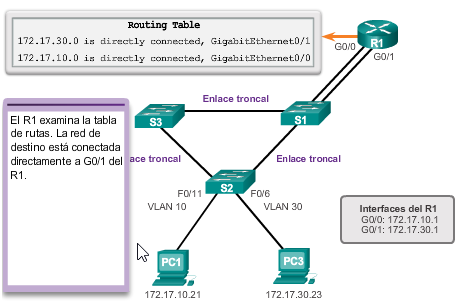
Aunque existen muchos pasos en el proceso de routing entre VLAN, cuando dos dispositivos en diferentes VLAN se comunican a través de un router, el proceso completo tiene lugar en una fracción de segundo.

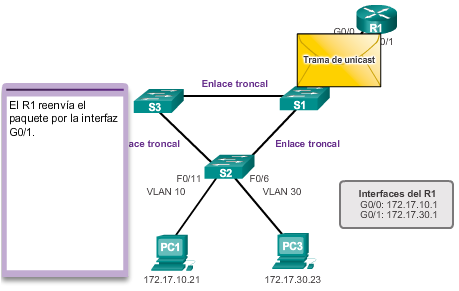


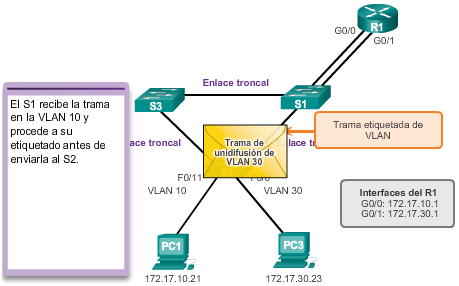


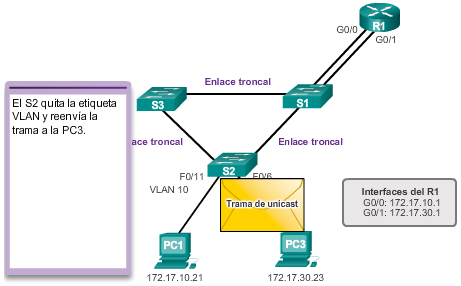












Para configurar el routing entre VLAN antiguo, comience con la configuración del switch.

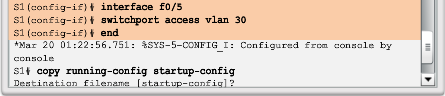
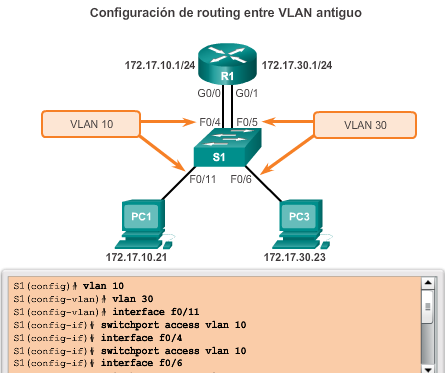
Como se muestra en la ilustración, el router R1 está conectado a los puertos del switch F0/4 y F0/5, que se configuraron para las VLAN 10 y 30 respectivamente.

Utilice el comando **vlan** *id\_vlan* del modo de configuración global para crear las VLAN. En este ejemplo las VLAN 10 y 30 se crearon en el switch S1.

Una vez que se crean las VLAN, los puertos de switch se asignan a las VLAN adecuadas. El comando **switchport access vlan** *id\_vlan* se ejecuta desde el modo de configuración de interfaz en el switch para cada interfaz a la cual se conecta el router.

En este ejemplo, las interfaces F0/4 y F0/11 se asignaron a la VLAN 10 con el comando **switchport access vlan 10**. Se utilizó el mismo proceso para asignar la interfaz F0/5 y F0/6 en el switch S1 a la VLAN 30.

Finalmente, para proteger la configuración y no perderla después de una recarga del switch, se ejecuta el comando **copy running-config startup-config**para guardar una copia de seguridad de la configuración en ejecución en la configuración de inicio.



A continuación, se puede configurar el router para que realice routing entre VLAN.

Las interfaces del router se configuran de manera similar a las interfaces de VLAN en los switches. Para configurar una interfaz específica, pase al modo de configuración de interfaz desde el modo de configuración global.

Como se muestra en la figura 1, cada interfaz se configura con una dirección IP mediante el comando **ip address***dirección\_ip máscara\_subred* en el modo de configuración de interfaz.

Como se muestra en el ejemplo, la interfaz G0/0 se configuró con la dirección IP 172.17.10.1 y la máscara de subred 255.255.255.0 mediante el comando **ip address 172.17.10.1 255.255.255.0**.

Las interfaces del router están deshabilitadas de manera predeterminada y es necesario habilitarlas con el comando **no shutdown** antes de utilizarlas. Una vez que se emite el comando del modo de configuración de interfaz **no shutdown**, se muestra una notificación que indica que el estado de la interfaz cambió a activó (up). Esto indica que la interfaz ahora está habilitada.

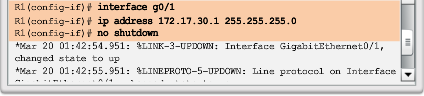
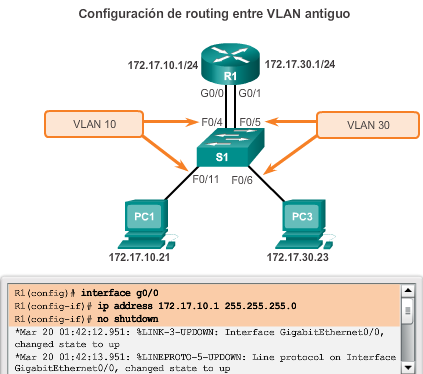
El proceso se repite para todas las interfaces del router. Es necesario asignar cada interfaz del router a una subred única para que se produzca el routing. En este ejemplo, la otra interfaz del router, G0/1, se configuró para utilizar la dirección IP 172.17.30.1, que se encuentra en una subred diferente que la interfaz G0/0.

Una vez que se asignan las direcciones IP a las interfaces físicas y que las interfaces se habilitan, el router es capaz de llevar a cabo routing entre VLAN.

Examine la tabla de routing con el comando**show ip route**.

En la figura 2, hay dos rutas visibles en la tabla de routing. Una ruta es la subred 172.17.10.0, que está conectada a la interfaz local G0/0. La otra ruta es la subred 172.17.30.0, que está conectada a la interfaz local G0/1. El router utiliza la tabla de enrutamiento para determinar dónde enviar el tráfico que recibe. Por ejemplo: si el router recibe un paquete en la interfaz G0/0 destinado a la subred 172.17.30.0, el router identificará que debe enviar el paquete por la interfaz G0/1 para que llegue a los hosts en la subred 172.17.30.0.

Observe la letra **C** a la izquierda de cada una de las entradas de ruta para las VLAN. Esta letra indica que la ruta es local para una interfaz conectada, que también está identificada en la entrada de ruta. Según el resultado de este ejemplo, si el tráfico estuviera destinado a la subred 172.17.30.0, el router debería reenviar el tráfico por la interfaz G0/1.



### Configurar un enrutamiento router-on-a-stick entre VLAN

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.

Las subinterfaces son interfaces virtuales basadas en software asignadas a interfaces físicas. Cada subinterfaz se configura de forma independiente con su propia dirección IP y máscara de subred. Esto permite que una única interfaz física forme parte de varias redes lógicas de manera simultánea.

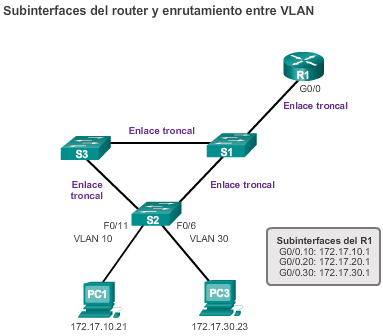
Al configurar el enrutamiento inter VLAN mediante el modelo router-on-a-stick, la interfaz física del router debe estar conectada al enlace troncal en el switch adyacente. En el router, se crean subinterfaces para cada VLAN única en la red. A cada subinterfaz se le asigna una dirección IP específica 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.

