Ejemplo de Configuración de Catalyst Switched Port Analyzer (SPAN)

Contenido

Introducción

Este documento describe las características recientes del analizador de puertos conmutados (SPAN) que se han implementado. La función SPAN, que a veces se denomina duplicación de puertos o supervisión de puertos, selecciona el tráfico de red para que lo analice un analizador de red. El analizador de red puede ser un dispositivo SwitchProbe de Cisco u otra sonda de control remoto (RMON). Previamente, SPAN era una función relativamente básica de los switches de la serie Catalyst de Cisco. Sin embargo, las versiones más recientes de Catalyst OS (CatOS) han introducido mejoras importantes y una gran cantidad de nuevas posibilidades que actualmente están a disposición del usuario. No se pretende que este documento sea una guía de configuración alternativa para la función SPAN; Este documento responde las preguntas más comunes sobre SPAN, tales como:

- ¿Qué es SPAN y cómo se configura?
- ¿Cuáles son las diferentes funciones disponibles (especialmente varias sesiones SPAN simultáneas) y qué nivel de software se necesita para ejecutarlas?
- ¿Afecta SPAN al funcionamiento del switch?

Prerequisites

Switches Catalyst que Soportan SPAN, RSPAN y ERSPAN

Catalyst Switches	Soporte SPAN	Compatibilidad de RSPAN	Soporte de ERSPAN
Catalyst Express de la serie 500 / 520	Yes	No	No
Serie Catalyst 6500/6000	Yes	Yes	Sí Supervisor 2T con PFC4, Supervisor 720 con PFC3B o PFC3BXL que ejecuta Cisco IOS Software Release 12.2(18)SXE o posterior. Supervisor 720 con el PFC3A que tiene la versión de hardware 3.2 o posterior y ejecuta Cisco IOS Software Release 12.2(18)SXE o posterior
Serie Catalyst 5500/5000	Yes	No	No
Series Catalyst 4900	Yes	Yes	No
Series Catalyst 4500/4000 (incluye 4912G)	Yes	Yes	No
Serie Catalyst 3750 Metro	Yes	Yes	No
Catalyst serie 3750/3750E/3750X	Yes	Yes	No
Catalyst serie 3560/3560E/3650X	Yes	Yes	No
Series Catalyst 3550	Yes	Yes	No
Serie Catalyst 3500 XL	Yes	No	No
Series Catalyst 2970	Yes	Yes	No
Series Catalyst	Yes	Yes	No

2960			
Series Catalyst 2955	Yes	Yes	No
Serie Catalyst 2950	Yes	Yes	No
Series Catalyst 2940	Yes	No	No
Catalyst 2948G-L3	No	No	No
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A	Yes	Yes	No
Serie Catalyst 2900XL	Yes	No	No
Series Catalyst 1900	Yes	No	No

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Esta información en este documento utiliza CatOS 5.5 como referencia para los Catalyst 4500/4000, 5500/5000 y 6500/6000 Series Switches. En los Catalyst 2900XL/3500XL Series Switches, se usa Cisco IOS® Software Release 12.0(5)XU. Aunque este documento se actualiza para incorporar los cambios al SPAN, consulte las notas de la versión de la documentación de su plataforma del switch para enterarse de los últimos desarrollos de la función SPAN.

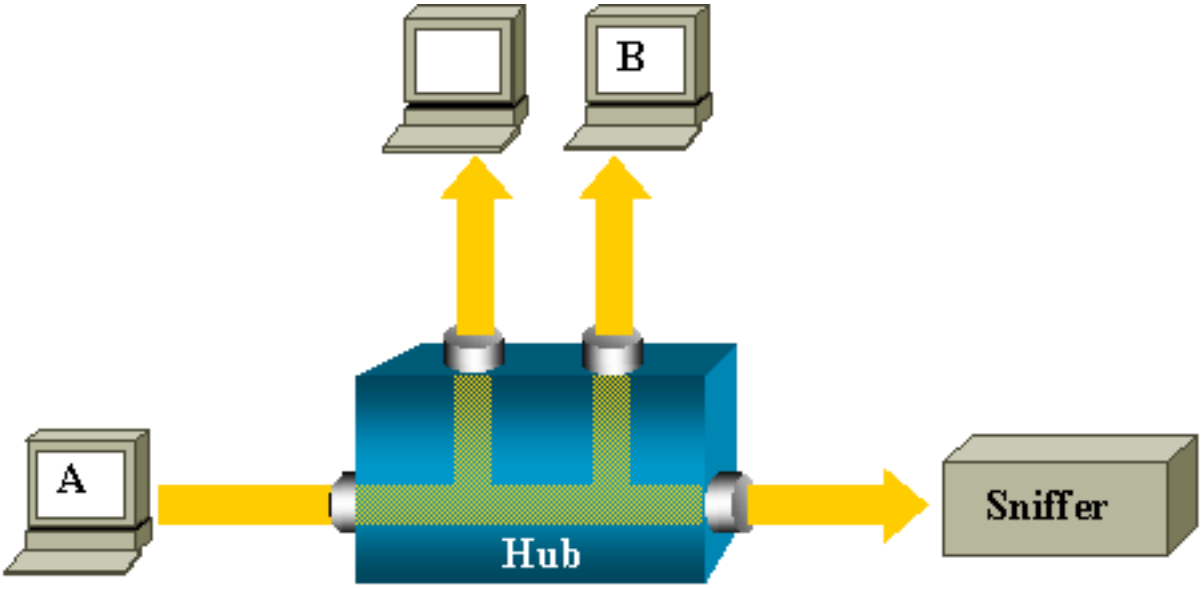
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

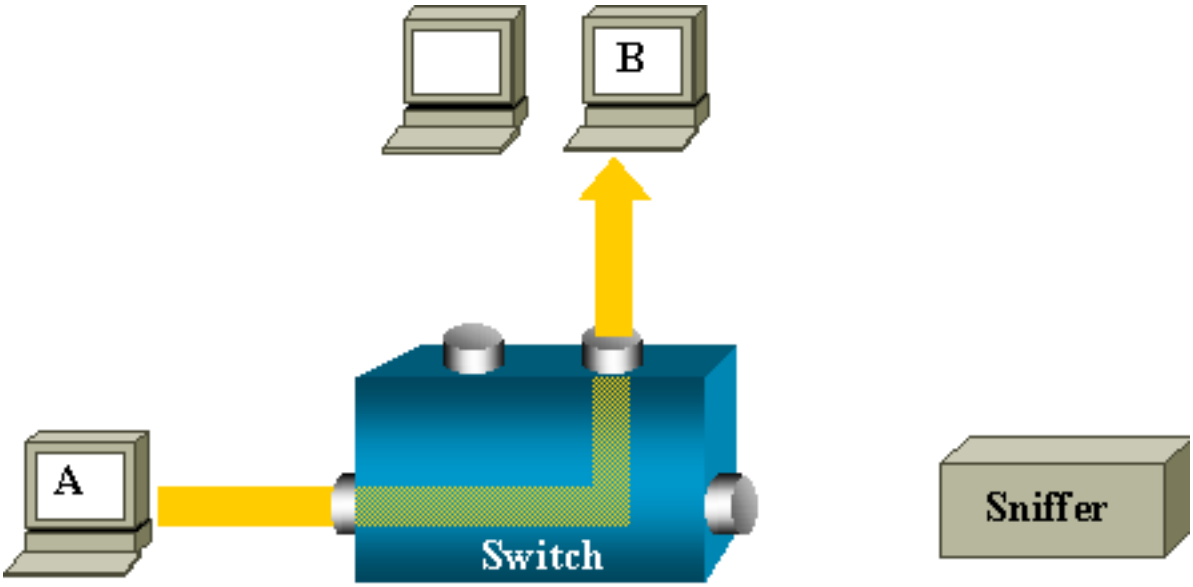
Descripción abreviada del tramo

¿Qué es SPAN y por qué es necesario? La función SPAN se incorporó a los switches dada la diferencia fundamental que tienen con los concentradores. Cuando un concentrador recibe un paquete en un puerto, el concentrador envía una copia de este paquete a todos los puertos excepto al puerto donde el concentrador recibió el paquete. Después de que el switch se reinicie, empieza a crear una tabla de reenvío de Capa 2 en base a la dirección de origen MAC de los diferentes paquetes que el switch recibe. Una vez que se ha elaborado esta tabla de reenvío, el switch reenvía el tráfico destinado a una dirección MAC directamente al puerto correspondiente.

Por ejemplo, si desea capturar el tráfico Ethernet enviado por el host A al host B y ambos están conectados a un concentrador, solo tiene que conectar un sniffer a este concentrador. Todos los demás puertos ven el tráfico entre los hosts A y B:



En un switch, después de aprender la dirección MAC B del host, el tráfico de unicast de A a B solo se envía al puerto B. Por consiguiente, el rastreador no detecta este tráfico:

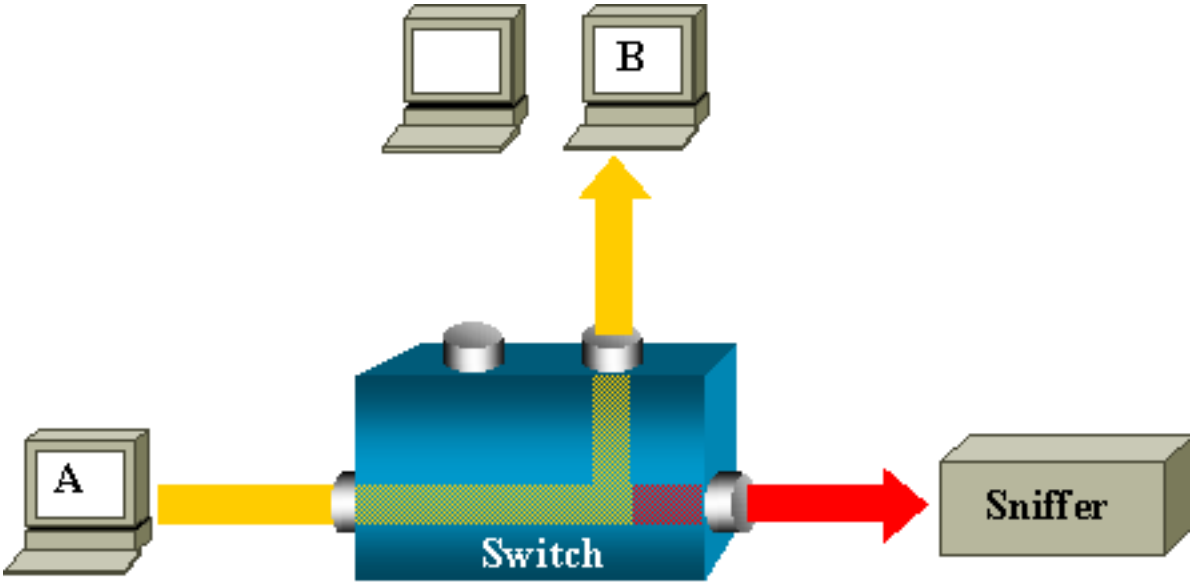


En esta configuración, el sniffer solo captura el tráfico que se inunda a todos los puertos, por ejemplo:

- Tráfico de broadcast
- Tráfico de multicast con CGMP o indagación de puerto de Internet Group Management Protocol (IGMP) inhabilitado
- Tráfico unicast desconocido

La inundación de unicast ocurre cuando el switch no tiene la MAC de destino en su tabla de memoria direccionable por contenido (CAM). El switch no sabe dónde enviar el tráfico. El switch inunda los paquetes a todos los puertos de la VLAN de destino.

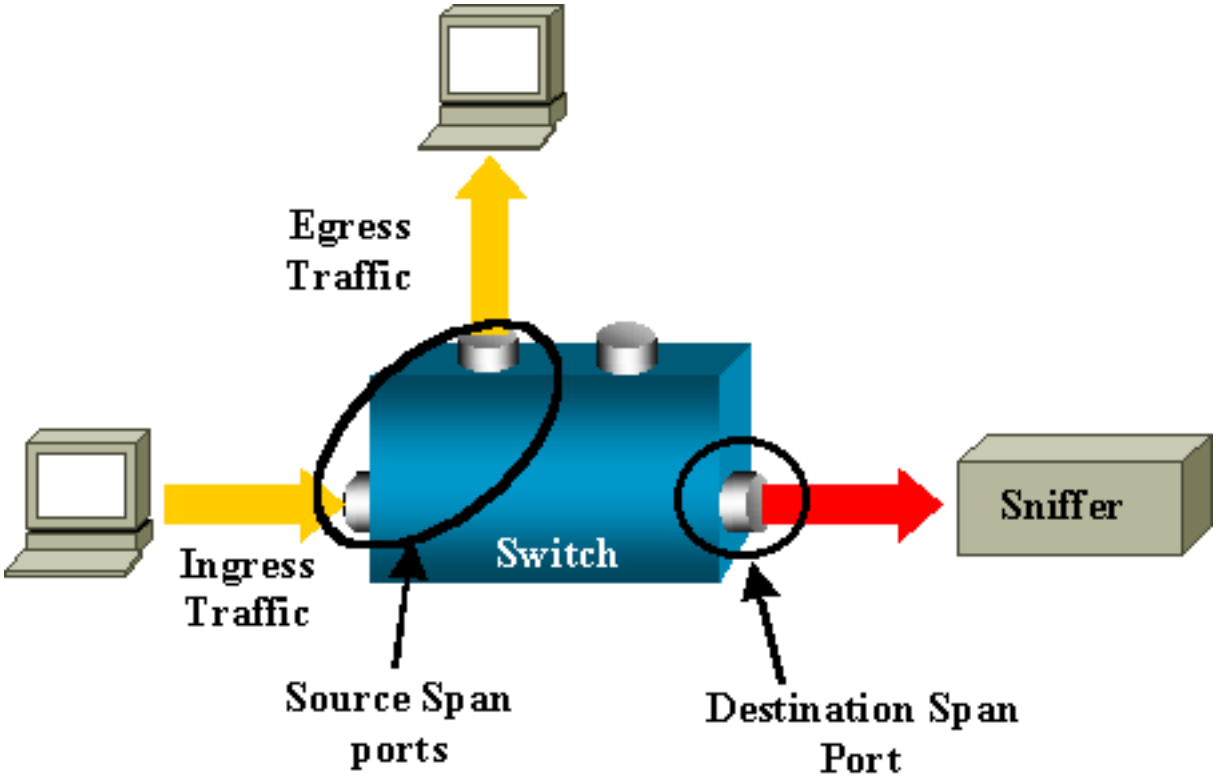
Se necesita una función adicional que copie artificialmente los paquetes de unicast que el host A envía al puerto del sniffer:



En este diagrama, el sniffer se asocia a un puerto que configurado para recibir una copia de cada paquete que envía el host A. Este puerto se denomina puerto SPAN. Las demás secciones de este documento describen cómo ajustar esta función con mucha precisión para hacer algo más que monitorear un puerto.

