

# Configurar o Catalyst Switched Port Analyzer (SPAN): Exemplo

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Catalyst Switches que Suportam SPAN, RSPAN e ERSPAN](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Breve descrição de amplitude](#)

[Terminologia de SPAN](#)

[Características da Porta de Origem](#)

[Características da VLAN de Origem](#)

[Características da Porta de Destino](#)

[Características da Porta Refletora](#)

[SPAN no Catalyst Express 500/520](#)

[SPAN nos Switches Catalyst 2900XL/3500XL](#)

[Recursos Disponíveis e Restrições](#)

[Exemplo de configuração](#)

[Diagrama de Rede](#)

[Exemplo de configuração do Catalyst 2900XL/3500XL](#)

[Explicação das Etapas de Configuração](#)

[SPAN no Catalyst 2948G-L3 e 4908G-L3](#)

[SPAN no Catalyst 8500](#)

[SPAN no Catalyst 2900, 4500/4000, 5500/5000 e 6500/6000 Series Switches que Executam o CatOS](#)

[SPAN local](#)

[PSPAN, VSPAN: Monitore algumas portas ou uma VLAN inteira](#)

[Monitore uma porta única com SPAN](#)

[Monitorar várias portas com SPAN](#)

[Monitorar VLANs com SPAN](#)

[SPAN de Entrada/Saída](#)

[Implementando SPAN em um tronco](#)

[Monitorar um subconjunto de VLANs pertencentes a um tronco](#)

[Truncamento da Porta de Destino](#)

[Crie diversas sessões simultâneas](#)

[Outras Opções de SPAN](#)

[SPAN remoto](#)

[Visão geral de RSPAN](#)

[Exemplo de configuração de RSPAN](#)

[Configuração do Tronco ISL entre os Dois Switches S1 e S2](#)

[Criação da VLAN de RSPAN](#)

[Configuração da Porta 5/2 de S2 como uma Porta de Destino RSPAN](#)

---

[Configuração de uma Porta de Origem RSPAN em S1](#)

[Verificar a configuração](#)

[Outras Configurações Possíveis com o Comando set rspan](#)

[Resumo de recursos e limitações](#)

[SPAN no Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E Series Switches](#)

[SPAN no Catalyst 4500/4000 e Catalyst 6500/6000 Series Switches que Executam o Cisco IOS System Software](#)

[Exemplo de configuração](#)

[Resumo de recursos e limitações](#)

[Impacto no desempenho de SPAN nas diferentes plataformas do Catalyst](#)

[Catalyst 2900XL/3500XL Series](#)

[Visão geral da arquitetura](#)

[Impacto de desempenho](#)

[Catalyst 4500/4000 Series](#)

[Visão geral da arquitetura](#)

[Impacto de desempenho](#)

[Catalyst 5500/5000 e 6500/6000 Series](#)

[Visão geral da arquitetura](#)

[Impacto de desempenho](#)

[Perguntas freqüentes e problemas comuns](#)

[Problemas de conectividade devido ao erro de configuração do SPAN](#)

[Porta de Destino Superior/Inferior de SPAN](#)

[Por que a Sessão de SPAN Cria um Loop de Bridging?](#)

[O SPAN afeta o desempenho?](#)

[É possível configurar SPAN em uma porta EtherChannel?](#)

[É Possível Ter Várias Sessões de SPAN em Execução ao Mesmo Tempo?](#)

[Erro "% Limite de Sessão Local Excedido"](#)

[Não é Possível Excluir uma Sessão de SPAN no Módulo de Serviço de VPN, com o Erro "% Sessão \[Nº da Sessão:\] Utilizada pelo Módulo de Serviço"](#)

[Por que Não é Possível Captar Pacotes Corrompidos com SPAN?](#)

[Erro : % Sessão 2 usada pelo módulo de serviço](#)

[A Porta Refletores Descarta Pacotes](#)

[A Sessão de SPAN é Sempre Utilizada com um FWSM no Catalyst 6500 Chassis](#)

[Uma Sessão de SPAN e de RSPAN Podem Ter o Mesmo ID Dentro do Mesmo Switch?](#)

[Uma Sessão de RSPAN Pode Funcionar em Domínios Diferentes de VTP?](#)

[Uma Sessão de RSPAN Pode Funcionar em WAN ou em Redes Diferentes?](#)

[Uma Sessão de Origem e a Sessão de Destino de RSPAN Podem Existir no Mesmo Catalyst Switch?](#)

[O Analisador de Rede/Dispositivo de Segurança Conectado à Porta de Destino de SPAN Não Pode Ser Alcançado](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve os recursos recentes do Switched Port Analyzer (SPAN) que foram implementados.

# Pré-requisitos

## Catalyst Switches que Suportam SPAN, RSPAN e ERSPAN

Catalyst Switches	Suporte a SPAN	Suporte a RSPAN	Suporte a ERSPAN
Catalyst Express 500/520 Series	Yes	No	No
Catalyst 6500/6000 Series	Yes	Yes	Sim Supervisor 2T com PFC4, Supervisor 720 com PFC3B ou PFC3BXL executando o Cisco IOS Software Release 12.2(18)SXE ou posterior. Supervisor 720 com PFC3A que tenha o hardware na versão 3.2 ou posterior e que esteja executando o Cisco IOS Software Release 12.2(18)SXE ou posterior
Catalyst 5500/5000 Series	Yes	No	No
Catalyst 4900 Series	Yes	Yes	No
Catalyst 4500/4000 Series (inclui 4912G)	Yes	Yes	No
Catalyst 3750 Metro Series	Yes	Yes	No
Catalyst séries 3750/3750E/3750X	Yes	Yes	No
Catalyst das séries 3560/3560E/3650X	Yes	Yes	No
Catalyst 3550 Series	Yes	Yes	No
Catalyst 3500 XL Series	Yes	No	No
Catalyst 2970 Series	Yes	Yes	No
Catalyst 2960 Series	Yes	Yes	No
Catalyst 2955 Series	Yes	Yes	No
Catalyst 2950 Series	Yes	Yes	No
Catalyst 2940 Series	Yes	No	No
Catalyst 2948G-L3	No	No	No
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A	Yes	Yes	No
Catalyst 2900XL Series	Yes	No	No

Catalyst 1900 Series	Yes	No	No
----------------------	-----	----	----

## Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

Estas informações neste documento usam o CatOS 5.5 como referência para os Switches das séries Catalyst 4500/4000, 5500/5000 e 6500/6000. Nos Catalyst 2900XL/3500XL Series Switches, o Cisco IOS<sup>®</sup> Software Release 12.0(5)XU é usado.

Embora este documento seja atualizado para refletir as alterações em SPAN, consulte as notas da versão da documentação da plataforma do switch para conhecer os desenvolvimentos mais recentes relacionados ao recurso SPAN.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O recurso SPAN, que às vezes é chamado de espelhamento de porta ou monitoramento de porta, seleciona o tráfego de rede para análise por um analisador de rede. O analisador de rede pode ser um dispositivo Cisco SwitchProbe ou outra sonda de monitoração remota (RMON).

Anteriormente, o SPAN era um recurso relativamente básico dos Cisco Catalyst Series Switches. Contudo, as versões mais recentes do Catalyst OS (CatOS) introduziram grandes aprimoramentos e muitas novas possibilidades que agora estão disponíveis para o usuário.

O objetivo deste documento não é ser um guia de configuração alternativo para o recurso SPAN. Este documento responde às perguntas mais comuns sobre SPAN, como:

- O que é SPAN e como configurá-lo?
- Quais são os diferentes recursos disponíveis (especialmente sessões de SPAN múltiplas e simultâneas) e qual nível de software é necessário para executá-los?
- O SPAN afeta o desempenho do switch?

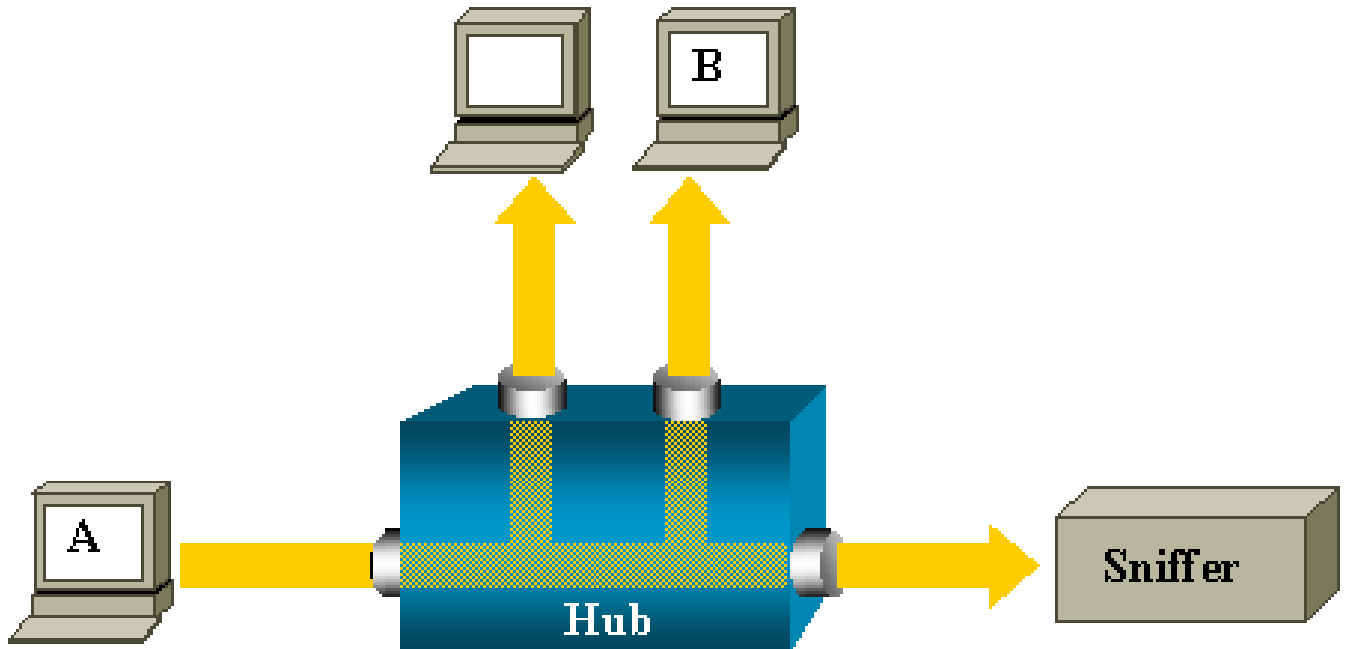
## Breve descrição de amplitude

O recurso SPAN foi introduzido em switches devido a uma diferença fundamental entre switches e hubs. Quando um hub recebe um pacote em uma porta, ele envia uma cópia desse pacote em todas as portas, exceto na porta em que ele recebeu o pacote.

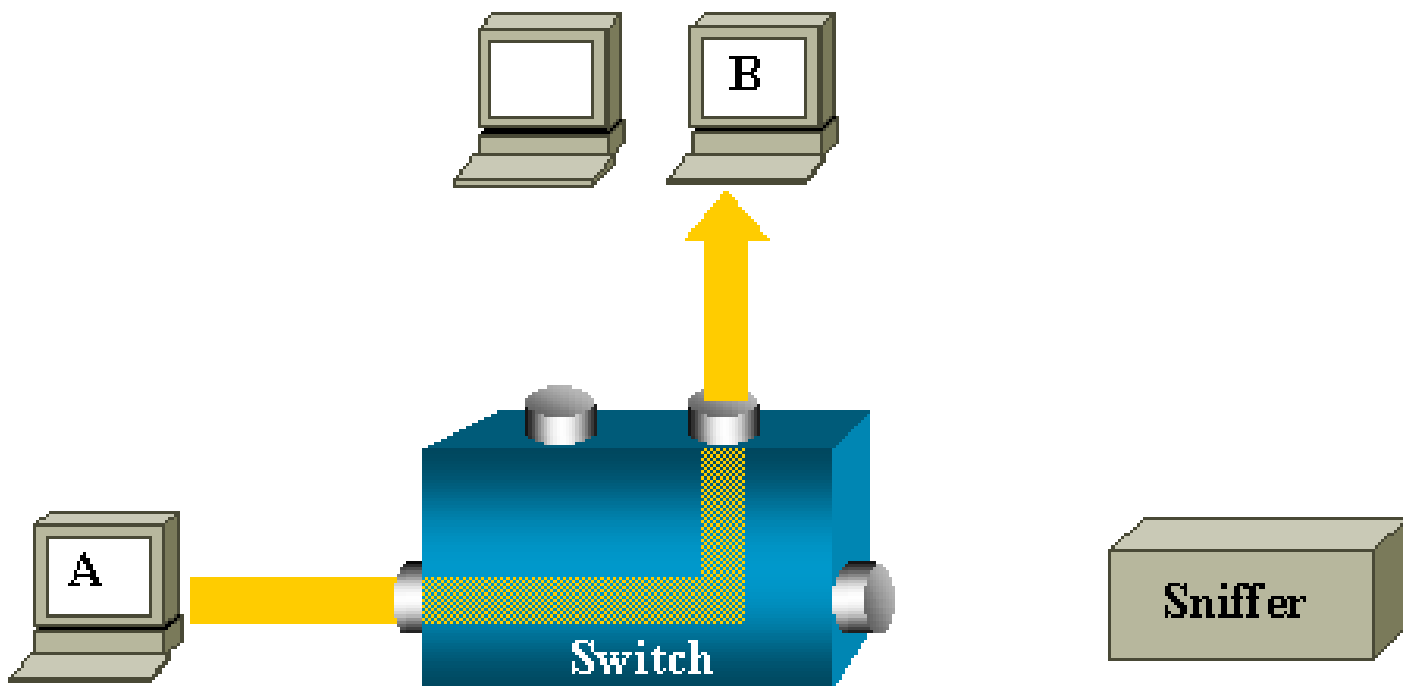
Após a inicialização de um switch, ele começa a criar uma tabela de encaminhamento da

Camada 2 com base no endereço MAC de origem dos diferentes pacotes recebidos pelo switch. Após a criação dessa tabela de encaminhamento, o switch encaminha o tráfego que é destinado a um endereço MAC diretamente para a porta correspondente.

Por exemplo, para capturar o tráfego Ethernet que é enviado pelo host A ao host B, e ambos estão conectados a um hub, simplesmente conecte um farejador a esse hub. Todas as outras portas veem o tráfego entre os hosts A e B:



Em um switch, depois que o endereço MAC do host B for conhecido, o tráfego de unicast de A para B será encaminhado apenas para a porta B. Desse modo, o farejador não verá esse tráfego:



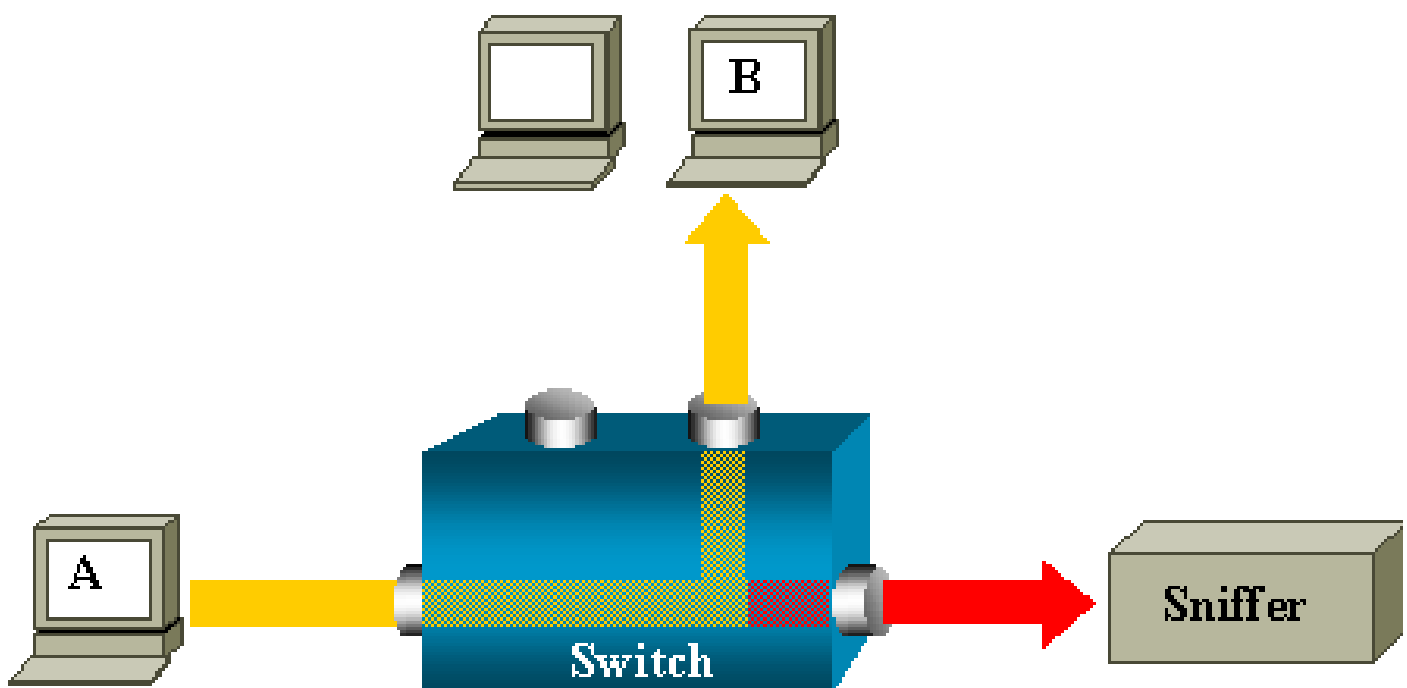
Nessa configuração, o farejador somente capta o tráfego que é inundado em todas as portas, como:

- Tráfego de broadcast
- Tráfego de multicast com CGMP ou com o snooping do Internet Group Management Protocol (IGMP) desabilitado.
- Tráfego de unicast desconhecido

A inundação de unicast ocorre quando o switch não tem o MAC de destino em sua tabela CAM (Content Addressable Memory).

O switch não sabe para onde enviar o tráfego. O switch inunda os pacotes a todas as portas na VLAN de destino.