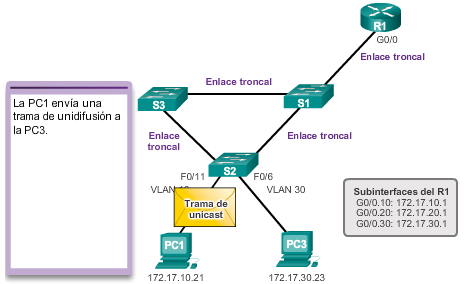
En términos de funcionamiento, utilizar el modelo router-on-a-stick es lo mismo que utilizar el modelo de routing entre VLAN antiguo, pero en lugar de utilizar las interfaces físicas para realizar el routing, se utilizan las subinterfaces de una única interfaz física.

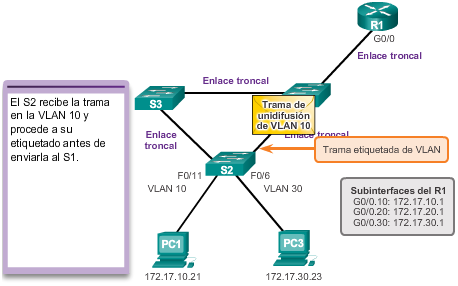
En la figura, PC1 desea comunicarse con PC3. La PC1 se encuentra en la VLAN 10, y la PC3, en la VLAN 30. Para que la PC1 se comunique con la PC3, la PC1 necesita enrutar sus datos a través del router R1, por medio de subinterfaces.

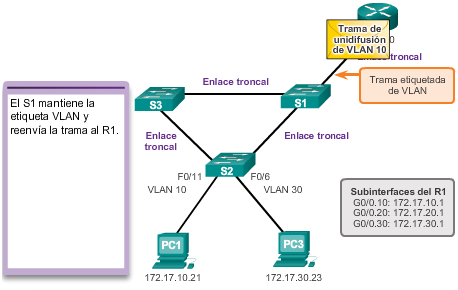
Haga clic en el botón Reproducir que se muestra en la figura para ver cómo se utilizan las subinterfaces para enrutar entre las VLAN. Cuando se detenga la animación, lea el texto a la izquierda de la topología. Haga clic en Reproducir nuevamente para seguir viendo la animación.

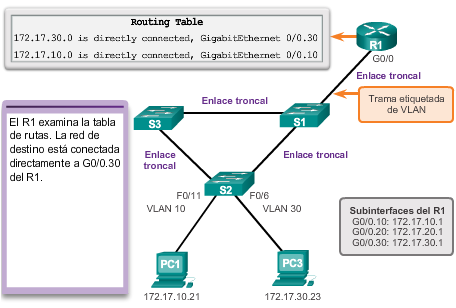
El uso de los enlaces troncales y las subinterfaces disminuye la cantidad de puertos de switch y de router que se utilizan. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de la subinterfaz del router puede ampliarse hasta un número mucho más alto de VLAN que una configuración con una interfaz física por diseño de VLAN.

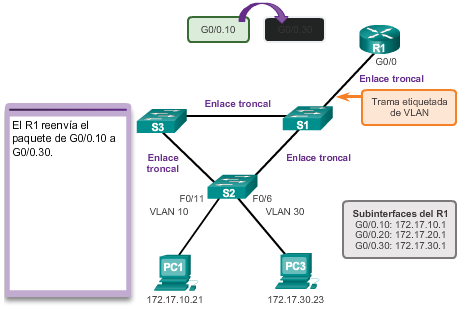


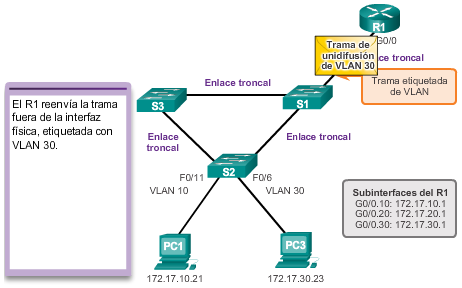


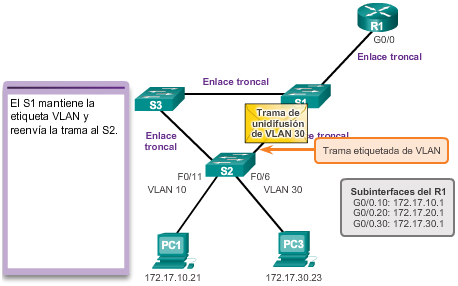


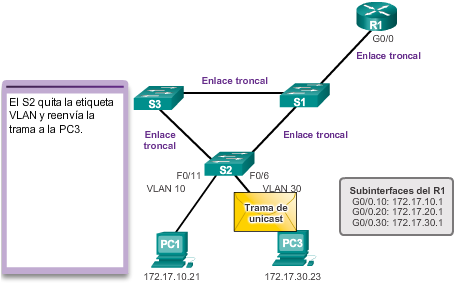












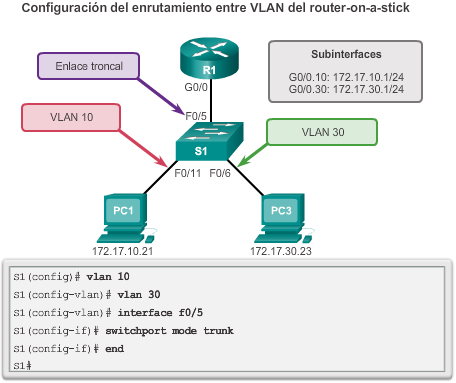
Para habilitar el routing entre VLAN utilizando el método router-on-a stick, comience por habilitar el enlace troncal en el puerto del switch que está conectado al router.

En la ilustración, el router R1 se conecta al switch S1 en el puerto de enlace troncal F0/5. Las VLAN 10 y 30 se agregaron al switch S1.

Debido a que el puerto del switch F0/5 está configurado como puerto de enlace troncal, no necesita asignarse a ninguna VLAN. Para configurar el puerto del switch F0/5 como un puerto de enlace troncal, ejecute el comando **switchport mode trunk**en el modo de configuración de la interfaz para el puerto F0/5.

**Nota**: el router no admite el protocolo de enlace troncal dinámico (DTP), que es utilizado por los switches, por lo que no pueden usarse los siguientes comandos:**switchport mode dynamic auto** o**switchport mode dynamic desirable.**

Ahora se puede configurar el router para que realice routing entre VLAN.



Cuando se utiliza una configuración de router-on-a-stick, la configuración del router es diferente en comparación con el routing entre VLAN antiguo. En la ilustración se muestra que hay varias subinterfaces configuradas.

Cada subinterfaz se crea con el comando**interface** *id\_interfaz id\_subinterfaz* en el modo de configuración global. La sintaxis para la subinterfaz es la interfaz física, en este caso **g0/0**, seguida de un punto y un número de subinterfaz. El número de subinterfaz es configurable, pero en general refleja el número de VLAN. En este ejemplo, las subinterfaces utilizan los números **10** y **30** como números de subinterfaz para que sea más fácil recordar las VLAN con las que están asociadas. La subinterfaz GigabitEthernet0/0.10 se crea con el comando **interface g0/0.10** del modo de configuración global.

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** *VLAN\_id*. En este ejemplo, la subinterfaz G0/0.10 se asignó a la VLAN 10.

**Nota:** hay una opción de palabra clave**native** que se puede agregar a este comando para establecer la VLAN nativa IEEE 802.1Q. En este ejemplo, la opción de palabra clave **native** se excluyó para dejar el valor predeterminado de VLAN nativa a la VLAN 1.