Terminología SPAN

- **Tráfico de entrada: tráfico que entra en el switch.**
- **Tráfico de salida: tráfico que sale del switch.**
- Puerto de origen (SPAN): un puerto que se monitorea con el uso de la función SPAN.
- VLAN de origen (SPAN): una VLAN cuyo tráfico se monitorea con el uso de la función SPAN.
- Puerto de destino (SPAN): un puerto que monitorea puertos de origen, generalmente donde está conectado un analizador de red.
- Puerto reflector: un puerto que copia paquetes a una VLAN RSPAN.
- **Puerto de monitor: un puerto de monitor también es un puerto de destino SPAN según la terminología de Catalyst 2900XL/3500XL/2950.**



- **SPAN local: la función SPAN es local cuando todos los puertos monitoreados están situados en el mismo switch que el puerto de destino.** Esta función es la opuesta a SPAN Remoto (RSPAN), que también se define en esta lista.
- **SPAN remoto (RSPAN): algunos puertos de origen no están situados en el mismo switch que el puerto de destino.** RSPAN es una función avanzada que requiere una VLAN especial para transportar el tráfico que SPAN monitorea entre los switches. No todos los switches soportan RSPAN. Verifique las respectivas release notes o la guía de configuración para ver si puede utilizarlo en el switch que implementa.
- **SPAN basado en puerto (PSPAN): el usuario especifica uno o varios puertos de origen en el switch y un puerto de destino.**
- **SPAN basado en VLAN (VSPAN): en un switch determinado, el usuario puede elegir monitorear todos los puertos que pertenecen a una VLAN determinada en un comando único.**
- **ESPAN: esto significa una versión mejorada de SPAN.** Durante la evolución de SPAN se ha utilizado varias veces este término para designar funciones adicionales. Por consiguiente, el término no es muy claro. En este documento se evita utilizar este término.
- **Origen administrativo: una lista de puertos de origen o VLAN que se han configurado para ser monitoreados.**
- **Origen operativo: una lista de puertos que se monitorean con eficacia.** Esta lista de puertos puede diferir del origen administrativo. Por ejemplo, un puerto que está en modo apagado puede aparecer en la fuente administrativa, pero no se controla de manera efectiva.

Características del Puerto de Origen

Un puerto de origen, también llamado un puerto monitoreado, es un puerto conmutado o ruteado que se monitorea para el análisis del tráfico de la red. En una única sesión SPAN local o una sesión de origen RSPAN, se puede monitorear el tráfico del puerto de origen, tal como el recibido (Rx), transmitido (Tx) o bidireccional (ambos). El switch soporta cualquier número de puertos de origen (hasta el número máximo de puertos disponibles en el switch) y cualquier número de VLAN de origen.

Un puerto de origen tiene estas características:

- Puede ser cualquier tipo de puerto, tal como EtherChannel, Fast Ethernet, Gigabit Ethernet, etc.
- Puede ser monitoreado en varias sesiones SPAN.
- No puede ser un puerto de destino.
- Cada puerto de origen se puede configurar con una dirección (entrada, salida o ambas) para monitorear. Para orígenes EtherChannel, la dirección monitoreada se aplica a todos los puertos físicos del grupo.
- Los puertos de origen pueden estar en la misma o en diferentes VLAN.
- Para los orígenes VLAN SPAN, todos los puertos activos de la VLAN de origen se incluyen como puertos de origen.

Filtrado de VLAN

Cuando se monitorea un puerto trunk como puerto de origen, todas las VLAN activas del trunk se monitorean de forma predeterminada. Puede utilizar el filtrado de VLAN para limitar el monitoreo del tráfico SPAN en los puertos de origen del trunk a VLAN específicas.

- El filtrado VLAN se aplica solo a puertos trunk o a puertos VLAN de voz.
- El filtrado VLAN se aplica solamente a sesiones basadas en puerto y no se permite en sesiones con orígenes VLAN.
- Cuando se especifica una lista de filtros VLAN, solo se monitorea las VLAN de la lista en los puertos trunk o en los puertos del acceso de VLAN de voz.
- El tráfico del SPAN procedente de otros tipos de puerto no se ve afectado por el filtrado de VLAN, lo que significa que todas las VLAN están permitidas en otros puertos.
- El filtrado VLAN afecta solo al tráfico reenviado al puerto SPAN de destino y no afecta solamente al switching del tráfico normal.
- No se puede mezclar VLAN de origen y VLAN de filtro dentro de una sesión. Puede tener VLAN de origen o VLAN de filtro, pero no ambas al mismo tiempo.

Características de la VLAN de Origen

VSPAN es el monitoreo del tráfico de red en una o más VLAN. La interfaz de origen de SPAN o RSPAN en VSPAN es un ID de VLAN, y el tráfico se monitorea en todos los puertos para esa VLAN.

VSPAN tiene estas características:

- Todos los puertos activos de la VLAN de origen se incluyen como puertos de origen y se pueden monitorear en una u otra dirección, o en ambas.
- En un puerto dado, solamente el tráfico de la VLAN monitoreada se envía al puerto de destino.
- Si un puerto de destino pertenece a una VLAN de origen, se excluye de la lista de origen y no se monitorea.
- Si se añade o se quita algún puerto de las VLAN de origen, el tráfico de la VLAN de origen recibido por esos puertos se añade o se quita de los orígenes monitoreados.
- No se puede utilizar VLAN de filtro en la misma sesión que orígenes VLAN.
- Solo se puede monitorear VLAN Ethernet.

Características del Puerto de Destino

Cada sesión SPAN local o sesión de destino RSPAN debe tener un puerto de destino (también llamado un puerto de monitoreo) que reciba una copia del tráfico de los puertos de origen y de las VLAN.

Un puerto de destino tiene estas características:

- Un puerto de destino debe residir en el mismo switch que el puerto de origen (para una sesión de SPAN local).
- Un puerto de destino puede ser cualquier puerto físico Ethernet.
- Un puerto de destino puede participar solamente en una sesión SPAN a la vez. Un puerto de destino en una sesión SPAN no puede ser un puerto destino para una segunda sesión SPAN.
- Un puerto de destino no puede ser un puerto de origen.
- Un puerto de destino no puede ser un grupo EtherChannel.**Nota:** A partir de Cisco IOS Software Release 12.2(33)SXH y posterior, la interfaz PortChannel puede ser un puerto de destino. Los EtherChannels de destino no soportan los protocolos EtherChannel Port Aggregation Control Protocol (PAgP) ni Link Aggregation Control Protocol (LACP); solo se soporta el modo activo, con todo el soporte del protocolo EtherChannel inhabilitado.**Nota:** Consulte Destinos locales SPAN RSPAN y ERSPAN para obtener más información.
- Un puerto de destino puede ser un puerto físico que se asigna a un grupo EtherChannel, incluso si se ha especificado el grupo EtherChannel como origen SPAN. El puerto se quita del grupo mientras está configurado como puerto de destino SPAN.
- El puerto no transmite ningún tráfico excepto el tráfico requeridos para la sesión SPAN a menos que se habilite el aprendizaje. Si se habilita el aprendizaje, el puerto también transmite el tráfico dirigido a los hosts que se han aprendido en el puerto de destino.**Nota:** Consulte Destinos locales SPAN RSPAN y ERSPAN para obtener más información.
- El estado del puerto destino es arriba/abajo por diseño. La interfaz muestra el puerto en este estado para hacer evidente que el puerto actualmente no se puede utilizar como puerto de producción.
- Si se habilita el tráfico de entrada para un dispositivo de la seguridad de la red. El puerto de destino reenvía el tráfico en la Capa 2.
- Un puerto de destino no participa en el spanning tree mientras la sesión SPAN está activa.
- Cuando es un puerto de destino, no participa en los ninguno de los protocolos de la Capa 2 (STP, VTP, CDP, DTP, PagP).
- Un puerto de destino que pertenece a un origen VLAN de cualquier sesión SPAN se excluye de la lista de origen y no se monitorea.
- Un puerto de destino recibe copias del tráfico enviado y recibido para todos los puertos de origen monitoreados. Si un puerto de destino tiene exceso de suscriptores, puede congestionarse. Esta congestión puede afectar al reenvío de tráfico en uno o más de los puertos de origen.

Características del Puerto Reflector

El puerto reflector es el mecanismo que copia los paquetes en una VLAN RSPAN. El puerto reflector reenvía solamente el tráfico de la sesión de origen RSPAN a la que está afiliado. Cualquier dispositivo conectado a un puerto establecido como puerto reflector pierde la conectividad hasta que se inhabilita la sesión de origen RSPAN.

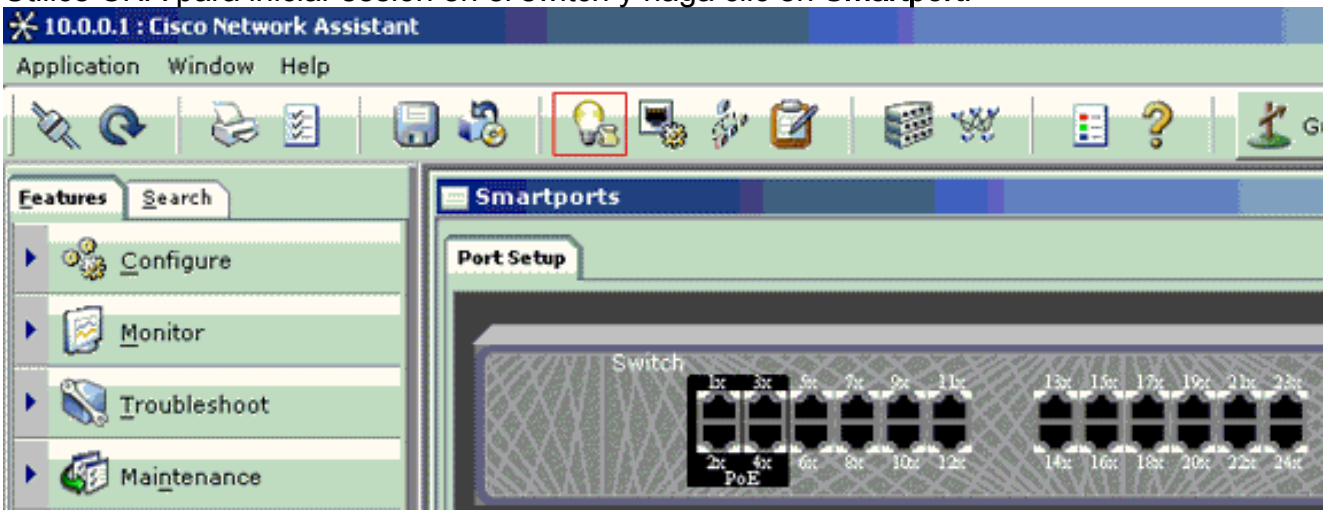
El puerto reflector tiene estas características:

- Es un puerto establecido en loopback.
- No puede ser un grupo EtherChannel, no hace trunk y no puede hacer el filtrado de protocolo.
- Puede ser un puerto físico que se asigna a un grupo EtherChannel, incluso si se especifica el grupo EtherChannel como origen SPAN. El puerto se quita del grupo mientras está configurado como puerto reflector.
- Un puerto utilizado como puerto reflector no puede ser un origen puerto de origen ni de destino de SPAN, ni puede ser un puerto reflector para más de una sesión a la vez.
- Es invisible para todas las VLAN.
- La VLAN nativa para el tráfico de loopback en un puerto reflector es la VLAN RSPAN.
- El puerto reflector hace loopback con el tráfico sin etiqueta para el switch. El tráfico se coloca entonces en la VLAN RSPAN y se inunda a cualquier puerto trunk que lleve la VLAN RSPAN.
- El spanning tree se inhabilita automáticamente en un puerto reflector.
- Un puerto reflector recibe copias del tráfico enviado y recibido para todos los puertos de origen monitoreados.

SPAN en Catalyst Express 500/520

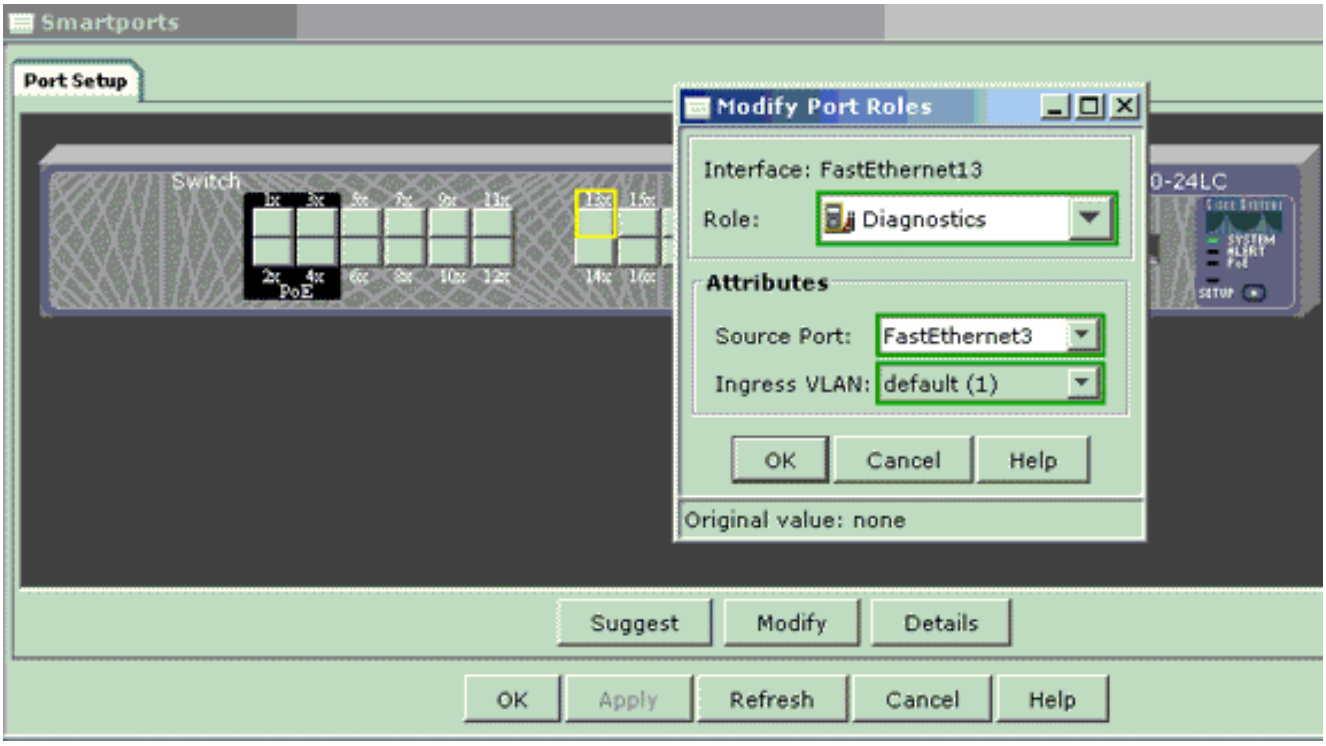
Catalyst Express 500 o Catalyst Express 520 soporta solo la función SPAN. Los puertos Catalyst Express 500/520 solo pueden configurarse para SPAN utilizando Cisco Network Assistant (CNA). Siga estos pasos para configurar SPAN:

1. Descargue e instale CNA en el PC. Puede descargar CNA desde la página Download Software (solo clientes registrados).
2. Siga los pasos dados en la Guía de Introducción para los Switches Catalyst Express 500 12.2(25)FY para personalizar las configuraciones de switch para Catalyst Express 500. Consulte la Guía de Introducción para los Switches Catalyst Express 520 para obtener más información sobre Catalyst Expres 520.
3. Utilice CNA para iniciar sesión en el switch y haga clic en **Smartport**.