É necessário ter um recurso extra que copie artificialmente os pacotes de unicast que o host A envia à porta do farejador:



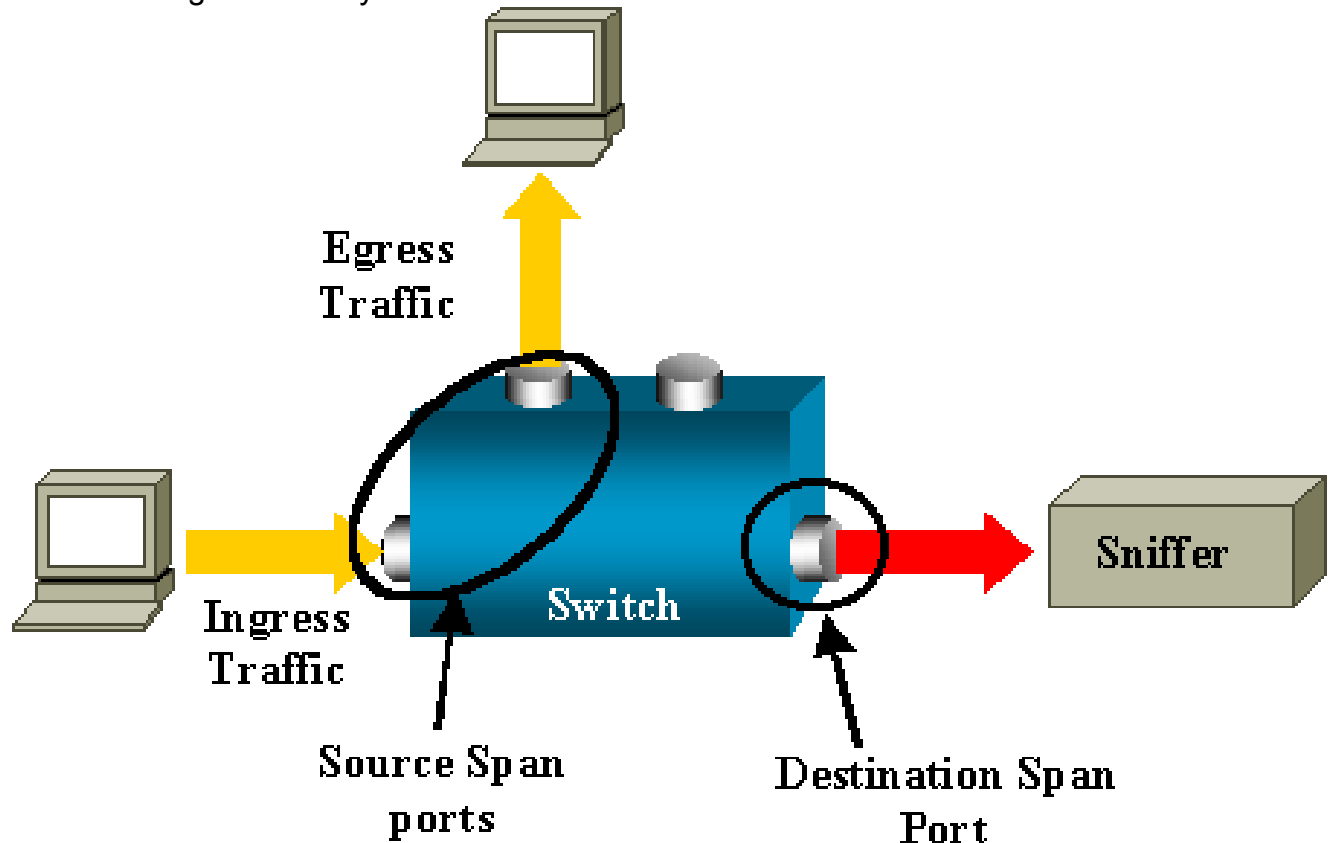
Neste diagrama, o farejador é anexado a uma porta que está configurada para receber uma cópia de cada pacote enviado pelo host A. Essa porta é chamada de porta SPAN.

As outras seções deste documento descrevem como você pode ajustar esse recurso de maneira muito precisa para fazer mais do que apenas monitorar uma porta.

## Terminologia de SPAN

- Tráfego de entrada — Tráfego que entra no switch.
- Tráfego de saída — Tráfego que sai do switch.
- [Porta \(SPAN\) de origem](#) — Uma porta é monitorada com o uso do recurso SPAN.
- [VLAN \(SPAN\) de origem](#) — Uma VLAN cujo tráfego é monitorado com o uso do recurso SPAN.

- [Porta \(SPAN\) de destino](#) — Uma porta que monitora as portas de origem, geralmente onde um analisador de rede é conectado.
- [Porta Refletores](#) — Uma porta que copia os pacotes em uma VLAN de RSPAN.
- Porta de monitoração — Uma porta de monitoração também é uma porta SPAN de destino na terminologia do Catalyst 2900XL/3500XL/2950.



- SPAN Local — O recurso SPAN é local quando as portas monitoradas estão todas localizadas no mesmo switch da porta de destino. Esse recurso é o oposto do SPAN Remoto (RSPAN, Remote SPAN), também definido nesta lista.
- SPAN Remoto (RSPAN) — Algumas portas de origem não estão localizadas no mesmo switch da porta de destino.

O RSPAN é um recurso avançado que exige uma VLAN especial para levar o tráfego monitorado pelo SPAN entre os switches.

O RSPAN não é suportado em todos os switches. Verifique as respectivas notas de versão ou o manual de configuração para ver se você pode usar o RSPAN no switch implantado.

- SPAN com base em porta (PSPAN) — O usuário especifica uma ou várias portas de origem no switch e uma porta de destino.
- SPAN com base em VLAN (VSPAN) — Em um switch específico, o usuário pode escolher monitorar todas as portas que pertencem a uma VLAN específica em um único comando.
- ESPAN — Uma versão de SPAN aprimorada. Esse termo foi usado várias vezes durante a

evolução do SPAN para nomear recursos adicionais, portanto, o termo não é muito claro e é evitado neste documento.

- Origem administrativa — Uma lista de portas ou VLANs de origem que foram configuradas para serem monitoradas.
- Origem operacional — Uma lista de portas que são monitoradas de maneira efetiva. Essa lista de portas pode ser diferente da origem administrativa.

Por exemplo, uma porta que estiver no modo de fechamento pode aparecer na fonte administrativa, mas não é efetivamente monitorada.

## Características da Porta de Origem

Uma porta de origem, também chamada de porta monitorada, é uma porta comutada ou roteada que você monitora para a análise do tráfego da rede.

Em uma sessão de SPAN local simples ou uma sessão de origem se RSPAN, você pode monitorar o tráfego de porta de origem, como o tráfego recebido (Rx), transmitido (Tx) ou bidirecional (ambos).

O switch suporta qualquer número de portas de origem (até o número máximo de portas disponíveis no switch) e qualquer número VLANs de origem.

Uma porta de origem apresenta as seguintes características:

- Pode ser qualquer tipo de porta, como EtherChannel, Fast Ethernet, Gigabit Ethernet, e assim por diante.
- Pode ser monitorada em sessões de SPAN múltiplas.
- Não pode ser uma porta de destino.
- Cada porta de origem pode ser configurada com uma direção (entrada, saída ou ambos) para monitoração. Para origens EtherChannel, a direção monitorada se aplica a todas as portas físicas no grupo.
- As portas de origem podem estar na mesma VLAN ou em VLANs diferentes.
- Para as origens de SPAN da VLAN, todas as portas ativas na VLAN de origem são incluídas como portas de origem.

## Filtragem de VLAN

Quando você monitora uma porta de tronco como uma porta de origem, todas as VLANs ativas no tronco são monitoradas como padrão. Você pode usar a filtragem de VLAN para limitar a monitoração de tráfego de SPAN nas portas de origem do tronco para VLANs específicas.

- A filtragem de VLAN se aplica somente a portas de tronco ou a portas de VLAN de voz.



- A filtragem de VLAN se aplica somente a sessões com base em porta e não é permitida em sessões com origens de VLAN.
- Quando é especificada uma lista de filtros de VLAN, somente as VLANs na lista são monitoradas em portas de tronco ou em portas de acesso de VLAN de voz.
- O tráfego de SPAN que chega de outros tipos de porta não é afetado pela filtragem de VLAN, o que significa que todas as VLANs são permitidas em outras portas.
- A filtragem de VLAN afeta somente o tráfego encaminhado para a porta de SPAN de destino e não afeta a comutação do tráfego normal.
- Você não pode combinar VLANs de origem e filtrar VLANs dentro de uma sessão. Você pode ter VLANs de origem ou filtrar VLANs, mas não ao mesmo tempo.

## Características da VLAN de Origem

O VSPAN é a monitoração do tráfego da rede em uma ou mais VLANs. A interface de origem SPAN ou RSPAN no VSPAN é um ID de VLAN, e o tráfego é monitorado em todas as portas para essa VLAN.

O VSPAN apresenta as seguintes características:

- Todas as portas ativas na VLAN de origem são incluídas como portas de origem e podem ser monitoradas em quaisquer ou ambas as direções.
- Em uma determinada porta, somente o tráfego na VLAN monitorada é enviado à porta de destino.
- Se uma porta de destino pertence a uma VLAN de origem, ela é excluída da lista de origem e não é monitorada.
- Se portas forem adicionadas ou removidas das VLANs de origem, o tráfego na VLAN de origem recebido por essas portas será adicionado ou removido das origens que são monitoradas.
- Não é possível usar o filtro de VLANs na mesma sessão com origens de VLAN.
- É possível monitorar somente as VLANs de Ethernet.

## Características da Porta de Destino

Cada sessão de SPAN local ou sessão de destino de RSPAN deve ter uma porta de destino (também chamada de porta de monitoração) que recebe uma cópia do tráfego das portas de origem e das VLAN.


Uma porta de destino apresenta as seguintes características:

- Uma porta de destino deve estar no mesmo switch que a porta de origem (para uma sessão

de SPAN local).

- Uma porta de destino pode ser qualquer porta física de Ethernet.
- Uma porta de destino pode participar de somente uma sessão de SPAN por vez. Uma porta de destino em uma sessão de SPAN não pode ser uma porta de destino para uma segunda sessão de SPAN.
- Uma porta de destino não pode ser uma porta de origem.
- Uma porta de destino não pode ser um grupo EtherChannel.

---

 Observação: do Cisco IOS Software Release 12.2(33)SXH e posterior, a interface PortChannel pode ser uma porta de destino. Os EtherChannels de destino não suportam os protocolos EtherChannel Port Aggregation Control Protocol (PAgP) ou Link Aggregation Control Protocol (LACP); somente o modo ativado é suportado, com todo o suporte ao protocolo EtherChannel desativado.

---

 Observação: consulte [Destinos locais de SPAN, RSPAN e ERSPAN](#) para obter mais informações.

---

- Uma porta de destino pode ser uma porta física atribuída a um grupo EtherChannel, mesmo se o grupo EtherChannel tiver sido especificado como uma origem de SPAN. A porta será removida do grupo enquanto ela estiver configurada como uma porta de destino de SPAN.
- A porta não transmitirá tráfego, exceto o tráfego necessário para a sessão de SPAN, a menos que a aprendizagem esteja habilitada. Se a aprendizagem estiver habilitada, a porta também transmitirá o tráfego direcionado aos hosts que foram conhecidos na porta de destino.

---

 Observação: consulte [Destinos locais de SPAN, RSPAN e ERSPAN](#) para obter mais informações.

---

- O estado da porta de destino é ativado/desativado por padrão. A interface mostra a porta nesse estado para tornar evidente que a porta não pode ser utilizada no momento como uma porta de produção.
- Se o encaminhamento de tráfego de entrada estiver habilitado para um dispositivo de segurança de rede. A porta de destino encaminha o tráfego na Camada 2.
- Uma porta de destino não participa da spanning tree enquanto a sessão de SPAN está ativa.
- Quando se trata de uma porta de destino, ela não participa de nenhum protocolo de Camada 2 (STP, VTP, CDP, DTP, PagP).
- Uma porta de destino que pertence a uma VLAN de origem de qualquer sessão de SPAN é

excluída da lista de origens e não é monitorada.

- Uma porta de destino recebe cópias do tráfego enviado e recebido para todas as portas de origem monitoradas. Se uma porta de destino receber um excesso de assinaturas, ela poderá ficar congestionada. Esse congestionamento poderá afetar o encaminhamento de tráfego em uma ou mais portas de origem.

## Características da Porta Refletora

A porta refletora é o mecanismo que copia pacotes em uma VLAN de RSPAN. A porta refletora encaminha somente o tráfego de uma sessão de origem de RSPAN com a qual ela está afiliada.

Os dispositivos conectados a uma porta definida como porta refletora perdem a conectividade até que a sessão de origem de RSPAN seja desabilitada.

A porta refletora apresenta as seguintes características:

- É uma porta definida para loopback.
- Ela não pode ser um grupo EtherChannel, não produz tronco e não pode fazer filtragem de protocolos.
- Ela poderá ser uma porta física atribuída a um grupo EtherChannel, mesmo se o grupo EtherChannel estiver especificado como uma origem de SPAN. A porta será removida do grupo enquanto ela estiver configurada como uma porta refletora.
- Uma porta utilizada como porta refletora não pode ser uma porta de origem ou de destino de SPAN, e uma porta não pode ser uma porta refletora para mais de uma sessão por vez.
- Ela é invisível para todas as VLANs.
- A VLAN nativa para o tráfego com loopback em uma porta refletora é a VLAN de RSPAN.
- A porta refletora faz o loopback do tráfego sem etiqueta para o switch. O tráfego é colocado na VLAN de RSPAN e inundado em todas as portas de tronco que transportam a VLAN de RSPAN.
- A spanning tree é desabilitada automaticamente em uma porta refletora.
- Uma porta refletora recebe cópias do tráfego enviado e recebido para todas as portas de origem monitoradas.

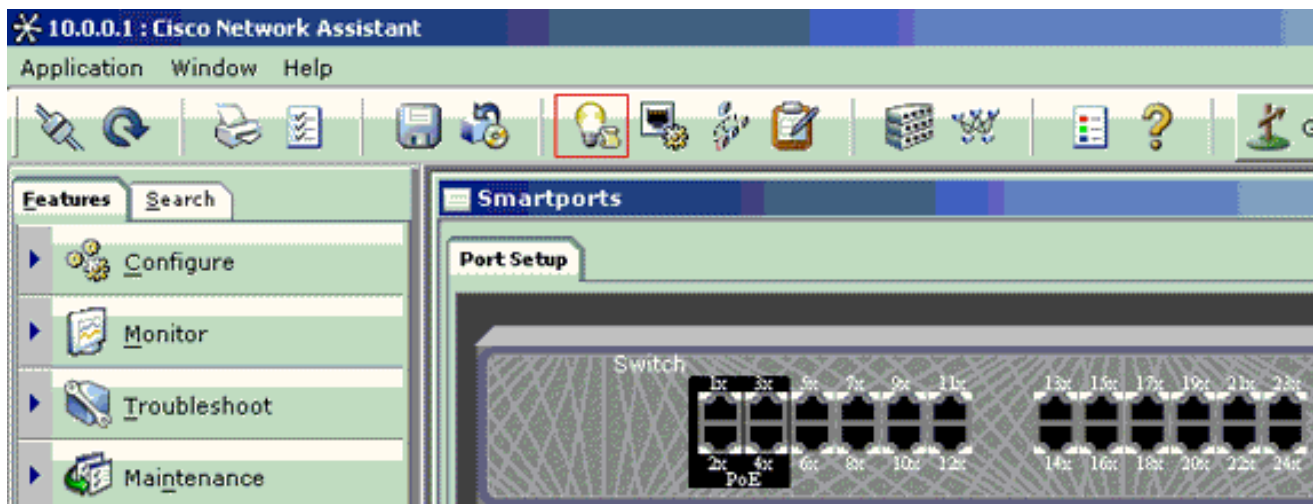
## SPAN no Catalyst Express 500/520

O Catalyst Express 500 ou Catalyst Express 520 suporta somente o recurso de SPAN. As portas do Catalyst Express 500/520 podem ser configuradas para SPAN somente com o uso do Cisco Network Assistant (CNA). Execute estas etapas para configurar o SPAN:

1. Faça download do CNA e instale-o no PC.

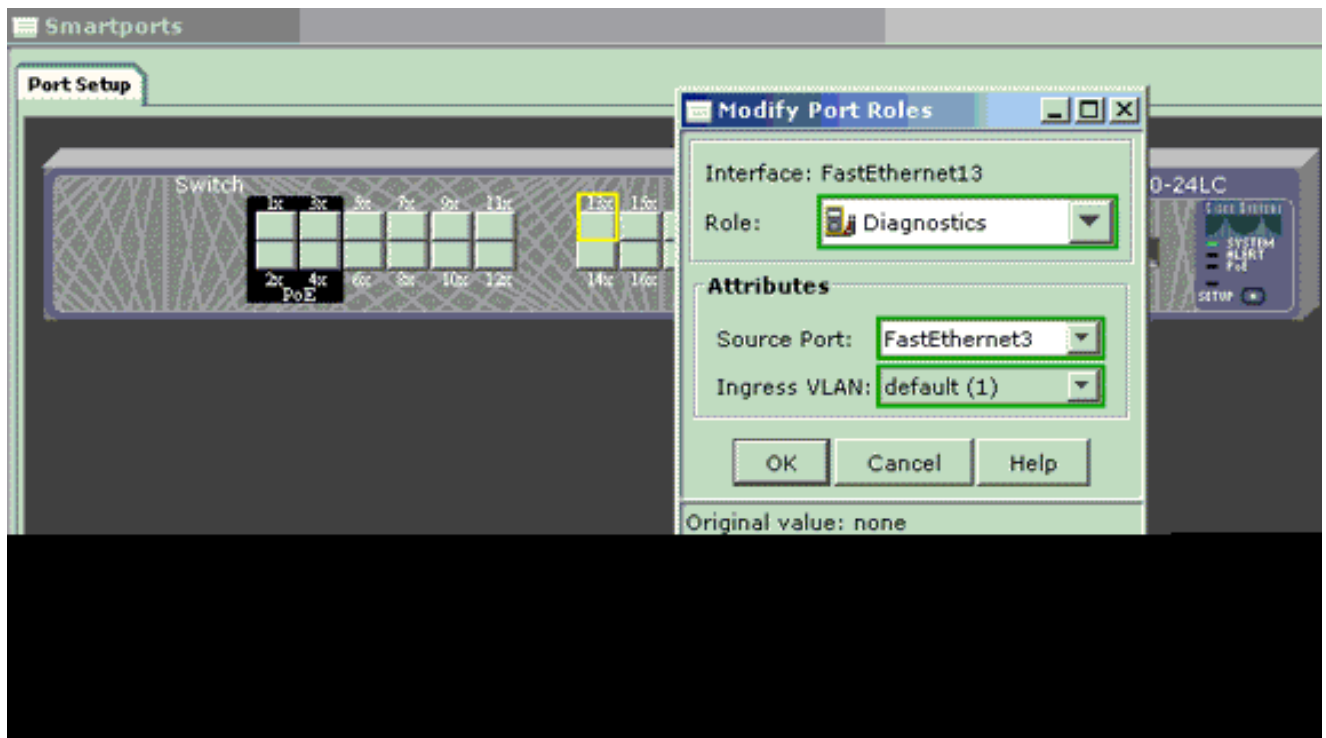
Você pode fazer download do CNA pela página Download de Software (somente clientes registrados).

2. Execute as etapas determinadas em [Guia de Introdução ao Catalyst Express 500 Switches 12.2\(25\)FY para personalizar as configurações de switch para o Catalyst Express 500](#). Consulte o [Guia de Introdução ao Catalyst Express 520 Switches para obter mais informações sobre o Catalyst Express 520](#).
3. Utilize o CNA para entrar no switch e clique em Smartport.



4. Clique em qualquer interface na qual você planeja conectar o PC para captar os rastreamentos do farejador.
5. Clique em Modify.  
  
Será exibida uma pequena caixa pop-up.
6. Escolha a função Diagnostics para a porta.
7. Escolha a porta de origem e selecione a VLAN que você planeja monitorar.

Se você não selecionar nenhuma, a porta somente receberá o tráfego. A VLAN de entrada permite que o PC conectado à porta de diagnóstico (Diagnostics) envie pacotes à rede que utiliza essa VLAN.



8. Clique em OK para fechar a caixa pop-up.
9. Clique em OK e em Apply para aplicar as configurações.
10. Você pode usar qualquer software farejador para rastrear o tráfego depois de configurar a porta de diagnóstico.

## SPAN nos Switches Catalyst 2900XL/3500XL

### Recursos Disponíveis e Restrições

O recurso de monitoração de portas não é muito abrangente no Catalyst 2900XL/3500XL. Desse modo, esse recurso é relativamente fácil de ser entendido.