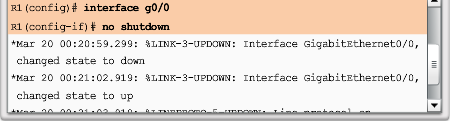
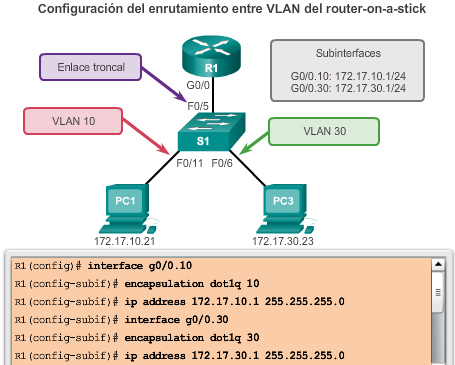
A continuación, asigne la dirección IP para la subinterfaz mediante el comando **ip address** *dirección\_ip máscara\_subred* en el modo de configuración de subinterfaz. En este ejemplo, la subinterfaz G0/0.10 se asignó a la dirección IP 172.17.10.1 mediante el comando **ip address 172.17.10.1 255.255.255.0**.

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. En este ejemplo, se configuró la otra subinterfaz del router (G0/0.30) con la dirección IP 172.17.30.1, que está en una subred diferente que la subinterfaz G0/0.10.

Una vez que se configuran las subinterfaces, es necesario habilitarlas.

A diferencia de las interfaces físicas, las subinterfaces no se habilitan con el comando **no shutdown** en el nivel del modo de configuración de subinterfaz del software IOS de Cisco. Introducir el comando **no shutdown** en el nivel de subinterfaz no tiene ningún efecto. En cambio, cuando se habilita la interfaz física con el comando **no shutdown**, todas las subinterfaces configuradas se habilitan. De manera similar, si la interfaz física está deshabilitada, todas las subinterfaces están deshabilitadas. En este ejemplo, en el modo de configuración de interfaz se introduce el comando **no shutdown** para la interfaz G0/0, lo que, a su vez, habilita todas las subinterfaces configuradas.

Las subinterfaces individuales pueden desactivarse administrativamente con el comando **shutdown**.

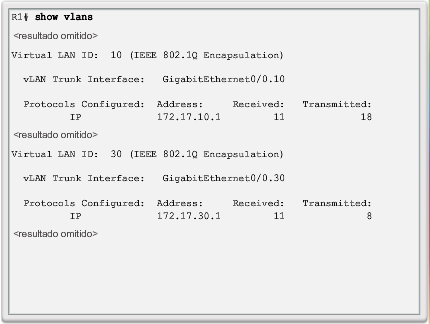


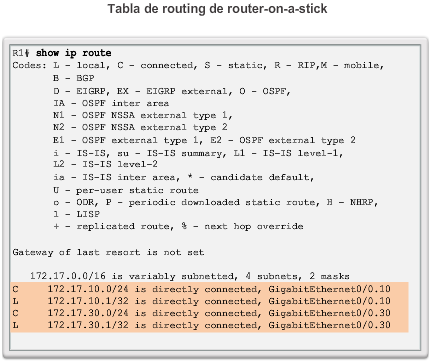
Los routers Cisco están configurados de manera predeterminada para enrutar el tráfico entre subinterfaces locales. Por lo tanto, no es necesario que esté habilitado el enrutamiento.

En la figura 1, el comando **show vlans** muestra información sobre las subinterfaces VLAN del IOS de Cisco. El resultado muestra las dos subinterfaces VLAN, GigabitEthernet0/0.10 y GigabitEthernet0/0.30.

A continuación, examine la tabla de routing con el comando **show ip route**(figura 2). En el ejemplo, las rutas definidas en la tabla de routing indican que están asociadas a subinterfaces específicas, en lugar de interfaces físicas separadas. Hay dos rutas en la tabla de routing: una ruta va a la subred 172.17.10.0, que está conectada a la subinterfaz local G0/0.10; la otra ruta va a la subred 172.17.30.0, que está conectada a la subinterfaz local G0/0.30. El router utiliza la tabla de enrutamiento para determinar dónde enviar el tráfico que recibe. Por ejemplo, si el router recibe un paquete en la subinterfaz G0/0.10 destinado a la subred 172.17.30.0, identificará que debe enviar el paquete por la subinterfaz G0/0.30 para que llegue a los hosts en la subred 172.17.30.0.

En la figura 3, utilice el verificador de sintaxis para configurar y verificar router-on-a-stick en el R1.





Después de configurar el router y el switch para llevar a cabo routing entre VLAN, el siguiente paso es verificar la conectividad de host a host. El acceso a los dispositivos en las VLAN remotas puede probarse con el comando **ping**.

En el ejemplo que se muestra en la ilustración, se inician los comandos **ping** y**tracert** desde la PC1 hasta la dirección de destino de la PC3.

**Prueba de ping**

El comando **ping** envía una solicitud de eco ICMP a la dirección de destino. Cuando un host recibe una solicitud de eco del ICMP, éste responde con una respuesta de eco del ICMP para confirmar que recibió dicha solicitud. El comando **ping** calcula el tiempo transcurrido, para lo cual utiliza la diferencia de tiempo entre el momento en que se envió la solicitud de eco y el momento en que se recibió la respuesta de eco. El tiempo transcurrido se utiliza para determinar la latencia de la conexión. Al recibir una respuesta con éxito, confirma que existe una ruta entre el dispositivo emisor y el dispositivo receptor.

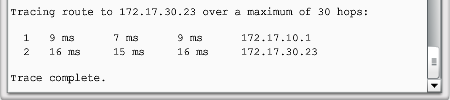
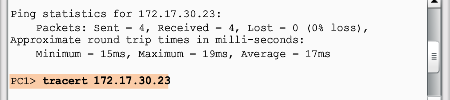
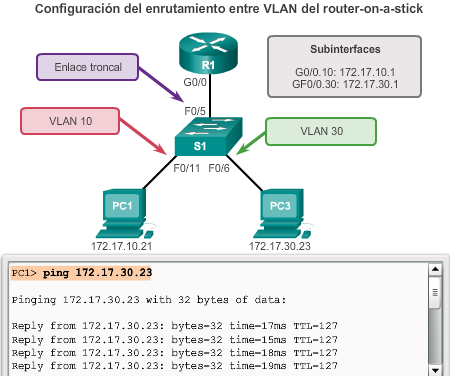
**Prueba de tracert**

Tracert es una utilidad práctica usada para confirmar la ruta enrutada tomada entre dos dispositivos. En los sistemas UNIX, la utilidad se especifica como **traceroute**. Tracert también utiliza el ICMP para determinar la ruta tomada, pero utiliza las solicitudes de eco del ICMP con valores de tiempo de vida específicos definidos en la trama.

El valor de tiempo de vida determina con exactitud la cantidad de saltos del router que el eco del ICMP puede alcanzar. La primera solicitud de eco del ICMP se envía con un valor de tiempo de vida configurado para expirar en el primer router en la ruta hacia el dispositivo de destino.

Cuando se excede el tiempo de espera de la solicitud de eco ICMP en la primera ruta, se reenvía un mensaje ICMP desde el router hasta el dispositivo de origen. El dispositivo registra la respuesta desde el router y procede a enviar otra solicitud de eco del ICMP, pero esta vez con un valor de tiempo de vida mayor. Esto permite a la solicitud de eco del ICMP atravesar el primer router y llegar al segundo dispositivo en la ruta hacia el destino final. El proceso se repite de manera recursiva hasta que, finalmente, se envía la solicitud de eco ICMP hacia el dispositivo de destino final. Una vez que la utilidad **tracert** termina de ejecutarse, se muestra una lista de las interfaces de entrada del router alcanzadas por la solicitud de eco ICMP en camino al destino.