4. Haga clic en cualquier interfaz en la que tenga previsto conectar el PC para capturar los seguimientos del sniffer.
5. Haga clic en **Modificar**. Aparece un pequeño cuadro emergente.
6. Elija el papel de **Diagnostics para el puerto.**
7. Elija el puerto de origen y seleccione la VLAN que planea monitorear. Si no selecciona ninguna, el puerto solo recibe tráfico. La VLAN de entrada permite que el PC conectado al

puerto de diagnóstico envíe paquetes a la red que utiliza mediante la VLAN.



8. Haga clic en OK para cerrar el cuadro emergente.
9. Haga clic en OK y, a continuación, en Apply para aplicar las configuraciones.
10. Puede utilizar cualquier software sniffer para seguir el tráfico una vez configurado el puerto de diagnóstico.

SPAN en los switches Catalyst 2900XL/3500XL

Funciones Disponibles y Restricciones

La función de supervisión del puerto no es muy amplia en el Catalyst 2900XL/3500XL. Por lo tanto, esta función es relativamente fácil de entender.

Puede crear tantas sesiones PSPAN locales como sea necesario. Por ejemplo, puede crear sesiones PSPAN en el puerto de configuración que ha seleccionado para que sea el puerto de destino SPAN. En este caso, ejecute el comando port monitor interfacepara enumerar los puertos de origen que desee monitorear. Un puerto de supervisión es un puerto de destino SPAN según la terminología de Catalyst 2900XL/3500XL.

- La restricción principal es que todos los puertos que se refieren a una sesión determinada (ya sea de origen o destino) deben pertenecer a la misma VLAN.
- Si configura la interfaz VLAN con una dirección IP, entonces el **comando port monitor solo monitorea el tráfico destinado a esa dirección IP.** También supervisa el tráfico de broadcast que recibe la interfaz VLAN. Sin embargo, no captura el tráfico que fluye en la propia VLAN real. Si no especifica ninguna interfaz en el **comando port monitor, el resto de los puertos que pertenecen a la misma VLAN que la interfaz se monitorea.**

Esta lista proporciona algunas restricciones. Consulte la guía de referencia de comandos (Catalyst 2900XL/3500XL) para obtener más información.

Nota: Los puertos ATM son los únicos puertos que no pueden funcionar como puertos de monitor. Sin embargo, puede supervisar los puertos ATM. Las restricciones de esta lista se aplican a los puertos que tienen la capacidad para monitorear puertos.

- Un puerto de monitor no puede estar en un grupo de puertos Fast EtherChannel o Gigabit EtherChannel.
- Un puerto de monitoreo no puede habilitarse como puerto de seguridad.
- Un puerto de monitoreo no puede ser un puerto de múltiples VLAN.
- Un puerto monitor debe ser miembro de la misma VLAN que el puerto monitoreado. No se permiten los cambios de afiliación de VLAN en puertos de monitoreo ni en puertos monitoreados.
- Un puerto monitor no puede ser un puerto de acceso dinámico ni un puerto trunk. Sin embargo, un puerto de acceso estático puede supervisar una VLAN en un troncal, una VLAN múltiple o un puerto de acceso dinámico. La VLAN monitoreada es la asociada al puerto de acceso estático.
- El monitoreo de puertos no funciona si tanto el puerto monitor como el monitoreado son puertos protegidos.

Tenga cuidado de que un puerto en el estado de monitor no ejecute el protocolo Spanning Tree Protocol (STP) mientras el puerto pertenezca a la VLAN de los puertos que refleja. El monitor de puerto puede ser parte de un bucle si, por ejemplo, lo conecta con un concentrador o un bridge y hace un bucle a otra parte de la red. En tal caso, es posible que termine en una condición catastrófica de bucle de bridging porque ya no está protegido por STP. Vea la sección ¿Por qué la Sesión SPAN Crea un Bucle de Bridging? de este documento para ver un ejemplo de cómo se puede producir esta condición.

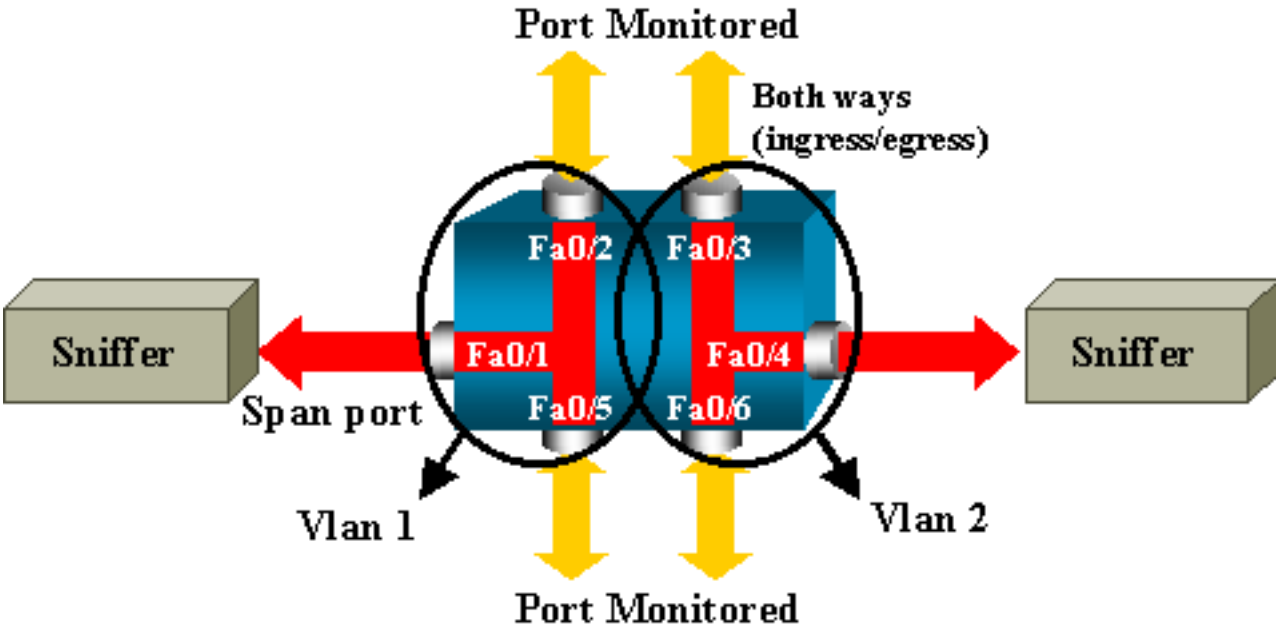
Ejemplo de configuración

Este ejemplo crea dos sesiones SPAN simultáneas.

- Port Fast Ethernet 0/1 (Fa0/1) monitorea el tráfico que los puertos Fa0/2 y Fa0/5 envían y reciben. Port Fa0/1 también monitorea el tráfico hacia la VLAN 1 de la interfaz de administración y desde ella.
- Puerto Fa0/4 monitorea puertos Fa0/3 y Fa0/6.

Los puertos Fa0/3, Fa0/4 y Fa0/6 se configuran todos en VLAN2. Otros puertos y la interfaz de administración se configuran en la VLAN 1 predeterminada.

Diagrama de la red



Configuración de muestra en el Catalyst 2900XL/3500XL

Configuración de Ejemplo SPAN 2900XL/3500XL

```
!--- Output suppressed.
!
interface FastEthernet0/1
port monitor FastEthernet0/2
port monitor FastEthernet0/5
port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
port monitor FastEthernet0/3
port monitor FastEthernet0/6
switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 2
!
!--- Output suppressed.
!
interface VLAN1
ip address 10.200.8.136 255.255.252.0
no ip directed-broadcast
no ip route-cache
!
!--- Output suppressed.
```

Explicación de los Pasos de la Configuración

Para configurar el puerto Fa0/1 como un puerto de destino, los puertos de origen Fa0/2 y Fa0/5, y la interfaz de administración (VLAN 1), seleccione la interfaz Fa0/1 en el modo de configuración:

```
Switch(config)#interface fastethernet 0/1
```

Ingrese la lista de puertos que deben monitorearse:

```
Switch(config-if)#port monitor fastethernet 0/2
Switch(config-if)#port monitor fastethernet 0/5
```

Con este comando, cada paquete que estos dos puertos reciben o transmiten se copia también al puerto Fa0/1. Ejecute una variación del **comando port monitor para configurar el monitoreo para la interfaz administrativa:**

```
Switch(config-if)#port monitor vlan 1
```

> **Nota:** Este comando no significa que el puerto Fa0/1 monitoree la VLAN 1 completa. La palabra clave **vlan1 hace referencia simplemente a la interfaz administrativa del switch.**

Este comando de ejemplo ilustra que la supervisión de un puerto en una VLAN diferente es imposible:

```
Switch(config-if)#port monitor fastethernet 0/3
FastEthernet0/1 and FastEthernet0/3 are in different vlan
```

Para finalizar la configuración, configure otra sesión. Esta vez, utilice Fa0/4 como puerto de destino SPAN:

```
Switch(config-if)#interface fastethernet 0/4
Switch(config-if)#port monitor fastethernet 0/3
Switch(config-if)#port monitor fastethernet 0/6
Switch(config-if)#^Z
```

Ejecute un **comando show running, o utilice el comando show port monitor para verificar la configuración:**

```
Switch#show port monitor
Monitor Port Port Being Monitored
--------------------- ---------------------
FastEthernet0/1 VLAN1
FastEthernet0/1 FastEthernet0/2
FastEthernet0/1 FastEthernet0/5
FastEthernet0/4 FastEthernet0/3
FastEthernet0/4 FastEthernet0/6
```

> **Nota:** Los Catalyst 2900XL y 3500XL no soportan SPAN solo en la dirección de recepción (Rx SPAN o SPAN de entrada) o solo en la dirección de transmisión (Tx SPAN o SPAN de salida). Todos los puertos SPAN se han diseñado para capturar tanto el tráfico Rx como Tx.

SPAN en 2948G-L3 y 4908G-L3 de Catalyst

Los Catalyst 2948G-L3 y Catalyst 4908G-L3 son routers con configuración de conmutación fija o switches de Capa 3. La característica SPAN del switch de Capa 3 se denomina indagación de

puerto. Sin embargo, la indagación de puerto no se soporta en estos switches. Consulte la sección Características no Soportadas del documento Release Notes para Catalyst 2948G-L3 y Catalyst 4908G-L3 para Cisco IOS Release 12.0(10)W5(18g).

SPAN en Catalyst 8500

Hay una función muy básica de SPAN disponible en el Catalyst 8540 denominada indagación de puerto. Consulte la documentación actual de Catalyst 8540 para obtener información adicional.

La indagación de puerto permite reflejar de manera transparente el tráfico de uno o más puertos de origen a un puerto de destino."

Ejecute el comando snoop para configurar la imagen réplica del tráfico basado en puerto, o indagación de puerto. Ejecute la forma **no de este comando para inhabilitar la indagación de puerto:**

```
snoop interface source_port direction snoop_direction

no snoop interface source_port
```

La variable **source_port hace referencia al puerto monitoreado.** La variable **snoop_direction es la dirección del tráfico en el puerto o puertos de origen monitoreados: recibir**, **transmitir** o **ambas**.

```
8500CSR#configure terminal
8500CSR(config)#interface fastethernet 12/0/15
8500CSR(config-if)#shutdown
8500CSR(config-if)#snoop interface fastethernet 0/0/1 direction both
8500CSR(config-if)#no shutdown
```

Este ejemplo muestra resultados del comando show snoop:

```
8500CSR#show snoop
Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option: (configured=enabled)(actual=enabled)
Snoop direction: (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```

> **Nota:** Este comando no es soportado en los puertos Ethernet de un Catalyst 8540 si se ejecuta una imagen de router switch ATM multiservicio (MSR), tal como 8540m-in-mz. En su lugar, debe utilizar una imagen de router switch de campus (CSR), tal como 8540c-in-mz.

SPAN en los Switches de las Series Catalyst 2900, 4500/4000, 5500/5000 y 6500/6000 que Ejecutan CatOS

Esta sección es aplicable solamente para estos Cisco Catalyst 2900 Series Switches:

- Cisco Catalyst 2948G-L2 Switch
- Cisco Catalyst 2948G-GE-TX Switch
- Cisco Catalyst 2980G-A Switch

Esta sección es aplicable para Cisco Catalyst 4000 Series Switches que incluyen:

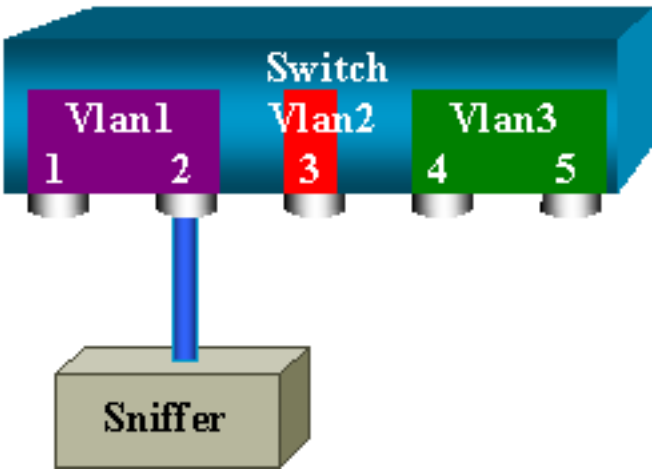
- Switches del chasis modular:Cisco Catalyst 4003 SwitchCisco Catalyst 4006 Switch
- Switch de Chasis Fijo: Cisco Catalyst 4912G Switch

SPAN local

Las funciones SPAN han sido agregadas de a una en CatOS y la configuración SPAN está compuesta de un único comando set span. Ahora existe una amplia gama de opciones disponibles para el comando:

```
switch (enable) set span
Usage: set span disable [dest_mod/dest_port|all]
set span <src_mod/src_ports...|src_vlans...|sc0>
<dest_mod/dest_port> [rx|tx|both]
[inpkts <enable|disable>]
[learning <enable|disable>]
[multicast <enable|disable>]
[filter <vlans...>]
[create]
```

El siguiente diagrama de red presenta las diferentes posibilidades de SPAN utilizando variaciones:



Este diagrama representa parte de una tarjeta de línea individual que se encuentra en la ranura 6 de un Switch Catalyst 6500/6000. In this scenario:

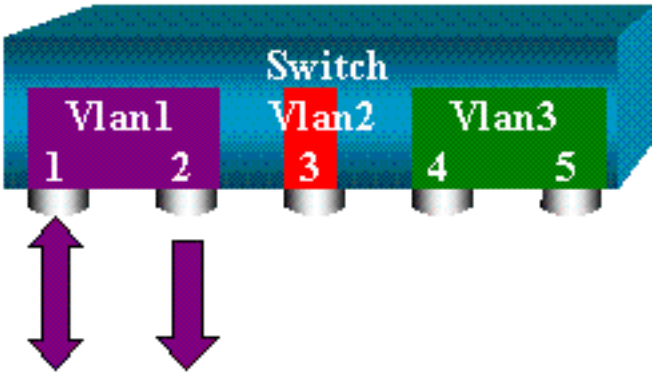
- Los puertos 6/1 y 6/2 pertenecen a la VLAN 1
- El puerto 6/3 pertenece a la VLAN 2
- Los puertos 6/4 y 6/5 pertenecen a la VLAN 3

Conecte un sniffer al puerto 6/2 y utilícelo como puerto monitor en varios casos diferentes.

PSPAN, VSPAN: Controle algunos puertos o una VLAN completa

Ejecute la forma más simple del **comando set span para monitorear un puerto único.** La sintaxis es **set span** ***source_port destination_port*** .

Supervisión en un solo puerto con SPAN

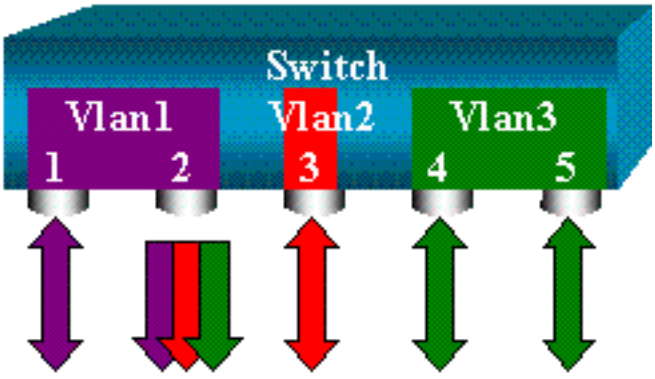