Você pode criar quantas sessões PSPAN locais forem necessárias. Por exemplo, você pode criar sessões de PSPAN na porta de configuração que você escolheu para ser uma porta de SPAN de destino. Nesse caso, emita a interface do [monitor de porta](#) para listar as portas de origem que você deseja monitorar. Uma porta de monitoração é uma porta SPAN de destino na terminologia do Catalyst 2900XL/3500XL.

- A principal restrição é que todas as portas relacionadas a uma sessão particular (de origem ou de destino) devem pertencer à mesma VLAN.
- Se você configura a interface de VLAN com um endereço IP, o comando port monitor monitora o tráfego destinado apenas a esse endereço IP. Ele também monitora o tráfego de broadcast recebido pela interface de VLAN. Porém, ele não captura o tráfego que flui na própria VLAN real. Se você não especifica nenhuma interface no comando port monitor, todas as outras portas que pertencem à mesma VLAN que a interface são monitoradas.

Essa lista fornece algumas restrições. Consulte o guia de referência de comandos (Catalyst

2900XL/3500XL) para obter mais informações.

---

 Observação: as portas ATM são as únicas portas que não podem ser portas de monitoramento. Entretanto, é possível monitorar as portas ATM. As restrições dessa lista se aplicam a portas que possuem o recurso de monitoração de portas.

---

- Uma porta de monitor não pode estar em um grupo de portas Fast EtherChannel nem Gigabit EtheChanell.
- Uma porta de monitor não pode ser ativada para segurança da porta.
- Uma porta de monitor não pode ser uma porta de vários VLANs.
- Uma porta de monitoração deve ser um membro da mesma VLAN que a porta monitorada. As alterações de associação de VLAN estão desabilitadas nas portas de monitoração e nas portas que são monitoradas.
- Uma porta de monitoração não pode ser uma porta de acesso dinâmico ou uma porta de tronco. No entanto, uma porta de acesso estático pode monitorar uma VLAN em um tronco uma multi-VLAN ou uma porta de acesso dinâmico. A VLAN monitorada é aquela que está associada à porta de acesso estático.
- A monitoração de portas não funcionará se a porta de monitoração e a porta monitorada forem portas protegidas.

Tenha cuidado para que uma porta no estado de monitoração não execute o Spanning Tree Protocol (STP) enquanto ela ainda pertencer à VLAN das portas que ela espelha. O monitor da porta pode fazer parte de um loop se, por exemplo, você conectá-lo a um hub ou a uma bridge para outra parte da rede. Nesse caso, você pode acabar em uma condição de loop catastrófica, porque o STP não o protegerá mais. Consulte a seção [Por que a Sessão de SPAN Cria um Loop de Bridging?](#) deste documento para obter um exemplo de como essa condição pode acontecer.

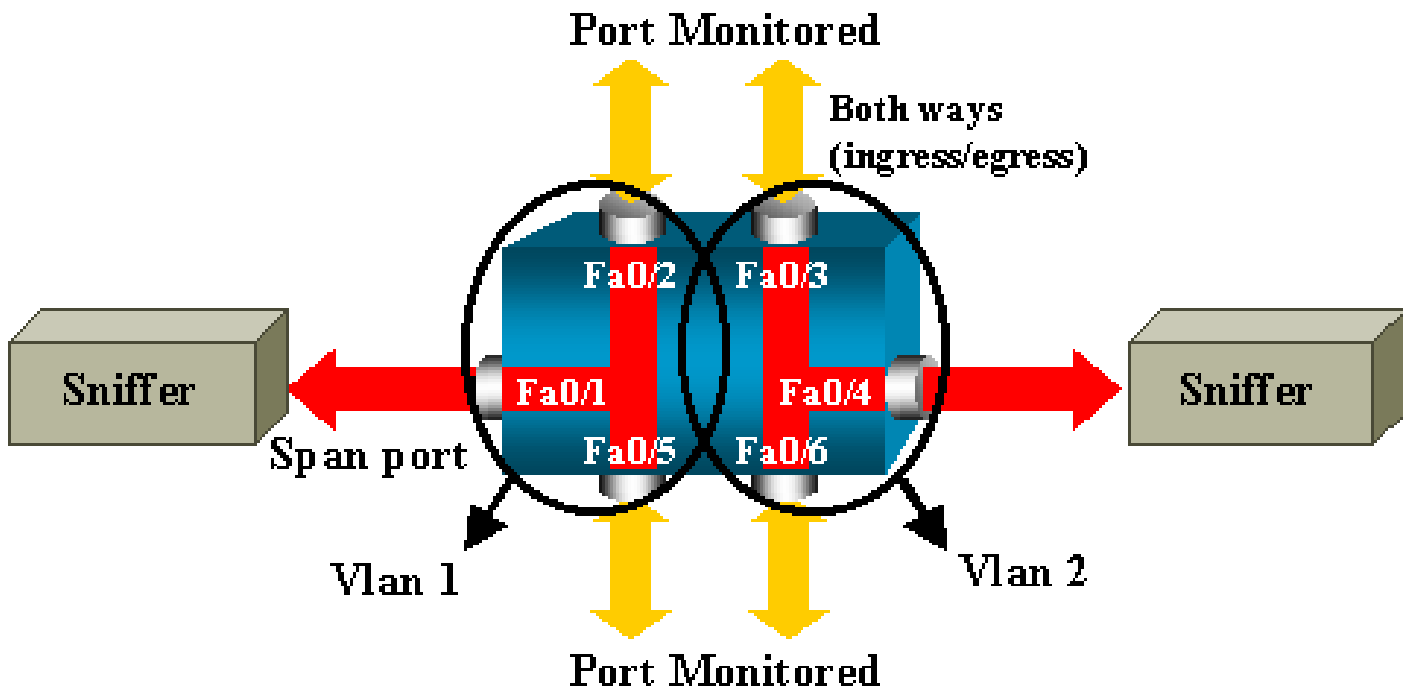
## Exemplo de configuração

Este exemplo cria duas sessões simultâneas de SPAN.

- A porta Fast Ethernet 0/1 (Fa0/1) monitora o tráfego que as portas Fa0/2 e Fa0/5 enviam e recebem. A porta Fa0/1 também monitora o tráfego de e para a interface de gerenciamento VLAN 1.
- A porta Fa0/4 monitora as portas Fa0/3 e Fa0/6.

As portas Fa0/3, Fa0/4 e Fa0/6 estão todas configuradas na VLAN 2. Outras portas e a interface de gerenciamento estão configuradas na VLAN 1 padrão.

## Diagrama de Rede



Exemplo de configuração do Catalyst 2900XL/3500XL

#### Exemplo de Configuração de 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.

```



## Explicação das Etapas de Configuração

Para configurar a porta Fa0/1 como uma porta de destino, as portas de origem Fa0/2 e Fa0/5 e a interface de gerenciamento (VLAN 1), selecione a interface Fa0/1 no modo de configuração:

```
<#root>  
Switch(config)#  
interface fastethernet 0/1
```


Insira a lista de portas a serem monitoradas:

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

Com esse comando, todos os pacotes recebidos ou transmitidos por essas duas portas também serão copiados para a porta Fa0/1. Emita uma variação do comando port monitor para configurar a monitoração para a interface administrativa:

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

---

 Observação: esse comando não significa que a porta Fa0/1 monitora a VLAN 1 inteira. A palavra-chave vlan 1 refere-se simplesmente à interface administrativa do switch.

---

Este exemplo de comando ilustra que a monitoração de uma porta em uma VLAN diferente é impossível:

```
<#root>  
Switch(config-if)#
```



```
port monitor fastethernet 0/3
```

FastEthernet0/1 and FastEthernet0/3 are in different vlan

Para concluir a configuração, configure outra sessão. Desta vez, use Fa0/4 como uma porta de SPAN de destino:

```
<#root>
```

```
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
```

Emita um comando show running ou use o comando show port monitor para verificar a configuração:


```
<#root>
```

```
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
```

---

 Observação: o Catalyst 2900XL e 3500XL não suportam SPAN somente na direção Rx (SPAN de Rx ou SPAN de ingresso) ou somente na direção Tx (SPAN de Tx ou SPAN de saída). Todas as portas de SPAN foram criadas para captar o tráfego de recebimento e de transmissão.

---

## SPAN no Catalyst 2948G-L3 e 4908G-L3

O Catalyst 2948G-L3 e o Catalyst 4908G-L3 são roteadores de configuração fixa ou switches de Camada 3. O recurso SPAN em um switch de Camada 3 é denominado espionagem de porta.

Porém, a espionagem de porta não é suportada nesses switches. Consulte a seção [Recursos Não Suportados do documento Notas de Versão do Catalyst 2948G-L3 e do Catalyst 4908G-L3 para Cisco IOS Software Release 12.0\(10\)W5\(18g\)](#).

## SPAN no Catalyst 8500

Um recurso muito básico do SPAN está disponível no Catalyst 8540 com o nome de espionagem de porta. Consulte a documentação atual do Catalyst 8540 para obter outras informações.

A espionagem de portas permite espelhar o tráfego de forma transparente de uma ou mais portas de origem para uma porta de destino".

Emita o comando snoop para configurar o espelhamento de tráfego com base em porta ou a espionagem. Emita a forma no desse comando para desabilitar a espionagem:

```
<#root>
```

```
snoop interface source_port direction snoop_direction
```

```
no snoop interface source_port
```

A variável source\_port se refere à porta monitorada. A variável snoop\_direction é a direção do tráfego na porta ou portas de origem que são monitoradas: receive, transmit ou both.

```
<#root>
```

```
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 exemplo mostra o resultado do comando show snoop:

```
<#root>
```

```
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)
```

---

 Observação: este comando não é suportado em portas Ethernet em um Catalyst 8540 se você executar uma imagem de roteador de switch ATM (MSR - ATM Switch Router) multisserviço, como 8540m-in-mz. Em vez disso, é preciso usar uma imagem de roteador de campus (CSR), como 8540c-in-mz.

---

## SPAN no Catalyst 2900, 4500/4000, 5500/5000 e 6500/6000 Series Switches que Executam o CatOS

Esta seção se aplica apenas aos seguintes Cisco Catalyst 2900 Series Switches:

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

Esta seção se aplica aos Cisco Catalyst 4000 Series Switches, que incluem:

- Switches de Chassis Modulares:
  - Cisco Catalyst 4003 Switch
  - Cisco Catalyst 4006 Switch
- Switch de Chassis Fixo:
  - Cisco Catalyst 4912G Switch

## SPAN local

Os recursos de SPAN foram adicionados um de cada vez ao CatOS, e uma configuração de SPAN consiste em um único comando `set span`. Agora há uma grande variedade de opções disponíveis para o comando:

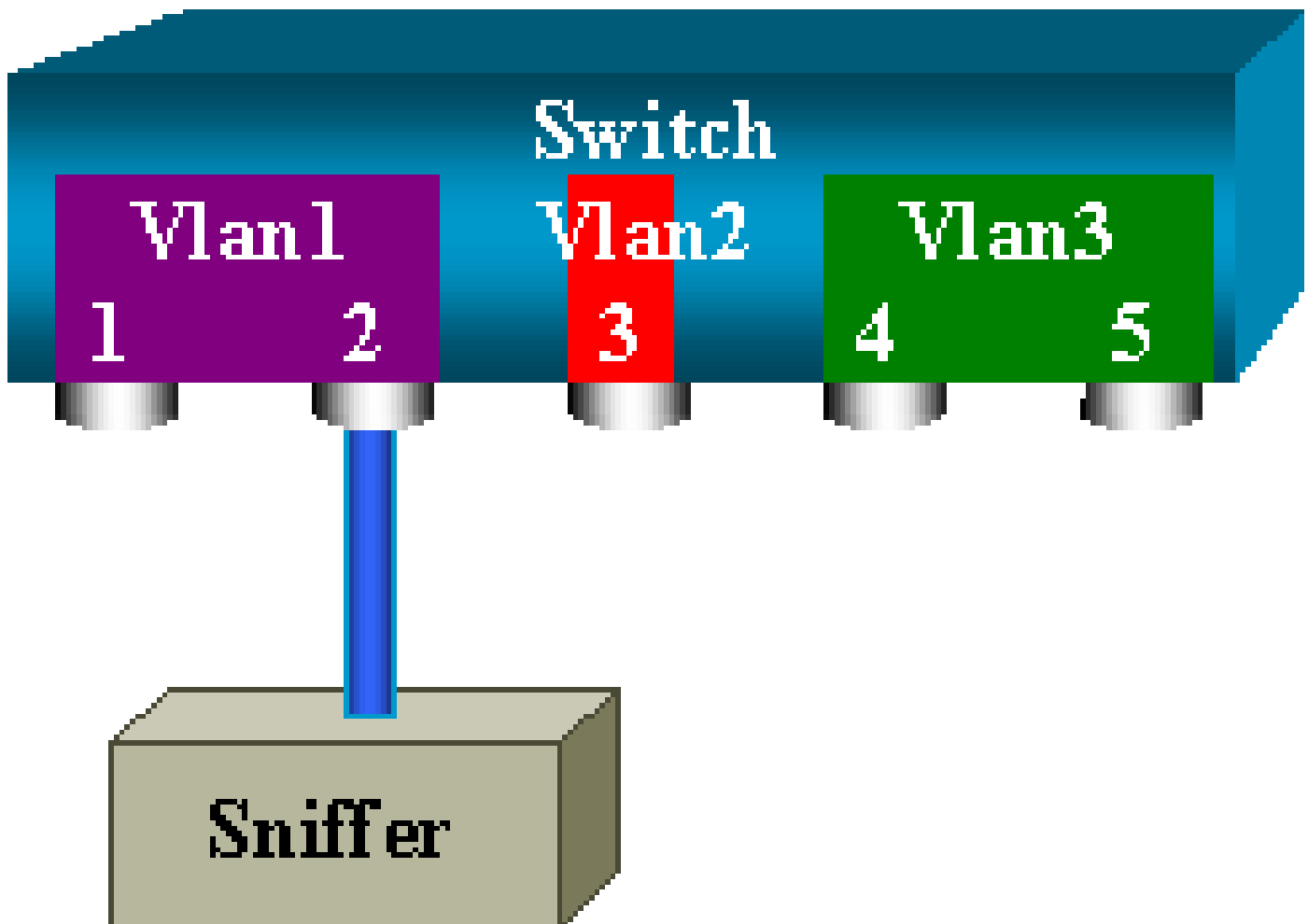
```
<#root>
```

```
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]
```

Este diagrama da rede apresenta as diferentes possibilidades de SPAN com o uso das variações:



Este diagrama representa parte de uma única placa de linha localizada no slot 6 de um Catalyst 6500/6000 Switch. Neste cenário:

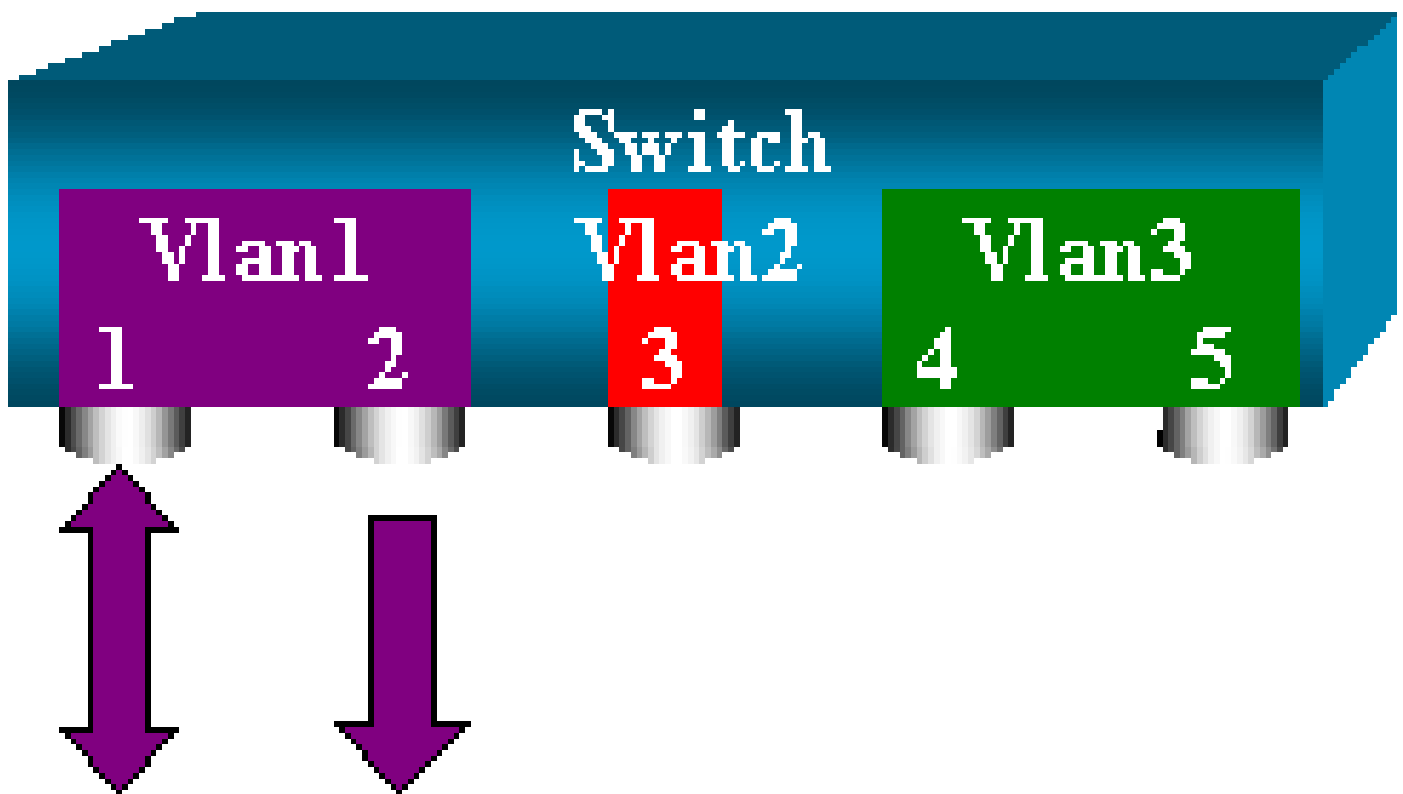
- As portas 6/1 e 6/2 pertencem à VLAN 1
- A porta 6/3 pertence à VLAN 2
- As portas 6/4 e 6/5 pertencem à VLAN 3

Conecte um farejador à porta 6/2 e utilize-o como uma porta de monitoração em diversos casos diferentes.

PSPAN, VSPAN: Monitore algumas portas ou uma VLAN inteira

Emita a forma mais simples do comando set span para monitorar uma única porta. A sintaxe é set span source\_port destination\_port .