En el ejemplo, la utilidad **ping** pudo enviar una solicitud de eco ICMP a la dirección IP de la PC3. Además, la utilidad **tracert**confirma que el camino a la PC3 es a través de la dirección IP de la subinterfaz 172.17.10.1 del router R1.



## Resolución de problemas de routing entre VLAN

### Problemas de configuración entre VLAN

Hay varias configuraciones de switch incorrectas comunes que puede producirse al configurar el routing entre varias VLAN.

Al utilizar el modelo de routing antiguo para routing entre VLAN, asegúrese de que los puertos del switch que se conectan a las interfaces del router estén configurados en las VLAN correctas. Si un puerto de switch no está configurado para la VLAN adecuada, los dispositivos configurados en esa VLAN no se pueden conectar a la interfaz del router, por lo que dichos dispositivos no pueden enviar datos a las demás VLAN.

Como se puede ver en la topología de la figura 1, la PC1 y la interfaz G0/0 del router R1 están configuradas en la misma subred lógica, como lo indica su asignación de dirección IP. Sin embargo, el puerto de switch F0/4 que se conecta a la interfaz G0/0 del router R1 no está configurado y permanece en la VLAN predeterminada. Dado que el router R1 está en una VLAN diferente que PC1, no pueden comunicarse.

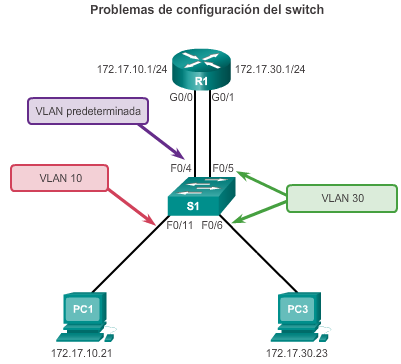
Para corregir este problema, ejecute el comando **switchport access vlan 10** en el modo de configuración de interfaz para el puerto de switch F0/4 en el switch S1. Cuando el puerto del switch se configura para la VLAN correcta, la PC1 puede comunicarse con la interfaz G0/0 del router R1, que le permite acceder a las otras VLAN conectadas al router R1.

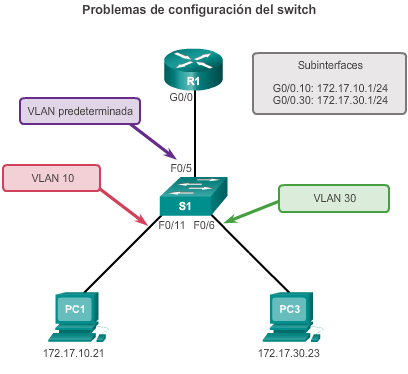
La topología de la figura 2 muestra el modelo de routing router-on-a-stick. Sin embargo, la interfaz F0/5 en el switch S1 no está configurada como enlace troncal y queda en la VLAN predeterminada para el puerto. Como resultado, el router no puede realizar enrutamiento entre las VLAN, porque cada una de las subinterfaces configuradas no puede enviar ni recibir el tráfico con etiquetas de VLAN.

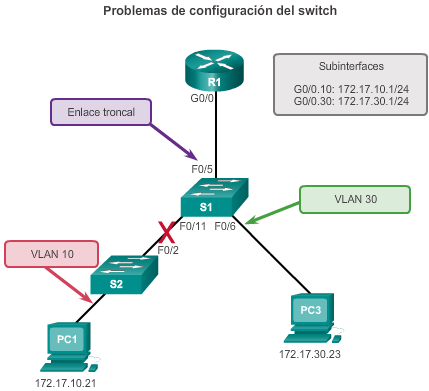
Para corregir este problema, emita el comando **switchport mode trunk** en el modo de configuración de interfaz para el puerto del switch F0/5 en el switch S1. Esto convierte a la interfaz en un puerto de enlace troncal, lo que permite que se establezca un enlace troncal entre el R1 y el S1. Una vez que el enlace troncal se establece correctamente, los dispositivos conectados a cada una de las VLAN pueden comunicarse con la subinterfaz asignada a su VLAN, lo que permite el routing entre VLAN.

En la topología de la figura 3 se muestra que el enlace troncal entre el S1 y S2 está inactivo. Dado que no hay una conexión o ruta redundante entre los dispositivos, ninguno de los dispositivos conectados al S2 puede llegar al router R1. Como resultado, ninguno de los dispositivos conectados al S2 puede realizar enrutamiento a otras VLAN a través del R1.

Para reducir el riesgo de una falla en el enlace entre switches que interrumpa el routing entre VLAN, se deben tener en cuenta enlaces redundantes y rutas alternativas en el diseño de red.





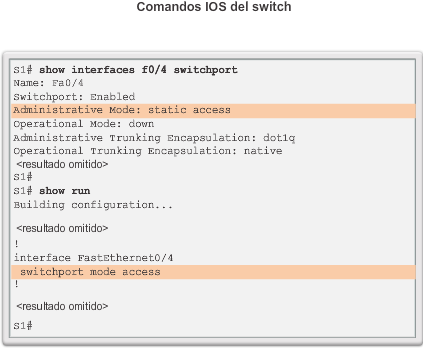


Cuando sospeche que hay un problema con una configuración del switch, utilice los distintos comandos de verificación para examinar la configuración e identificar el problema.

En el resultado de pantalla de la figura 1, se muestran los resultados de los comandos**show interfaces** *id-interfaz***switchport**. Supongamos que ejecutó estos comandos porque sospecha que la VLAN 10 no se asignó al puerto F0/4 en el switch S1. En el área superior resaltada se muestra que el puerto F0/4 en el switch S1 está en modo de acceso, pero no se muestra que se haya asignado directamente a la VLAN 10. En el área inferior resaltada se confirma que el puerto F0/4 todavía está establecido en la VLAN predeterminada. Los comandos **show running-config** y **show interface***id-interfaz* **switchport** son útiles para identificar problemas de asignación de VLAN y de configuración de puertos.

En la figura 2 se muestra que la comunicación entre el router R1 y el switch S1 se interrumpió después de modificar la configuración de un dispositivo. Se supone que el enlace entre el router y el switch es un enlace troncal. En el resultado de pantalla, se muestran los resultados de los comandos **show interface***id\_interfaz* **switchport** y **show running-config**. El área superior resaltada confirma que el puerto F0/4 en el switch S1 está en el modo de acceso, no en el modo de enlace troncal. El área inferior resaltada también confirma que el puerto F0/4 se configuró para el modo de acceso.

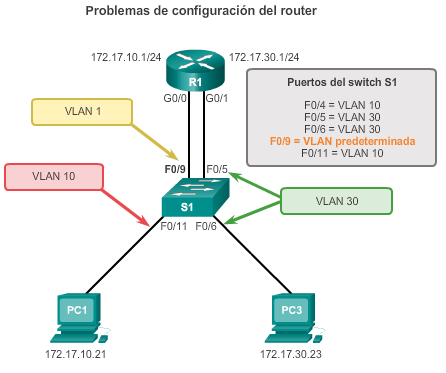




Al habilitar el routing entre VLAN en un router, uno de los errores de configuración más comunes es conectar la interfaz física del router al puerto de switch incorrecto. Esto ubica la interfaz del router en la VLAN incorrecta y evita que alcance otros dispositivos dentro de la misma subred.

Como se muestra en la ilustración, la interfaz G0/0 del router R1 está conectada al puerto F0/9 del switch S1. El puerto de switch F0/9 está configurado para la VLAN predeterminada, no para la VLAN 10. Esto evita que la PC1 pueda comunicarse con la interfaz del router. Por lo tanto, no puede realizar enrutamiento hacia la VLAN 30.