```
switch (enable) set span 6/1 6/2

Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

Con esta configuración, cada paquete que es recibido o enviado por el puerto 6/1 se copia en el puerto 6/2. Una descripción clara de esto aparece al ingresar la configuración. Ejecute el comando show span para recibir un resumen de la configuración de SPAN actual:

```
switch (enable) show span
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active

Total local span sessions: 1
```

Monitoreo de varios puertos con SPAN



El **comando set span source_ports destination_port le permite al usuario especificar más de un puerto de origen.** Enumere simplemente todos los puertos en los que desee implementar SPAN y

separe los puertos con comas. El intérprete de líneas de comando también permite utilizar el guión para especificar un rango de puertos. Este ejemplo ilustra esta capacidad de especificar más de un puerto. El ejemplo utiliza SPAN en el puerto 6/1 y un rango de tres puertos, del 6/3 al 6/5:

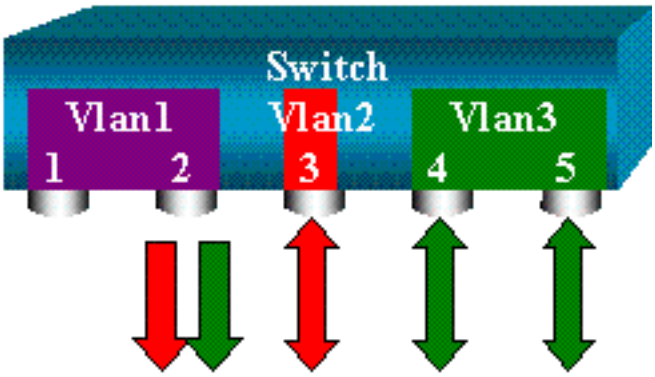
> **Nota:** Únicamente puede haber un puerto de destino. Especifique siempre el puerto de destino después del origen de SPAN.

```
switch (enable) set span 6/1,6/3-5 6/2

2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1,6/3-5
Oper Source : Port 6/1,6/3-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

> **Nota:** A diferencia de los Catalyst 2900XLI/3500XL Switches, el Catalyst 4500/4000, 5500/5000, y 6500/6000 puede puertos de monitor que pertenezcan a varias VLAN diferentes con versiones de CatOS anteriores a 5.1. Aquí, los puertos reflejados se asignan a las VLAN 1, 2, y 3.

Monitoreo de VLAN con SPAN

Finalmente, el **comando set span permite configurar un puerto para monitorear el tráfico local para una VLAN entera.** El comando es **set span** ***source_vlan(s) destination_port*** .



Utilice una lista de una o más redes VLAN como origen, en vez de una lista de puertos:

```
switch (enable) set span 2,3 6/2
2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 2-3
Oper Source : Port 6/3-5,15/1
Direction : transmit/receive
```

```
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

Con esta configuración, cada paquete que entra o sale de la VLAN 2 o 3 se duplica en el puerto 6/2.

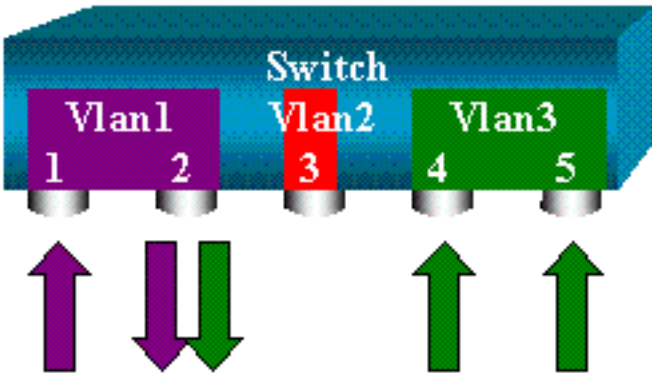
> **Nota:** El resultado es exactamente el mismo que si se implementa SPAN individualmente en todos los puertos que pertenecen a las VLAN que el comando especifica. Compare los campos `Oper Source` y `Admin Source` . El campo `Admin Source enumera básicamente todos los puertos configurados para la sesión SPAN, y el campo Oper Source enumera los puertos que utilizan SPAN.`

SPAN de entrada/salida

En el ejemplo de la sección Monitoreo de VLAN con SPAN, se monitorea el tráfico que entra y sale de los puertos especificados. El campo `Direction: transmit/receive lo muestra.` Los switches Catalyst de la serie 4500/4000, 5500/5000 y 6500/6000 permiten recopilar únicamente el tráfico de salida o únicamente de entrada en un puerto determinado. Añada la palabra clave **rx (recepción) o tx (transmisión) al final del comando.** El valor predeterminado es **both (tx y rx).**

set span *source_port destination_port* **[rx | tx | both]**

En este ejemplo, la sesión captura todo el tráfico entrante para las VLAN 1 y 3, y lo duplica en el puerto 6/2:




```
switch (enable) set span 1,3 6/2 rx
2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 1,3
Oper Source : Port 1/1,6/1,6/4-5,15/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

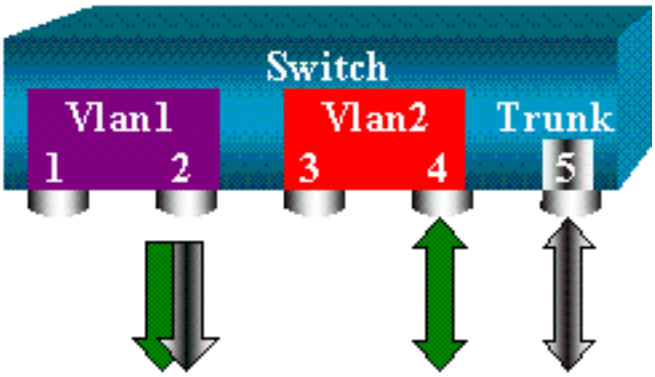
Implementa SPAN en un enlace troncal.

Los trunks son un caso especial en un switch debido a que son puertos que transportan varias VLAN. Si se selecciona un tronco como puerto de origen, se monitorea el tráfico para todas las VLAN.

Supervise un subconjunto de VLAN que pertenece a un tronco

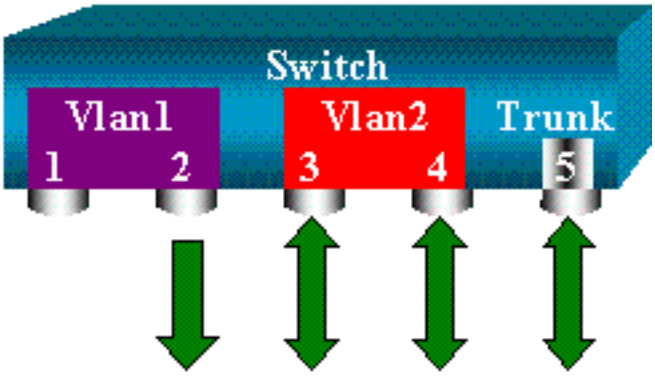
En el siguiente diagrama, el puerto 6/5 es ahora un trunk que transporta todas las VLAN. Imagine que desea utilizar SPAN en el tráfico de VLAN2 para los puertos 6/4 y 6/5. Ejecute simplemente este comando:

```
switch (enable) set span 6/4-5 6/2
```



En este caso, el tráfico que se recibe en el puerto SPAN es una mezcla de tráfico deseado y de todas las VLAN que transporta el trunk 6/5. Por ejemplo, no hay manera de distinguir en el puerto destino si un paquete viene del puerto 6/4 en el VLAN2 o del puerto 6/5 de la VLAN1. Otra posibilidad es utilizar SPAN en toda la VLAN 2:

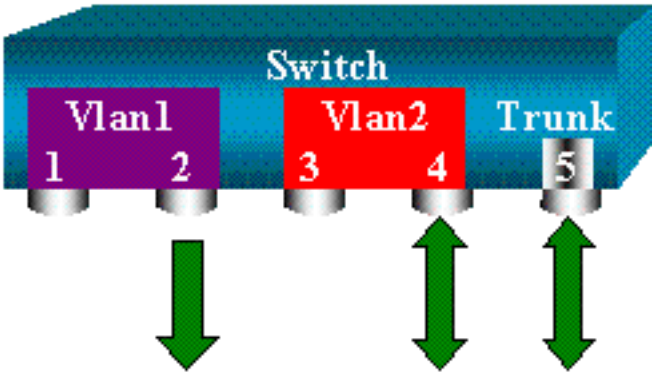
```
switch (enable) set span 2 6/2
```



Con esta configuración, al menos, solo se controla el tráfico que pertenece a la VLAN 2 del trunk. El problema es que ahora también recibe el tráfico que no deseaba del puerto 6/3. El CatOS incluye otra palabra clave que permite seleccionar algunas VLAN para supervisarla desde un trunk:

```
switch (enable) set span 6/4-5 6/2 filter 2
2000 Sep 06 02:31:51 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
```

```
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/4-5
Oper Source : Port 6/4-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : 2
Status : active
```



Este comando alcanza el objetivo porque se selecciona la VLAN 2 en todos los trunk supervisados. Puede especificar varias VLAN con esta opción de filtro.

> **Nota:** Esta opción de filtro solo se soporta en Switches Catalyst 4500/4000 y Catalyst 6500/6000. El Catalyst 5500/5000 no soporta la opción de filtro que está disponible con el **comando set span.**

Conexión troncal en el puerto de destino

Si tiene puertos de origen que pertenecen a diferentes VLAN o si utiliza SPAN en varias VLAN de un puerto trunk, es posible que desee identificar a qué VLAN pertenece un paquete que se recibe en el puerto SPAN de destino. Esta identificación es posible si se habilita el trunking en el puerto de destino antes de configurar el puerto para SPAN. De esta forma, todos los paquetes reenviados al sniffer también se etiquetan con sus correspondientes ID de VLAN.

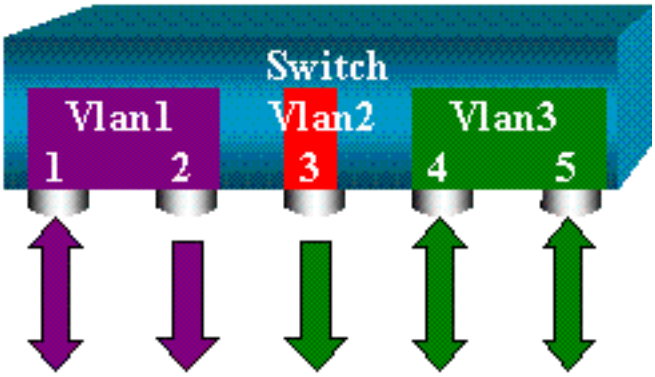
> **Nota:** El sniffer necesita reconocer la encapsulación correspondiente.

```
switch (enable) set span disable 6/2
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/4-5
2000 Sep 06 02:52:22 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
switch (enable) set trunk 6/2 nonegotiate isl

Port(s) 6/2 trunk mode set to nonegotiate.
Port(s) 6/2 trunk type set to isl.
switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become
isl trunk
switch (enable) set span 6/4-5 6/2
Destination : Port 6/2
Admin Source : Port 6/4-5
Oper Source : Port 6/4-5
```

```
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
2000 Sep 06 02:53:23 %SYS-5-SPAN_CFGSTATECHG:local span session active for
destination port 6/2
```

Cree varias sesiones simultáneas

Hasta ahora, se ha creado una sola sesión SPAN. Cada vez que se ejecuta un nuevo **comando set span, se invalida la configuración previa.** El CatOS ahora tiene la capacidad de ejecutar varias sesiones simultáneamente, por lo que puede tener diferentes puertos de destino a la vez. Ejecute el **comando set span source destination create para añadir una sesión SPAN adicional.** En esta sesión, se monitorea el puerto 6/1 a 6/2, y al mismo tiempo, se monitorea VLAN 3 al puerto 6/3:




```
switch (enable) set span 6/1 6/2
2000 Sep 05 08:49:04 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:49:05 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
switch (enable) set span 3 6/3 create
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:55:38 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/3
```

Ahora ejecute el **comando show span para determinar si dispone de dos sesiones a la vez:**

```
switch (enable) show span
```

```
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
--------------------------------------------------------------------
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
Total local span sessions: 2
```

Se han creado sesiones adicionales. Es necesario que elimine algunas sesiones. El comando es el siguiente:

set span disable {all | *destination_port***}**

Se identifica una sesión por su puerto de destino, ya que solo puede haber un puerto de destino por sesión. Elimine la primera sesión que se creó, que es la que utiliza el puerto 6/2 como destino:

```
switch (enable) set span disable 6/2
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/1
2000 Sep 05 09:04:33 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
```

Ahora puede verificar que solo queda una sesión:

```
switch (enable) show span
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active

Total local span sessions: 1
```

Ejecute el comando siguiente para inhabilitar todas las sesiones actuales de una sola vez:

```
switch (enable) set span disable all
This command will disable all span session(s).
Do you want to continue (y/n) [n]?y
Disabled all local span sessions
2000 Sep 05 09:07:07 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/3
```

```
switch (enable) show span
No span session configured
```

Otras opciones SPAN

La sintaxis del **comando set span es la siguiente:**

```
switch (enable) set span
Usage: set span disable [dest_mod/dest_port|all]
set span <src_mod/src_ports...|src_vlans...|sc0>
<dest_mod/dest_port> [rx|tx|both]
[inpkts
```