Monitore uma porta única com SPAN



```
<#root>
```

```
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
```

Com essa configuração, cada pacote recebido ou enviado pela porta 6/1 é copiado na porta 6/2. Uma descrição clara disso aparece quando você insere a configuração. Emita o comando `show span` para receber um resumo da configuração de SPAN atual:

```
<#root>
```

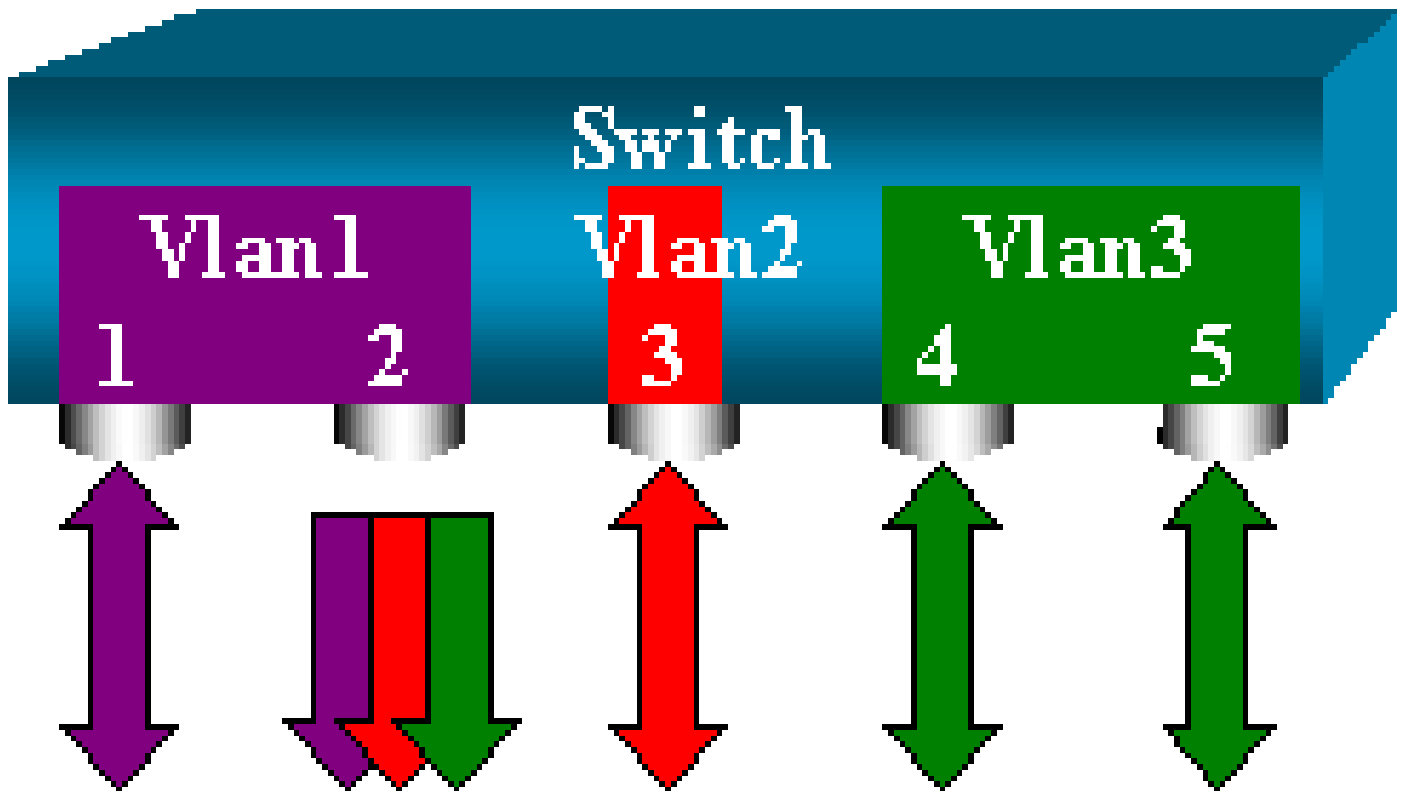
```
switch (enable)
```

```
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
```

Monitorar várias portas com SPAN




O comando `set span source_ports destination_port` permite que o usuário especifique mais de uma porta de origem. Basta listar todas as portas nas quais você deseja implementar o SPAN e para separá-las com vírgulas.

O intérprete da linha de comando também permite que você utilize o hífen para especificar um intervalo de portas.

Esse exemplo ilustra a capacidade de especificar mais de uma porta. O exemplo usa o SPAN na porta 6/1 e um intervalo de três portas, de 6/3 a 6/5:

---

 Observação: pode haver apenas uma porta de destino. Sempre especifique a porta de destino depois de uma origem de SPAN.

---

```
<#root>
```

```
switch (enable)
```

```
set span 6/1,6/3-5 6/2
```

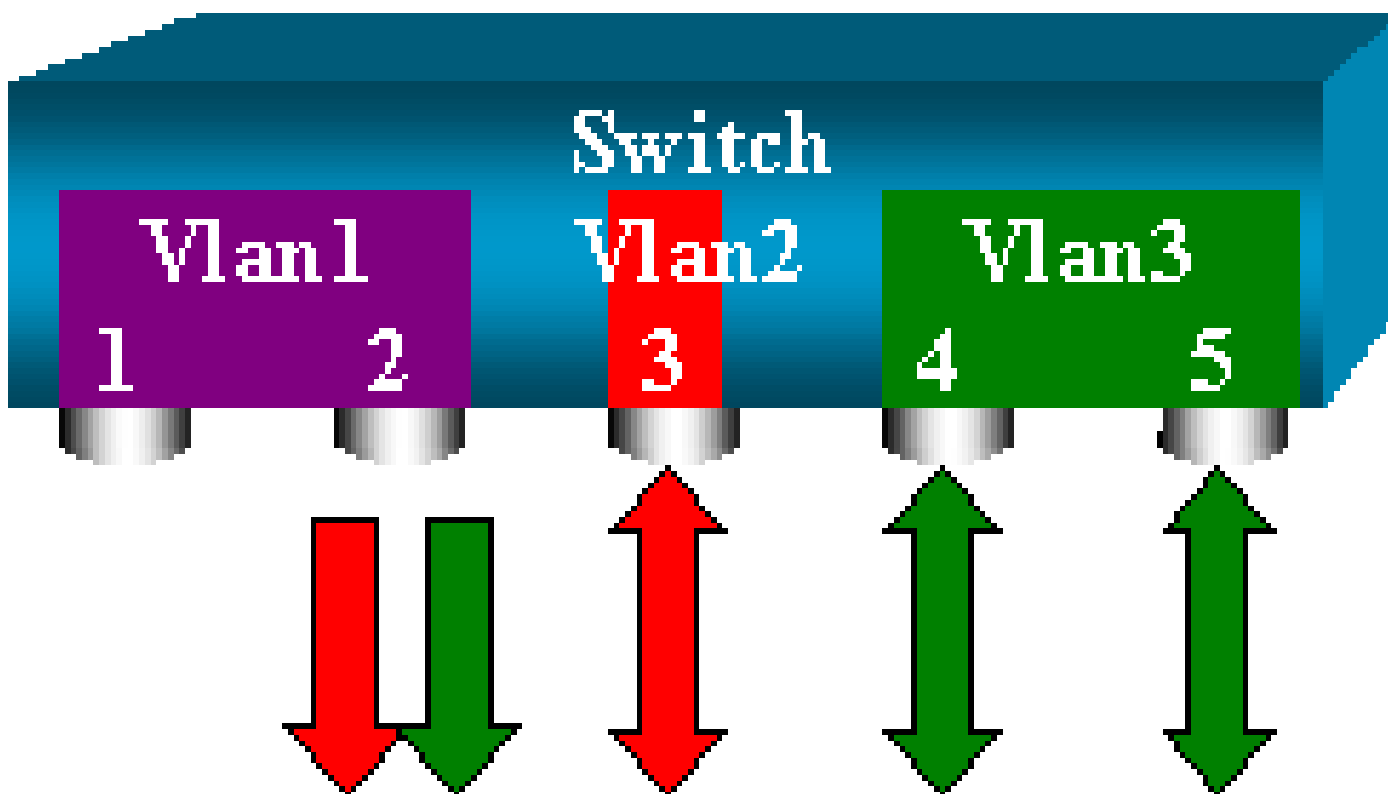
```
2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1,6/3-5
Oper Source : Port 6/1,6/3-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
```

```
Status : active
switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

✎ Observação: ao contrário dos Switches Catalyst 2900XL/3500XL, o Catalyst 4500/4000, 5500/5000 e 6500/6000 pode monitorar portas que pertencem a várias VLANs diferentes com versões do CatOS anteriores à 5.1. Aqui, as portas espelhadas são atribuídas às VLANs 1, 2 e 3.

## Monitorar VLANs com SPAN

Eventualmente, o comando `set span` permite configurar uma porta para monitorar o tráfego local para uma VLAN inteira. O comando é `set span source_vlan(s) destination_port`.



Utilize uma lista de uma ou mais VLANs como origem, em vez de uma lista de portas:

```
<#root>
```

```
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
```

Com essa configuração, todos os pacotes que entram ou saem das VLANs 2 ou 3 são duplicados na porta 6/2.

---

 Observação: o resultado é exatamente o mesmo se você implementar o SPAN individualmente em todas as portas que pertencem às VLANs especificadas pelo comando. Compare o campo Oper Source e o campo Admin Source. O campo Admin Source basicamente relaciona todas as portas configuradas para a sessão de SPAN, e o campo Oper Source relaciona as portas que utilizam o SPAN.

---

## SPAN de Entrada/Saída

No exemplo da seção [Monitorar VLANs com SPAN, o tráfego que entra e sai das portas especificadas é monitorado.](#)

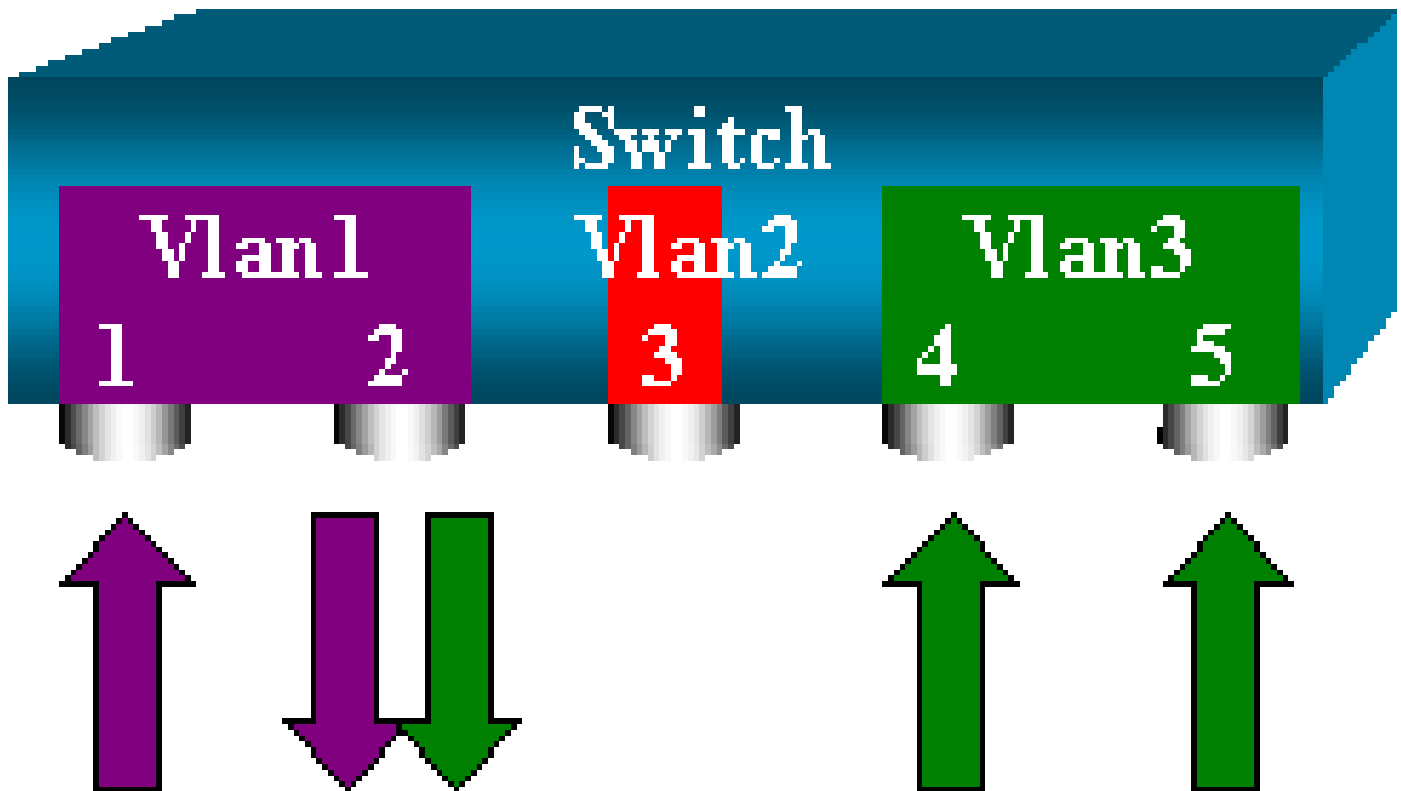
O campo `Direction: transmit/receive` mostra isso. O Catalyst 4500/4000, 5500/5000 e os 6500/6000 Series Switches permitem coletar somente o tráfego de saída ou de entrada em uma porta específica.

Adicione a palavra-chave `rx` (recebimento) ou `tx` (transmissão) ao final do comando. O valor padrão é `both` (tx e rx).

```
<#root>
```

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

Nesse exemplo, a sessão capta todo o tráfego recebido pelas VLANs 1 e 3 e o espelha para a porta 6/2:



```
<#root>
```

```
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
```

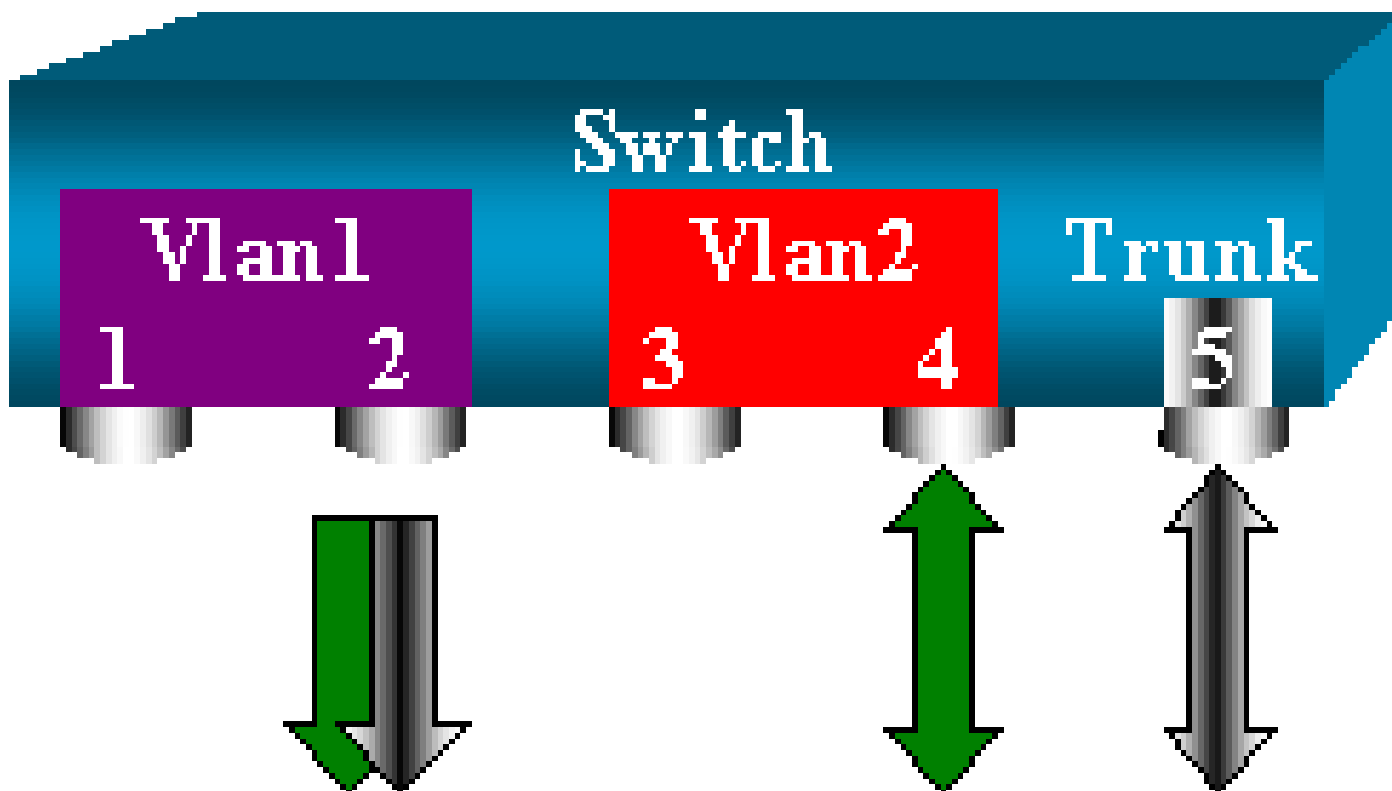
### Implementando SPAN em um tronco

Os troncos são um caso especial no switch, pois eles são portas que carregam várias VLANs. Se um tronco é selecionado como uma porta de origem, o tráfego de todas as VLANs nesse tronco é monitorado.

Monitorar um subconjunto de VLANs pertencentes a um tronco

Neste diagrama, a porta 6/5 é agora um tronco que carrega todas as VLANs. Imagine que você quer usar o SPAN no tráfego da VLAN 2 para as portas 6/4 e 6/5. Basta emitir este comando:

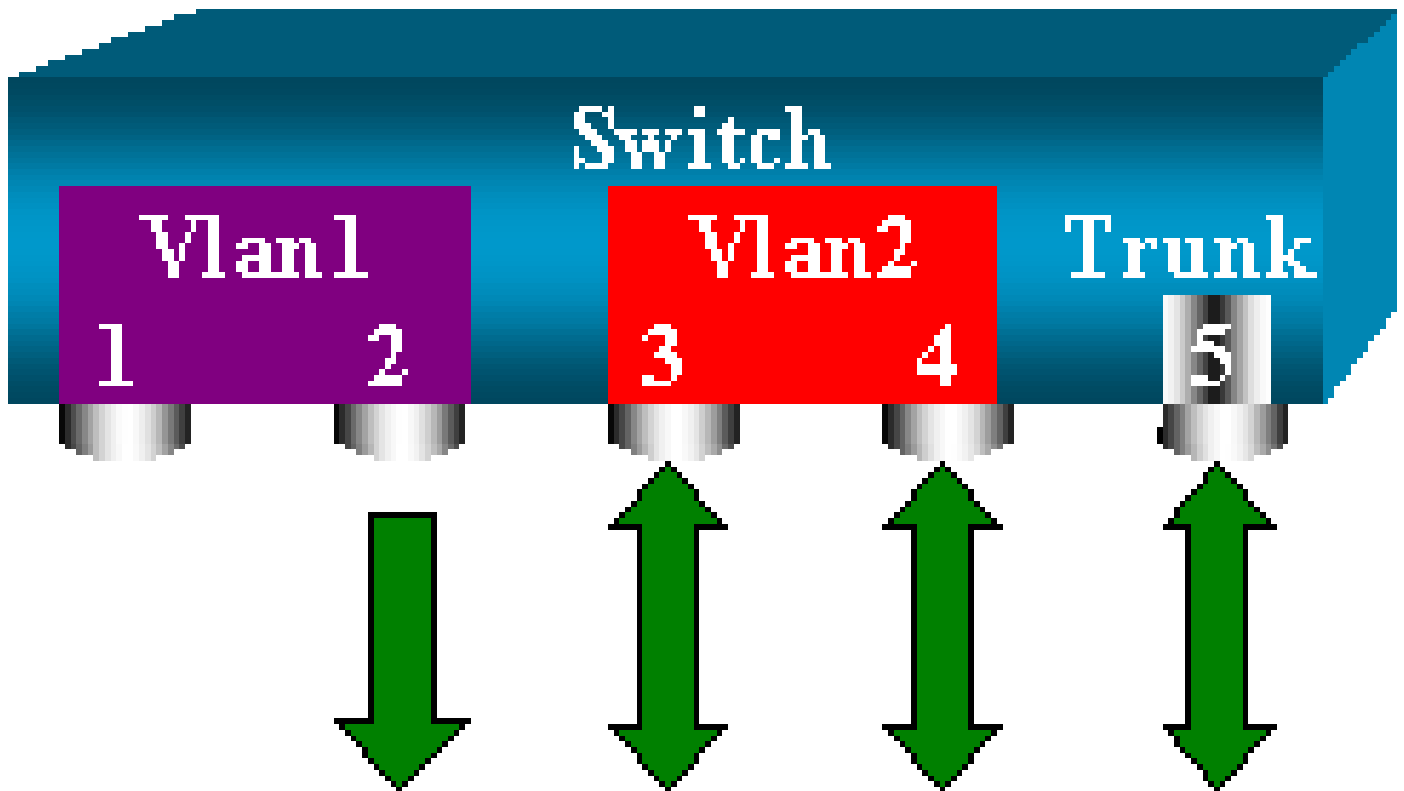
```
<#root>  
switch (enable)  
set span 6/4-5 6/2
```



Nesse caso, o tráfego recebido na porta de SPAN é uma mistura do tráfego que você quer e de todas as VLANs que o tronco 6/5 carrega.

Por exemplo, não há nenhuma maneira de distinguir, na porta de destino, se um pacote vem da porta 6/4 na VLAN 2 ou da porta 6/5 na VLAN 1. Outra possibilidade é usar SPAN em todo o VLAN 2:

```
<#root>  
switch (enable)  
set span 2 6/2
```



Com essa configuração, pelo menos, você monitora apenas o tráfego pertencente à VLAN 2 do tronco. O problema é que agora você também recebe o tráfego indesejado da porta 6/3.

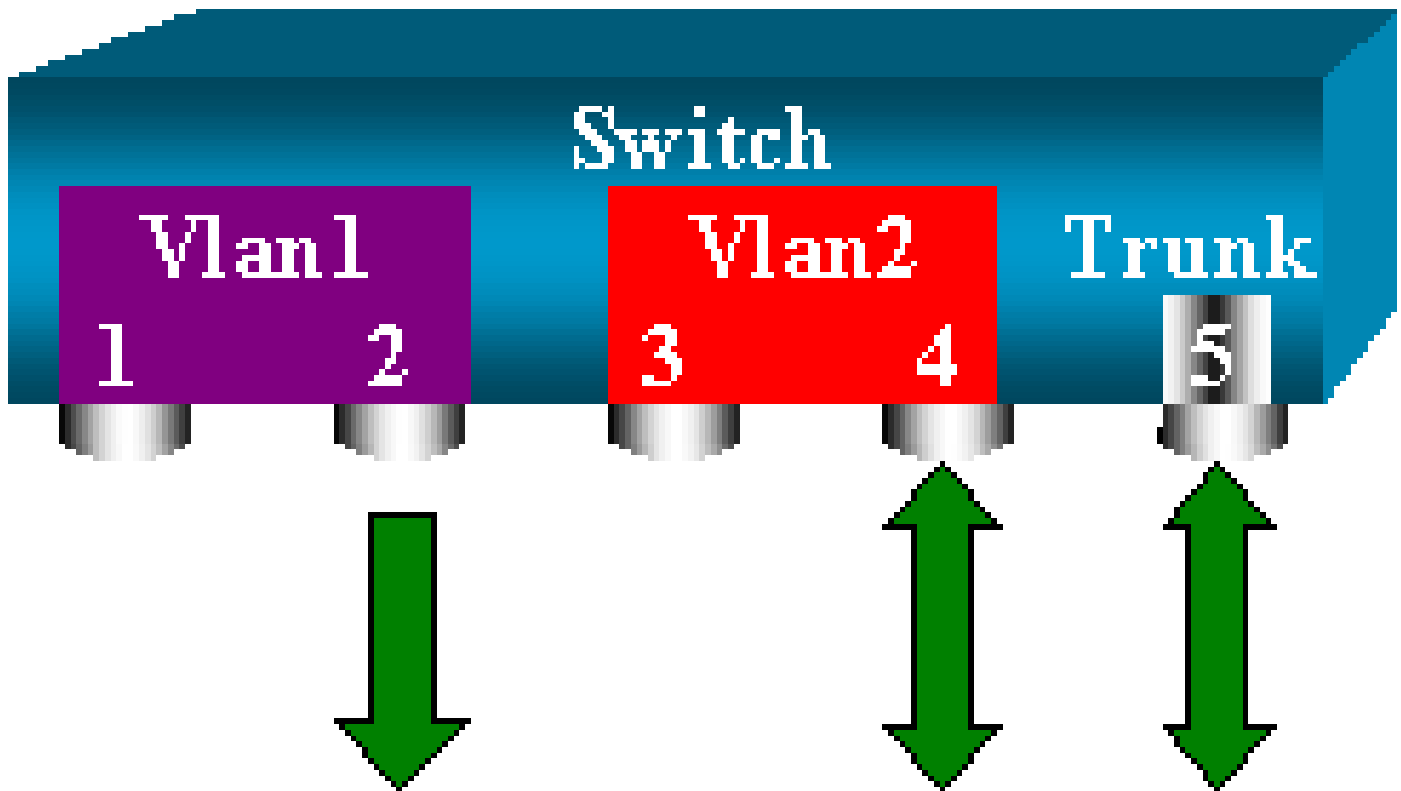
O CatOS inclui outra palavra-chave que permite selecionar algumas VLANs para monitorar a partir de um tronco:

```
<#root>
```


```
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
```



Esse comando atinge o objetivo, porque você seleciona a VLAN 2 em todos os troncos que são monitorados. Você pode especificar várias VLANs com essa opção de filtro.

 Observação: essa opção de filtro é suportada apenas nos Switches Catalyst 4500/4000 e Catalyst 6500/6000. O Catalyst 5500/5000 não suporta a opção de filtro disponível com o comando `set span`.

### Truncamento da Porta de Destino

Se você tiver portas de origem que pertencem a várias VLANs diferentes, ou se você utilizar o SPAN em várias VLANs de uma porta de tronco, talvez você queira identificar a que VLAN um pacote recebido na porta de SPAN de destino pertence.

Essa identificação é possível se você habilitar o entroncamento na porta de destino antes de configurar a porta para o SPAN. Dessa maneira, todos os pacotes encaminhados ao farejador também são etiquetados com seus respectivos IDs de VLAN.

 Observação: o farejador precisa reconhecer o encapsulamento correspondente.

```
<#root>
```

```
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
```

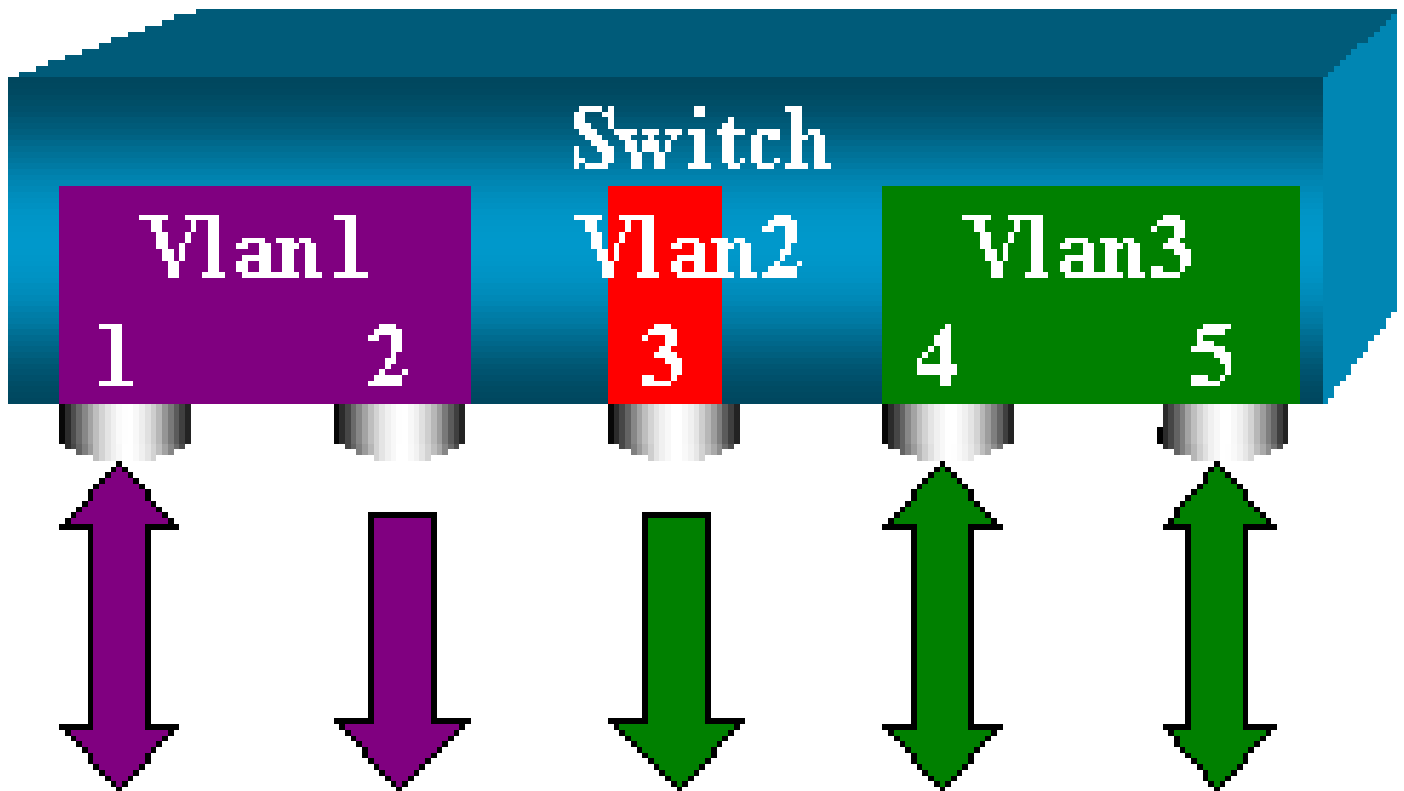
```
Port(s) 6/2 trunk mode set to nonegotiate.
Port(s) 6/2 trunk type set to isl.
switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become
isl trunk
switch (enable)
```

```
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
```

## Crie diversas sessões simultâneas

Até o momento, somente uma única sessão de SPAN foi criada. Sempre que você emite um novo comando set span, a configuração anterior é invalidada. O CatOS agora possui a capacidade de executar várias sessões simultâneas, de modo que ele possa ter portas de destino diferentes ao mesmo tempo. Emita o comando set span source destination create para adicionar uma sessão de SPAN adicional. Nessa sessão a porta 6/1 a 6/2 é monitorada e, ao mesmo tempo, o VLAN 3 a porta 6/3 é monitorada:



```
<#root>
```

```
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
```

Agora, emita o comando `show span` para determinar se você tem duas sessões ao mesmo tempo:

```
<#root>
```

```
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
```

As sessões adicionais são criadas. É necessário um modo de excluir algumas sessões. O comando é:

```
<#root>
```

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

Como só pode haver uma porta de destino por sessão, a porta de destino identifica uma sessão. Exclua a primeira sessão criada, que é a sessão que utiliza a porta 6/2 como o destino:

```
<#root>
```

```
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
```

Agora você pode verificar que só resta uma sessão:

```
<#root>
```

```
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
```

Emita esse comando pra desabilitar todas as sessões atuais em uma única etapa:

```
<#root>
```

```
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
```

## Outras Opções de SPAN

A sintaxe do comando set span é:

<#root>

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]

[inpmts

]

[learning

]

[multicast

]

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

Essa seção apresenta brevemente as opções discutidas neste documento:

- `sc0` — Você especifica a palavra-chave `sc0` em uma configuração de SPAN quando é necessário monitorar o tráfego para a interface de gerenciamento `sc0`. Esse recurso está disponível no Catalyst 5500/5000 e nos 6500/6000 Switches, versão de código CatOS 5.1 ou posterior.
- `inpkts enable/disable` — Essa opção é extremamente importante. Conforme afirmado neste documento, uma porta configurada como o destino de SPAN ainda pertence à sua VLAN original. Os pacotes recebidos em uma porta de destino entram na VLAN, como se essa porta fosse uma porta de acesso normal. Esse comportamento pode ser desejado. Se você utilizar um PC como um farejador, talvez você queira que ele esteja completamente conectado à VLAN. Contudo, a conexão poderá ser perigosa se você conectar a porta de destino a outro equipamento de rede que cria um loop na rede. A porta SPAN de destino não executa o STP, e você pode se envolver em um loop de Bridging perigoso. Consulte a seção [Por que a Sessão de SPAN Cria um Loop de Bridging?](#) deste documento para entender como essa situação pode ocorrer. A configuração padrão para essa opção está desabilitada, o que significa que a porta de SPAN de destino descarta os pacotes recebidos pela porta. Esse descarte protege a porta de loops de bridging. Essa opção aparece no CatOS 4.2.
- `learning enable/disable` — Essa opção permite desabilitar a aprendizagem na porta de destino. Por padrão, a aprendizagem está habilitada, e a porta de destino aprende os endereços MAC a partir dos pacotes de entrada recebidos pela porta. Esse recurso aparece no CatOS 5.2 no Catalyst 4500/4000 e 5500/5000 e no CatOS 5.3 no Catalyst 6500/6000.
- `multicast enable/disable` — Como sugere o nome, essa opção permite habilitar ou desabilitar a monitoração de pacotes de multicast. O padrão é `enable`. Esse recurso está disponível no Catalyst 5500/5000 e 6500/6000, CatOS 5.1 e posteriores.
- `spanning port 15/1` — No Catalyst 6500/6000, você pode usar a porta 15/1 (ou 16/1) como uma origem de SPAN. A porta pode monitorar o tráfego que é encaminhado à placa de recurso de switch de multicamada (MSFC, Multilayer Switch Feature Card). A porta capta o tráfego roteado por software ou direcionado para o MSFC.

## SPAN remoto

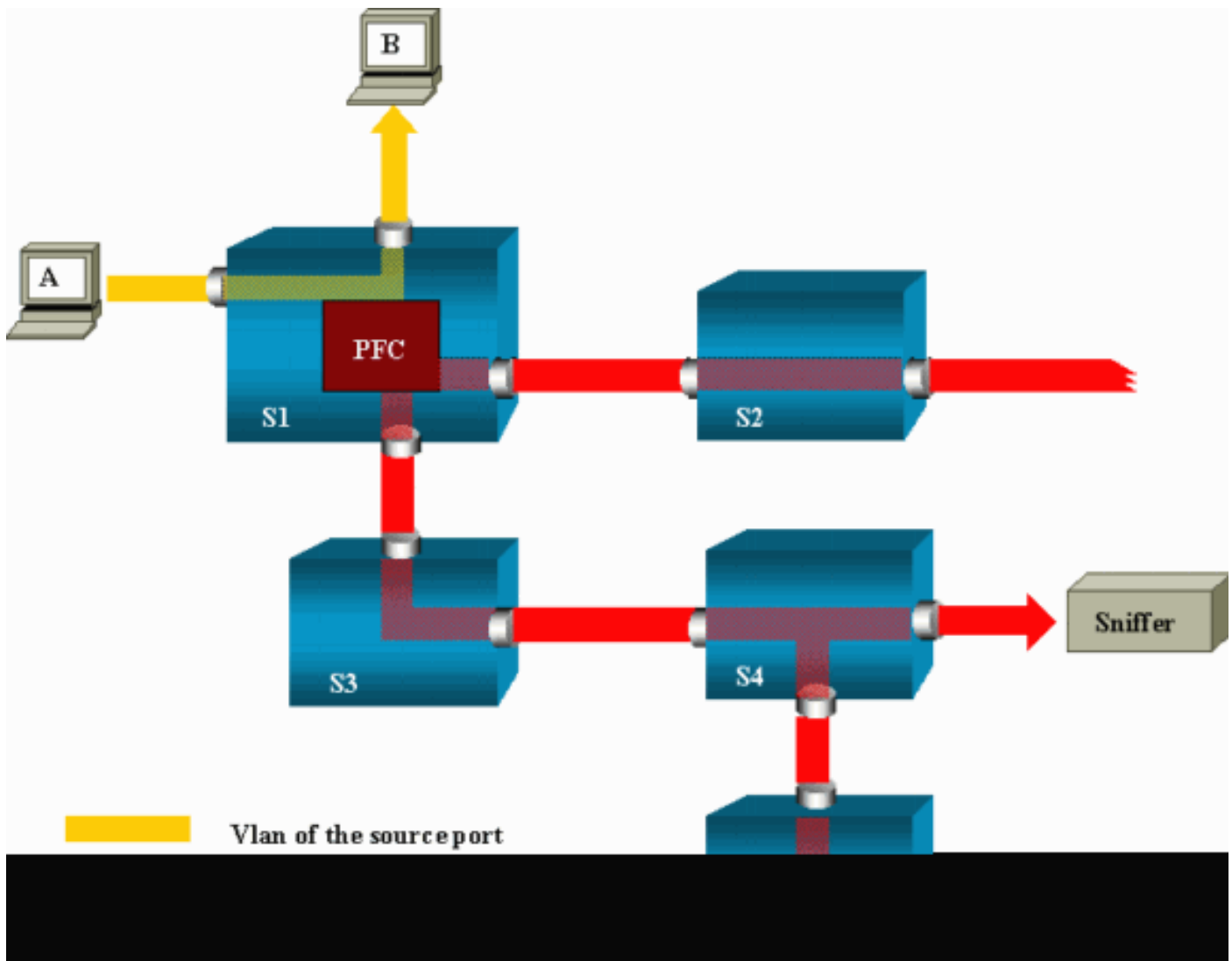
### Visão geral de RSPAN

O RSPAN permite monitorar portas de origem dispersas em uma rede comutada, não apenas localmente em um switch com SPAN. Esse recurso aparece no CatOS 5.3 no Catalyst 6500/6000 Series Switches e é adicionado no Catalyst 4500/4000 Series Switches no CatOS 6.3 e posteriores.

A funcionalidade funciona exatamente como uma sessão de SPAN normal. O tráfego monitorado pelo SPAN não é copiado diretamente para a porta de destino, mas inundado em uma VLAN de

RSPAN especial. A porta de destino pode estar localizada em qualquer local neste VLAN RSPAN. Pode haver várias portas de destino.

Esse diagrama ilustra a estrutura de uma sessão RSPAN:



Neste exemplo, você configura o RSPAN para monitorar o tráfego enviado pelo host A. Quando A gera um quadro destinado a B, o pacote é copiado por um circuito integrado específico de aplicação (ASIC, Application Specified Integrated Circuit) da placa de recurso de política (PFC, Policy Feature Card) do Catalyst 6500/6000 em uma VLAN de RSPAN predefinida. A partir de então, o pacote é inundado para todas as outras portas que pertencem à VLAN de RSPAN. Todas as relações entre os switches que são demonstradas aqui são troncos, que é um requisito do RSPAN. As únicas portas de acesso são as portas de destino, onde os farejadores estão conectados (aqui, em S4 e S5).

Veja algumas observações sobre este design:

- S1 é chamado de switch de origem. Os pacotes só entram na VLAN de RSPAN nos switches configurados como origem de RSPAN. No momento, um switch só pode ser a origem para uma sessão de RSPAN, o que significa que um switch de origem só pode alimentar uma VLAN de RSPAN por vez.

- S2 e S3 são switches intermediários. Eles não são origens de RSPAN e não possuem portas de destino. Um switch pode ser intermediário para qualquer número de sessões de RSPAN.
- S4 e S5 são switches de destino. Algumas de suas portas são configuradas para serem o destino de uma sessão de RSPAN. Atualmente, um Catalyst 6500/6000 pode ter até 24 portas de destino RSPAN, para uma ou diversas sessões diferentes. Você também pode perceber que S4 é um switch intermediário e de destino.
- Você pode ver que os pacotes de RSPAN são inundados na VLAN de RSPAN. Mesmo os switches que não estão no caminho para uma porta de destino, como o S2, recebem o tráfego para a VLAN de RSPAN. Você pode achar útil remover essa VLAN nesses links de S1-S2.
- Para atingir a inundação, a aprendizagem é desabilitada na VLAN de RSPAN.
- Para evitar loops, o STP foi mantido na VLAN de RSPAN. Dessa forma, o RSPAN não pode monitorar os BPDUs.

#### Exemplo de configuração de RSPAN

As informações desta seção ilustram a instalação desses diferentes elementos com um projeto de RSPAN muito simples. S1 e S2 são dois Switches Catalyst 6500/6000. Para monitorar algumas portas de S1 ou VLANs de S2, é necessário estabelecer uma VLAN de RSPAN dedicada. O restante dos comandos possui sintaxe semelhante à utilizada em uma sessão de SPAN típica.



#### Configuração do Tronco ISL entre os Dois Switches S1 e S2

Para começar, coloque o mesmo domínio de VLAN Trunk Protocol (VTP) em cada switch e configure um lado como o entroncamento desejável. A negociação do VTP faz o resto. Emita este comando no S1:

```
<#root>
```

```
S1> (enable)
```

```
set vtp domain cisco
```

```
VTP domain cisco modified
```

Emita estes comandos no S2:

```
<#root>
```

```
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
```

## Criação da VLAN de RSPAN

Uma sessão de RSPAN precisa de uma VLAN RSPAN. Você deve criar esta VLAN. Não é permitido converter uma VLAN existente em uma VLAN de RSPAN. Este exemplo utiliza a VLAN 100:

```
<#root>
```

```
S2> (enable)
```

```
set vlan 100 rspan
```

```
Vlan 100 configuration successful
```

Emita este comando em um switch configurado como um servidor VTP. O conhecimento de RSPAN VLAN 100 é propagado automaticamente no domínio VTP total.

## Configuração da Porta 5/2 de S2 como uma Porta de Destino RSPAN

```
<#root>
```

```
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
```

## Configuração de uma Porta de Origem RSPAN em S1

Neste exemplo, o tráfego de entrada que entra em S1 através da porta 6/2 é monitorado. Emita este comando:

```
<#root>
```

```
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 os pacotes de entrada na porta 6/2 são inundados na VLAN 100 de RSPAN e alcançam a porta de destino configurada em S1 através do tronco.

## Verificar a configuração

O comando show rspan oferece um resumo da configuração de RSPAN atual no switch. Mais uma vez, pode haver somente uma sessão de RSPAN de origem por vez.

```
<#root>
```

```
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
```

### Outras Configurações Possíveis com o Comando set rspan

Você utiliza diversas linhas de comando para configurar a origem e o destino com RSPAN. Com exceção dessa diferença, o SPAN e o RSPAN se comportam da mesma forma. Você poderá até mesmo utilizar o RSPAN localmente, em um único Switch, caso deseje ter várias portas de SPAN de destino.

### Resumo de recursos e limitações

Esta tabela resume os diferentes recursos que foram introduzidos e fornece a versão mínima do CatOS necessária para executar o recurso na plataforma especificada:

Recurso	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
opção habilitar/desabilitar inpkts	4.4	4.2	5.1
Várias sessões, portas em VLANs diferentes	5.1	5.1	5.1
opção sc0	—	5.1	5.1
opção multicast enable/disable	—	5.1	5.1
opção learning enable/disable	5.2	5.2	5.3
RSPAN	6.3	—	5.3

Esta tabela fornece um breve resumo das restrições atuais no número de sessões de SPAN possíveis:

Recurso	Catalyst 4500/4000 Range of Switches	Catalyst 5500/5000 Range of Switches	Catalyst 6500/6000 Range of Switches
Rx ou ambas as sessões SPAN	5	1	2
Sessões de SPAN de Tx	5	4	4



Sessões do Mini Analisador de Protocolo	Not Supported	Not Supported	1
Sessões de origem de RSPAN, Rx, Tx ou ambas	5	Not Supported	1 Supervisor Engine 720 suporta duas sessões de origem de RSPAN.
Destino de RSPAN	5	Not Supported	24
Sessões totais	5	5	30

Consulte estes documentos para obter informações sobre as restrições e diretrizes de configuração adicionais:

- [Configuração de SPAN e RSPAN](#) (Catalyst 4500/4000)
- [Configuração de SPAN e RSPAN](#)(Catalyst 6500/6000)

## SPAN no Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E Series Switches

Estas são as diretrizes para a configuração do recurso SPAN no Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E Series Switches:

- Os Catalyst 2950 Switches podem ter somente uma sessão de SPAN ativa por vez e podem monitorar somente portas de origem. Esses switches não podem monitorar VLANs.
- Os Catalyst 2950 e 3550 Switches podem encaminhar tráfego para destinos de porta SPAN no Cisco IOS Software Release 12.1(13)EA1 e posterior.
- Os Catalyst 3550, 3560 e 3750 Switches podem suportar até duas sessões de SPAN por vez e podem monitorar portas de origem e VLANs.
- Os Catalyst 2970, 3560 e 3750 Switches não requerem a configuração de uma porta refletora durante a configuração de uma sessão de RSPAN.
- Os Catalyst 3750 Switches suportam a configuração de sessão com o uso de portas de origem e de destino que residem em qualquer um dos membros do switch stack.
- Somente uma porta de destino é permitida pela sessão de SPAN, e a mesma porta não pode ser uma porta de destino para várias sessões de SPAN. Desse modo, você não pode ter duas sessões de SPAN que utilizam a mesma porta de destino.

Os comandos de configuração do recurso de SPAN são semelhantes no Catalyst 2950 e no Catalyst 3550. Porém, o Catalyst 2950 não pode monitorar as VLANs. Você pode configurar o SPAN, como neste exemplo:

```
<#root>
```

```
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#
```

Você também pode configurar uma porta como um destino para o SPAN e o RSPAN locais para o mesmo tráfego de VLAN. Para monitorar o tráfego para uma vlan específica que reside em dois switches conectados diretamente, configure estes comandos no switch que tem a porta de destino. Neste exemplo, nós monitoramos o tráfego da VLAN 5 que é propagado através de dois switches:

```
<#root>
```

```
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.*

No switch remoto, utilize esta configuração:

```
<#root>
```

```
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
```

No exemplo anterior, uma porta foi configurada como uma porta de destino para que o SPAN e o RSPAN locais monitorem o tráfego para a mesma VLAN que reside nos dois switches.


---

 Observação: ao contrário dos Switches das Séries 2900XL e 3500XL, os Switches das Séries Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E suportam SPAN no tráfego da porta de origem somente na direção Rx (Rx SPAN ou Pressione SPAN), somente na direção Tx (SPAN de Tx ou SPAN de saída) ou em ambos.


---

 Observação: os comandos na configuração não são suportados no Catalyst 2950 com Cisco IOS Software Release 12.0(5.2)WC(1) ou qualquer software anterior ao Cisco IOS Software Release 12.1(6)EA2. Consulte a seção [Ativação do Analisador de Porta de Switch](#) do Gerenciamento de Switches para configurar o SPAN em um Catalyst 2950 com software anterior ao Cisco IOS Software Release 12.1(6)EA2.

---

 Observação: os Switches Catalyst 2950 que usam o Cisco IOS Software Release 12.1.(9)EA1d e as versões anteriores no Cisco IOS Software Release 12.1 oferecem suporte a SPAN. Entretanto, todos os pacotes que são vistos na porta de destino de SPAN (conectada ao dispositivo de detecção ou ao PC) possuem uma etiqueta IEEE 802.1Q, mesmo que a porta de origem de SPAN (porta monitorada) não seja uma porta de tronco 802.1Q. Se o dispositivo de detecção ou o cartão de interface da rede (NIC) do PC não entenderem os pacotes etiquetados com 802.1Q, o dispositivo poderá descartar os pacotes ou ter dificuldade ao tentar decodificá-los. A capacidade de ver os quadros etiquetados com 802.1Q é importante somente quando a porta de origem de SPAN é uma porta de tronco. Com o Cisco IOS Software Release 12.1(11)EA1 e posteriores, é possível habilitar e

---

 desabilitar a colocação de etiquetas dos pacotes na porta de destino de SPAN. Emita o [comando monitor session session number destination interface interface id encapsulation dot1q para habilitar o encapsulamento de pacotes na porta de destino](#). Se você não especificar a palavra-chave de encapsulamento, os pacotes serão enviados sem etiquetas, que é o padrão no Cisco IOS Software Release 12.1(11)EA1 e posteriores.

Recurso	Catalyst 2950/3550
Ingresso (inpkts) opção de habilitação/desabilitação	Cisco IOS Software Release 12.1(12c)EA1
RSPAN	Cisco IOS Software Release 12.1(12c)EA1
Recurso	Catalyst 29401, 2950, 2955, 2960, 2970, 3550, 3560, 3750
Rx ou ambas as sessões SPAN	2
Sessões de SPAN de Tx	2
Sessões de origem de RSPAN, Rx, Tx ou ambas	2
Destino de RSPAN	2
Sessões totais	2

<sup>1</sup> Os Switches Catalyst 2940 suportam apenas SPAN local. O RSPAN não é suportado nessa plataforma.

Consulte os seguintes guias de configuração para obter mais informações sobre a configuração de SPAN e RSPAN:

- [Configuração de SPAN \(Catalyst 2940\)](#)
- [Configuração de SPAN e RSPAN \(Catalyst 2950 e 2955\)](#)
- [Configuração de SPAN e RSPAN \(Catalyst 2960\)](#)
- [Configuração de SPAN e RSPAN \(Catalyst 3550\)](#)
- [Configuração de SPAN e RSPAN \(Catalyst 3560\)](#)
- [Configuração de SPAN e RSPAN \(Catalyst 3560-E e 3750-E\)](#)
- [Configuração de SPAN e RSPAN \(Catalyst 3750\)](#)

## SPAN no Catalyst 4500/4000 e Catalyst 6500/6000 Series Switches que Executam o Cisco IOS System Software

O recurso SPAN é suportado nos Catalyst 4500/4000 e Catalyst 6500/6000 Series Switches que executam o Cisco IOS system software. Ambas as plataformas utilizam a interface de linha de comando (CLI, Command Line Interface) idêntica (e uma configuração semelhante) à

configuração abordada pela seção [SPAN nos Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560E, 3750 e 3750E Series Switches](#). Consulte estes documentos para obter informações sobre a configuração relacionada:

- [Configuração de SPAN e RSPAN](#) (Catalyst 6500/6000)
- [Configuração de SPAN e RSPAN](#) (Catalyst 4500/4000)

## Exemplo de configuração

Você pode configurar o SPAN, como neste exemplo:

```
<#root>
```

```
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#
```

## Resumo de recursos e limitações

Esta tabela resume os diferentes recursos que foram introduzidos e fornece a versão mínima do Cisco IOS Software necessária para executar o recurso na plataforma especificada:

Recurso	Catalyst 4500/4000 (Cisco IOS Software)	Catalyst 6500/6000 (Cisco IOS Software)
Ingresso (inpkts) opção de habilitação/desabilitação	Cisco IOS Software Release 12.1(19)EW	Sem suporte no momento <sup>1</sup>
RSPAN	Cisco IOS Software Release 12.1(20)EW	Cisco IOS Software Release 12.1(13)E

<sup>1</sup> O recurso não está disponível no momento e a disponibilidade desses recursos geralmente não é publicada até a versão.

 Observação: o recurso SPAN dos Cisco Catalyst 6500/6000 Series Switches tem uma limitação com relação ao protocolo PIM. Quando um switch é configurado para o PIM e o SPAN, o Analisador de Rede/Farejador vinculado à porta de destino de SPAN pode ver os pacotes de PIM que não fazem parte da porta de origem de SPAN/tráfego de VLAN. Esse problema ocorre devido a uma limitação da arquitetura de encaminhamento de pacotes do switch. A porta de destino de SPAN não executa nenhuma verificação da origem dos pacotes. Esse problema também é documentado na ID do Cisco bug CSCdy57506 (somente clientes registrados) .

Esta tabela fornece um breve resumo das restrições atuais no número de sessões de SPAN e RSPAN possíveis:

Recurso	Catalyst 4500/4000 (Cisco IOS Software)
Rx ou ambas as sessões SPAN	2
Sessões de SPAN de Tx	4
Sessões de origem de RSPAN, Rx, Tx ou ambas	2 (Rx, Tx ou ambos) e até 4 para Tx apenas
Destino de RSPAN	2
Sessões totais	6

Consulte os [Limites de Sessão de SPAN, RSPAN e ERSPAN Local para os switches Catalyst 6500/6000 que executam o Cisco IOS software.](#)

No Catalyst 6500 Series, é importante observar que o SPAN de saída está concluído no supervisor. Isso permite que todo o tráfego que sai do SPAN seja enviado através da tela ao supervisor e, em seguida, à porta de destino de SPAN, que pode usar recursos de sistema significativos e afetar o tráfego do usuário. O SPAN de entrada será feito nos módulos de entrada, de modo que o desempenho do SPAN seja a soma de todos os mecanismos de replicação participantes. O desempenho do recurso SPAN depende do tamanho do pacote e do tipo de ASIC disponível no mecanismo de replicação.

Com versões anteriores ao Cisco IOS Software Release 12.2(33)SXH, uma interface de canal de porta, um EtherChannel, não pode ser um destino de SPAN. Com o Cisco IOS Software Release 12.2(33)SXH e posteriores, um EtherChannel pode ser um destino de SPAN. Os EtherChannels de destino não suportam os protocolos EtherChannel Port Aggregation Control Protocol (PAgP) ou Link Aggregation Control Protocol (LACP); somente o modo ativado é suportado, com todo o

suporte ao protocolo EtherChannel desativado.

Consulte estes documentos para obter informações sobre as restrições e diretrizes de configuração adicionais:

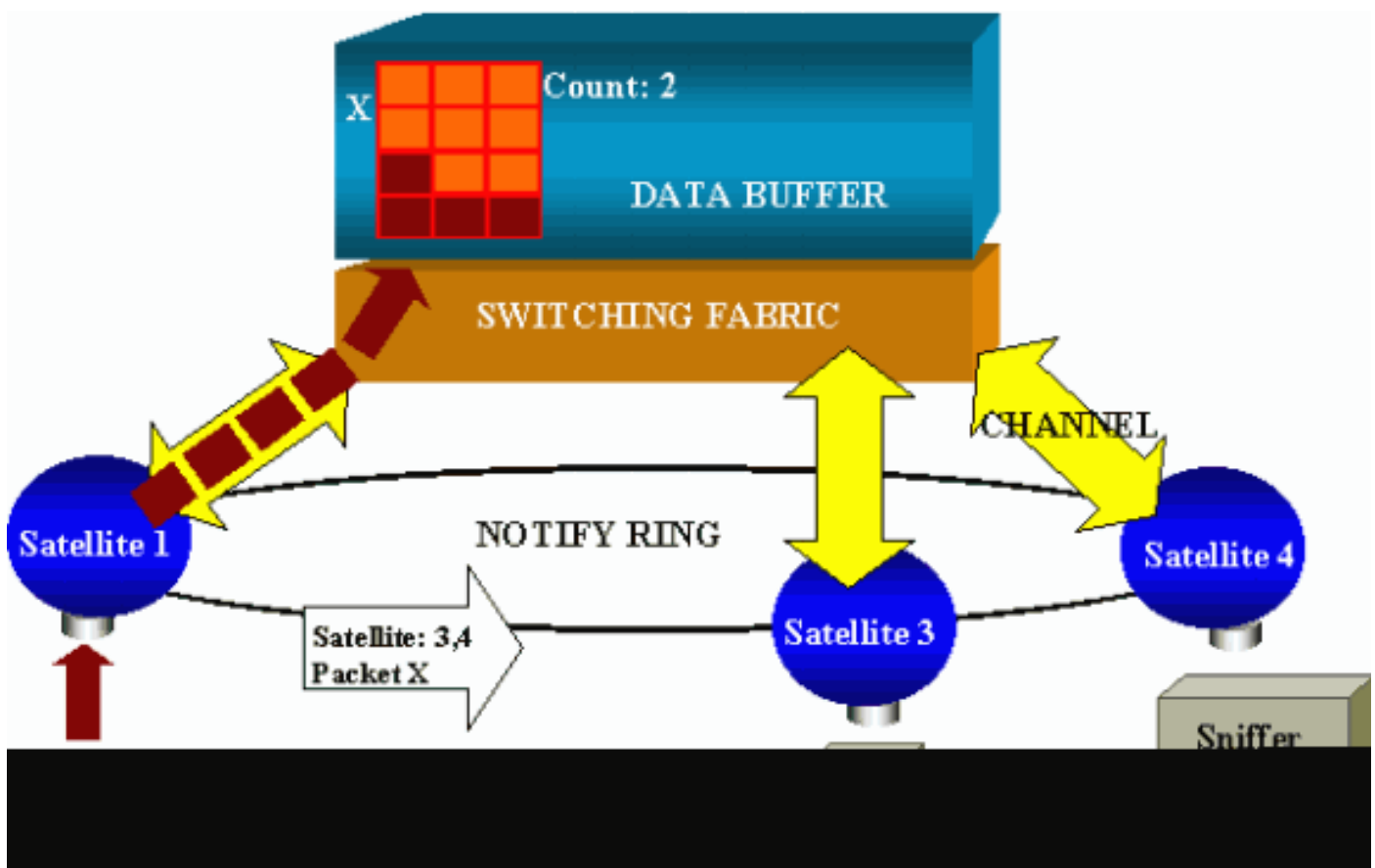
- [Configuração de SPAN e RSPAN \(Catalyst 4500/4000\)](#)
- [Configuração do SPAN Local, SPAN Remoto \(RSPAN\) e RSPAN Encapsulado \(Catalyst 6500/6000\)](#)

## Impacto no desempenho de SPAN nas diferentes plataformas do Catalyst

### Catalyst 2900XL/3500XL Series

Visão geral da arquitetura

Esta é uma visão muito simplificada da arquitetura interna dos Switches 2900XL/3500XL:



As portas do switch são vinculadas a satélites que se comunicam a uma tela de switching através de canais radiais. Além disso, todos os satélites estão interconectados por meio de um anel de notificação de alta velocidade dedicado à sinalização de tráfego.

Quando um satélite recebe um pacote a partir de uma porta, o pacote é dividido em células e enviado à tela de switching por meio de um ou mais canais. Em seguida, o pacote é armazenado

na memória compartilhada. Cada satélite tem informações sobre as portas de destino. No diagrama nesta seção, o satélite 1 sabe que o pacote X deve ser recebido pelos satélites 3 e 4. O satélite 1 envia uma mensagem aos outros satélites através do anel de notificação. Em seguida, os satélites 3 e 4 podem começar a recuperação das células da memória compartilhada através de seus canais radiais e podem eventualmente encaminhar o pacote. Como o satélite de origem conhece o destino, ele também transmite um índice que especifica o número de vezes que o pacote é transferido por download por outros satélites. Cada vez que um satélite recupera o pacote da memória compartilhada, o índice sofre um decréscimo. Quando o índice atinge 0, a memória compartilhada pode ser liberada.

### Impacto de desempenho

Para monitorar algumas portas com SPAN, um pacote deve ser copiado do buffer de dados para um satélite mais uma vez. O impacto na tela de switching de alta velocidade pode ser desconsiderado.

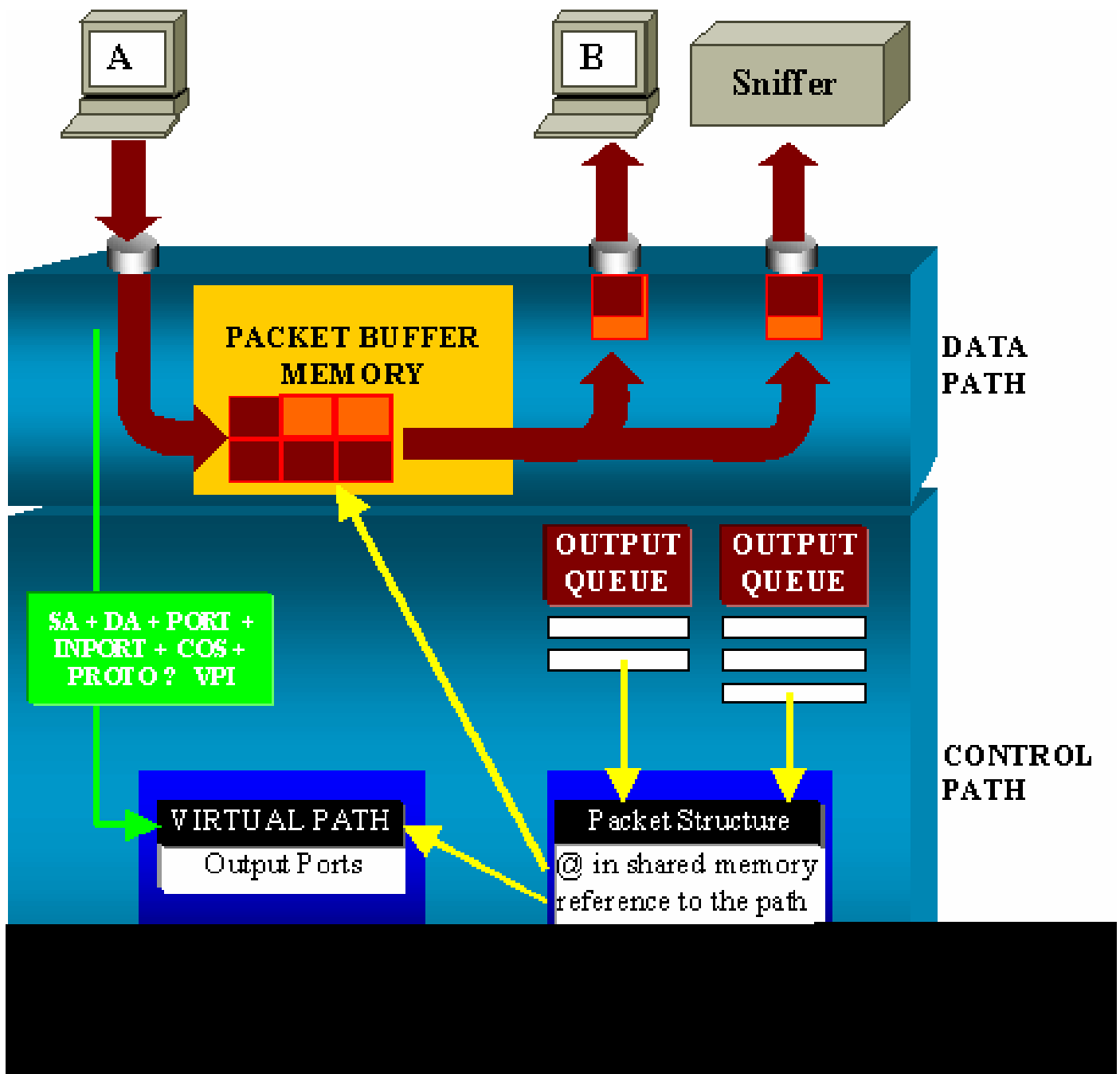
A porta de monitoramento recebe cópias do tráfego transmitido e recebido para todas as portas monitoradas. Nessa arquitetura, um pacote com vários destinos ficará armazenado na memória até que todas as cópias estejam encaminhadas. Se a porta de monitoramento estiver com 50% de excesso de assinaturas por um período prolongado, provavelmente ela fique congestionada e mantenha parte da memória compartilhada. Há uma possibilidade de que umas ou várias portas monitoradas também passem por uma desaceleração.

## Catalyst 4500/4000 Series

### Visão geral da arquitetura

O Catalyst 4500/4000 é baseado em uma tela de switching de memória compartilhada. Este diagrama é uma visão geral de alto nível do trajeto de um pacote através do switch. A implementação real é muito mais complexa:





Em um Catalyst 4500/4000, você pode distinguir o caminho dos dados. O caminho dos dados corresponde à transferência real dos dados dentro do switch, do caminho de controle, onde todas as decisões são tomadas.

Quando um pacote entra no switch, um buffer é alocado na Memória de Buffer de Pacotes (uma memória compartilhada).

Uma estrutura de pacotes que aponta para esse buffer é inicializada na tabela de descrição de pacotes (PDT, Packet Descriptor Table).

Quando os dados forem copiados na memória compartilhada, o caminho de controle determinará onde comutar o pacote. Para determinar isso, um valor de hash é computado a partir destas informações:

- O endereço de origem de pacote

- Endereço de destino
- VLAN
- Tipo de protocolo
- Porta de entrada
- Classe de serviço (CoS, Class of Service) (uma etiqueta IEEE 802.1p ou um padrão da porta)

Esse valor é utilizado para encontrar o Índice de caminho virtual (VPI) de uma estrutura de caminhos na Tabela de caminhos virtuais (VPT). A entrada do caminho virtual no VPT mantém vários campos relacionados a esse fluxo específico.

Os campos incluem as portas de destino. A estrutura do pacote no PDT foi atualizada agora com uma referência ao caminho virtual e contador.

No exemplo desta seção, o pacote deve ser transmitido a duas portas diferentes, então o contador é iniciado em 2. Finalmente, a estrutura de pacotes é adicionada à fila de saída das duas portas de destino.

A partir de então, os dados são copiados da memória compartilhada no buffer de saída da porta, e o contador de estrutura de pacotes sofre um decréscimo. Quando ele atinge 0, o buffer de memória compartilhada é liberado.

### Impacto de desempenho

Com o uso do recurso SPAN, um pacote deve ser enviado a duas portas diferentes, como no exemplo da seção [Visão Geral da Arquitetura](#).

O envio do pacote a duas portas não é um problema, porque a tela de switching não faz bloqueios.

Se a porta SPAN de destino estiver congestionada, os pacotes serão descartados na fila de saída e liberados corretamente da memória compartilhada. T

Portanto, não há impacto na operação do switch.

## Catalyst 5500/5000 e 6500/6000 Series

### Visão geral da arquitetura

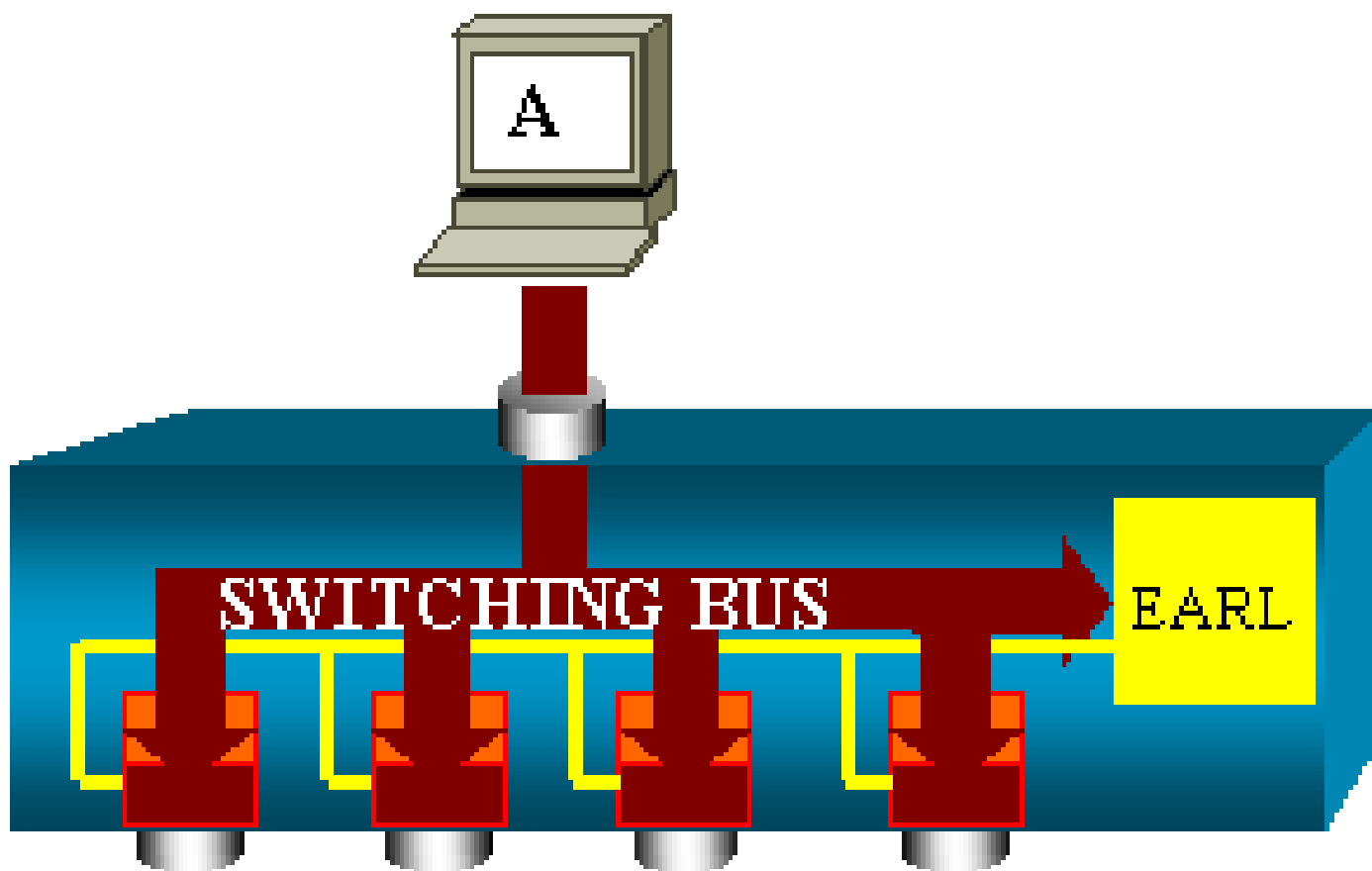
No Catalyst 5500/5000 e 6500/6000 Series Switches, um pacote recebido em uma porta é transmitido no barramento de switching interno.

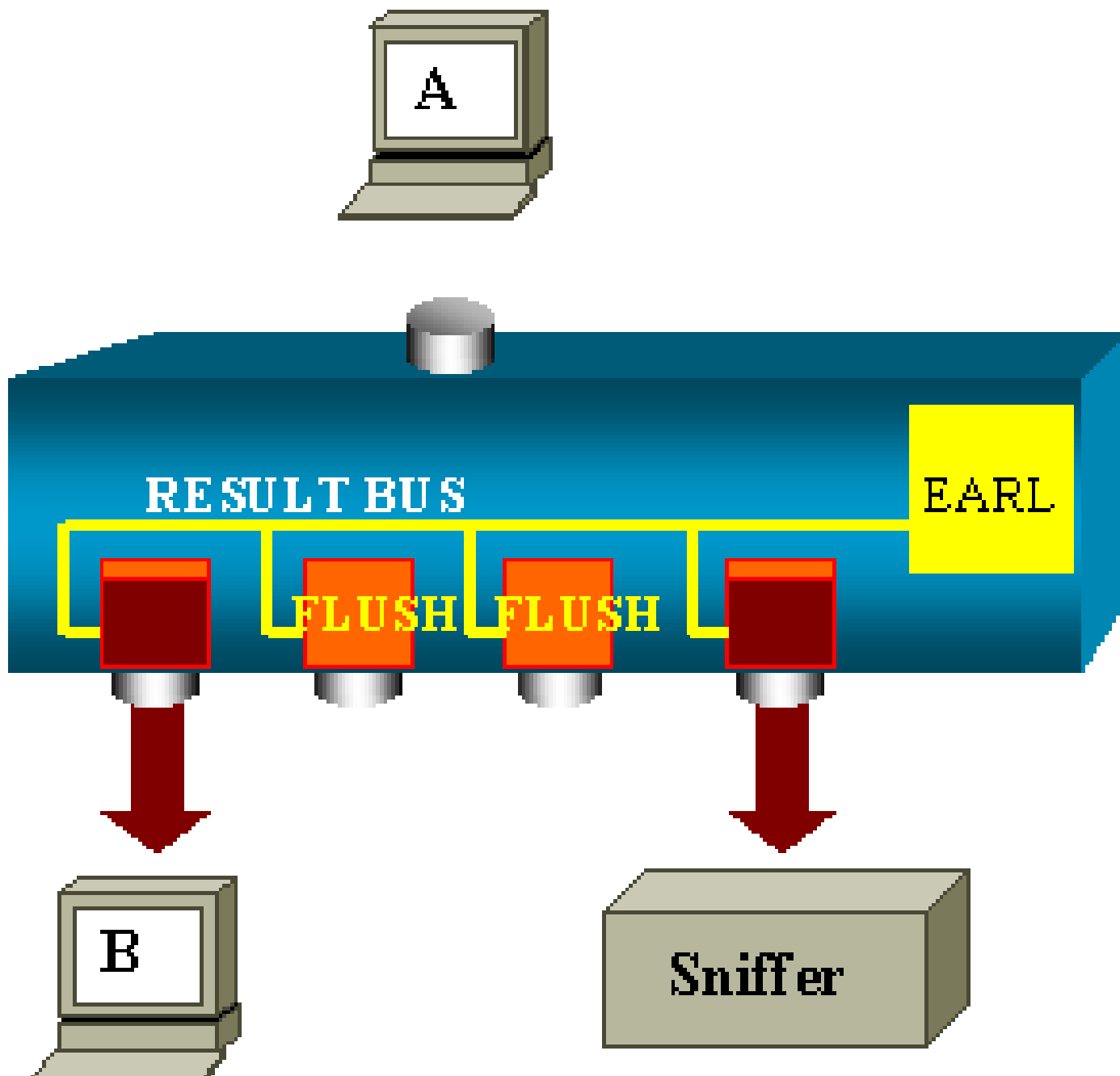
Cada placa de linha no switch começa a armazenar esse pacote em buffers internos.

Ao mesmo tempo, a lógica de reconhecimento de endereço codificado (EARL, Encoded Address

Recognition Logic) recebe o cabeçalho do pacote e computa um índice de resultados. O EARL envia o índice de resultados a todas as placas de linha através do barramento do resultado.

O conhecimento desse índice permite que a placa de linha decida individualmente se deve descarregar ou transmitir o pacote quando ela receber o pacote no buffer.





### Impacto de desempenho

O fato de uma ou várias portas finalmente transmitirem o pacote não tem qualquer influência na operação do Switch. Dessa maneira, quando você pensa nessa arquitetura, o recurso de SPAN não tem nenhum impacto no desempenho.

## Perguntas freqüentes e problemas comuns


### Problemas de conectividade devido ao erro de configuração do SPAN

Os problemas de conectividade devido ao erro de configuração de SPAN ocorrem com frequência nas versões do CatOS anteriores à versão 5.1. Com essas versões, só é possível ter uma sessão de SPAN.

A sessão permanece na configuração, mesmo quando você desabilita o SPAN. Com a emissão do comando `set span enable`, um usuário reativa a sessão de SPAN armazenada.

A ação ocorre com frequência devido a um erro tipográfico, por exemplo, se o usuário quer habilitar o STP. Poderão ocorrer sérios problemas de conectividade se a porta de destino for utilizada para encaminhar o tráfego do usuário.

---

 Cuidado: este problema ainda está na implementação atual do CatOS. Tenha cuidado na escolha da porta como um destino de SPAN.

---

## Porta de Destino Superior/Inferior de SPAN

Quando as portas são colocadas em SPAN para a monitoração, o estado da porta é mostrado como UP/DOWN (ativado/desativado).

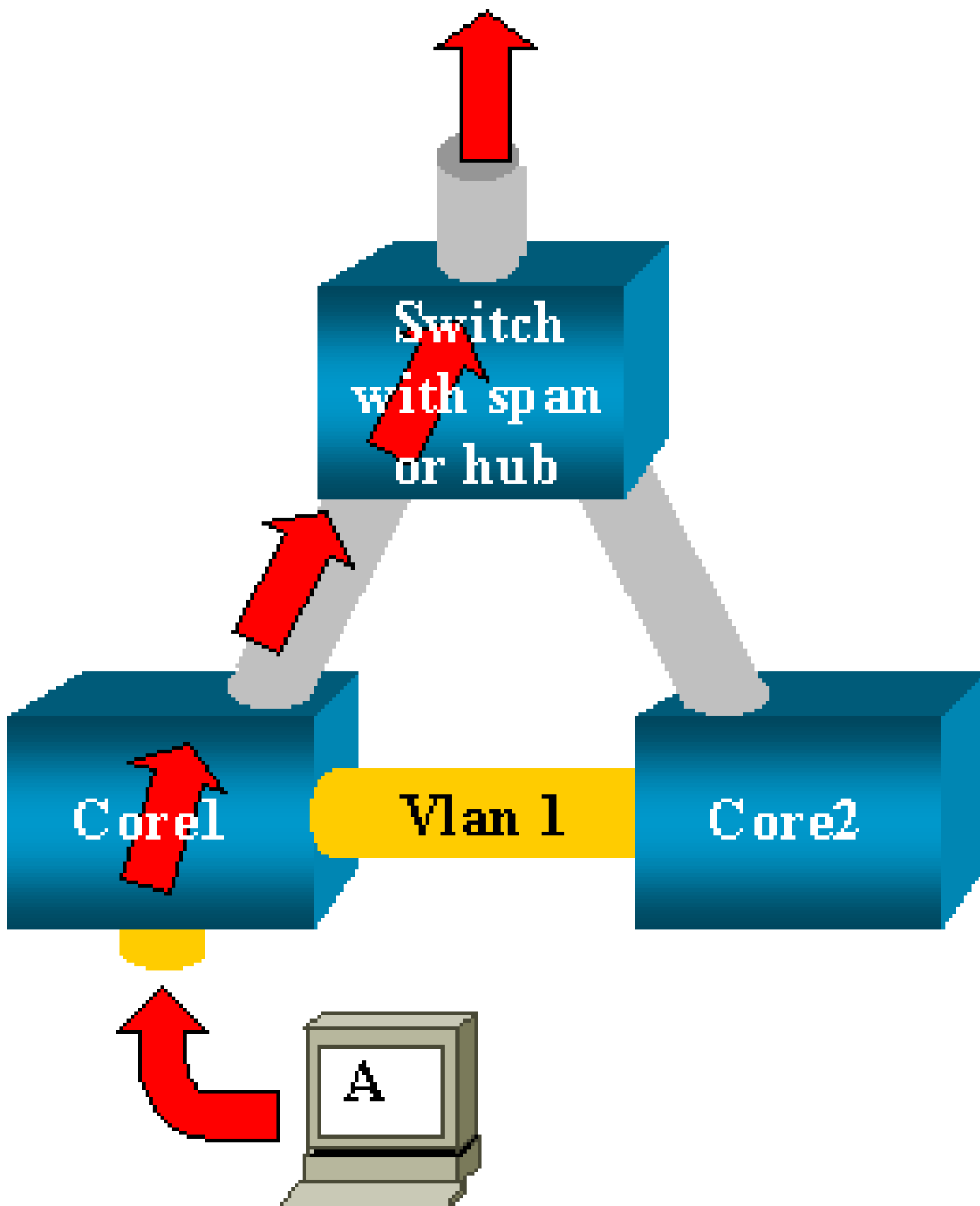
Quando você configura uma sessão de SPAN para monitorar a porta, a interface de destino mostra o estado inativo (monitoração), por padrão.

A interface mostra a porta nesse estado para tornar evidente que a porta não pode ser utilizada no momento como uma porta de produção. A porta como monitoração ativado/desativado é normal.

## Por que a Sessão de SPAN Cria um Loop de Bridging?

A criação de um loop de bridging ocorre geralmente quando o administrador tenta falsificar o recurso RSPAN. Além disso, o problema pode ser causado por um erro de configuração.

Este é um exemplo do cenário:



Há dois switches centrais conectados por um tronco. Neste exemplo, cada switch possui diversos servidores, clientes ou outras bridges conectadas a ele.

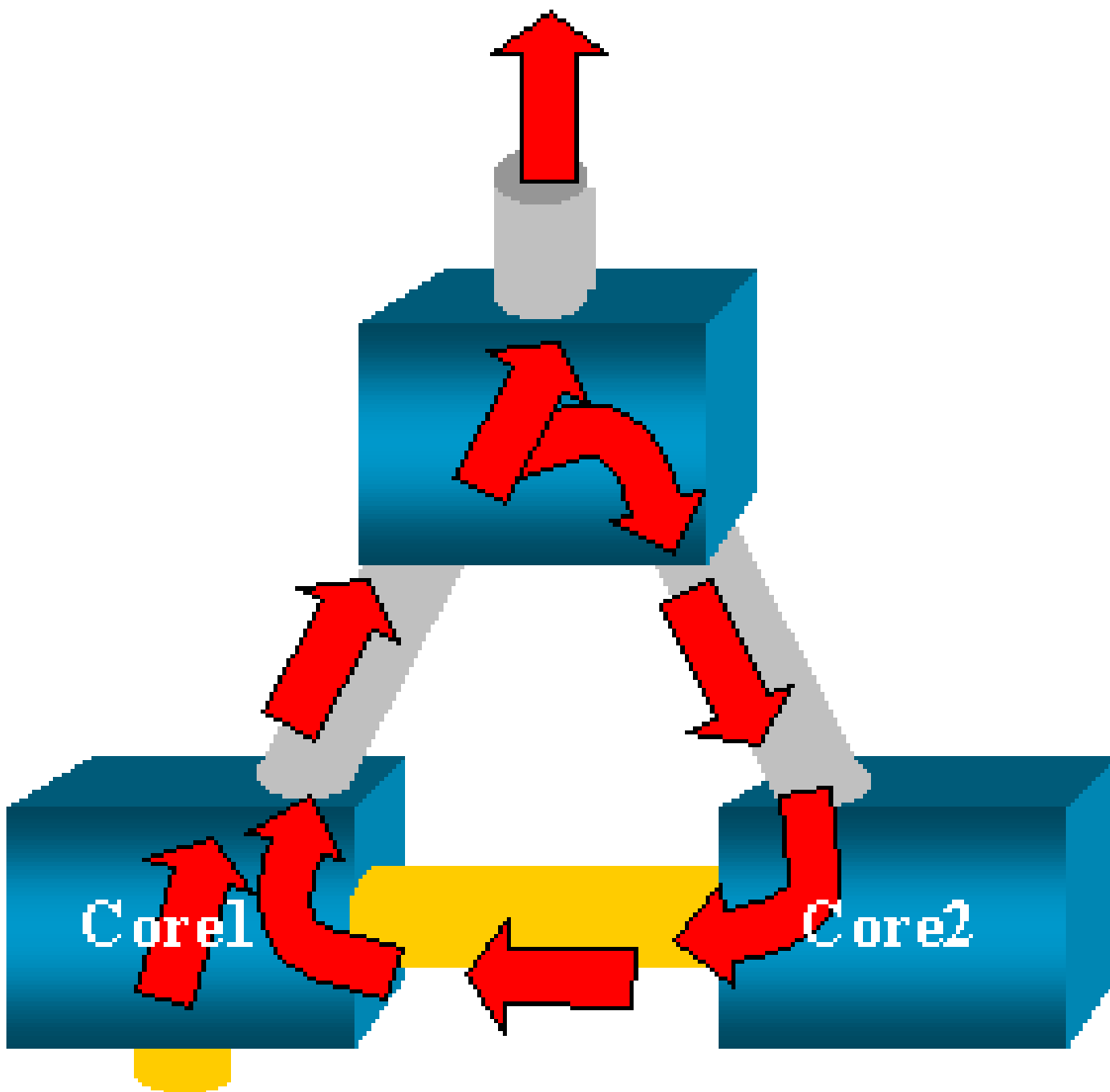
O administrador quer monitorar a VLAN 1, que aparece em diversas bridges com SPAN.

O administrador cria uma sessão de SPAN que monitora toda a VLAN 1 em cada switch central e, para mesclar essas duas sessões, conecta a porta de destino ao mesmo hub (ou ao mesmo switch, com o uso de outra sessão de SPAN).


O administrador atinge o objetivo. Cada pacote único recebido por um switch central na VLAN 1 é duplicado na porta de SPAN e encaminhado para o hub. Um farejador eventualmente capta o tráfego.

O único problema é que o tráfego também é injetado novamente no núcleo 2 através da porta de SPAN de destino.


A reinjeção do tráfego no núcleo 2 cria um Loop de Bridging na VLAN 1. Lembre-se de que uma porta SPAN de destino não executa o STP e não pode impedir esse loop.



---

 Observação: devido à introdução da opção `inpkts` (pacotes de entrada) no CatOS, uma porta de destino de SPAN descarta qualquer pacote de entrada por padrão, o que evita esse cenário de falha. Porém, o problema potencial ainda está presente nos Catalyst 2900XL/3500XL Series Switches.

---

 Observação: mesmo quando a opção `inpkts` impede o loop, a configuração mostrada nesta seção pode causar alguns problemas na rede. Os problemas de rede podem ocorrer devido aos problemas de aprendizagem do endereço MAC associados à aprendizagem habilitada na porta de destino.

---

## O SPAN afeta o desempenho?

Consulte as seguintes seções deste documento para obter informações sobre do impacto no desempenho para as plataformas do Catalyst especificadas:

- [Catalyst 2900XL/3500XL Series](#)
- [Catalyst 4500/4000 Series](#)
- [Catalyst 5500/5000 e 6500/6000 Series](#)

## É possível configurar SPAN em uma porta EtherChannel?

Um EtherChannel não será formado se uma das portas no conjunto for uma porta de destino de SPAN. Se você tentar configurar o SPAN nessa situação, o switch informará que:

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

Você pode usar uma porta em um grupo EtherChannel como uma porta de origem de SPAN.

## É Possível Ter Várias Sessões de SPAN em Execução ao Mesmo Tempo?

Nos Catalyst 2900XL/3500XL Series Switches, o número de portas de destino disponíveis no switch é o único limite para o número de sessões de SPAN.

Nos Catalyst 2950 Series Switches, você pode ter apenas uma porta de monitoração atribuída por vez.

Se você selecionar outra porta como a porta monitora, a porta monitora anterior será desabilitada e a porta recém-selecionada se tornará a monitora.

Nos Catalyst 4500/4000, 5500/5000 e 6500/6000 Switches, com CatOS 5.1 e mais recente, é possível ter várias sessões simultâneas de SPAN.



Consulte as seções [Criar Várias Sessões Simultâneas](#) e [Resumo de Recursos e Limitações deste documento](#).

## Erro "% Limite de Sessão Local Excedido"

Essa mensagem aparece quando a sessão de SPAN permitida excede o limite para o Supervisor Engine:

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

Os Supervisor Engines têm uma limitação de sessões de SPAN. Consulte a seção [Limites de Sessão de SPAN, RSPAN e ERSPAN Local de Configuração de SPAN, RSPAN e ERSPAN Local para obter mais informações](#).

## Não é Possível Excluir uma Sessão de SPAN no Módulo de Serviço de VPN, com o Erro "% Sessão [Nº da Sessão:] Utilizada pelo Módulo de Serviço"

Com esse problema, o módulo do Virtual Private Network (VPN) é introduzido no chassi, onde já tinha sido introduzido um módulo de switch fabric.

O Cisco IOS Software cria automaticamente uma sessão de SPAN para o módulo de serviço VPN de modo lidar com o tráfego de multicast.

Emita este comando para excluir a sessão de SPAN criada pelo software para o módulo de serviço VPN:

```
<#root>
```

```
Switch(config)#
```

```
no monitor session session_number service-module
```



Observação: se você excluir a sessão, o módulo de serviço VPN descartará o tráfego multicast.

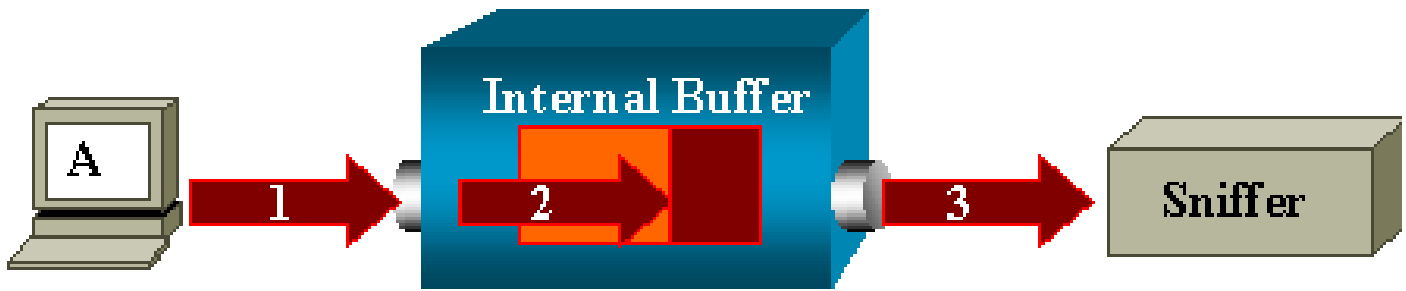
---

## Por que Não é Possível Capturar Pacotes Corrompidos com SPAN?

Você não pode capturar pacotes corrompidos com SPAN devido à maneira com a qual os switches funcionam no geral. Quando um pacote passa por um switch, os seguintes eventos acontecem:

1. O pacote alcança a porta de ingresso.

2. O pacote é armazenado em, no mínimo, um buffer.
3. O pacote é retransmitido eventualmente na porta de saída.



Se o switch recebe um pacote corrompido, a porta de entrada geralmente o descarta. Portanto, você não vê o pacote na porta de saída.

Um switch não é completamente transparente com respeito à captação do tráfego.

Do mesmo modo, quando você vê um pacote corrompido no farejador no cenário desta seção, você sabe que os erros foram gerados na etapa 3, no segmento de saída.

Se você acredita que um dispositivo envia pacotes corrompidos, você pode escolher colocar o host de envio e o dispositivo farejador em um hub. O hub não executa nenhuma verificação de erro.

Dessa maneira, diferente do switch, o hub não descarta os pacotes. Assim, você pode ver os pacotes.

## Erro : % Sessão 2 usada pelo módulo de serviço

Se um módulo de serviço de firewall (FWSM, Firewall Service Module) foi, por exemplo, instalado e removido posteriormente no CAT6500, ele habilita automaticamente o recurso Refletor de SPAN.

O recurso Refletor de SPAN utiliza uma sessão de SPAN no switch.

Caso não precise mais dele, você deverá poder inserir o comando no monitor session service module de dentro do modo de configuração do CAT6500 e, em seguida, inserir imediatamente a nova configuração de SPAN desejada.

## A Porta Refletora Descarta Pacotes

Uma porta refletora recebe cópias do tráfego enviado e recebido para todas as portas de origem monitoradas. Se uma porta refletora receber um excesso de assinaturas, ela poderá ficar congestionada.

Isso pode afetar o encaminhamento de tráfego em uma ou mais portas de origem.

Se a largura de banda da porta refletora não for suficiente para o volume de tráfego das portas de origem correspondentes, os pacotes em excesso serão descartados.

Uma porta de 10/100 se reflete em 100 Mbps. Uma porta de gigabit se reflete em 1 Gbps.

## A Sessão de SPAN é Sempre Utilizada com um FWSM no Catalyst 6500 Chassis

Quando você utiliza o Supervisor Engine 720 com um FWSM no chassi que executa o Cisco Native IOS, uma sessão de SPAN é utilizada por padrão. Se você faz uma verificação de sessões não utilizadas com o comando `show monitor`, a sessão 1 é utilizada:

```
<#root>
```

```
Cat6K#
```

```
show monitor
```

```
Session 1
```

```
-----
```

```
Type : Service Module Session
```

Quando um blade de firewall está no chassi do Catalyst 6500, a sessão é instalada automaticamente para o suporte da replicação de multicast do hardware, já que um FWSM não pode replicar streams de multicast.

Se os streams de multicast originados no FWSM precisam ser replicados na Camada 3 para as várias placas de linha, a sessão automática copia o tráfego ao supervisor através de um canal da tela.

Se você tem uma origem de multicast que gera um stream de multicast do FWSM, você precisa do refletor de SPAN.

Se você coloca a origem de multicast na VLAN externa, o refletor de SPAN não é necessário. O refletor de SPAN é incompatível com BPDUs de bridging através do FWSM.

Você pode usar o comando `no monitor session service module` para desabilitar o refletor de SPAN.

## Uma Sessão de SPAN e de RSPAN Podem Ter o Mesmo ID Dentro do Mesmo Switch?

Não, não é possível utilizar o mesmo ID de sessão para uma sessão de SPAN regular e uma sessão de destino de RSPAN. Cada sessão de SPAN e RSPAN devem ter um ID de sessão diferente.

## Uma Sessão de RSPAN Pode Funcionar em Domínios Diferentes de VTP?

Yes. Uma sessão de RSPAN pode funcionar em domínios de VTP diferentes. Mas é necessário assegurar-se de que a VLAN de RSPAN esteja presente nos bancos de dados dos domínios de VTP.

Além disso, assegure-se de que nenhum dispositivo de Camada 3 esteja presente no caminho de origem da sessão para o destino da sessão.

## Uma Sessão de RSPAN Pode Funcionar em WAN ou em Redes Diferentes?

Não. A sessão de RSPAN não pode cruzar nenhum dispositivo de Camada 3, porque o RSPAN é um recurso de LAN (Camada 2).

Para monitorar o tráfego ao longo de uma WAN ou de diferentes redes, utilize o ERSPAN (Encapsulated Remote SwitchPort Analyser).

O recurso ERSPAN suporta portas de origem, VLANs de origem e portas de destino em diferentes switches, o que fornece a monitoração remota de vários switches ao longo da rede.

O ERSPAN consiste em uma sessão de origem de ERSPAN, tráfego roteável encapsulado por GRE de ERSPAN e uma sessão de destino de ERSPAN.

Você configura as sessões de origem de ERSPAN e as sessões de destino separadamente em switches diferentes.

No momento, o recurso ERSPAN é suportado em:

- Supervisor 720 com PFC3B ou PFC3BXL executado em Cisco IOS Software Release 12.2(18)SXE ou posterior
- Supervisor 720 com PFC3A que tenha o hardware na versão 3.2 ou posterior e que esteja executando o Cisco IOS Software Release 12.2(18)SXE ou posterior

Consulte [Configuring Local SPAN, Remote SPAN \(RSPAN\), and Encapsulated RSPAN - Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX para obter mais informações sobre o ERSPAN.](#)

## Uma Sessão de Origem e a Sessão de Destino de RSPAN Podem Existir no Mesmo Catalyst Switch?

Não. O RSPAN não funciona quando a sessão de origem de RSPAN e a sessão de destino de RSPAN estão no mesmo switch.

Se uma sessão de origem de RSPAN está configurada com uma VLAN de RSPAN específica, e uma sessão de destino de RSPAN para essa VLAN de RSPAN está configurada no mesmo switch, a porta de destino da sessão de destino de RSPAN não transmite os pacotes captados da sessão de origem de RSPAN devido a limitações de hardware. Isso não é suportado nos 4500 Series e 3750 Series Switches.

Este problema está documentado no bug da Cisco ID [CSCeg08870 \(somente clientes registrados\)](#).

Este é um exemplo:

```
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
```

A solução para esse problema é utilizar o SPAN regular.

## O Analisador de Rede/Dispositivo de Segurança Conectado à Porta de Destino de SPAN Não Pode Ser Alcançado

As características básicas de uma porta de destino de SPAN são que ela não transmite nenhum tráfego, exceto o tráfego necessário para a sessão de SPAN.

Se você precisa de acessar (acessibilidade de IP) o analisador de rede/dispositivo de segurança através da porta de destino de SPAN, é necessário habilitar o encaminhamento de tráfego de entrada.

Quando a entrada é habilitada, a porta de destino de SPAN aceita os pacotes recebidos, que são etiquetados potencialmente, dependendo do modo de encapsulamento especificado, e comutados normalmente.

Quando você configura uma porta de destino de SPAN, é possível especificar se o recurso de entrada será ou não habilitado e qual VLAN utilizar para comutar os pacotes de entrada sem etiqueta.

A especificação de uma VLAN de entrada não é necessária quando o encapsulamento de ISL é configurado, já que todos os pacotes encapsulados por ISL possuem etiquetas de VLAN.

Embora a porta seja para encaminhamento de STP, ela não participa do STP; desse modo, tenha cuidado ao configurar o recurso para que não seja introduzido um loop de spanning tree na rede.

Quando a entrada e um encapsulamento de tronco são especificados em uma porta de destino de SPAN, a porta começa a encaminhar em todas as VLANs ativas.

A configuração de uma VLAN inexistente como uma VLAN de entrada não é permitida.

```
monitor session session_number destination interface interface [encapsulation {isl | dot1q}]
ingress [vlan vlan_IDs]
```

Este exemplo mostra como configurar uma porta de destino com encapsulamento 802.1q e pacotes de entrada com o uso da VLAN 7 nativa.

<#root>

```
Switch(config)#
```

```
monitor session 1 destination interface fastethernet 5/48
encapsulation dot1q ingress vlan 7
```

Com essa configuração, o tráfego das origens de SPAN associado à sessão 1 é copiado para fora da interface Fast Ethernet 5/48, com o encapsulamento 802.1q.

O tráfego de entrada é aceitado e comutado, com os pacotes sem etiqueta classificados na VLAN 7.

## Informações Relacionadas

- [Como configurar o SPAN e o RSPAN nos Cisco Catalyst 4500 switches que executam o Cisco IOS Software](#)
- [Uma porta de destino de SPAN é mostrada como “não conectada” e não se comunica com o restante da rede](#)
- [Suporte ao Produto - Switches](#)
- [Suporte de tecnologia de switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.