Para corregir este problema, conecte físicamente la interfaz G0/0 del router R1 al puerto F0/4 del switch S1. Esto ubica la interfaz del router en la VLAN correcta y permite el routing entre VLAN. Alternativamente, cambie la asignación de VLAN del puerto de switch F0/9 a la VLAN 10. Esto también permite que la PC1 se comunique con la interfaz G0/0 del router R1.



Con configuraciones de router-on-a-stick, un problema común es asignar una ID de VLAN incorrecta a la subinterfaz.

Como se muestra en la figura 1, el router R1 se configuró con la VLAN incorrecta en la subinterfaz G0/0.10, lo que evita que los dispositivos configurados en la VLAN 10 se comuniquen con la subinterfaz G0/0.10. Esto, a la vez, evita que dichos dispositivos puedan enviar datos a otras VLAN en la red.

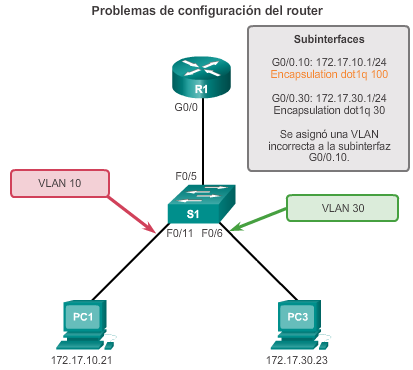
El uso de los comandos **show interfaces** y **show running-config**puede ser útil para la resolución de problemas de este tipo, tal como se muestra en la ilustración.

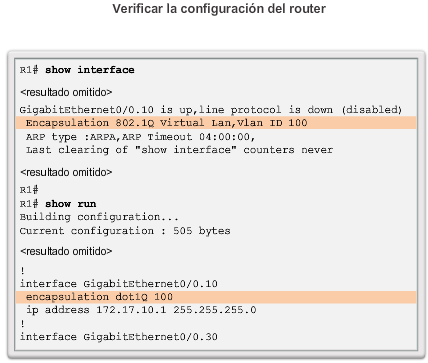
El comando **show interfaces** genera muchos resultados, lo que a veces dificulta encontrar el problema, tal como se muestra en la figura 2. Sin embargo, en la sección superior resaltada muestra que la subinterfaz G0/0.10 en el router R1 utiliza la VLAN 100.

El comando **show running-config**confirma que la subinterfaz G0/0.10 en el router R1 se configuró para permitir el acceso al tráfico de la VLAN 100 y no al de la VLAN 10.

Para corregir este problema, configure la subinterfaz G0/0.10 para que esté en la VLAN correcta mediante el comando**encapsulation dot1q 10** en el modo de configuración de subinterfaz. Una vez asignada la subinterfaz a la VLAN correcta, los dispositivos en esa VLAN pueden acceder a ella, y el router puede realizar routing entre VLAN.

Con la correcta verificación, los problemas de configuración del router se resuelven rápidamente, lo que permite que el routing entre VLAN funcione de forma adecuada.



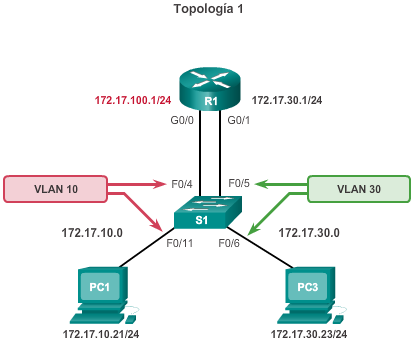


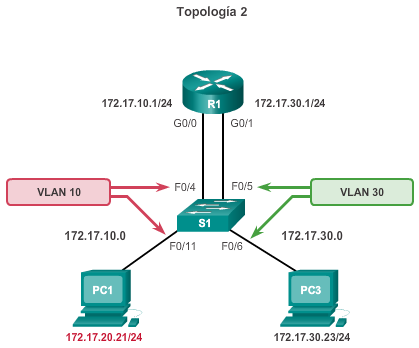
### Problemas de direccionamiento IP

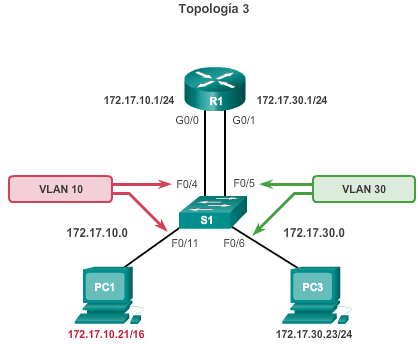
Las VLAN corresponden a subredes únicas en la red. Para que el routing entre VLAN funcione, es necesario conectar un router a todas las VLAN, ya sea por medio de interfaces físicas separadas o subinterfaces. A cada interfaz o subinterfaz se le debe asignar una dirección IP que corresponda a la subred a la cual está conectada. Esto permite que los dispositivos en la VLAN se comuniquen con la interfaz del router y habilita el routing del tráfico a otras VLAN conectadas al router.

Los siguientes son algunos errores comunes de direccionamiento IP:

* Como se muestra en la figura 1, el router R1 se configuró con la dirección IP incorrecta en la interfaz G0/0. Esto evita que la PC1 pueda comunicarse con el router R1 en la VLAN 10. Para corregir este problema, asigne la dirección IP correcta a la interfaz G0/0 del router R1 mediante el comando **ip address 172.17.10.1 255.255.255.0**. Una vez asignada la interfaz del router a la dirección IP correcta, la PC1 puede utilizar la interfaz del router como gateway predeterminado para acceder a otras VLAN.
* En la figura 2, la PC1 se configuró con la dirección IP incorrecta para la subred asociada con la VLAN 10. Esto evita que la PC1 pueda comunicarse con el router R1 en la VLAN 10. Para corregir este problema, asigne la dirección IP correcta a PC1. Según el tipo de computadora que utilice, los detalles de configuración pueden ser diferentes.
* En la figura 3, la PC1 se configuró con la máscara de subred incorrecta. Según la máscara de subred configurada para PC1, PC1 está en la red 172.17.0.0. El resultado es que la PC1 calcula que la PC3, con la dirección IP 172.17.30.23, se encuentra en la misma subred que la PC1. La PC1 no reenvía el tráfico destinado a la PC3 a la interfaz G0/0 del router R1, por lo tanto, el tráfico nunca llega a la PC3. Para corregir este problema, cambie la máscara de subred en PC1 a 255.255.255.0. Según el tipo de computadora que utilice, los detalles de configuración pueden ser diferentes.



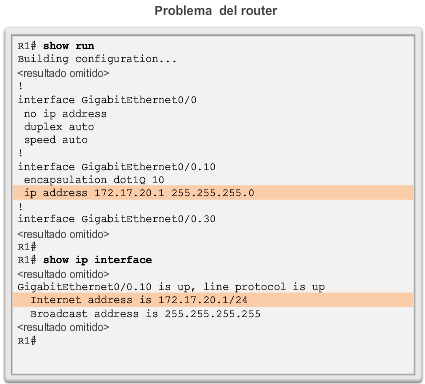


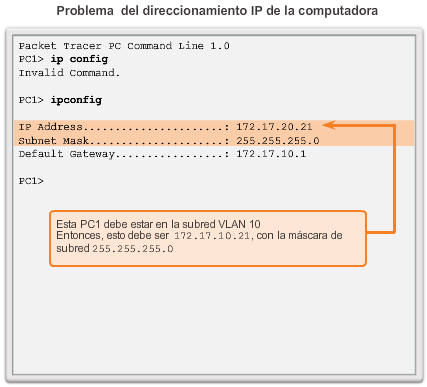


A cada interfaz o subinterfaz se le debe asignar una dirección IP que corresponda a la subred a la cual está conectada. Un error común es configurar incorrectamente una dirección IP para una subinterfaz. En la figura 1, se muestra el resultado del comando **show running-config**. El área resaltada muestra que la subinterfaz G0/0.10 en el router R1 tiene la dirección IP 172.17.20.1. La VLAN para esta subinterfaz debería admitir tráfico de la VLAN 10. La dirección IP se configuró de manera incorrecta. El comando **show ip interface** resulta útil en esta configuración. La segunda área resaltada muestra la dirección IP incorrecta.

Algunas veces, el problema es que el dispositivo de usuario final, como una computadora personal, está mal configurado. En la figura 2, se muestra la configuración IP para la PC1 que aparece en pantalla. La dirección IP es 172.17.20.21, con la máscara de subred 255.255.255.0. Sin embargo, en esta situación la PC1 debería estar en la VLAN 10, con la dirección 172.17.10.21 y la máscara de subred 255.255.255.0.

**Nota**: si bien la configuración de las ID de subinterfaz de manera que coincidan con el número de VLAN facilita la administración de la configuración entre VLAN, no es un requisito. Al trabajar en la resolución de problemas de direccionamiento, asegúrese de que la subinterfaz esté configurada con la dirección correcta para esa VLAN.





## Conmutación de capa 3

### Funcionamiento y configuración del switching de capa 3

El método router-on-a-stick es fácil de implementar porque los routers suelen estar disponibles en cada red. Como se muestra en la ilustración, la mayoría de las redes empresariales utilizan switches multicapa para obtener altas velocidades de procesamiento de paquetes con switching basado en hardware. Los switches de capa 3 suelen tener un rendimiento de switching de paquetes en el orden de los millones de paquetes por segundo (pps), mientras que los routers tradicionales proporcionan switching de paquetes en el orden de 100 000 a más de 1 millón de pps.

Todos los switches multicapa Catalyst admiten los siguientes tipos de interfaces de capa 3:

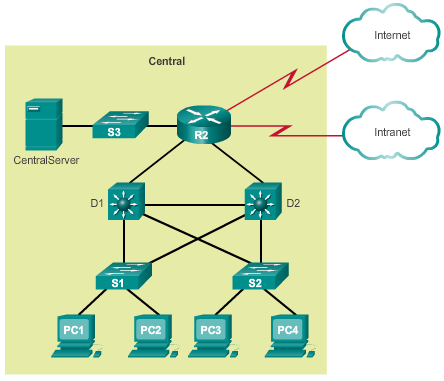
**Puerto enrutado:** una interfaz puramente de capa 3 similar a la interfaz física de un router IOS de Cisco.

**Interfaz virtual del switch (SVI):** una interfaz VLAN virtual para routing entre VLAN. En otras palabras, las SVI son las interfaces VLAN enrutadas de manera virtual.

Los switches de alto rendimiento, como el Catalyst 6500 y el Catalyst 4500, realizan casi todas las funciones que incluyen a las capas 3 y superiores del modelo OSI con switching basado en hardware y en Cisco Express Forwarding.

Todos los switches Cisco Catalyst de capa 3 admiten protocolos de routing, pero varios modelos de switches Catalyst requieren un software mejorado para admitir características específicas de protocolos de routing. Los switches de la serie Catalyst 2960 que ejecutan IOS versión 12.2(55) o posterior admiten routing estático.

Los switches Catalyst utilizan diversas configuraciones predeterminadas para las interfaces. Todos los miembros de las familias de switches Catalyst 3560 y 4500 utilizan interfaces de capa 2 de manera predeterminada, mientras que los miembros de la familia de switches Catalyst 6500 que ejecutan el IOS de Cisco utilizan interfaces de capa 3 de forma predeterminada. Las configuraciones de interfaz predeterminadas no aparecen en la configuración de inicio o en ejecución. Según la familia de switches Catalyst que se utilice, es posible que los comandos **switchport** o **no switchport** del modo de configuración de interfaz estén presentes en los archivos de configuración en ejecución o de configuración de inicio.



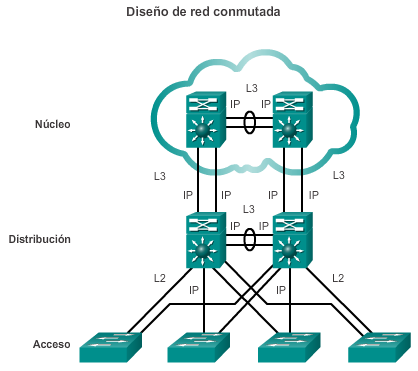
En los comienzos de las redes conmutadas, el switching era rápido (a menudo, tenía la velocidad del hardware, es decir que la velocidad era equivalente al tiempo físico que tomaba recibir las tramas y reenviarlas a otros puertos) y el routing era lento (debía procesarse mediante software). Esto hizo que los diseñadores de redes ampliaran la porción conmutada de la red al máximo posible. El acceso, la distribución y las capas de núcleo solían configurarse para comunicarse en la capa 2, pero esta topología generaba problemas de bucles. Para resolver estos problemas, se utilizaron tecnologías de árbol de expansión a fin de prevenir los bucles sin necesidad de renunciar a la flexibilidad y la redundancia de las conexiones entre switches.

Sin embargo, a medida que las tecnologías de redes evolucionaron, el routing se volvió más rápido y económico. Hoy en día, el routing se puede llevar a cabo a la velocidad del hardware. Una consecuencia de esta evolución es que el routing se puede transferir a las capas de núcleo y de distribución sin afectar el rendimiento de la red.

Muchos usuarios están en VLAN separadas, y cada VLAN suele ser una subred distinta. Por lo tanto, resulta lógico configurar los switches de distribución como gateways de capa 3 para los usuarios de la VLAN de cada switch de acceso. Esto significa que cada switch de distribución debe tener direcciones IP que coincidan con la VLAN de cada switch de acceso.

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

La arquitectura de red representada no depende del árbol de expansión, porque no existen bucles físicos en la porción de capa 2 de la topología.



Una SVI es una interfaz virtual configurada en un switch multicapa, como se muestra en la ilustración. Se puede crear una SVI para cualquier VLAN que exista en el switch. Una SVI se considera virtual porque no hay un puerto físico dedicado a la interfaz. Puede realizar las mismas funciones para la VLAN que una interfaz del router y puede configurarse de manera similar a una interfaz tal (es decir, dirección IP, ACL de entrada y de salida, etcétera). La SVI para la VLAN proporciona procesamiento de capa 3 para los paquetes que provienen de todos los puertos de switch asociados a dicha VLAN o que se dirigen a ella.

De manera predeterminada, se crea una SVI para la VLAN predeterminada (VLAN 10) a fin de permitir la administración remota del switch. Las SVI adicionales deben crearse de forma explícita. Las SVI se crean la primera vez que se ingresa al modo de configuración de interfaz de VLAN para una SVI de VLAN en particular, por ejemplo, cuando se introduce el comando**interface vlan 10**. El número de VLAN utilizado se corresponde con la etiqueta VLAN asociada con las tramas de datos en un enlace troncal encapsulado 802.1Q o bien con la ID de VLAN (VID) configurada para un puerto de acceso. Al crear una SVI como gateway para la VLAN 10, nombre “VLAN 10” a la interfaz SVI. Configure y asigne una dirección IP a cada SVI de VLAN.

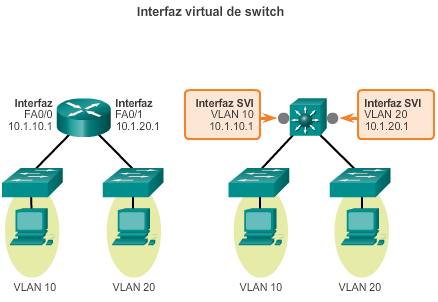
Al crear una SVI, asegúrese de que esa VLAN en particular esté presente en la base de datos de VLAN. En la ilustración, el switch debe tener presentes las VLAN 10 y VLAN 20 en la base de datos de VLAN, de lo contrario, la interfaz SVI permanece desactivada.

A continuación se detallan algunos de los motivos para configurar una SVI:

* Para proporcionar un gateway a una VLAN a fin de poder enrutar el tráfico dentro o fuera de esa VLAN.
* Para proporcionar conectividad IP de capa 3 al switch.
* Para admitir las configuraciones de puente y de protocolo de routing.

A continuación, se detallan algunas de las ventajas de las SVI (la única desventaja es que los switches multicapa son más costosos):

* Es mucho más veloz que router-on-a-stick, porque todo el switching y el routing se realizan por hardware.
* El routing no requiere enlaces externos del switch al router.
* No se limita a un solo enlace. Se pueden utilizar EtherChannels de capa 2 entre los switches para obtener más ancho de banda.
* La latencia es mucho menor, porque no hace falta que salga del switch.



**Puertos enrutados y puertos de acceso en switches**

Un puerto enrutado es un puerto físico que funciona de manera similar a una interfaz en un router. A diferencia de los puertos de acceso, los puertos enrutados no se asocian a una VLAN determinada. Los puertos enrutados se comportan como una interfaz del router normal. Además, debido a la eliminación de la funcionalidad de capa 2, los protocolos de capa 2 (tales como STP), no funcionan en interfaces enrutadas. Sin embargo, algunos protocolos, como LACP y EtherChannel, funcionan en la capa 3.

A diferencia de los routers IOS de Cisco, los puertos enrutados en un switch IOS de Cisco no admiten subinterfaces.

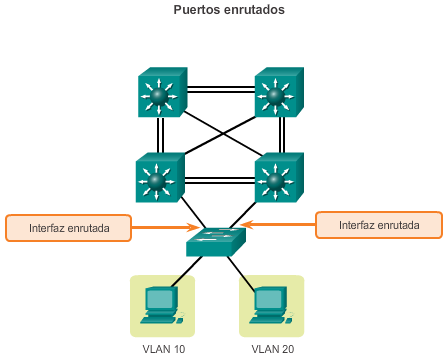
Los puertos enrutados se utilizan para enlaces punto a punto. Las conexiones de routers WAN y dispositivos de seguridad son ejemplos del uso de puertos enrutados. En una red conmutada, los puertos enrutados se suelen configurar entre los switches de las capas de núcleo y de distribución. En la ilustración,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

Para configurar los puertos enrutados, utilice el comando **no switchport** del modo de configuración de interfaz en los puertos adecuados. Por ejemplo, la configuración predeterminada de las interfaces en los switches Catalyst 3560 es de interfaces de capa 2, por lo que se deben configurar de forma manual como puertos enrutados. Además, asigne una dirección IP y otros parámetros de capa 3, según sea necesario. Después de asignar la dirección IP, verifique que el routing IP esté habilitado de manera global y que los protocolos de routing aplicables estén configurados.

A continuación, se detallan algunas de las ventajas de los puertos enrutados:

* Los switches multicapa puede tener tanto una SVI como puertos enrutados en un mismo switch.
* Los switches multicapa reenvían el tráfico de capa 2 o capa 3 mediante hardware, lo que contribuye a un routing más veloz.

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



Un switch Catalyst 2960 puede funcionar como un dispositivo de capa 3 y realizar enrutamiento entre VLAN y una cantidad limitada de rutas estáticas.

Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch en la red. Por ejemplo, la plantilla lanbase-routing de SDM se puede habilitar para permitir que el switch realice enrutamiento entre VLAN y admita el routing estático.

En la figura 1, se introduce el comando**show sdm prefer** en el switch S1 y se aplica la plantilla predeterminada. La plantilla predeterminada es la configuración predeterminada de fábrica de los switches Catalyst 2960. La plantilla predeterminada no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será dual-ipv4-and-ipv6 default.

La plantilla SDM se puede cambiar en el modo de configuración global con el comando **sdm prefer**.

**Nota**: en las figuras 2, 4, 6 y 7, el comando **do** se utiliza para ejecutar comandos de los modos EXEC del usuario o EXEC privilegiado desde otros modos de configuración del router.

En la figura 2, las opciones de plantillas SDM se muestran con el comando **sdm prefer?** La plantilla SDM cambia a lanbase-routing. El switch se debe volver a cargar para que la nueva plantilla tenga efecto.

En la figura 3, la plantilla lanbase-routing está activa en el S1. Con esa plantilla, se admite el routing estático para un máximo de 750 rutas estáticas.

En la figura 4, la interfaz F0/6 en el S1 está asignada a la VLAN 2. Las SVI para las VLAN 1 y 2 también se configuraron con las direcciones IP 192.168.1.1/24 y 192.168.2.1/24, respectivamente. El routing IP se habilita con el comando **ip routing** del modo de configuración global.

**Nota**: el comando **ip routing** se habilita de manera automática en los routers Cisco. Sin embargo, el comando correspondiente para IPv6, **ipv6 unicast-routing**, está deshabilitado de manera predeterminada en los routers y los switches Cisco.

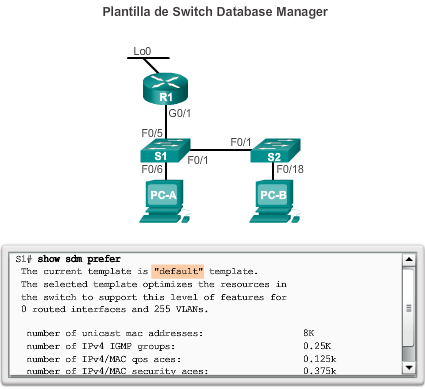
En la figura 5, el router R1 tiene dos redes IPv4 configuradas: la interfaz G0/1 tiene la dirección IP 192.168.1.10/24, y la interfaz loopback Lo0 tiene la dirección IP 209.165.200.225/27. Se muestra el resultado del comando **show ip route**.

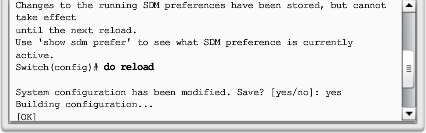
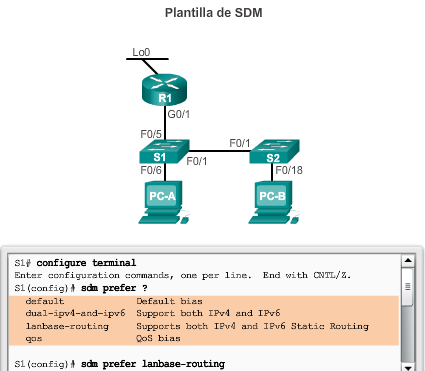
En la figura 6, se muestra una ruta predeterminada configurada en el S1. Se muestra el resultado del comando **show ip route**.

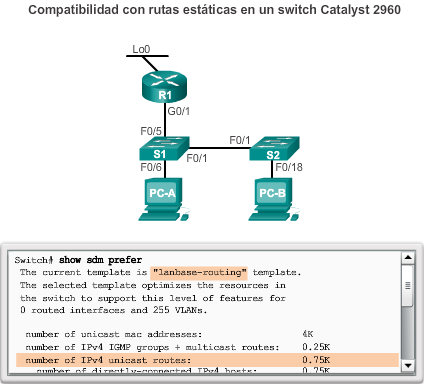
En la figura 7, se muestra una ruta estática a la red remota 192.168.2.0/24 (VLAN 2) configurada en el R1. Se muestra el resultado del comando **show ip route**.

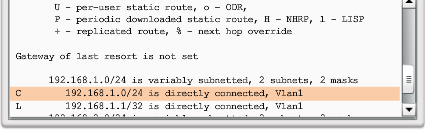
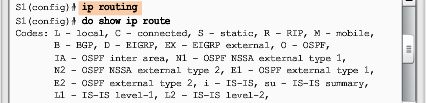
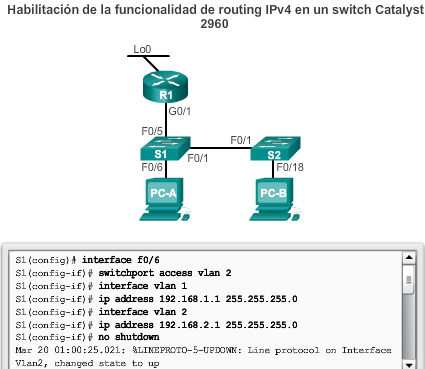
En la Figura 8, la PC-A está configurada con la dirección IP 192.168.2.2/24 en la VLAN 2, y la PC-B está configurada con la dirección IP 192.168.1.2/24 en la VLAN 1. La PC-B puede hacer ping a la PC-B y la interfaz loopback en el R1.

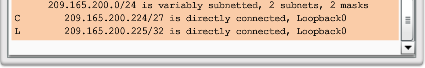
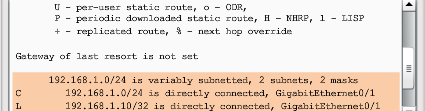
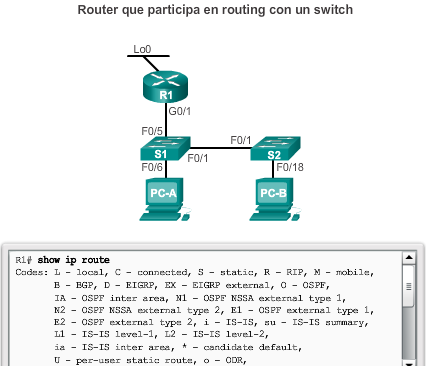
En la figura 9, utilice el verificador de sintaxis para configurar el routing estático en el S1.

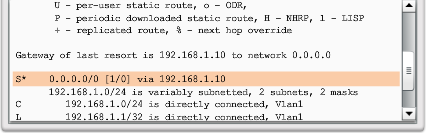
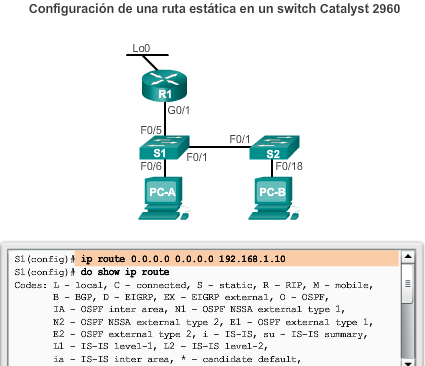


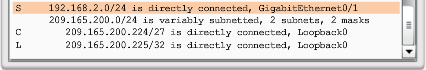
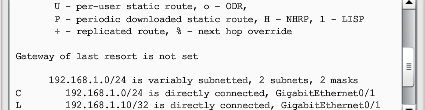
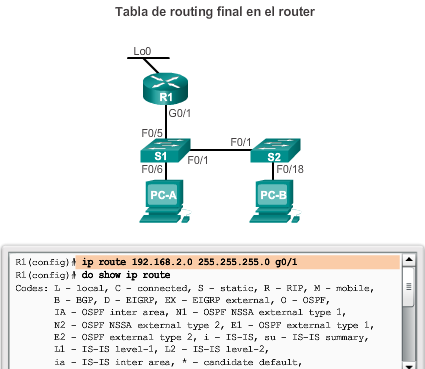


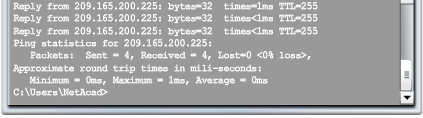
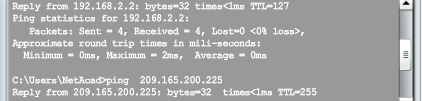
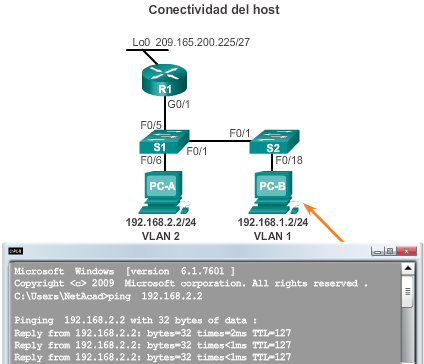












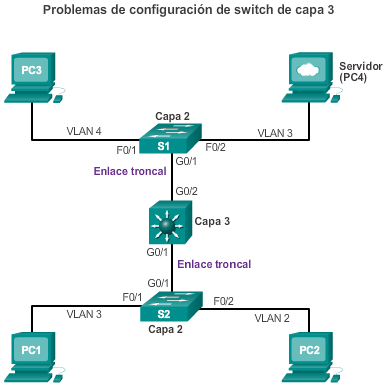
## Conmutación de capa 3

### Resolución de problemas de switching de capa 3

Los problemas comunes al routing entre VLAN antiguo y con router-on-a-stick también se manifiestan en el contexto de switching de capa 3. Para resolver problemas de switching de capa 3, se debe revisar la corrección de los siguientes elementos:

* **VLAN:** las VLAN deben estar definidas en todos los switches. Las VLAN deben estar habilitadas en los puertos de enlace troncal. Los puertos deben estar en las VLAN correctas.
* **SVI:** la SVI debe tener la dirección IP o la máscara de subred correcta. La SVI debe estar activada. La SVI debe coincidir con el número de VLAN.
* **Routing:** el routing debe estar habilitado. Cada interfaz o red debe estar agregada al protocolo de routing.
* **Hosts:** los hosts deben tener la dirección IP o la máscara de subred correcta. Los hosts deben contar con un gateway predeterminado asociado con una SVI o un puerto enrutado.

Para resolver problemas de switching de capa 3, debe familiarizarse con la implementación y el diseño de la disposición de la topología.



## Resumen

El enrutamiento inter VLAN es el proceso de tráfico de enrutamiento entre diferentes VLAN, mediante un router dedicado o un switch multicapa. El enrutamiento inter VLAN facilita la comunicación entre los dispositivos aislados por los límites de la VLAN.

El routing entre VLAN antiguo dependía de que un puerto de router físico estuviera disponible para cada VLAN configurada. Esto fue reemplazado por la topología de router-on-a-stick, que depende de un router externo con subinterfaces de enlace troncal a un switch de capa 2. Con la opción de router-on-a-stick, se deben configurar en cada subinterfaz lógica el direccionamiento IP y la información de VLAN adecuados, y se debe configurar una encapsulación de enlace troncal que coincida con la interfaz troncal del switch.

También existe la opción de multicapa entre VLAN mediante switching de capa 3. El switching de capa 3 incluye SVI y puertos enrutados. El switching de capa 3 se suele configurar en las capas de distribución y de núcleo del modelo de diseño jerárquico. El switching de capa 3 con SVI es una forma de routing entre VLAN. Un puerto enrutado es un puerto físico que funciona de manera similar a una interfaz en un router. A diferencia de los puertos de acceso, los puertos enrutados no se asocian a una VLAN determinada.

Los switches Catalyst 2960 se pueden utilizar para routing multicapa entre VLAN. Estos switches admiten routing estático, pero no son compatibles con protocolos de routing dinámico. Para habilitar el routing IP en los switches 2960, son necesarias plantillas SDM.

La resolución de problemas de routing entre VLAN con un router o con un switch de capa 3 es similar. Los errores comunes suelen estar relacionados con las configuraciones de VLAN, enlace troncal, la interfaz de capa 3 y las direcciones IP.