```
[filter <vlans...>]
[create]
```

Esta sección presenta brevemente las opciones que trata este documento:

- **sc0: especifique la palabra clave sc0 en una configuración de SPAN cuando necesite monitorear el tráfico al sc0 de la interfaz de administración.** Esta característica está disponible en los Switches Catalyst 5500/5000 y 6500/6000, versión del código CatOS 5.1 o posterior.
- **inpkts *enable/disable***: esta opción es extremadamente importante. Tal como se afirma en este documento, un puerto configurado como destino SPAN continúa perteneciendo a la VLAN original. Los paquetes recibidos en un puerto destino entran luego a la VLAN, como si este puerto fuera un puerto de acceso normal. Es posible que se desee este comportamiento. Si utiliza un PC como sniffer, es posible que desee que este PC esté completamente conectado a la VLAN. Sin embargo, la conexión puede ser peligrosa si conecta el puerto de destino a otro equipo en red que cree un bucle en la red. El puerto SPAN de destino no ejecuta el STP, lo cual puede dar lugar a una situación de loop de conexión peligrosa. Vea la sección ¿Por qué la Sesión SPAN Crea un Bucle de Bridging? de este documento para comprender cómo puede suceder esta situación. La configuración predeterminada para esta opción es inhabilitar, lo que significa que el puerto de destino SPAN descarta los paquetes que recibe el puerto. De esta forma, protege el puerto contra los bucles de bridging. Esta opción se encuentra en CatOS 4.2.
- **learning *enable/disable*** : esta opción permite inhabilitar el aprendizaje en el puerto de destino. El aprendizaje está habilitado de manera predeterminada y el puerto de destino aprende las direcciones MAC de los paquetes entrantes que recibe. Esta función se encuentra en CatOS 5.2 en los Catalyst 4500/4000 y 5500/5000, y en CatOS 5.3 en el Catalyst 6500/6000.
- **multicast *enable/disable***: como su nombre sugiere, esta opción permite habilitar o inhabilitar el monitoreo de los paquetes multicast. El valor predeterminado es habilitar. Esta función también está disponible en los Catalyst 5500/5000 y 6500/6000, CatOS 5.1 y versiones posteriores.
- **spanning port 15/1**: en el Catalyst 6500/6000, puede utilizar el puerto 15/1 (o 16/1) como origen SPAN. El puerto puede monitorear el tráfico reenviado a la Tarjeta de Función de Switch Multicapa (MSFC). El puerto captura el tráfico ruteado por software o dirigido a la MSFC.

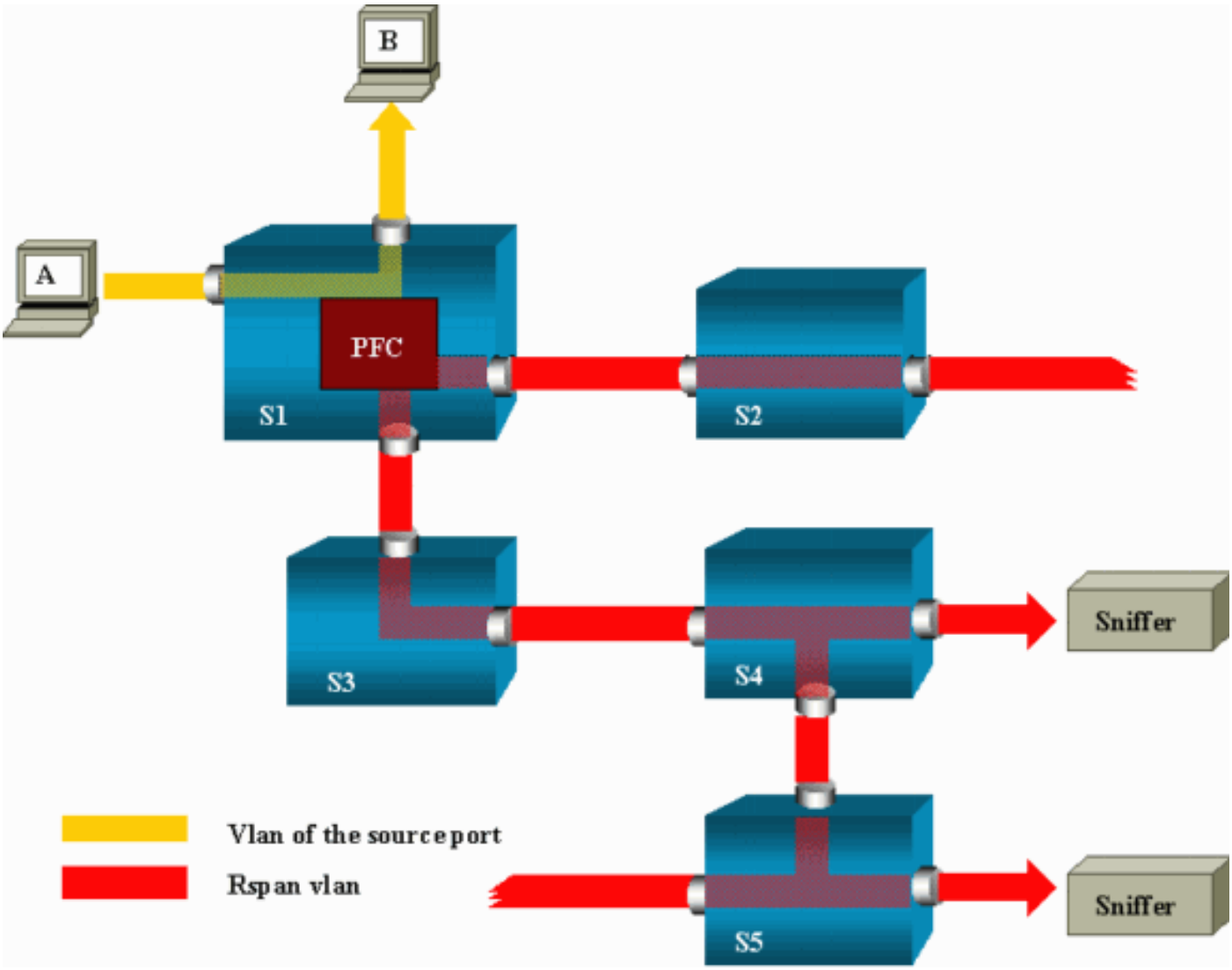
SPAN remoto

Información general sobre RSPAN

RSPAN permite monitorear los puertos de origen distribuidos en una red conmutada, no solo de forma local en un switch con SPAN. Esta función se encuentra en CatOS 5.3 en los switches Catalyst de la Serie 6500/6000 y se ha añadido en los Switches Catalyst de la Serie 4500/4000 en CatOS 6.3 y versiones posteriores.

La funcionalidad funciona exactamente como una sesión SPAN normal. El tráfico monitoreado por SPAN, no se copia directamente en el puerto de destino, sino que se desborda a una VLAN RSPAN especial. El puerto de destino puede ubicarse en cualquier lugar de esta VLAN RSPAN. Puede haber varios puertos de destino.

Este diagrama ilustra la estructura de una sesión RSPAN:



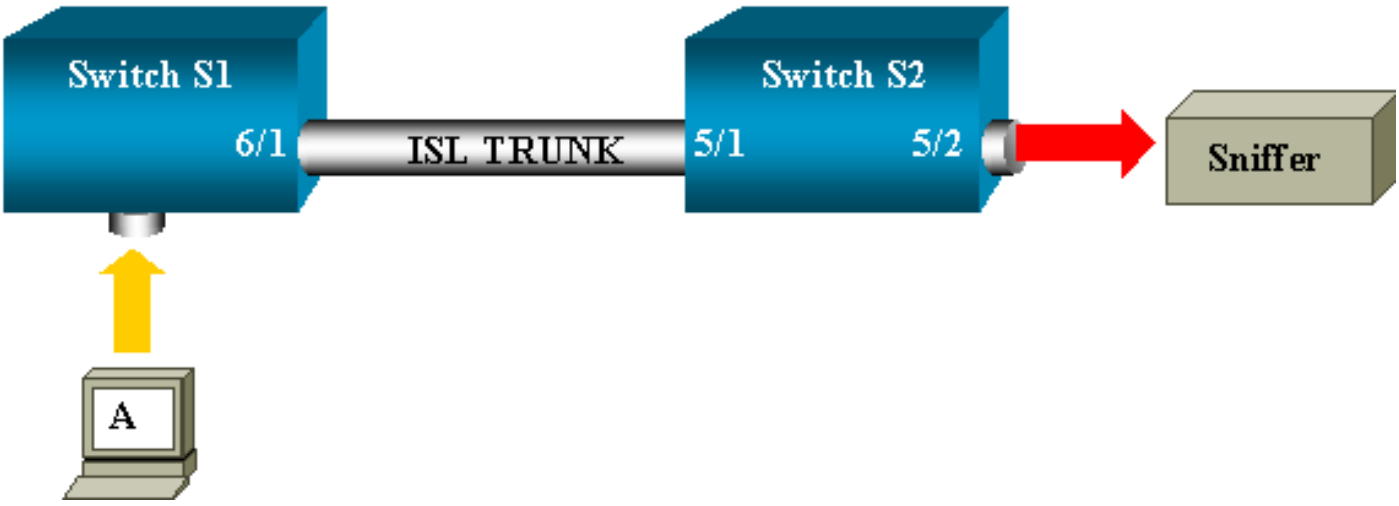
En este ejemplo, se configura RSPAN para que monitoree el tráfico que envía el host A. Cuando A genera una trama destinada a B, el paquete es copiado por un circuito integrado específico de la aplicación (ASIC) de la Tarjeta de Funciones de Política (PFC) del Catalyst 6500/6000 en una VLAN RSPAN. Desde allí, el paquete se desborda a todos los demás puertos que pertenecen a la VLAN RSPAN. Todos los enlaces entre switches que se muestran aquí son trunks, ya que es un requisito para RSPAN. Los únicos puertos de acceso son los puertos de destino, en los que se conectan los rastreadores (en este caso, S4 y S5).

A continuación, algunos comentarios sobre el diseño:

- S1 se conoce como switch de origen. Los paquetes solo entran en la VLAN RSPAN en switches configurados como origen RSPAN. Actualmente, un switch solo puede ser el origen de una sesión RSPAN, lo que quiere decir que un switch de origen solo puede alimentar una VLAN RSPAN a la vez.
- S2 y S3 son switches intermedios. No son orígenes RSPAN y no tienen puertos de destino. Un switch puede actuar como intermediario para cualquier número de sesiones RSPAN.
- Los switches S4 y S5 son switches de destino. Algunos de sus puertos se configuran para ser destino para una sesión de RSPAN. Actualmente, Catalyst 6500/6000 puede tener hasta 24 puertos de destino RSPAN, para una o varias sesiones diferentes. Podrá notar también que S4 es un switch de destino e intermedio.
- Como puede ver, los paquetes RSPAN se desbordan a la VLAN RSPAN. Incluso los switches que no se encuentran en la ruta hacia un puerto de destino, tales como S2, reciben tráfico de VLAN RSPAN. Es posible que le parezca útil recortar esta VLAN en esos enlaces S1-S2.
- La inundación se consigue mediante la inhabilitación del aprendizaje en la VLAN RSPAN.
- Para evitar bucles, el STP se ha conservado en la VLAN RSPAN. Por lo tanto, RSPAN no puede monitorear Unidades de Datos de Protocolo de Bridge (BDPU).

Ejemplo de configuración de RSPAN

La información de esta sección ilustra la configuración de estos diferentes elementos con un diseño RSPAN muy simple. S1 y S2 son dos switches Catalyst 6500/6000. Para monitorear algunos puertos S1 o VLAN de S2, debe configurar una VLAN RSPAN dedicada. El resto de los comandos posee una sintaxis muy similar a la que se utiliza en una sesión SPAN típica.



Configuración del Tronco ISL entre los dos switches S1 y S2

Para comenzar, coloque el mismo dominio de Protocolo Trunk VLAN (VTP) en cada switch y configure un lado como conexión trunking deseable. La negociación VTP hace el resto. Ejecute este comando en S1:

```
S1> (enable) set vtp domain cisco
VTP domain cisco modified
```

Ejecute estos comandos en S2:

```
S2> (enable) set vtp domain cisco
VTP domain cisco modified
S2> (enable) set trunk 5/1 desirable
Port(s) 5/1 trunk mode set to desirable.
S2> (enable) 2000 Sep 12 04:32:44 %PAGP-5-PORTFROMSTP:Port 5/1 left bridge
port 5/1
2000 Sep 12 04:32:47 %DTP-5-TRUNKPORTON:Port 5/1 has become isl trunk
```

Creación de la VLAN RSPAN

Una sesión RSPAN requiere una VLAN RSPAN específica. Debe crear esta VLAN. No es posible convertir una VLAN existente en una VLAN RSPAN. Este ejemplo utiliza la VLAN 100:

```
S2> (enable) set vlan 100 rspan
Vlan 100 configuration successful
```

Ejecute este comando en un switch configurado como servidor VTP. El conocimiento de RSPAN VLAN 100 se propaga automáticamente en todo el dominio VTP.

Configuración del Puerto 5/2 de S2 como Puerto de Destino RSPAN

```
S2> (enable) set rspan destination 5/2 100
Rspan Type : Destination
Destination : Port 5/2
Rspan Vlan : 100
Admin Source : -
Oper Source : -
Direction : -
Incoming Packets: disabled
Learning : enabled
Multicast : -
Filter : -
Status : active
2000 Sep 12 04:34:47 %SYS-5-SPAN_CFGSTATECHG:remote span destination session
active for destination port 5/2
```

Configuración de puerto de origen RSPAN en S1

En este ejemplo, se monitorea el tráfico entrante que entra en S1 a través del puerto 6/2. Ejecutar este comando:

```
S1> (enable) set rspan source 6/2 100 rx
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
Filter : -
Status : active
S1> (enable) 2000 Sep 12 05:40:37 %SYS-5-SPAN_CFGSTATECHG:remote span
source session active for remote span vlan 100
```

Todos los paquetes entrantes en el puerto 6/2 se desbordan a la RSPAN VLAN 100 y llegan al

puerto de destino configurado en S1 mediante el trunk.

Verifique la Configuración

El **comando show rspan proporciona un resumen de la configuración RSPAN actual en el switch.** Nuevamente, solo puede haber una sesión RSPAN de origen a la vez.

```
S1> (enable) show rspan
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
Filter : -
Status : active
Total remote span sessions: 1
```

Otras Configuraciones Posibles con el Comando set rspan

Se utilizan varias líneas de comandos para configurar el origen y el destino con RSPAN. Aparte de esta diferencia, SPAN y RSPAN realmente se comportan de la misma manera. Incluso puede utilizar RSPAN localmente, en un solo switch, si desea tener varios puertos de tramo de destino.

Limitaciones y resumen de características

Esta tabla resume las diferentes funciones introducidas y proporciona la versión mínima de CatOS que se necesita para ejecutar la función en la plataforma especificada:

Función	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/60
opción inpkts *enable/disable*	4.4	4.2	5.1
Sesiones múltiples, puertos en diferentes VLAN	5.1	5.1	5.1
opción sc0	—	5.1	5.1
opción multicast *enable/disable*	—	5.1	5.1
opción learning *enable/disable*	5.2	5.2	5.3
RSPAN	6.3	—	5.3

Esta tabla ofrece un resumen de las restricciones actuales sobre la cantidad de posibles sesiones de SPAN:

Función	Rangos de switches Catalyst 4500/4000	Rangos de switches Catalyst 5500/5000	Rangos de switches Catalyst 6500/6000
Rx o ambas sesiones SPAN	5	1	2
Sesiones Tx SPAN	5	4	4
Sesiones de Mini Protocol Analyzer	No soportados	No soportados	1
Rx, Tx o ambas sesiones fuente RSPAN	5	No soportados	1 Supervisor Engine 720 soporta sesiones de origen de RSPAN.
Destino RSPAN	5	No soportados	24

Total de sesiones	5	5	30

Consulte estos documentos para ver restricciones adicionales y pautas de configuración:

- Configuración de SPAN y RSPAN (Catalyst 4500/4000)
- Configuración de SPAN y RSPAN(Catalyst 6500/6000)

SPAN en los Switches de las Series Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 y 3750-E

A continuación, se describen las pautas para configurar la función SPAN en los Switches Catalyst de la Serie 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 y 3750-E.

- Los Catalyst 2950 Switches pueden tener solamente una sección SPAN activa a la vez y pueden monitorear solamente puertos de origen. Estos switches no pueden supervisar VLAN.
- Los switches Catalyst 2950 y 3550 pueden reenviar tráfico en un puerto SPAN de destino en la versión de software IOS de Cisco 12.1(13)EA1 y versiones posteriores.
- Los Switches Catalyst 3550, 3560 y 3750 puede soportar hasta dos sesiones SPAN a la vez y pueden monitorear tanto puertos de origen como VLAN.
- Los Switches Catalyst 2970, 3560 y 3750 no requieren la configuración de un puerto reflector al configurar una sesión RSPAN.
- Los Switches Catalyst 3750 soportan la configuración de sesión mediante el uso de puertos de origen y destino que residen en cualquiera de los miembros de pila del switch.
- Solo se permite un puerto de destino por sesión SPAN, y el mismo puerto no puede ser un puerto de destino para varias sesiones SPAN. Por lo tanto, no se puede tener dos sesiones SPAN que utilicen el mismo puerto de destino.

Los comandos de configuración de la función SPAN son similares en el Catalyst 2950 y el Catalyst 3550. Sin embargo, el Catalyst 2950 no puede monitorear VLAN. Puede configurar SPAN como se muestra en este ejemplo:

```
C2950#configure terminal
C2950(config)#
C2950(config)#monitor session 1 source interface fastethernet 0/2

!--- This configures interface Fast Ethernet 0/2 as source port.

C2950(config)#monitor session 1 destination interface fastethernet 0/3

!--- This configures interface Fast Ethernet 0/3 as destination port.

C2950(config)#

C2950#show monitor session 1
Session 1---------
Source Ports:
RX Only: None
TX Only: None
Both: Fa0/2
Destination Ports: Fa0/3
C2950#
```

También puede configurar un puerto como destino para SPAN y RSPAN local para el mismo tráfico VLAN. Para monitorear el tráfico para una vlan determinada que resida en dos switches

conectados directamente, configure estos comandos en el switch que tenga el puerto de destino. En este ejemplo, monitoreamos el tráfico de la VLAN 5 que se extiende entre dos switches:

```
c3750(config)#monitor session 1 source vlan < Remote RSPAN VLAN ID >
c3750(config)#monitor session 1 source vlan 5
c3750(config)#monitor session 1 destination interface fastethernet 0/3

!--- This configures interface FastEthernet 0/3 as a destination port.
```

En el switch remoto, utilice esta configuración:

```
c3750_remote(config)#monitor session 1 source vlan 5

!--- Specifies VLAN 5 as the VLAN to be monitored.

c3750_remote(config)#monitor session 1 destination remote vlan
```

En el ejemplo anterior se configuró un puerto como puerto de destino tanto para RSPAN como para SPAN local, para monitorear el tráfico para la misma VLAN que reside en dos switches.

> **Nota:** A diferencia de los switches de la serie 2900XL y 3500XL, los switches Catalyst de las series 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 y 3750-E soportan SPAN en el tráfico del puerto de origen, solo en la dirección Rx (Rx SPAN o SPAN de entrada), solo en la dirección Tx (Tx SPAN o SPAN de salida) o en ambas.

> **Nota:** Los comandos de la configuración no se soportan en el Catalyst 2950 con Cisco IOS Software Release 12.0(5.2)WC(1) ni con ningún software que sea anterior a Cisco IOS Software Release 12.1(6)EA2. Consulte la sección Habilitación del Analizador de Puertos del Switch de Administración de Switches para configurar SPAN en un Catalyst 2950 con software anterior a Cisco IOS Software Release 12.1(6)EA2.

> **Nota:** Los Switches Catalyst 2950 que utilizan Cisco IOS Software Release 12.1.(9)EA1d y versiones anteriores del tren Cisco IOS Software Release 12.1 soportan SPAN. Sin embargo, todos los paquetes que se ven en el puerto de destino de SPAN (conectado con el dispositivo sniffer o el PC) tienen una etiqueta IEEE 802.1Q, aunque el puerto de origen de SPAN (puerto monitoreado) pudiera no ser un puerto trunk 802.1Q. Si el dispositivo sniffer o la tarjeta de interfaz de red (NIC) del PC no entienden los paquetes con etiquetas 802.1Q, es posible que el dispositivo descarte los paquetes o tenga dificultades al intentar descodificar los paquetes. La capacidad ara ver las tramas con etiquetas 802.1Q solo es importante cuando el puerto de origen SPAN es un puerto trunk. Con Cisco IOS Software Release 12.1(11)EA1 y versiones posteriores, puede habilitar e inhabilitar el etiquetado de los paquetes en el puerto de destino SPAN. Ejecute el comando monitor session session_number destination interface interface_id encapsulation dot1q para habilitar la encapsulación de los paquetes en el puerto de destino. Si no se especifica la **palabra clave encapsulación, los paquetes se envían sin etiqueta, que es la opción predeterminada en Cisco IOS Software Release 12.1(11)EA1 y versiones posteriores.**

Función	Catalyst 2950/3550

Opción Ingress (inpkts) *enable/disable*	Cisco IOS Software Release 12.1(12c)EA1
RSPAN	Cisco IOS Software Release 12.1(12c)EA1

Función	**Catalyst 29401, 2950, 2955, 2960, 2970, 3550, 3560, 3750**
Rx o ambas sesiones SPAN	2
Sesiones Tx SPAN	2
Rx, Tx o ambas sesiones fuente RSPAN	2
Destino RSPAN	2
Total de sesiones	2

[1] Los switches Catalyst 2940 sólo admiten SPAN local. RSPAN no se soporta en esta plataforma.

Consulte las guías de configuración si desea obtener más información sobra la configuración de SPAN y RSPAN:

- Configuración de SPAN (Catalyst 2940)
- Configuración de SPAN y RSPAN (Catalyst 2950 y 2955)
- Configuración de SPAN y RSPAN (Catalyst 2960)
- Configuración de SPAN y RSPAN (Catalyst 3550)
- Configuración de SPAN y RSPAN (Catalyst 3560)
- Configuración de SPAN y RSPAN (Catalyst 3560-E y 3750-E)
- Configuración de SPAN y RSPAN (Catalyst 3750)

SPAN en los Switches de las Series Catalyst 4500/4000 y Catalyst 6500/6000 que Ejecutan Cisco IOS System Software

La función SPAN se soporta en los Switches de las Series Catalyst 4500/4000 y Catalyst 6500/6000 que ejecutan el software del sistema de Cisco IOS. Ambas plataformas de switch utilizan idéntica interfaz de línea de comandos (CLI) y una configuración que es similar a la configuración que se trata en la sección SPAN en los Switches de las Series Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560E, 3750 y 3750E. Consulte estos documentos para ver la configuración relacionada:

- Configuración de SPAN y RSPAN (Catalyst 6500/6000)
- Configuración de SPAN y RSPAN (Catalyst 4500/4000)

Ejemplo de configuración

Puede configurar SPAN como se muestra en este ejemplo:

```
4507R#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

4507R(config)#monitor session 1 source interface fastethernet 4/2

!--- This configures interface Fast Ethernet 4/2 as source port.

4507R(config)#monitor session 1 destination interface fastethernet 4/3

!--- The configures interface Fast Ethernet 0/3 as destination port.

4507R#show monitor session 1
```

```
Session 1---------
Type : Local Session
Source Ports :
Both : Fa4/2
Destination Ports : Fa4/3

4507R#
```

Limitaciones y resumen de características

Esta tabla resume las diferentes funciones introducidas y proporciona la versión mínima del software Cisco IOS que se necesita para ejecutar la función en la plataforma especificada:

Función	Catalyst 4500/4000 (Cisco IOS Software)	Catalyst 6500/6000 (Cisco IOS Software)
Opción Ingress (inpkts) *enable/disable*	Cisco IOS Software Release 12.1(19)EW	No compatible actualmente [1]
RSPAN	Cisco IOS Software Release 12.1(20)EW	Cisco IOS Software Release 12.1(13)E

[1] Actualmente la función no está disponible y la disponibilidad de estas funciones no se publica normalmente hasta la publicación.

> **Nota**: La función SPAN de los Cisco Catalyst 6500/6000 Series Switches tiene una limitación con respecto al Protocolo PIM. Cuando un switch se configura tanto para PIM como para SPAN, el analizador de red/sniffer asociado al puerto de destino de SPAN puede ver los paquetes PIM que no forman parte del tráfico de la VLAN o del puerto de origen SPAN. Este problema se produce debido a una limitación en la arquitectura de reenvío de paquetes del switch. El puerto de destino de SPAN no realiza ningún control para verificar el origen de los paquetes. Este problema también se documenta en el Id. de bug Cisco CSCdy57506 (solo clientes registrados).

En esta tabla se ofrece un breve resumen de las restricciones actuales para la cantidad de posibles sesiones SPAN y RSPAN:

Función	Catalyst 4500/4000 (Cisco IOS Software)
Rx o ambas sesiones SPAN	2
Sesiones Tx SPAN	4
Rx, Tx o ambas sesiones fuente RSPAN	2 (Rx, Tx o ambos) y hasta 4 para Tx únicamente
Destino RSPAN	2
Total de sesiones	6

Consulte Límites de sesión de SPAN Local, RSPAN y ERSPAN para Switches Catalyst 6500/6000 que ejecutan Cisco IOS Software.

En la Serie Catalyst 6500, es importante observar que el SPAN de salida se realiza en el supervisor. Esto permite que todo el tráfico sujeto al SPAN de salida se envíe a través de fabric al supervisor y, a continuación, al puerto destino de SPAN, lo que puede utilizar una cantidad significativa de recursos del sistema y afectar al tráfico de usuarios. El SPAN de entrada se realizará en los módulos de entrada, así que el rendimiento de SPAN sería la suma de todos los motores participantes en la réplica. El rendimiento de la función SPAN depende del tamaño de los paquetes y del tipo de ASIC disponible en el motor de réplica.

Con versiones anteriores a Cisco IOS Software Release 12.2(33)SXH, una interfaz de puerto-canal, un EtherChannel no puede ser un destino SPAN. Con Cisco IOS Software Release 12.2(33)SXH y versiones posteriores, un EtherChannel puede ser un destino SPAN. Los EtherChannels de destino no soportan los protocolos EtherChannel Port Aggregation Control Protocol (PAgP) ni Link Aggregation Control Protocol (LACP); solo se soporta el modo activo, con todo el soporte del protocolo EtherChannel inhabilitado.

Consulte estos documentos para ver restricciones adicionales y pautas de configuración:

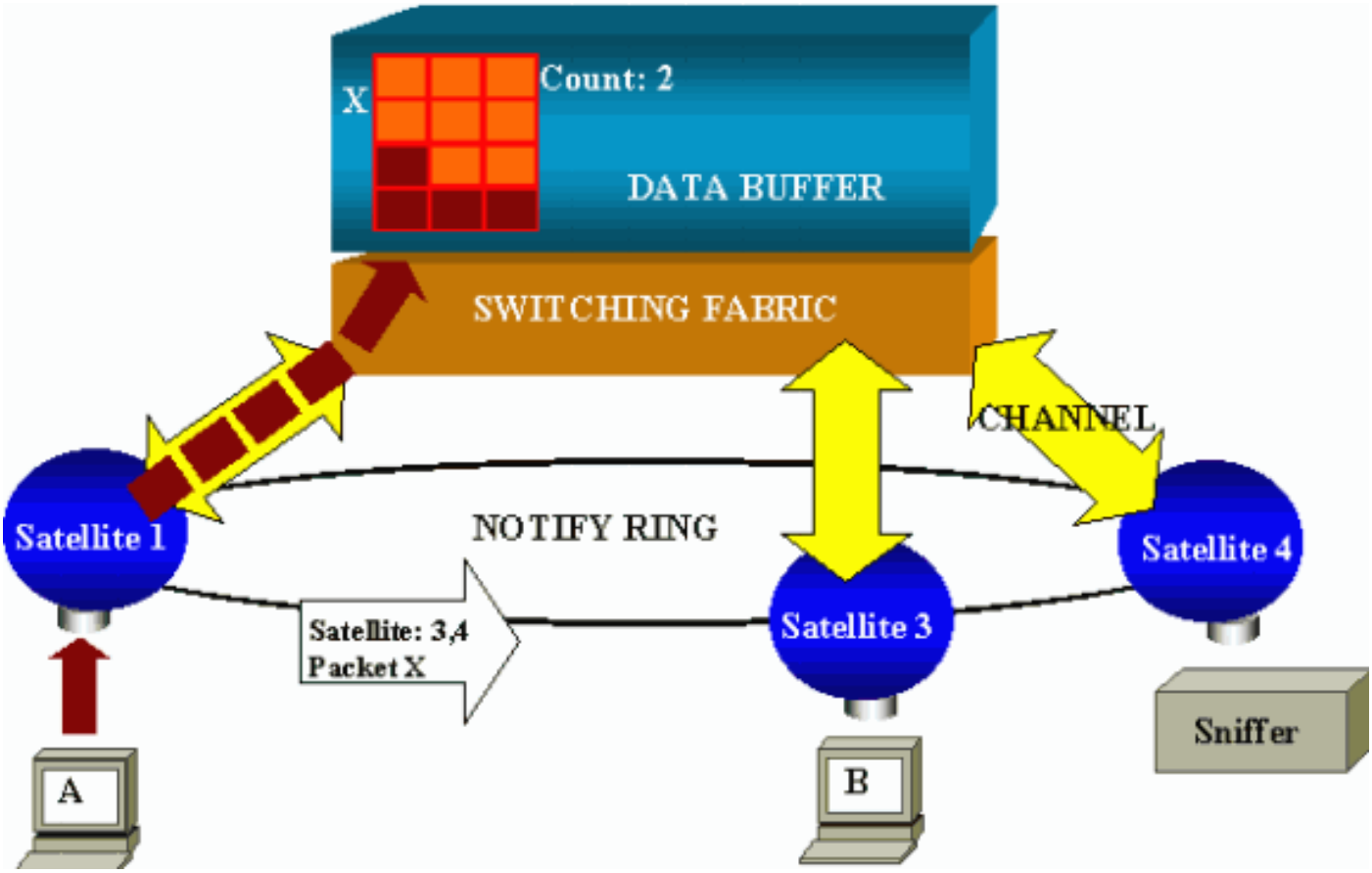
- Configuración de SPAN y RSPAN (Catalyst 4500/4000)
- Configuración de SPAN Local, SPAN Remoto (RSPAN) y RSPAN Encapsulado (Catalyst 6500/6000)

Impacto de SPAN en el rendimiento en las diferentes plataformas de Catalyst

Serie Catalyst 2900XL/3500XL

Descripción general de la arquitectura

Ésta es una vista muy simple de la arquitectura interna de los switches 2900XL/3500XL:



Los puertos del switch se asocian a los satélites que comunican con un fabric de switching mediante canales radiales. En la parte superior, todos los satélites se interconectan a través de un anillo notificador de alta velocidad, dedicado al tráfico de señalización.

Cuando un satélite recibe un paquete desde un puerto, el paquete se divide en celdas y se envía

a la estructura de conmutación a través de uno o más canales. Luego se almacena el paquete en la memoria compartida. Cada satélite tiene conocimiento de los puertos destino. En el diagrama de esta sección, el satélite 1 sabe que el paquete X debe ser recibido por los satélites 3 y 4. El satélite 1 envía un mensaje a los demás satélites a través del anillo de notificación. A continuación, los satélites 3 y 4 pueden empezar a recuperar las celdas de la memoria compartida mediante su canal radial y, en caso necesario, reenviar el paquete. Debido a que el satélite de origen conoce el destino, este satélite también transmite un índice que especifica la cantidad de veces que los demás satélites descargan ese paquete. Cada vez que un satélite recupera el paquete de la memoria compartida, este índice disminuye. Cuando el índice llega a cero, se puede liberar la memoria compartida.

Impacto en el rendimiento

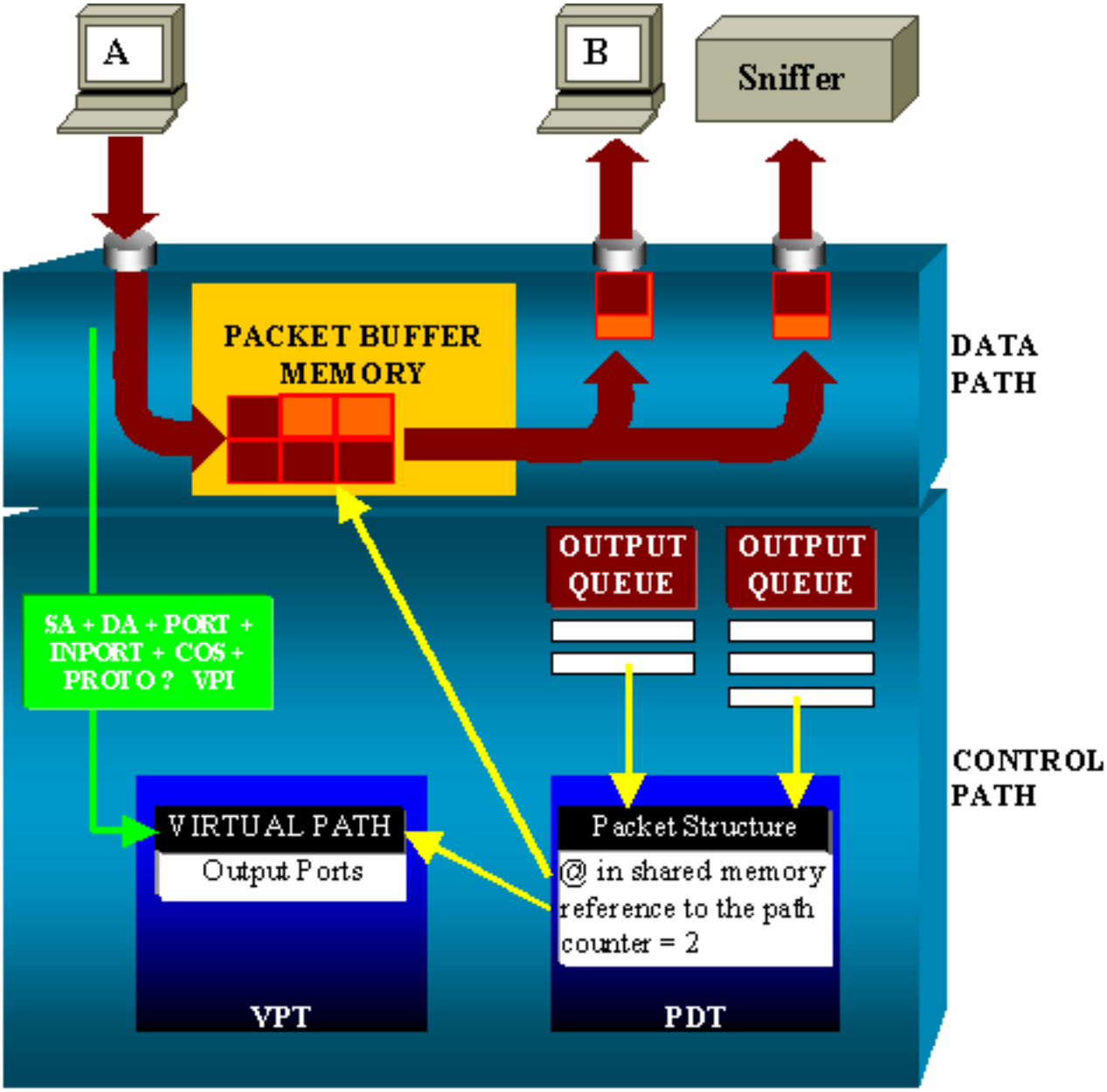
Para monitorear algunos puertos con SPAN, un paquete se debe copiar del búfer de datos a un satélite una vez más. El impacto en la estructura de conmutación de alta velocidad es despreciable.

El puerto de monitoreo recibe copias del tráfico transmitido y recibido para todos los puertos monitoreados. En esta arquitectura, un paquete con múltiples destinos es almacenado en memoria hasta que se hayan reenviado todas las copias. Si el puerto de supervisión tiene un exceso de suscriptores del 50 por ciento durante un periodo de tiempo continuado, es probable que el puerto se congestione y se quede parte de la memoria compartida. Existe la posibilidad de que uno o más puertos supervisados también experimenten una caída.

Series Catalyst 4500/4000

Descripción general de la arquitectura

El Catalyst 4500/4000 se basa en una estructura de conmutación de memoria compartida. El siguiente diagrama muestra una descripción general de alto nivel del trayecto de un paquete a través del switch. La verdadera implementación es, de hecho, mucho más compleja:



En un Catalyst 4500/4000, puede distinguir la trayectoria de los datos. La trayectoria de los datos corresponde a la transferencia real de datos dentro del switch, desde la trayectoria de control, donde se toman todas las decisiones.

Cuando un paquete entra en el switch, se asigna un búfer al memoria búfer del paquete (una memoria compartida). La estructura de un paquete que apunta a este búfer se inicializa en la Tabla descriptora del paquete (PDT). Mientras se copian los datos en la memoria compartida, la trayectoria de control determina dónde conmutar el paquete. Para llevar a cabo esta determinación, se computa un valor de hash a partir de esta información:

- La dirección de origen del paquete
- Dirección de destino
- VLAN
- Tipo de protocolo
- Puerto de entrada
- Clase de servicio (CoS) (etiqueta IEEE 802.1p o puerto predeterminado)

Este valor se utiliza para encontrar el índice de trayecto virtual (VPI) de una estructura de trayecto en la tabla de trayecto virtual (VPT). Esta entrada de trayectoria virtual en el VPT contiene varios campos relacionados con este flujo particular. Este campo incluye los puertos de destino. La

estructura de paquetes en la PDT es actualizada con una referencia al trayecto virtual y al contador. En el ejemplo de esta sección, el paquete debe ser transmitido a dos puertos diferentes, así que el contador se inicializa a 2. Finalmente, la estructura del paquete se añade a la cola de salida de los dos puertos de destino. Desde allí, los datos se copian desde la memoria compartida al búfer de salida del puerto y el contador de estructura del paquete disminuye. Cuando llega a cero, el búfer de la memoria compartida se libera.

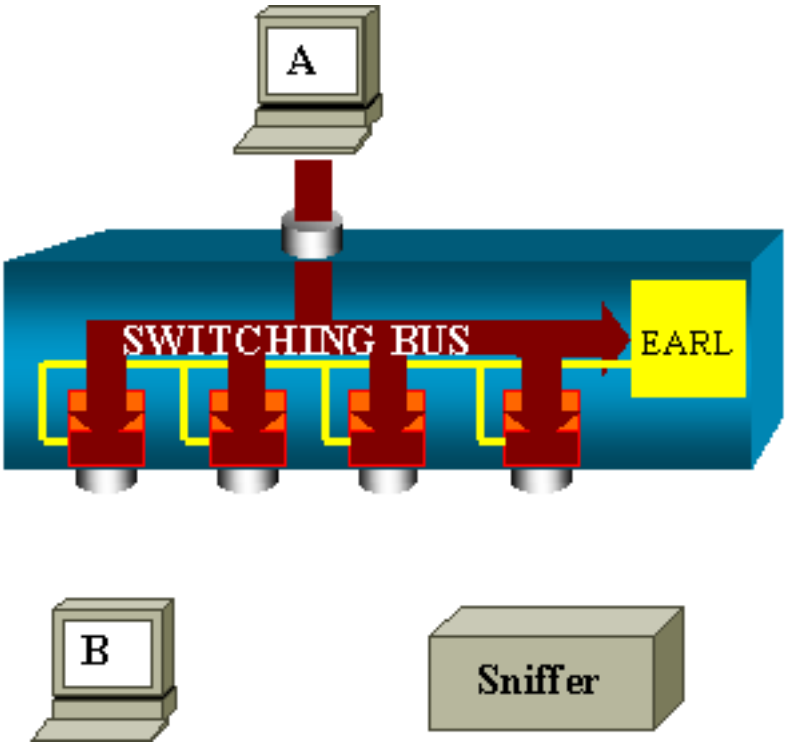
Impacto en el rendimiento

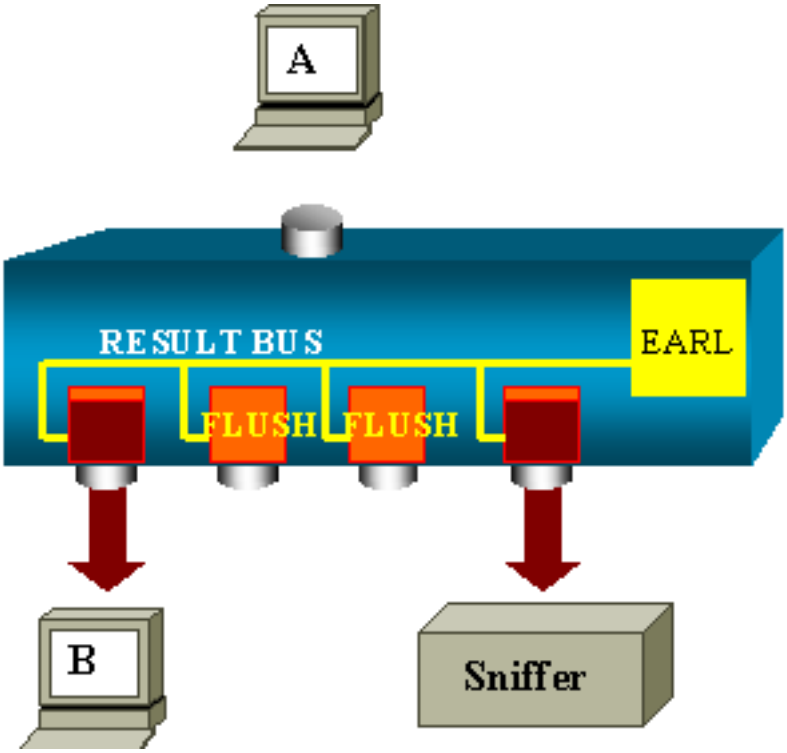
Con el uso de la función SPAN, un paquete se debe enviar a dos puertos diferentes, como en el ejemplo de la sección Descripción General de la Arquitectura. El envío del paquete a dos puertos no es un problema porque el entramado de conmutación no es bloqueante. Si el puerto de tramo de destino está congestionado, los paquetes se colocan en la cola de salida y se liberan correctamente de la memoria compartida. Por lo tanto, la operación del switch no se ve afectada.

Catalyst de serie 5500/5000 y 6500/6000

Descripción general de la arquitectura

En los switches Catalyst de las Series 5500/5000 y 6500/6000, un paquete recibido en un puerto se transmite al bus de switching interno. Cada tarjeta de línea del switch comienza a almacenar este paquete en sus búferes internos. Simultáneamente, la Lógica de reconocimiento de dirección codificada (EARL) recibe el encabezado del paquete y calcula un índice de resultado. EARL envía el índice de resultado a todas las tarjetas de línea a través del bus de resultados. El conocimiento de este índice permite que la tarjeta de línea decida de manera individual si debe vaciar o transmitir el paquete mientras la tarjeta de línea recibe el paquete en sus búferes.





Impacto en el rendimiento

Ya sea que uno o varios puertos transmitan eventualmente el paquete, no influye en absoluto sobre la operación del switch. Por lo tanto, si se tiene en cuenta esta arquitectura, la función SPAN no tiene efecto en el rendimiento.

Preguntas mas frecuentes y problemas comunes

Problemas de conectividad debido a la configuración incorrecta de SPAN

Los problemas de conectividad debido a la mala configuración del SPAN ocurren con frecuencia en las versiones de CatOS anteriores a la 5.1. Con estas versiones, solamente es posible una sesión SPAN. La sesión permanece en la configuración, incluso cuando se inhabilita SPAN. Con la ejecución de comando set span enable, un usuario reactiva a la sesión SPAN almacenada. Esta acción suele producirse debido a un error tipográfico, por ejemplo, si el usuario desea habilitar STP. Pueden ocurrir problemas de conectividad graves si el puerto de destino se utiliza para reenviar tráfico de usuario.

> **Precaución:** Este problema aún persiste en la implementación actual de CatOS. Tenga cuidado con el puerto que selecciona como destino SPAN.

Puerto de Destino SPAN Arriba/Abajo

Cuando se extienden los puertos para supervisión, el estado del puerto indica UP/DOWN (Activado/Desactivado).

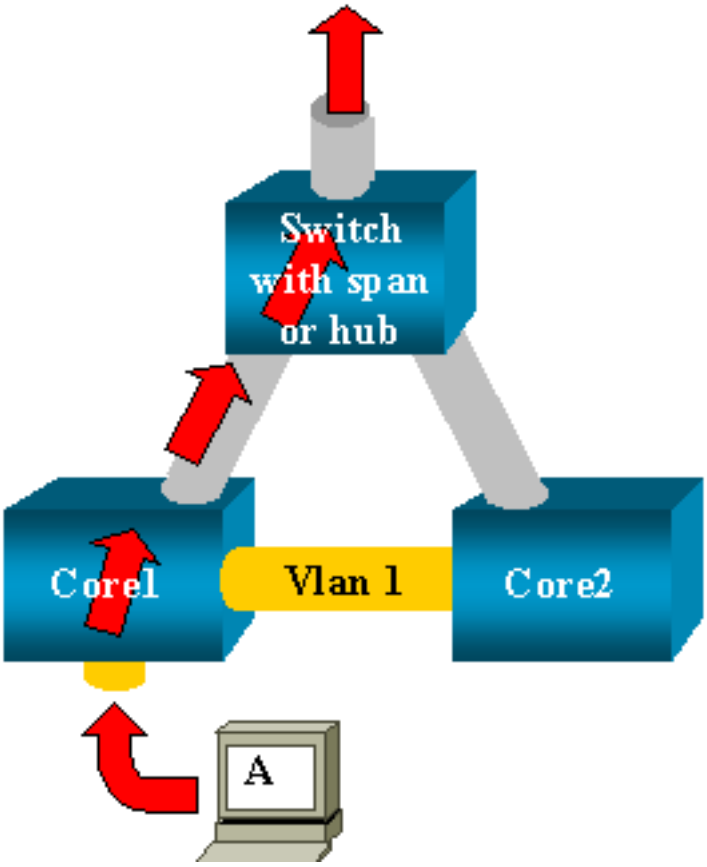
Cuando se configura una sesión SPAN para supervisar el puerto, la interfaz de destino muestra el estado desactivado (monitoreo), por diseño. La interfaz muestra el puerto en este estado para hacer evidente que el puerto actualmente no se puede utilizar como puerto de producción. El

puerto como supervisión activada/desactivada es normal.

¿Por qué la Sesión SPAN Crea un Bucle de Bridging?

La creación de un bucle de conexión en bridge suele producirse cuando el administrador intenta fingir la función RSPAN. También un error de configuración puede provocar el problema.

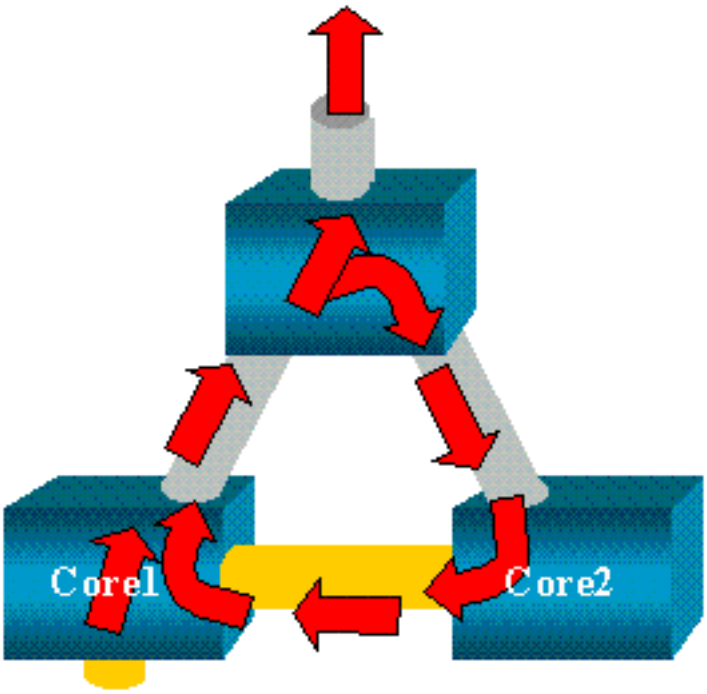
Éste es un ejemplo del escenario:



Hay dos switches de núcleo que están enlazados mediante un trunk. En este ejemplo, cada switch tiene varios servidores, clientes u otros bridges conectados a ellos. El administrador desea controlar la VLAN 1, que aparece en varios bridges con SPAN. El administrador crea una sesión SPAN que controla toda la VLAN 1 en cada switch de núcleo y, para fusionar estas dos sesiones, conecta el puerto de destino al mismo concentrador (o al mismo switch, utilizando otra sesión SPAN).

De esta manera, el administrador consigue su objetivo. Cada paquete individual que recibe el switch de núcleo en la VLAN 1 se duplica en el puerto SPAN y se reenvía al concentrador. Un sniffer captura finalmente el tráfico.

El único problema es que el tráfico también se reinyecta en el núcleo 2 a través del puerto SPAN de destino. La reinyección del tráfico en el núcleo 2 crea un loop de conexión en puente en la VLAN 1. Recuerde que un puerto SPAN de destino no ejecuta STP y no puede evitar tal loop.



Nota: Debido a la introducción de las opciones inpkts (paquetes de entrada) en CatOS, un puerto de destino SPAN descarta todos los paquetes entrantes de manera predeterminada; por lo tanto, evita esta situación de fallo. No obstante, el problema potencial sigue todavía presente en los switches Catalyst de la serie 2900XL/3500XL.

Nota: Incluso cuando la opción inpkts evita el bucle, la configuración que muestra esta sección puede causar algunos problemas en la red. Los problemas en la red se pueden producir debido a problemas de aprendizaje de la dirección MAC asociados con la habilitación del aprendizaje en el puerto de destino.

¿Afecta SPAN al rendimiento?

Vea las siguientes secciones de este documento para obtener más información sobre el impacto en el rendimiento para las plataformas Catalyst especificadas:

- Serie Catalyst 2900XL/3500XL
- Series Catalyst 4500/4000
- Catalyst de serie 5500/5000 y 6500/6000

¿Puede configurar SPAN en un puerto EtherChannel?

No se forma un EtherChannel si uno de los puertos del agrupamiento es un puerto de destino SPAN. Si intenta configurar SPAN en esta situación, el switch le dirá:

```
Channel port cannot be a Monitor Destination Port
Failed to configure span feature
```

Puede utilizar un puerto en un agrupamiento EtherChannel como puerto de origen SPAN.

¿Se Puede Tener Varias Sesiones SPAN Ejecutándose al Mismo Tiempo?

En los switches Catalyst de la serie 2900XL/3500XL, la cantidad de puertos de destino disponibles en el switch es el único límite a la cantidad de sesiones SPAN.

En los Switches Catalyst de la Serie 2950, solo se puede tener asignado un puerto de monitor en cualquier momento. Si selecciona otro puerto como el puerto de control, se desactiva el puerto de control anterior y el puerto recientemente seleccionado se convierte en el puerto de control.

En los switches Catalyst 4500/4000, 5500/5000 y 6500/6000 con la versión 5.1 y versiones posteriores de CatOS, puede tener varias sesiones SPAN simultáneas. Vea las secciones Creación de Varias Sesiones Simultáneas y Limitaciones y Resumen de Funciones de este documento.

Error "% Local Session Limit Has Been Exceeded"

Este mensaje aparece cuando la sesión SPAN permitida sobrepasa el límite para el Supervisor Engine:

```
% Local Session limit has been exceeded
```

Los Supervisor Engine tienen un límite de sesiones SPAN. Consulte la sección Límites de sesión de SPAN Local, RSPAN y ERSPAN de Configuración de SPAN Local, RSPAN and ERSPAN para obtener más información.

No se Puede Eliminar una Sesión SPAN en el Módulo de Servicio VPN, con el Error "% Session [Session No:] Used by Service Module"

Con este problema, el módulo de Red Privada Virtual (VPN) se inserta en el chasis, donde ya se ha insertado un módulo switch fabric. Cisco IOS Software crea automáticamente una sesión SPAN para el módulo de servicio VPN para gestionar el tráfico multicast.

Ejecute este comando para eliminar la sesión SPAN que crea el software para el módulo de servicio VPN:

```
Switch(config)#no monitor session session_number service-module
```

Nota: Si se elimina la sesión, el módulo de servicio VPN descarta el tráfico multidifusión.

¿Por qué No se Puede Capturar Paquetes Dañados con SPAN?

No es posible capturar paquetes dañados con SPAN debido a la manera en que funcionan los switches en general. Cuando un paquete atraviesa un switch, este evento tiene lugar.

1. El paquete alcanza el puerto de ingreso.
2. El paquete se almacena al menos en un buffer.
3. El paquete se retransmite finalmente al puerto de salida.

Si el switch recibe un paquete dañado, el puerto de ingreso, por lo general, lo descarta. Por lo tanto, no se ve el paquete en el puerto de salida. Un switch no es totalmente transparente en lo que se refiere a la captura de tráfico. De manera similar, cuando se ve un paquete corrupto en el sniffer en la situación descrita en esta sección, se sabe que los errores fueron generados en el paso 3 en el segmento de salida.

Si cree que un dispositivo envía paquetes dañados, puede optar por colocar el host remitente y el sniffer en un concentrador. El concentrador no realiza ninguna comprobación de errores. Por lo tanto, a diferencia del switch, el concentrador no descarta los paquetes. De esta manera, puede visualizar los paquetes.

Error: % de la sesión 2 utilizada por el módulo de servicio

Si, por ejemplo, se instaló en el CAT6500 un Módulo de servicio firewall (FWSM) y después se quitó, entonces se habilitó automáticamente la **función SPAN**. La función Reflector de SPAN utiliza una sesión SPAN en el Switch. Si ya no lo necesita, debe poder no ingresar el comando **no monitor session service module desde el modo de configuración del CAT6500 y, a continuación, ingresar inmediatamente la nueva configuración de SPAN deseada.**

El Puerto Reflector Descarta Paquetes

Un puerto reflector recibe copias del tráfico enviado y recibido para todos los puertos de origen monitoreados. Si un puerto reflector tiene exceso de suscriptores, podría congestionarse. Esto podría afectar al reenvío de tráfico en uno o más de los puertos de origen. Si el ancho de banda del puerto reflector no es suficiente para el volumen de tráfico de los puertos de origen correspondientes, los paquetes excedentes se descartan. Un puerto 10/100 refleja a 100 Mbps. Un puerto Gigabit refleja a 1 Gbps.

La Sesión SPAN Siempre se Utiliza con un FWSM en el Chasis Catalyst 6500

Cuando se utiliza el Supervisor Engine 720 con un FWSM en el chasis que ejecuta Cisco Native IOS, de forma predeterminada se utiliza una sesión SPAN. Si busca sesiones no utilizadas con el **comando show monitor, se utiliza la** *sesión 1:*

```
Cat6K#show monitor
Session 1
---------
Type : Service Module Session
```

Cuando un blade firewall está en el chasis del Catalyst 6500, esta sesión se instala automáticamente para el soporte de la replicación de multicast de hardware, porque un FWSM no puede replicar secuencias multicast. Si las secuencias multicast originadas detrás del FWSM se deben replicar en la Capa 3 a varias tarjetas de línea, la sesión automática copia el tráfico al supervisor a través de un canal fabric.

Si tiene un origen multicast que genere una secuencia multicast desde detrás del FWSM, necesita el reflector SPAN. Si coloca el origen multicast en la VLAN exterior, el reflector de SPAN no es necesario. El reflector de SPAN es incompatible con el bridging de BPDU a través del FWSM. No se puede utilizar el comando **no monitor session service module para inhabilitar el reflector de SPAN.**

¿Pueden una Sesión SPAN y RSPAN Tener el Mismo ID Dentro del Mismo Switch?

No, no es posible utilizar el mismo ID de sesión para una sesión SPAN regular y una sesión de destino RSPAN. Cada sesión SPAN y RSPAN deben tener un ID de sesión diferentes.

¿Puede una Sesión RSPAN Funcionar a Través de Diversos Dominios VTP?

Yes. Una sesión RSPAN puede atravesar diferentes dominios VTP. No obstante, asegúrese de que la VLAN RSPAN esté presente en las bases de datos de estos dominios VTP. También debe asegurarse de que no haya ningún dispositivo de la Capa 3 presente en la trayectoria de la sesión de origen a la sesión de destino.

¿Puede una Sesión RSPAN Funcionar a Través de WAN o de Diferentes Redes?

No. La sesión RSPAN no puede cruzar ningún dispositivo de la Capa 3, dado que RSPAN es una función de LAN (Capa 2). Para monitorear el tráfico a través de una WAN o de diferentes redes, utilice el Analizador de switchport remoto encapsulado (ERSPAN). La función ERSPAN soporta puertos de origen, VLAN de origen y puertos de destino en diferentes switches, lo que proporciona monitoreo remoto de múltiples switches a través de la red.

ERSPAN consta de una sesión de origen ERSPAN, tráfico encapsulado GRE ERSPAN ruteable y una sesión de destino ERSPAN. Usted debe configurar por separado las sesiones de origen ERSPAN y las sesiones de destino en diferentes switches.

Actualmente, la función ERSPAN se soporta en:

- Supervisor 720 con PFC3B o PFC3BXL ejecutando Cisco IOS Software Release 12.2(18)SXE o posterior
- Supervisor 720 con el PFC3A que tiene la versión de hardware 3.2 o posterior y ejecuta Cisco IOS Software Release 12.2(18)SXE o posterior

Consulte Configuración de SPAN Local, SPAN Remoto (RSPAN) y RSPAN Encapsulado - Guía de Configuración de Catalyst 6500 Series Cisco IOS Software, 12.2SX para obtener más información sobre ERSPAN.

¿Puede una Sesión de Origen RSPAN y la Sesión de Destino Existir en el Mismo Switch de Catalyst?

No. El RSPAN no funciona cuando la sesión de origen RSPAN y la sesión del destino RSPAN están en el mismo switch.

Si se configura una sesión de origen de RSPAN con una VLAN RSPAN determinada y una sesión de destino RSPAN para esa VLAN RSPAN en el mismo switch, el puerto de destino de la sesión de destino RSPAN no transmitirá los paquetes capturados de la sesión de origen de RSPAN debido a las limitaciones del hardware. Esto no se soporta en los Switches de las Series 4500 y

3750. Este problema se documenta en el Id. de bug Cisco CSCeg08870 (solo clientes registrados).

Aquí tiene un ejemplo:

```
monitor session 1 source interface Gi6/44
monitor session 1 destination remote vlan 666
monitor session 2 destination interface Gi6/2
monitor session 2 source remote vlan 666
```

La solución alternativa para este problema es utilizar SPAN normal.

El Analizador de Red/Dispositivo de Seguridad Conectado al Puerto de Destino SPAN no es Accesible

La característica básica de un puerto de destino de SPAN es que no transmite ningún tráfico excepto el tráfico requerido para la sesión SPAN. Si necesita alcanzar (alcance IP) el analizador de red/dispositivo de seguridad a través del puerto destino de SPAN, necesita habilitar el reenvío del tráfico de entrada.

Cuando se habilita la entrada, el puerto destino de SPAN acepta los paquetes entrantes, que potencialmente se marcan con etiqueta que depende del modo de encapsulación especificado, y los conmuta normalmente. Cuando se configura un puerto destino de SPAN, se puede especificar si la función de entrada está habilitada y qué VLAN utilizar para conmutar los paquetes de entrada sin etiqueta. La especificación de una VLAN de entrada no es necesaria cuando se configura la encapsulación ISL, dado que todos los paquetes encapsulados ISL tienen etiquetas VLAN. Aunque el puerto haga reenvío STP, no participa en el STP, así que debe tener cuidado cuando configure esta función para no introducir un bucle spanning-tree en la red. Cuando se especifica tanto la entrada como una encapsulación trunk en un puerto de destino SPAN, el puerto va reenviando a todas las VLAN activas. La configuración de una VLAN inexistente como VLAN de entrada no se permite.

monitor session ***session_number destination interface interface [encapsulation {isl*** **| dot1q}] ingreso [vlan** ***vlan_IDs*****]**

Este ejemplo muestra cómo configurar un puerto de destino con encapsulación 802.1q y paquetes de ingreso con el uso de la VLAN nativa 7.

```
Switch(config)#monitor session 1 destination interface fastethernet 5/48
encapsulation dot1q ingress vlan 7
```

Con esta configuración, el tráfico de los orígenes de SPAN asociados con la sesión 1 se copian de la interfaz Fast Ethernet 5/48, con encapsulación 802.1q. El tráfico de entrada se acepta y se conmuta; los paquetes sin etiquetas se clasifican en VLAN 7.

Información Relacionada

- Cómo configurar SPAN y RSPAN en los Switches Cisco Catalyst 4500 que ejecutan Cisco IOS Software
- Un puerto de destino de SPAN se muestra como "no conectado" y no se comunica con el resto de la red

- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems