Konfigurationsbeispiel für Catalyst Switched Port Analyzer (SPAN)

Inhalt

Einführung

In diesem Dokument werden die neuesten implementierten Funktionen des Switched Port Analyzer (SPAN) beschrieben. Die SPAN-Funktion, die manchmal auch als Port-Spiegelung oder Port-Überwachung bezeichnet wird, wählt Netzwerkverkehr zur Analyse durch einen Netzwerkanalyst aus. Der Netzwerkanalysator kann ein Cisco SwitchProbe-Gerät oder eine andere Remote Monitoring (RMON)-Prüfung sein. Früher war SPAN eine relativ einfache Funktion bei Switches der Cisco Catalyst-Serie. Mit den neuesten Versionen des Catalyst OS (CatOS) wurden dem Benutzer jedoch zahlreiche Verbesserungen und neue Möglichkeiten eröffnet. Dieses Dokument ist nicht als alternative Konfigurationsanleitung für die SPAN-Funktion vorgesehen. Dieses Dokument beantwortet die häufigsten Fragen zu SPAN, z. B.:

- Was ist SPAN und wie wird es konfiguriert?
- Welche verschiedenen Funktionen sind verfügbar (insbesondere mehrere, gleichzeitige SPAN-Sitzungen), und welche Softwareebene ist für deren Ausführung erforderlich?
- Wirkt sich SPAN auf die Switch-Leistung aus?

Voraussetzungen

Catalyst Switches mit Unterstützung von SPAN, RSPAN und ERSPAN

Catalyst-Switches	SPAN-Unterstützung	RSPAN-Unterstützung	ERSPAN-Unterstützung
Catalyst Express der Serien 500 und 520	Ja	Nein	Nein
Catalyst Serie 6500/6000	Ja	Ja	Ja Supervisor 2T mit PFC4, Supervisor 720 mit PFC3B oder PFC3BXL mit Cisco IOS Software Release 12.2(18)SXE oder höher. Supervisor 720 mit PFC3A mit Hardwareversion 3.2 oder höher und Cisco IOS Software Release 12.2(18)SXE oder höher
Catalyst Serie 5500/5000	Ja	Nein	Nein
Catalyst Serie 4900	Ja	Ja	Nein
Catalyst Serie 4500/4000 (einschließlich 4912G)	Ja	Ja	Nein
Catalyst Serie 3750 Metro	Ja	Ja	Nein
Catalyst Serie 3750/3750E/3750X	Ja	Ja	Nein
Catalyst Serie 3560/3560E/3650X	Ja	Ja	Nein
Catalyst Serie 3550	Ja	Ja	Nein
Catalyst Serie 3500 XL	Ja	Nein	Nein
Catalyst Serie 2970	Ja	Ja	Nein

Catalyst Serie 2960	Ja	Ja	Nein
Catalyst Serie 2955	Ja	Ja	Nein
Catalyst Serie 2950	Ja	Ja	Nein
Catalyst Serie 2940	Ja	Nein	Nein
Catalyst 2948G-L3	Nein	Nein	Nein
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A	Ja	Ja	Nein
Catalyst Serie 2900XL	Ja	Nein	Nein
Catalyst Serie 1900	Ja	Nein	Nein

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

In diesem Dokument wird CatOS 5.5 als Referenz für Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 verwendet. Auf den Catalyst Switches der Serien 2900XL/3500XL wird die Cisco IOS® Softwareversion 12.0(5)XU verwendet. Obwohl dieses Dokument aktualisiert wird, um Änderungen am SPAN wiederzugeben, finden Sie in den Versionshinweisen zur Switch-Plattform die neuesten Entwicklungen zur SPAN-Funktion.

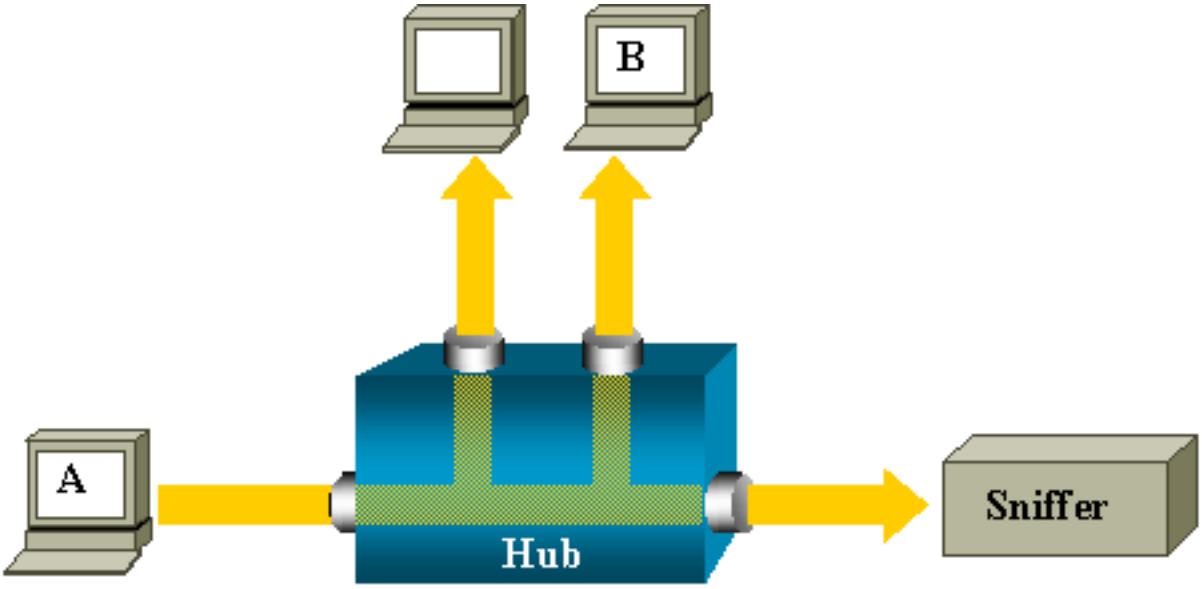
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

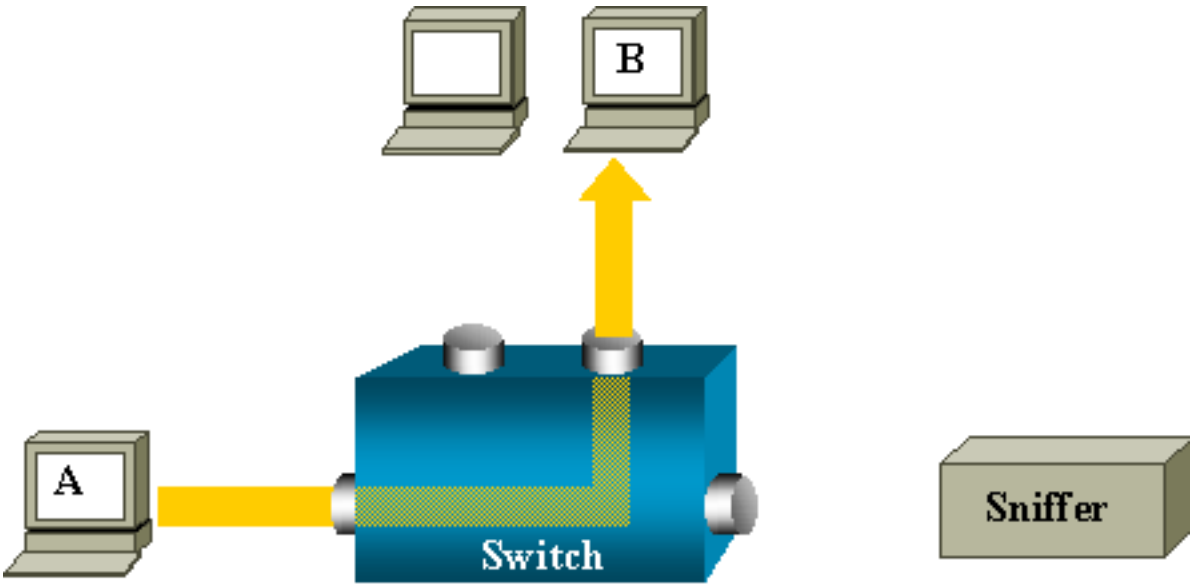
Kurze Beschreibung des SPAN

Was ist SPAN und warum wird es benötigt? Die SPAN-Funktion wurde auf Switches eingeführt, da Switches einen grundlegenden Unterschied zu Hubs aufweisen. Wenn ein Hub ein Paket an einem Port empfängt, sendet der Hub eine Kopie dieses Pakets an allen Ports außer an dem, an dem der Hub das Paket empfangen hat. Nach dem Booten eines Switches beginnt der Aufbau einer Layer-2-Weiterleitungstabelle auf Basis der Quell-MAC-Adresse der verschiedenen Pakete, die der Switch empfängt. Nachdem diese Weiterleitungstabelle erstellt wurde, leitet der Switch Datenverkehr, der für eine MAC-Adresse bestimmt ist, direkt an den entsprechenden Port weiter.

Wenn Sie beispielsweise Ethernet-Datenverkehr erfassen möchten, der von Host A an Host B gesendet wird und beide mit einem Hub verbunden sind, fügen Sie einfach einen Sniffer an diesen Hub an. Alle anderen Ports sehen den Datenverkehr zwischen den Hosts A und B:



Nachdem die MAC-Adresse des Hosts B auf einem Switch abgerufen wurde, wird der Unicast-Datenverkehr von A nach B nur an den B-Port weitergeleitet. Der Sniffer sieht daher diesen Datenverkehr nicht:

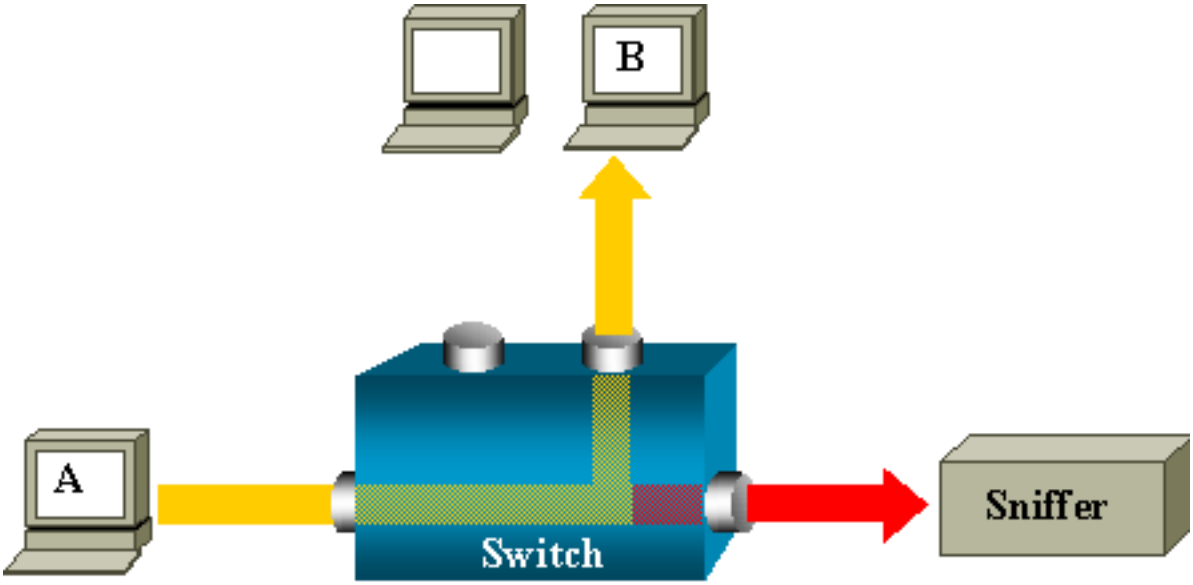


In dieser Konfiguration erfasst der Sniffer nur Datenverkehr, der an alle Ports überflutet wird, z. B.:

- Broadcast-Datenverkehr
- Multicast-Datenverkehr mit CGMP oder IGMP-Snooping (Internet Group Management Protocol) deaktiviert
- Unbekannter Unicast-Datenverkehr

Unicast-Flooding tritt auf, wenn der Switch die Ziel-MAC-Adresse nicht in seiner CAM-Tabelle (Content-Addressable Memory) hat. Der Switch weiß nicht, wohin der Datenverkehr gesendet werden soll. Der Switch überflutet die Pakete mit allen Ports im Ziel-VLAN.

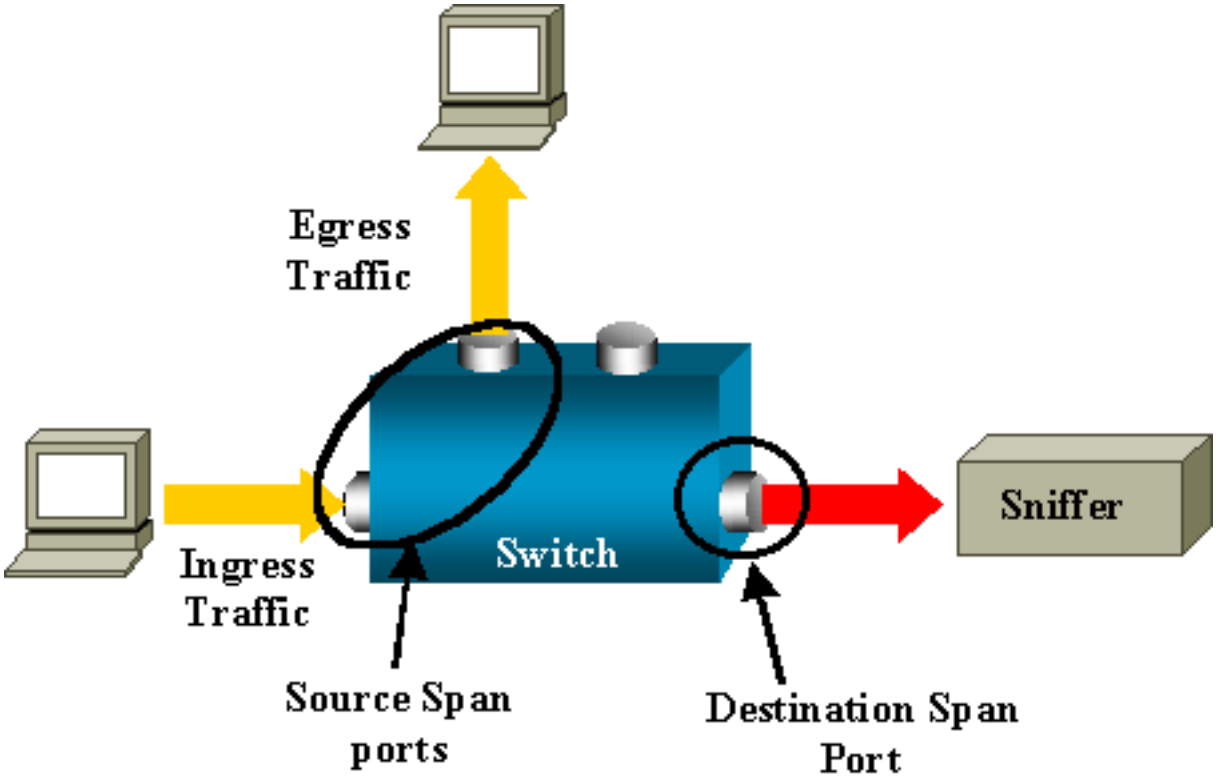
Eine zusätzliche Funktion ist erforderlich, die Unicast-Pakete, die Host A an den Sniffer-Port senden, künstlich kopiert:



In diesem Diagramm ist der Sniffer an einen Port angeschlossen, der so konfiguriert ist, dass er eine Kopie jedes Pakets empfängt, das Host A sendet. Dieser Port wird als SPAN-Port bezeichnet. In den anderen Abschnitten dieses Dokuments wird beschrieben, wie Sie diese Funktion sehr präzise einstellen können, um mehr zu erreichen als nur einen Port zu überwachen.

SPAN-Terminologie

- **Eingehender Datenverkehr** - Datenverkehr, der in den Switch gelangt.
- **Ausgangsdatenverkehr** - Datenverkehr, der den Switch verlässt.
- Source (SPAN)-Port - Ein Port, der mithilfe der SPAN-Funktion überwacht wird.
- Source (SPAN) VLAN: Ein VLAN, dessen Datenverkehr mithilfe der SPAN-Funktion überwacht wird.
- **Ziel-Port (SPAN): Ein Port, der Quellports überwacht, normalerweise wenn ein Netzwerkanalyst angeschlossen ist.**
- Reflector Port - Ein Port, der Pakete auf ein RSPAN-VLAN kopiert.
- **Monitor-Port** - Ein Monitor-Port ist auch ein Ziel-SPAN-Port in der Terminologie Catalyst 2900XL/3500XL/2950.



- **Lokaler SPAN** - Die SPAN-Funktion ist lokal, wenn sich alle überwachten Ports auf demselben Switch wie der Zielport befinden. Diese Funktion steht im Gegensatz zu Remote SPAN (RSPAN), das in dieser Liste ebenfalls definiert wird.
- **Remote SPAN (RSPAN)** - Einige Quellports befinden sich nicht auf demselben Switch wie der Zielport. RSPAN ist eine erweiterte Funktion, für die ein spezielles VLAN erforderlich ist, um den von SPAN überwachten Datenverkehr zwischen Switches zu übertragen. RSPAN wird nicht auf allen Switches unterstützt. Prüfen Sie in den entsprechenden Versionshinweisen oder im Konfigurationsleitfaden, ob Sie RSPAN auf dem bereitgestellten Switch verwenden können.
- **Port-based SPAN (PSPAN)** - Der Benutzer gibt einen oder mehrere Quell-Ports am Switch und einen Zielport an.
- **VLAN-basiertes SPAN (VSPAN)** - Auf einem bestimmten Switch kann der Benutzer alle Ports eines bestimmten VLANs mit einem einzigen Befehl überwachen.
- **ESPAN** - Dies bedeutet eine verbesserte SPAN-Version. Dieser Begriff wurde während der Entwicklung des SPAN mehrfach verwendet, um zusätzliche Funktionen zu benennen. Daher ist der Begriff nicht sehr klar. Die Verwendung dieses Begriffs wird in diesem Dokument vermieden.
- **Administrative Source**: Eine Liste der Quellports oder VLANs, die für die Überwachung konfiguriert wurden.
- **Operative Quelle**: Eine Liste der Ports, die effektiv überwacht werden. Diese Port-Liste kann sich von der administrativen Quelle unterscheiden. Ein Port, der sich im heruntergefahrenen Modus befindet, kann beispielsweise in der administrativen Quelle erscheinen, wird aber nicht effektiv überwacht.

Merkmale des Quell-Ports

Ein Quellport, auch als überwachter Port bezeichnet, ist ein Switch- oder gerouteter Port, den Sie zur Analyse des Netzwerkverkehrs überwachen. In einer einzigen lokalen SPAN-Sitzung oder RSPAN-Quellsitzung können Sie den Quellport-Datenverkehr, wie z. B. "Receive" (Rx),

"Transported (Tx)" oder "Bidirectional" (beide), überwachen. Der Switch unterstützt eine beliebige Anzahl von Quell-Ports (bis zur maximalen Anzahl der verfügbaren Ports auf dem Switch) und eine beliebige Anzahl von Quell-VLANs.

Ein Quellport weist die folgenden Merkmale auf:

- Dabei kann es sich um einen beliebigen Port-Typ handeln, z. B. EtherChannel, Fast Ethernet, Gigabit Ethernet usw.
- Sie kann in mehreren SPAN-Sitzungen überwacht werden.
- Es darf sich nicht um einen Zielport handeln.
- Jeder Quellport kann mit einer Richtung (Eingang, Ausgang oder beide) konfiguriert werden, die überwacht werden soll. Für EtherChannel-Quellen gilt die überwachte Richtung für alle physischen Ports in der Gruppe.
- Quellports können sich in den gleichen oder unterschiedlichen VLANs befinden.
- Für VLAN SPAN-Quellen werden alle aktiven Ports im Quell-VLAN als Quell-Ports enthalten.

VLAN-Filterung

Wenn Sie einen Trunk-Port als Quellport überwachen, werden alle VLANs, die auf dem Trunk aktiv sind, standardmäßig überwacht. Sie können die VLAN-Filterung verwenden, um die Überwachung des SPAN-Datenverkehrs an Trunk-Quellports auf bestimmte VLANs zu beschränken.

- Die VLAN-Filterung gilt nur für Trunk-Ports oder Sprach-VLAN-Ports.
- Die VLAN-Filterung gilt nur für Port-basierte Sitzungen und ist in Sitzungen mit VLAN-Quellen nicht zulässig.
- Wenn eine VLAN-Filterliste angegeben wird, werden nur die VLANs in der Liste auf Trunk-Ports oder Sprach-VLAN-Zugriffsports überwacht.
- SPAN-Datenverkehr von anderen Port-Typen wird durch die VLAN-Filterung nicht beeinflusst, d. h., alle VLANs sind an anderen Ports zulässig.
- Die VLAN-Filterung betrifft nur den an den SPAN-Zielport weitergeleiteten Datenverkehr und hat keine Auswirkungen auf das Umschalten des normalen Datenverkehrs.
- Sie können Quell-VLANs nicht mischen und VLANs innerhalb einer Sitzung filtern. Sie können Quell-VLANs haben oder VLANs filtern, aber nicht beide gleichzeitig.

Merkmale des Quell-VLAN

VSPAN ist die Überwachung des Netzwerkverkehrs in einem oder mehreren VLANs. Die SPAN- oder RSPAN-Quellschnittstelle in VSPAN ist eine VLAN-ID, und der Datenverkehr wird auf allen Ports für dieses VLAN überwacht.

Das VSPAN zeichnet sich durch folgende Merkmale aus:

- Alle aktiven Ports im Quell-VLAN sind als Quell-Ports enthalten und können in eine oder beide Richtungen überwacht werden.
- An einem bestimmten Port wird nur Datenverkehr im überwachten VLAN an den Zielport gesendet.
- Wenn ein Zielport zu einem Quell-VLAN gehört, wird er von der Quellliste ausgeschlossen und nicht überwacht.
- Wenn Ports zu den Quell-VLANs hinzugefügt oder aus diesen entfernt werden, wird der

Datenverkehr im Quell-VLAN, der von diesen Ports empfangen wird, zu den Quellen hinzugefügt oder aus diesen entfernt, die überwacht werden.
- Sie können keine Filter-VLANs in derselben Sitzung mit VLAN-Quellen verwenden.
- Sie können nur Ethernet-VLANs überwachen.

Merkmale des Zielports

Jede lokale SPAN-Sitzung oder RSPAN-Zielsitzung muss über einen Zielport (auch als Überwachungsport bezeichnet) verfügen, der eine Kopie des Datenverkehrs von den Quellports und VLANs empfängt.

Ein Zielport weist die folgenden Merkmale auf:

- Ein Zielport muss sich auf demselben Switch wie der Quellport befinden (für eine lokale SPAN-Sitzung).
- Ein Zielport kann jeder physische Ethernet-Port sein.
- Ein Zielport kann jeweils nur an einer SPAN-Sitzung teilnehmen. Ein Zielport in einer SPAN-Sitzung darf kein Zielport für eine zweite SPAN-Sitzung sein.
- Ein Zielport kann kein Quellport sein.
- Ein Zielport kann keine EtherChannel-Gruppe sein.**Hinweis**: Ab der Cisco IOS-Softwareversion 12.2(33)SXH kann die Port-Channel-Schnittstelle ein Zielport sein. Ziel-EtherChannels unterstützen die PAgP- (Port Aggregation Control Protocol) oder LACP-EtherChannel-Protokolle (Link Aggregation Control Protocol) nicht. Es wird nur der On-Modus unterstützt, wobei alle EtherChannel-Protokolle deaktiviert sind.**Hinweis**: Weitere Informationen finden Sie unter Lokale SPAN-, RSPAN- und ERSPAN-Ziele.
- Ein Zielport kann ein physischer Port sein, der einer EtherChannel-Gruppe zugewiesen wird, selbst wenn die EtherChannel-Gruppe als SPAN-Quelle angegeben wurde. Der Port wird aus der Gruppe entfernt, während er als SPAN-Zielport konfiguriert ist.
- Der Port leitet keinen Datenverkehr weiter, mit Ausnahme des für die SPAN-Sitzung erforderlichen Datenverkehrs, es sei denn, die Lernfunktion ist aktiviert. Wenn die Lernfunktion aktiviert ist, überträgt der Port auch den Datenverkehr an Hosts, die auf dem Zielport gelernt wurden.**Hinweis**: Weitere Informationen finden Sie unter Lokale SPAN-, RSPAN- und ERSPAN-Ziele.
- Der Status des Zielports ist standardmäßig aktiv/inaktiv. Die Schnittstelle zeigt den Port in diesem Zustand an, um sicherzustellen, dass der Port derzeit nicht als Produktionsport verwendbar ist.
- Wenn die Weiterleitung des eingehenden Datenverkehrs für ein Netzwerksicherheitsgerät aktiviert ist. Der Zielport leitet den Datenverkehr auf Layer 2 weiter.
- Ein Zielport ist nicht am Spanning Tree beteiligt, während die SPAN-Sitzung aktiv ist.
- Wenn es sich um einen Zielport handelt, ist er nicht an einem der Layer-2-Protokolle (STP, VTP, CDP, DTP, PagP) beteiligt.
- Ein Zielport, der zu einem Quell-VLAN einer SPAN-Sitzung gehört, wird von der Quellliste ausgeschlossen und nicht überwacht.
- Ein Zielport empfängt Kopien von gesendetem und empfangenen Datenverkehr für alle überwachten Quell-Ports. Wenn ein Zielport überbelegt ist, kann dieser überlastet werden. Diese Überlastung kann die Weiterleitung des Datenverkehrs an einem oder mehreren Quellports beeinträchtigen.

Merkmale des Reflektorports

Der Reflektorport ist der Mechanismus, der Pakete auf ein RSPAN-VLAN kopiert. Der Reflektorport leitet nur den Datenverkehr von der RSPAN-Quellsitzung weiter, der er angehört. Jedes Gerät, das mit einem als Reflektorport festgelegten Port verbunden ist, verliert die Verbindung, bis die RSPAN-Quellsitzung deaktiviert ist.

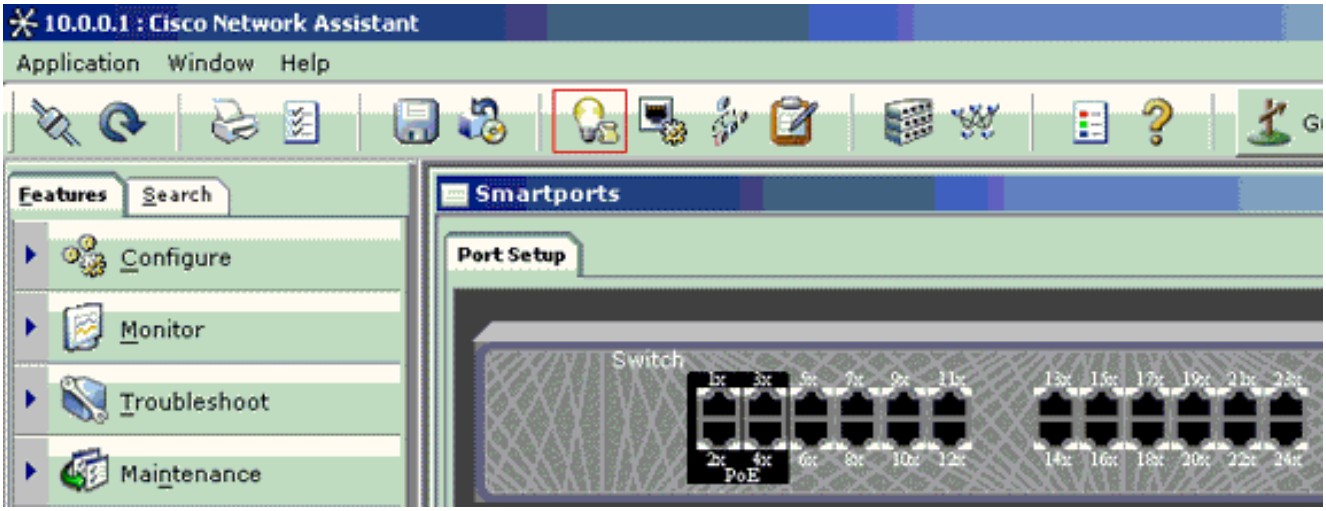
Der Reflektorport weist die folgenden Merkmale auf:

- Es ist ein Loopback-Port.
- Es kann keine EtherChannel-Gruppe sein, es ist kein Trunk, und es kann keine Protokollfilterung durchgeführt werden.
- Es kann sich um einen physischen Port handeln, der einer EtherChannel-Gruppe zugewiesen wird, selbst wenn die EtherChannel-Gruppe als SPAN-Quelle angegeben ist. Der Port wird aus der Gruppe entfernt, während er als Reflektorport konfiguriert ist.
- Ein Port, der als Reflektorport verwendet wird, kann weder ein SPAN-Quell- oder Zielport sein, noch kann ein Port gleichzeitig ein Reflektorport für mehr als eine Sitzung sein.
- Sie ist für alle VLANs nicht sichtbar.
- Das native VLAN für Looped-Back-Datenverkehr an einem Reflektorport ist das RSPAN-VLAN.
- Der Reflektor-Port schleift ungetaggten Datenverkehr zurück zum Switch. Der Datenverkehr wird dann im RSPAN-VLAN platziert und an alle Trunk-Ports geleitet, die das RSPAN-VLAN übertragen.
- Spanning Tree wird auf einem Reflektorport automatisch deaktiviert.
- Ein Reflektorport empfängt Kopien von gesendetem und empfangenem Datenverkehr für alle überwachten Quell-Ports.

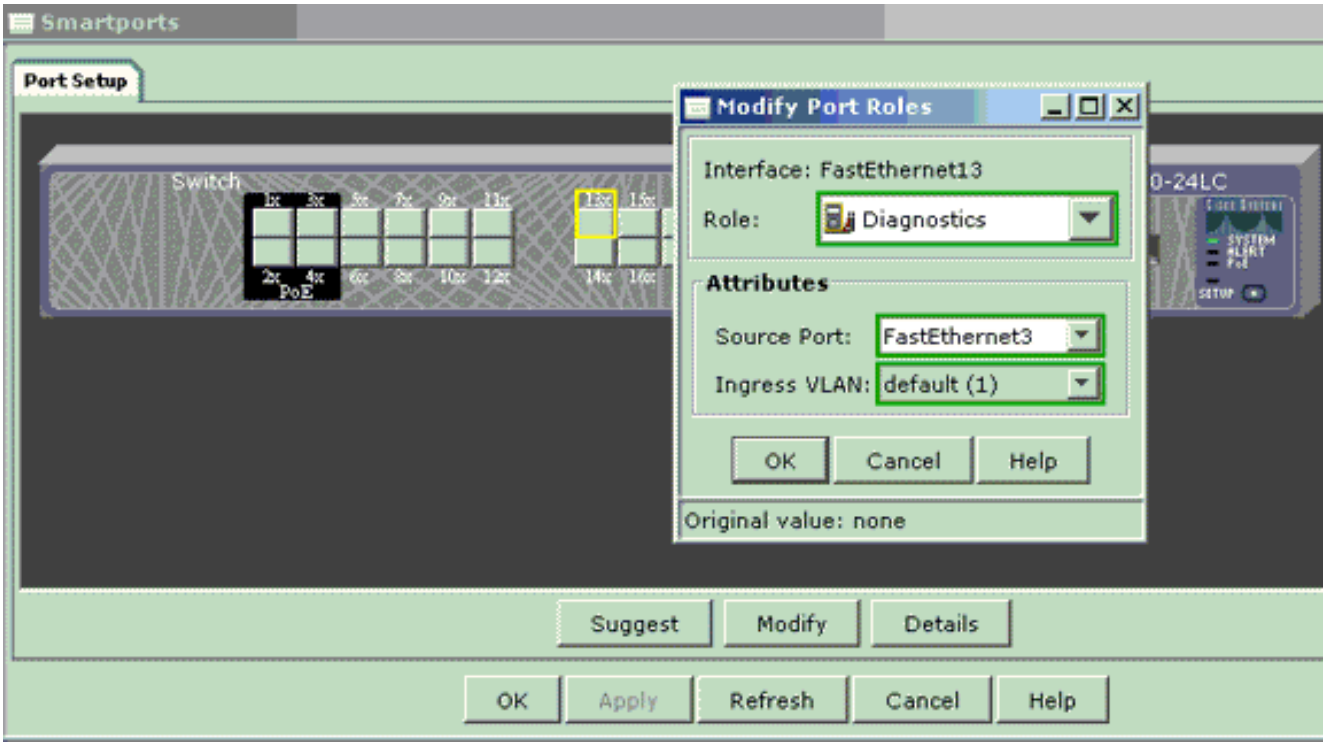
SPAN auf Catalyst Express 500/520

Catalyst Express 500 oder Catalyst Express 520 unterstützen nur die SPAN-Funktion. Catalyst Express 500/520-Ports können nur mit dem Cisco Network Assistant (CNA) für SPAN konfiguriert werden. Gehen Sie wie folgt vor, um das SPAN zu konfigurieren:

1. Laden Sie CNA herunter, und installieren Sie es auf dem PC. Sie können CNA von der Seite Download Software herunterladen (nur registrierte Kunden).
2. Führen Sie die Schritte aus, die im Einführungsleitfaden für die Catalyst Express 500 Switches 12.2(25)FY beschrieben werden, um die Switch-Einstellungen für Catalyst Express 500 anzupassen. Weitere Informationen zu Catalyst Express 520 Switches finden Sie im Einführungsleitfaden für Catalyst Express 520.
3. Verwenden Sie CNA, um sich beim Switch anzumelden, und klicken Sie auf **Smartport**.



4. Klicken Sie auf eine beliebige Schnittstelle, an die Sie den PC anschließen möchten, um die Sniffer-Traces zu erfassen.
5. Klicken Sie auf **Ändern**. Ein kleines Popup-Fenster wird angezeigt.
6. Wählen Sie die **Diagnosefunktion** für den Port aus.
7. Wählen Sie den Quellport aus, und wählen Sie das VLAN aus, das Sie überwachen möchten. Wenn Sie none auswählen, empfängt der Port nur Datenverkehr. Das Eingangs-VLAN ermöglicht es dem mit dem Diagnoseport verbundenen PC, Pakete an das Netzwerk zu senden, das dieses VLAN
verwendet.



8. Klicken Sie auf **OK**, um das Popup-Feld zu schließen.
9. Klicken Sie auf **OK** und dann auf Einstellungen **anwenden**.
10. Sie können jede Sniffer-Software verwenden, um den Datenverkehr zu verfolgen, sobald Sie den Diagnoseport eingerichtet haben.

SPAN bei Catalyst Switches der Serie 2900XL/3500XL

Verfügbare Funktionen und Einschränkungen

Die Port-Überwachungsfunktion des Catalyst 2900XL/3500XL ist nicht sehr umfangreich. Daher ist diese Funktion relativ leicht zu verstehen.

Sie können so viele lokale PSPAN-Sitzungen wie erforderlich erstellen. Sie können beispielsweise PSPAN-Sitzungen auf dem Konfigurationsport erstellen, den Sie als Ziel-SPAN-Port ausgewählt haben. Geben Sie in diesem Fall den Befehl **Port Monitor *Interface* (Schnittstelle für die Portüberwachung)** ein, um die zu überwachenden Quellports aufzulisten. Ein Monitor-Port ist ein Ziel-SPAN-Port in der Terminologie Catalyst 2900XL/3500XL.

- Die Haupteinschränkung besteht darin, dass alle Ports, die sich auf eine bestimmte Sitzung beziehen (Quelle oder Ziel), demselben VLAN angehören müssen.
- Wenn Sie die VLAN-Schnittstelle mit einer IP-Adresse konfigurieren, überwacht der Befehl **Port Monitor** den Datenverkehr, der nur an diese IP-Adresse gerichtet ist. Er überwacht außerdem den Broadcast-Datenverkehr, der von der VLAN-Schnittstelle empfangen wird. Der Datenverkehr, der im tatsächlichen VLAN selbst fließt, wird jedoch nicht erfasst. Wenn Sie im Befehl **Port Monitor** keine Schnittstelle angeben, werden alle anderen Ports überwacht, die demselben VLAN wie die Schnittstelle angehören.

Diese Liste enthält einige Einschränkungen. Weitere Informationen finden Sie im Befehlsreferenz (Catalyst 2900XL/3500XL).

> **Hinweis**: ATM-Ports sind die einzigen Ports, die keine Überwachungsports sein können. Sie können jedoch auch ATM-Ports überwachen. Die Einschränkungen in dieser Liste gelten für Ports mit Portüberwachungsfunktion.

- Ein Monitorport kann nicht in einer Fast EtherChannel- oder Gigabit EtherChannel-Portgruppe sein.
- Ein Monitorport kann nicht für die Port-Sicherheit aktiviert werden.
- Ein Monitorport darf kein Multi-VLAN-Port sein.
- Ein Überwachungsport muss ein Mitglied desselben VLAN sein wie der überwachte Port. Änderungen an der VLAN-Mitgliedschaft sind für überwachte Ports und Ports nicht zulässig.
- Ein Monitorport kann kein dynamischer Zugriffsport oder Trunk-Port sein. Ein statischer Access-Port kann jedoch ein VLAN auf einem Trunk, einem Multi-VLAN oder einem Dynamic-Access-Port überwachen. Das überwachte VLAN ist das VLAN, das dem statischen Access-Port zugeordnet ist.
- Die Portüberwachung funktioniert nicht, wenn sowohl der Überwachungsport als auch der überwachte Port geschützt sind.

Achten Sie darauf, dass ein Port im Überwachungsstatus das Spanning Tree Protocol (STP) nicht ausführt, während der Port weiterhin dem VLAN der Ports angehört, die er spiegelt. Der Port-Monitor kann Teil einer Schleife sein, wenn Sie ihn beispielsweise mit einem Hub oder einer Bridge verbinden und mit einem anderen Teil des Netzwerks schleifen. In diesem Fall können Sie in eine katastrophale Bridging-Schleife gelangen, da STP Sie nicht mehr schützt. Siehe Warum erstellt die SPAN-Sitzung eine Bridging-Schleife? -Abschnitt dieses Dokuments ein Beispiel dafür, wie diese Bedingung auftreten kann.

Konfigurationsbeispiel

In diesem Beispiel werden zwei gleichzeitige SPAN-Sitzungen erstellt.

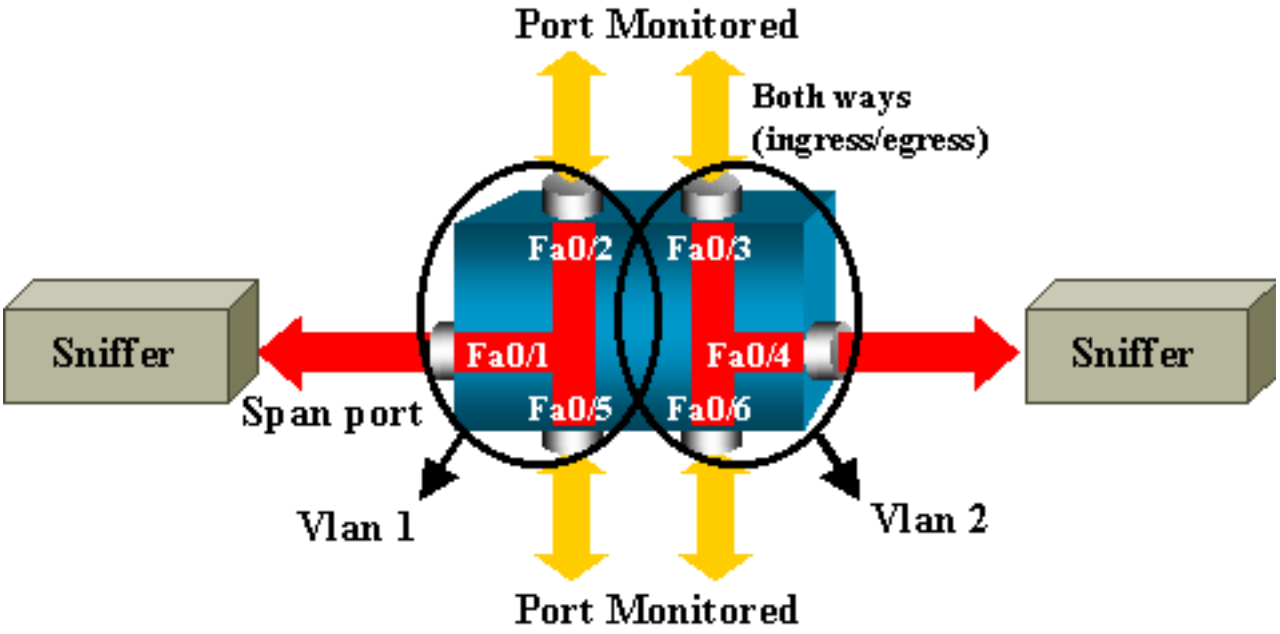
- Port Fast Ethernet 0/1 (Fa0/1) überwacht den Datenverkehr, der über die Ports Fa0/2 und

Fa0/5 gesendet und empfangen wird. Port Fa0/1 überwacht auch den Datenverkehr zur und von der Verwaltungsschnittstelle VLAN 1.

- Port Fa0/4 überwacht die Ports Fa0/3 und Fa0/6.

Die Ports Fa0/3, Fa0/4 und Fa0/6 werden alle in VLAN 2 konfiguriert. Andere Ports und die Verwaltungsschnittstelle werden im Standard-VLAN 1 konfiguriert.

Netzwerkdiagramm



Beispielkonfiguration auf dem Catalyst 2900XL/3500XL

2900XL/3500XL SPAN - Beispielkonfiguration

```
!--- 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.
```

Erläuterung der Konfigurationsschritte

Um Port Fa0/1 als Zielport zu konfigurieren, wählen Sie die Quell-Ports Fa0/2 und Fa0/5 und die Management-Schnittstelle (VLAN 1) im Konfigurationsmodus die Schnittstelle Fa0/1 aus:

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

Geben Sie die Liste der zu überwachenden Ports ein:

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

Mit diesem Befehl wird jedes Paket, das diese beiden Ports empfangen oder übertragen, ebenfalls in Port Fa0/1 kopiert. Führen Sie eine Änderung des Befehls **Port Monitor aus**, um die Überwachung für die Verwaltungsschnittstelle zu konfigurieren:

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

> **Hinweis**: Dieser Befehl bedeutet nicht, dass Port Fa0/1 das gesamte VLAN 1 überwacht. Das **VLAN 1**-Schlüsselwort bezieht sich lediglich auf die Verwaltungsschnittstelle des Switches.

Dieser Beispielbefehl veranschaulicht, dass der Monitor eines Ports in einem anderen VLAN nicht möglich ist:

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

Um die Konfiguration abzuschließen, konfigurieren Sie eine weitere Sitzung. Diesmal Fa0/4 als Ziel-SPAN-Port verwenden:

```
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
```

Führen Sie einen Befehl **show running** aus, oder verwenden Sie den Befehl **show port monitor**, um die Konfiguration zu überprüfen:

```
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
```

Hinweis: Die Catalyst Switches 2900XL und 3500XL unterstützen SPAN nicht nur in Rx-Richtung (Rx SPAN oder Eingangs-SPAN) oder nur in Tx-Richtung (Tx SPAN oder Ausgangs-SPAN). Alle SPAN-Ports sind so konzipiert, dass sowohl Rx- als auch Tx-Datenverkehr erfasst wird.

SPAN auf dem Catalyst 2948G-L3 und 4908G-L3

Die Catalyst Switches 2948G-L3 und 4908G-L3 sind fest konfigurierte Switch-Router oder Layer-3-Switches. Die SPAN-Funktion auf einem Layer-3-Switch wird als Port-Snooping bezeichnet. Port-Snooping wird auf diesen Switches jedoch nicht unterstützt. Weitere Informationen finden Sie im Abschnitt *Nicht unterstützte* Funktionen im Dokument Versionshinweise für Catalyst 2948G-L3 und Catalyst 4908G-L3 für Cisco IOS Release 12.0(10)W5(18g).

SPAN auf dem Catalyst 8500

Eine sehr einfache SPAN-Funktion ist auf dem Catalyst 8540 unter dem Namen Port Snooping verfügbar. Weitere Informationen finden Sie in der aktuellen Dokumentation zu Catalyst 8540.

Mit Port-Snooping kann der Datenverkehr von einem oder mehreren Quell-Ports auf transparente Weise zu einem Zielport gespiegelt werden."

Geben Sie den Befehl **snoop** ein, um eine portbasierte Datenverkehrsspiegelung oder Snooping einzurichten. Geben Sie die **no**-Form dieses Befehls ein, um Snooping zu deaktivieren:

```
snoop interface source_port direction snoop_direction

no snoop interface source_port
```

Die Variable ***source_port bezieht sich auf den überwachten Port.*** Die Variable ***snoop_direction*** ist die Richtung des Datenverkehrs auf dem bzw. den Quellports, die überwacht werden: **empfangen**, **übertragen** oder **beides**.

```
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
```

Dieses Beispiel zeigt die Ausgabe des Befehls **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)
```

Hinweis: Dieser Befehl wird auf Ethernet-Ports in einem Catalyst 8540 nicht unterstützt, wenn Sie ein Multiservice ATM Switch Router (MSR)-Image wie 8540m-in-mz ausführen. Stattdessen müssen Sie ein CSR-Image (Campus Switch Router) wie 8540c-in-mz verwenden.

SPAN für Catalyst Switches der Serien 2900, 4500/4000, 5500/5000 und 6500/6000, die CatOS ausführen

Dieser Abschnitt gilt nur für die folgenden Cisco Catalyst Switches der Serie 2900:

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

Dieser Abschnitt gilt für Cisco Catalyst Switches der Serie 4000 mit folgenden Funktionen:

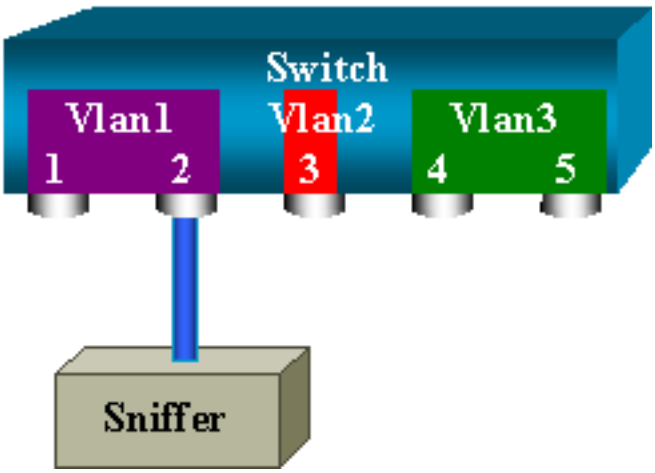
- Modulare Chassis-Switches:Cisco Catalyst Switch der Serie 4003Cisco Catalyst Switch der Serie 4006
- Switch mit fester Chassis: Cisco Catalyst Switch der Serie 4912G

Lokaler SPAN

SPAN-Funktionen wurden dem CatOS einzeln hinzugefügt, und eine SPAN-Konfiguration besteht aus einem einzigen **set span-**Befehl. Für den Befehl stehen jetzt zahlreiche Optionen zur Verfügung:

```
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]
```

In diesem Netzwerkdiagramm werden die verschiedenen SPAN-Möglichkeiten durch die Verwendung von Variationen vorgestellt:



Dieses Diagramm stellt einen Teil einer einzigen Linecard dar, die sich in Steckplatz 6 eines Catalyst 6500/6000-Switches befindet. In diesem Szenario:

- Die Ports 6/1 und 6/2 gehören zu VLAN 1.
- Port 6/3 gehört zu VLAN 2

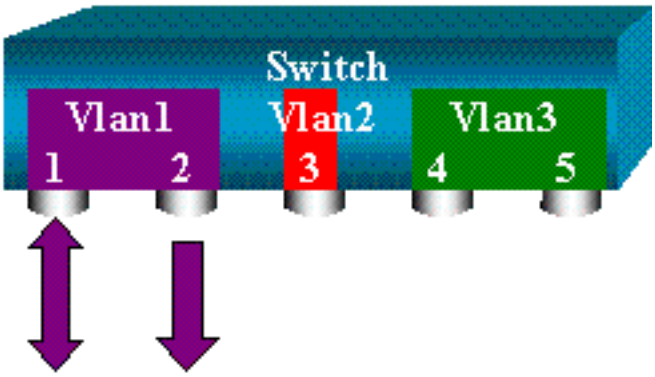
- Die Ports 6/4 und 6/5 gehören zu VLAN 3

Schließen Sie einen Sniffer an Port 6/2 an, und verwenden Sie ihn in verschiedenen Fällen als Monitorport.

PSPAN, VSPAN: Überwachung einiger Ports oder eines gesamten VLAN

Geben Sie die einfachste Form des Befehls **set span** ein, um einen einzelnen Port zu überwachen. Die Syntax lautet **span** ***source_port destination_port*****.**

Überwachung eines einzelnen Ports mit SPAN

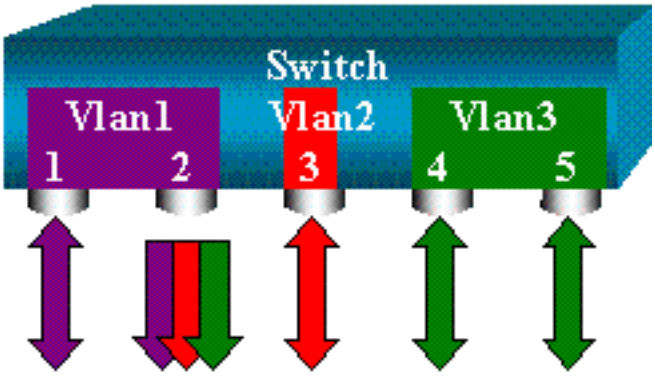



```
switch (enable) set span 6/1 6/2

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
```

Bei dieser Konfiguration wird jedes Paket, das über Port 6/1 empfangen oder gesendet wird, auf Port 6/2 kopiert. Wenn Sie die Konfiguration eingeben, wird dies klar beschrieben. Geben Sie den Befehl **show span** ein, um eine Zusammenfassung der aktuellen SPAN-Konfiguration zu erhalten:

```
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
```

Überwachung mehrerer Ports mit SPAN



Mit dem **Befehl set span** *source_ports destination_port* **kann der Benutzer mehr als einen Quellport angeben.** Listen Sie einfach alle Ports auf, an denen Sie das SPAN implementieren möchten, und trennen Sie die Ports durch Kommas. Mit dem Befehlszeileninterpreter können Sie auch den Bindestrich verwenden, um einen Port-Bereich anzugeben. In diesem Beispiel wird die Möglichkeit veranschaulicht, mehr als einen Port anzugeben. Im Beispiel wird SPAN für Port 6/1 und einen Bereich von drei Ports zwischen 6/3 und 6/5 verwendet:

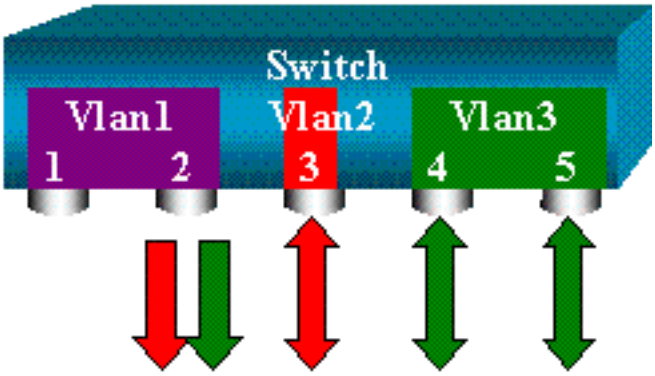
> **Hinweis**: Es kann nur einen Zielport geben. Geben Sie immer den Zielport nach der SPAN-Quelle an.

```
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
```

> **Hinweis**: Im Gegensatz zu Catalyst Switches der Serien 2900XL/3500XL können die Catalyst Switches der Serien 4500/4000, 5500/500 und 6500/6000 Ports überwachen, die zu mehreren verschiedenen VLANs mit CatOS-Versionen gehören. vor 5.1. Hier werden die gespiegelten Ports den VLANs 1, 2 und 3 zugewiesen.

VLANs mit SPAN überwachen

Mit dem Befehl **set span** können Sie einen Port so konfigurieren, dass der lokale Datenverkehr für ein gesamtes VLAN überwacht wird. Der Befehl lautet **span** *source_vlan(s) destination_port*.



Verwenden Sie eine Liste von einem oder mehreren VLANs als Quelle anstelle einer Port-Liste:

```
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
```

Bei dieser Konfiguration wird jedes Paket, das in VLAN 2 oder 3 eingeht oder es verlässt, auf Port 6/2 dupliziert.

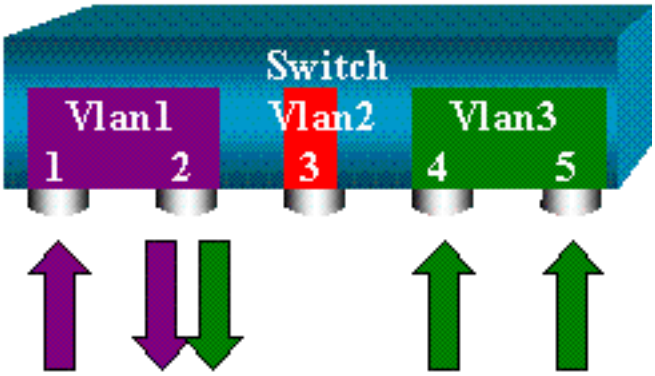
> **Hinweis**: Das Ergebnis ist genau das gleiche, wenn Sie SPAN auf allen Ports, die zu den vom Befehl angegebenen VLANs gehören, einzeln implementieren. Vergleichen Sie das Feld `Oper Source` und das Feld `Admin Source`. Im Feld `Admin Source` werden im Grunde alle Ports aufgelistet, die Sie für die SPAN-Sitzung konfiguriert haben. Im Feld `Oper Source` werden die Ports aufgelistet, die SPAN verwenden.

Eingangs-/Ausgangs-SPAN

Im Beispiel im Abschnitt Monitor VLANs with SPAN (Monitor-VLANs mit SPAN) wird der ein- und ausgehende Datenverkehr der angegebenen Ports überwacht. Die `Richtung: Das` Feld `"Senden/Empfangen"` zeigt dies. Mit den Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 können Sie nur ausgehenden (ausgehenden) oder nur eingehenden (eingehenden) Datenverkehr an einem bestimmten Port sammeln. Fügen Sie das **rx** (Receive)- oder **tx** (Transmit)-Schlüsselwort am Ende des Befehls hinzu. Der Standardwert ist **beides** (tx und rx).

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

In diesem Beispiel erfasst die Sitzung den gesamten eingehenden Datenverkehr für die VLANs 1 und 3 und spiegelt den Datenverkehr auf Port 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
```

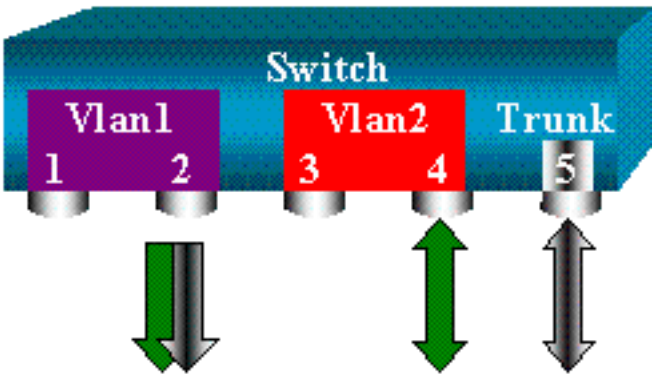
Implementieren von SPAN auf einem Trunk

Trunks sind ein Sonderfall in einem Switch, da sie Ports sind, die mehrere VLANs übertragen. Wenn ein Trunk als Quellport ausgewählt wird, wird der Datenverkehr für alle VLANs auf diesem Trunk überwacht.

Überwachen einer Teilmenge von VLANs, die zu einem Trunk gehören

In diesem Diagramm ist Port 6/5 nun ein Trunk, der alle VLANs überträgt. Stellen Sie sich vor, Sie möchten SPAN für den Datenverkehr in VLAN 2 für die Ports 6/4 und 6/5 verwenden. Geben Sie einfach den folgenden Befehl ein:

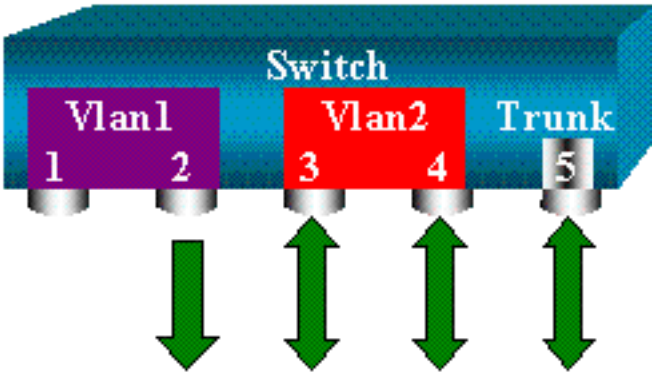
```
switch (enable) set span 6/4-5 6/2
```



In diesem Fall ist der Datenverkehr, der auf dem SPAN-Port empfangen wird, eine Mischung aus dem gewünschten Datenverkehr und allen VLANs, die vom Trunk 6/5 übertragen werden. Beispielsweise kann auf dem Zielport nicht unterschieden werden, ob ein Paket von Port 6/4 in

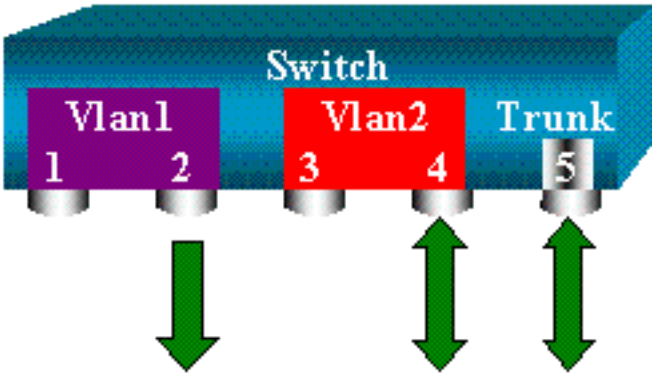
VLAN 2 oder von Port 6/5 in VLAN 1 stammt. Eine weitere Möglichkeit besteht in der Verwendung von SPAN für das gesamte VLAN 2:

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



Zumindest bei dieser Konfiguration überwachen Sie nur den Datenverkehr, der zu VLAN 2 gehört, vom Trunk. Das Problem besteht darin, dass Sie jetzt auch Datenverkehr empfangen, den Sie nicht von Port 6/3 wollten. CatOS enthält ein weiteres Schlüsselwort, mit dem Sie einige VLANs zur Überwachung aus einem Trunk auswählen können:

```
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
```



Mit diesem Befehl wird das Ziel erreicht, da Sie VLAN 2 für alle überwachten Trunks auswählen. Mit dieser Filteroption können Sie mehrere VLANs angeben.

> **Hinweis**: Diese Filteroption wird nur für Catalyst Switches der Serien 4500/4000 und 6500/6000 unterstützt. Der Catalyst 5500/5000 unterstützt die mit dem Befehl **set span** verfügbare Filteroption nicht.

Trunking am Ziel-Port

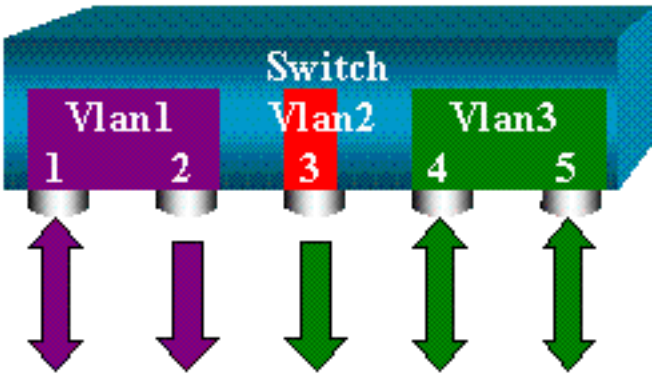
Wenn Sie Quellports haben, die zu mehreren verschiedenen VLANs gehören, oder wenn Sie SPAN auf mehreren VLANs auf einem Trunk-Port verwenden, sollten Sie ermitteln, zu welchem VLAN ein Paket gehört, das Sie auf dem Ziel-SPAN-Port empfangen. Diese Identifizierung ist möglich, wenn Sie Trunking auf dem Zielport aktivieren, bevor Sie den Port für SPAN konfigurieren. Auf diese Weise werden alle Pakete, die an den Sniffer weitergeleitet werden, auch mit ihren jeweiligen VLAN-IDs versehen.

Hinweis: Ihr Sniffer muss die entsprechende Kapselung erkennen.

```
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
```

Mehrere gleichzeitige Sitzungen erstellen

Bisher wurde nur eine einzelne SPAN-Sitzung erstellt. Jedes Mal, wenn Sie einen neuen Befehl **set span** eingeben, wird die vorherige Konfiguration ungültig. Das CatOS kann jetzt mehrere Sitzungen gleichzeitig ausführen, sodass verschiedene Zielports gleichzeitig verwendet werden können. Geben Sie den Befehl **set span** ***source destination*** **create** ein, um eine zusätzliche SPAN-Sitzung hinzuzufügen. In dieser Sitzung wird Port 6/1 bis 6/2 überwacht, und gleichzeitig wird VLAN 3 zu Port 6/3 überwacht:




```
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
```

Führen Sie jetzt den Befehl **show span** aus, um zu ermitteln, ob zwei Sitzungen gleichzeitig stattfinden:

```
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
```

Zusätzliche Sitzungen werden erstellt. Sie benötigen eine Möglichkeit, einige Sitzungen zu löschen. Der Befehl lautet:

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

Da es pro Sitzung nur einen Zielport geben kann, wird eine Sitzung vom Zielport identifiziert. Löschen Sie die erste erstellte Sitzung, die Port 6/2 als Ziel verwendet:

```
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
```

Sie können jetzt überprüfen, ob nur eine Sitzung verbleibt:

```
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
```

Geben Sie diesen Befehl ein, um alle aktuellen Sitzungen in einem einzigen Schritt zu deaktivieren:

```
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
```

Andere SPAN-Optionen

Die Syntax für den Befehl **set span** lautet:

```
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]
```

In diesem Abschnitt werden kurz die Optionen vorgestellt, die in diesem Dokument behandelt werden:

- **sc0**: Sie geben das **sc0-**Schlüsselwort in einer SPAN-Konfiguration an, wenn Sie den Datenverkehr zur Verwaltungsschnittstelle sc0 überwachen müssen. Diese Funktion ist auf den Catalyst Switches der Serien 5500/5000 und 6500/6000 verfügbar, Codeversion CatOS

5.1 oder höher.

- **inpkts *enable/disable* (Aktivieren/*Deaktivieren)* - Diese Option ist äußerst wichtig.** Wie in diesem Dokument ausgeführt, gehört ein Port, den Sie als SPAN-Ziel konfigurieren, weiterhin zum ursprünglichen VLAN. Pakete, die an einem Zielport empfangen werden, geben dann das VLAN ein, als handele es sich um einen normalen Zugriffsport. Dieses Verhalten kann gewünscht werden. Wenn Sie einen PC als Sniffer verwenden, können Sie möchten, dass dieser PC vollständig mit dem VLAN verbunden ist. Dennoch kann die Verbindung gefährlich sein, wenn Sie den Ziel-Port mit anderen Netzwerkgeräten verbinden, die eine Schleife im Netzwerk erzeugen. Der Ziel-SPAN-Port führt das STP nicht aus, und Sie können am Ende in eine gefährliche Bridging-Loop-Situation gelangen. Siehe Warum erstellt die SPAN-Sitzung eine Bridging-Schleife? -Abschnitt dieses Dokuments beschrieben, um zu verstehen, wie diese Situation auftreten kann. Die Standardeinstellung für diese Option ist "disable". Dies bedeutet, dass der Ziel-SPAN-Port Pakete verwirft, die der Port empfängt. Diese Rückwürfe schützen den Port vor Überbrückungsschleifen. Diese Option wird in CatOS 4.2 angezeigt.
- **learning *enable/disable***: Mit dieser Option können Sie die Lernfunktion auf dem Zielport deaktivieren. Standardmäßig ist die Lernfunktion aktiviert, und der Zielport empfängt MAC-Adressen von eingehenden Paketen, die der Port empfängt. Diese Funktion wird in CatOS 5.2 für Catalyst 4500/4000 und 5500/5000 und in CatOS 5.3 für Catalyst 6500/6000 angezeigt.
- **multicast *enable/disable***: Wie der Name bereits andeutet, können Sie mit dieser Option die Überwachung von Multicast-Paketen aktivieren oder deaktivieren. Der Standardwert ist enable. Diese Funktion ist für Catalyst 5500/5000 und 6500/6000, CatOS 5.1 und höher verfügbar.
- **Spanning Port 15/1** - Auf dem Catalyst 6500/6000 können Sie Port 15/1 (oder 16/1) als SPAN-Quelle verwenden. Der Port kann den an die Multilayer Switch Feature Card (MSFC) weitergeleiteten Datenverkehr überwachen. Der Port erfasst Datenverkehr, der per Software weitergeleitet oder an die MSFC weitergeleitet wird.

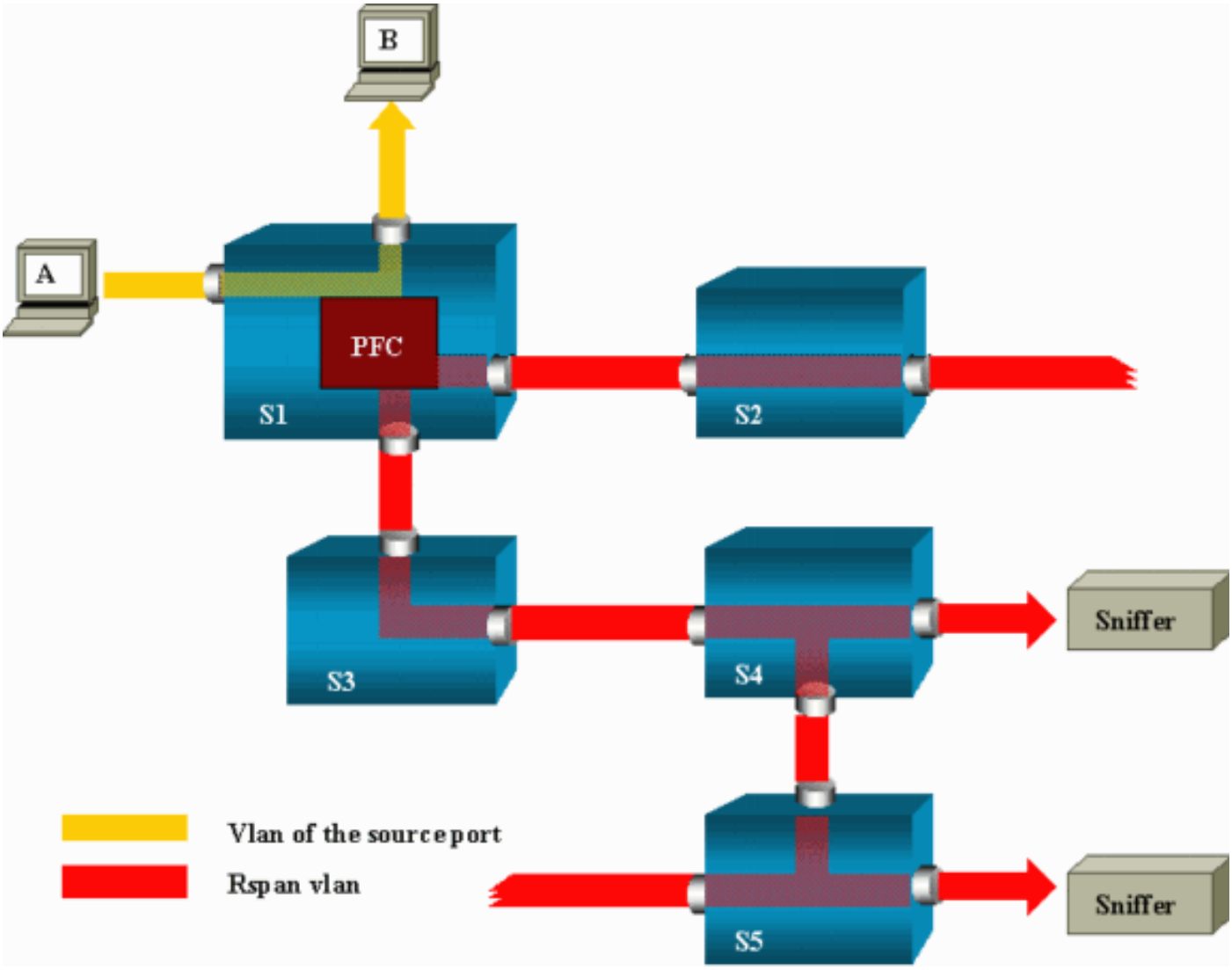
Remote-SPAN

RSPAN - Übersicht

Mit RSPAN können Sie Quellports überwachen, die über ein Switch-Netzwerk verteilt sind, nicht nur lokal auf einem Switch mit SPAN. Diese Funktion wird in CatOS 5.3 für Catalyst Switches der Serien 6500/6000 angezeigt und in Catalyst Switches der Serien 4500/4000 in CatOS 6.3 und höher hinzugefügt.

Die Funktion funktioniert genau wie eine reguläre SPAN-Sitzung. Der durch das SPAN überwachte Datenverkehr wird nicht direkt in den Zielport kopiert, sondern in ein spezielles RSPAN-VLAN überflutet. Der Zielport kann sich dann an einer beliebigen Stelle in diesem RSPAN-VLAN befinden. Es können sogar mehrere Zielports vorhanden sein.

Dieses Diagramm zeigt die Struktur einer RSPAN-Sitzung:



In diesem Beispiel konfigurieren Sie RSPAN zur Überwachung des Datenverkehrs, der von Host A gesendet wird. Wenn A einen Frame erzeugt, der für B bestimmt ist, wird das Paket von einer anwendungsspezifischen integrierten Schaltung (ASIC) der Catalyst 6500/6000 Policy Feature Card (PFC) in ein vordefiniertes RSPAN-VLAN kopiert. Von dort wird das Paket an alle anderen Ports geleitet, die zum RSPAN-VLAN gehören. Alle hier gezeichneten Interswitch-Verbindungen sind Trunks, was für RSPAN erforderlich ist. Die einzigen Access-Ports sind Zielports, an die die Sniffer angeschlossen sind (hier auf S4 und S5).

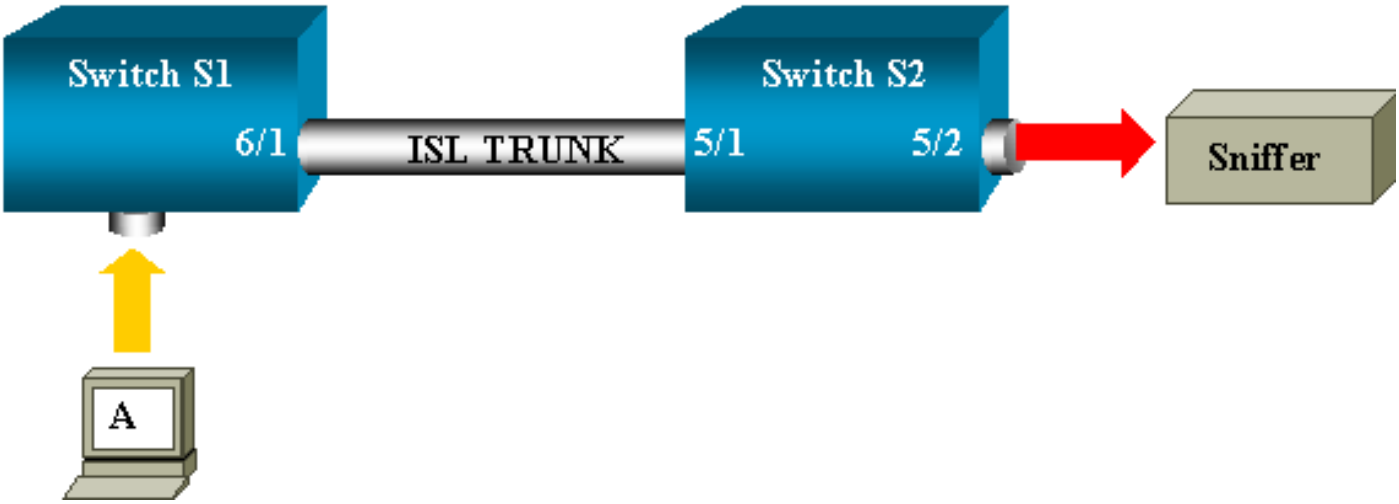
Dies sind einige Bemerkungen zu diesem Design:

- S1 wird als Quell-Switch bezeichnet. Pakete geben das RSPAN-VLAN nur in Switches ein, die als RSPAN-Quelle konfiguriert sind. Derzeit kann ein Switch nur die Quelle für eine RSPAN-Sitzung sein, d. h. ein Quell-Switch kann jeweils nur ein RSPAN-VLAN Feed durchführen.
- S2 und S3 sind Zwischenschalter. Sie sind keine RSPAN-Quellen und verfügen nicht über Zielports. Ein Switch kann für eine beliebige Anzahl von RSPAN-Sitzungen als Zwischenstation fungieren.
- S4 und S5 sind Zielswitches. Einige ihrer Ports sind als Ziel für eine RSPAN-Sitzung konfiguriert. Derzeit kann ein Catalyst 6500/6000 bis zu 24 RSPAN-Ziel-Ports für eine oder mehrere verschiedene Sitzungen haben. Sie können auch bemerken, dass S4 sowohl ein Ziel- als auch ein zwischengeschalteter Switch ist.
- Wie Sie sehen, werden RSPAN-Pakete in das RSPAN-VLAN geflutet. Auch Switches, die sich

nicht auf dem Pfad zu einem Zielport wie S2 befinden, empfangen den Datenverkehr für das RSPAN-VLAN. Es ist hilfreich, dieses VLAN auf solchen S1-S2-Verbindungen zu deaktivieren.
- Um die Flooding zu erreichen, wird das Lernen im RSPAN-VLAN deaktiviert.
- Um Schleifen zu vermeiden, wurde das STP im RSPAN-VLAN beibehalten. Aus diesem Grund kann RSPAN keine Bridge Protocol Data Units (BPDUs) überwachen.

RSPAN-Konfigurationsbeispiel

Die Informationen in diesem Abschnitt veranschaulichen die Einrichtung dieser verschiedenen Elemente mit einem sehr einfachen RSPAN-Design. S1 und S2 sind zwei Catalyst 6500/6000-Switches. Um einige S1-Ports oder VLANs von S2 aus zu überwachen, müssen Sie ein dediziertes RSPAN-VLAN einrichten. Die übrigen Befehle haben eine ähnliche Syntax wie die Befehle, die Sie in einer typischen SPAN-Sitzung verwenden.



Einrichtung des ISL-Trunks zwischen den beiden Switches S1 und S2

Legen Sie zunächst für jeden Switch die gleiche VLAN Trunk Protocol (VTP)-Domäne fest, und konfigurieren Sie eine Seite als "Trunking wünschenswert". Die VTP-Aushandlung übernimmt den Rest. Geben Sie diesen Befehl für S1 aus:

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

Geben Sie die folgenden Befehle für S2 aus:

```
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
```

Erstellung des RSPAN-VLANs

Eine RSPAN-Sitzung benötigt ein bestimmtes RSPAN-VLAN. Sie müssen dieses VLAN erstellen. Ein vorhandenes VLAN kann nicht in ein RSPAN-VLAN konvertiert werden. In diesem Beispiel

wird das VLAN 100 verwendet:

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

Geben Sie diesen Befehl auf einem Switch aus, der als VTP-Server konfiguriert ist. Das Wissen über RSPAN VLAN 100 wird automatisch in die gesamte VTP-Domäne weitergeleitet.

Konfiguration von Port 5/2 von S2 als RSPAN-Zielport

```
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
```

Konfiguration eines RSPAN-Quellports auf S1

In diesem Beispiel wird eingehender Datenverkehr, der über Port 6/2 in S1 eingeht, überwacht. Geben Sie den folgenden Befehl ein:

```
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
```

Alle eingehenden Pakete an Port 6/2 werden jetzt im RSPAN VLAN 100 geflutet und erreichen den Zielport, der auf S1 über den Trunk konfiguriert ist.

Überprüfen der Konfiguration

Der Befehl **show rspan** gibt eine Zusammenfassung der aktuellen RSPAN-Konfiguration auf dem Switch. Auch hier kann jeweils nur eine Quell-RSPAN-Sitzung stattfinden.

```
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
```

Weitere Konfigurationen, die mit dem Befehl set rspan möglich sind

Sie verwenden mehrere Befehlszeilen, um die Quelle und das Ziel mit RSPAN zu konfigurieren. Abgesehen von diesem Unterschied verhalten sich SPAN und RSPAN wirklich genauso. Sie können RSPAN sogar lokal auf einem einzigen Switch verwenden, wenn Sie mehrere Ziel-SPAN-Ports haben möchten.

Funktionsübersicht und Einschränkungen

In dieser Tabelle sind die verschiedenen Funktionen zusammengefasst, die eingeführt wurden, und es wird die CatOS-Mindestversion bereitgestellt, die zum Ausführen der Funktion auf der angegebenen Plattform erforderlich ist:

Funktion	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
inpkts ***enable/disable***-Option	4,4	4,2	5,1
Mehrere Sitzungen, Ports in verschiedenen VLANs	5,1	5,1	5,1
sc0-Option	—	5,1	5,1
Multicast-Option ***aktivieren/deaktivieren***	—	5,1	5,1
Learning ***enable/disable*****-Option**	5,2	5,2	5,3
RSPAN	6,3	—	5,3

Diese Tabelle enthält eine kurze Zusammenfassung der aktuellen Einschränkungen hinsichtlich der Anzahl möglicher SPAN-Sitzungen:

Funktion	Catalyst Switches der Serie 4500/4000	Catalyst Switches der Serien 5500/5000	Catalyst Switches der Serien 6500/6000
Rx- oder beide SPAN-Sitzungen	5	1	2
Tx SPAN-Sitzungen	5	4	4
Mini Protocol Analyzer-Sitzungen	Nicht unterstützt	Nicht unterstützt	1
Rx-, Tx- oder beide RSPAN-Quellsitzungen	5	Nicht unterstützt	1 Die Supervisor Engine 720 unterstützt zwei RSPAN-Quellsitzungen.
RSPAN-Ziel	5	Nicht unterstützt	24
Gesamtsitzungen	5	5	30

Weitere Einschränkungen und Konfigurationsrichtlinien finden Sie in diesen Dokumenten:

- Konfigurieren von SPAN und RSPAN (Catalyst 4500/4000)
- Konfigurieren von SPAN und RSPAN(Catalyst 6500/6000)

SPAN für die Catalyst Switches der Serien 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 und 3750-E

Dies sind Richtlinien für die Konfiguration der SPAN-Funktion auf den Catalyst Switches 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 und 3750-E. Switches der Serie:

- Die Catalyst Switches der Serie 2950 können jeweils nur eine SPAN-Sitzung aktiv haben und nur Quellports überwachen. Diese Switches können VLANs nicht überwachen.
- Die Catalyst Switches der Serien 2950 und 3550 können Datenverkehr an einen SPAN-Zielport in Version 12.1(13)EA1 und höher der Cisco IOS-Software weiterleiten.
- Die Catalyst Switches der Serien 3550, 3560 und 3750 können bis zu zwei SPAN-Sitzungen gleichzeitig unterstützen und Quellports sowie VLANs überwachen.
- Bei den Catalyst Switches der Serien 2970, 3560 und 3750 muss beim Konfigurieren einer RSPAN-Sitzung kein Reflektorport konfiguriert werden.
- Die Catalyst Switches der Serie 3750 unterstützen die Sitzungskonfiguration unter Verwendung von Quell- und Ziel-Ports, die sich in einem der Switch-Stack-Elemente befinden.
- Pro SPAN-Sitzung ist nur ein Zielport zulässig, und derselbe Port kann kein Zielport für mehrere SPAN-Sitzungen sein. Aus diesem Grund können Sie nicht zwei SPAN-Sitzungen durchführen, die denselben Zielport verwenden.

Die Konfigurationsbefehle für die SPAN-Funktionen sind auf dem Catalyst 2950 und Catalyst 3550 ähnlich. Der Catalyst 2950 kann die VLANs jedoch nicht überwachen. Sie können das SPAN wie in diesem Beispiel konfigurieren:

```
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#
```

Sie können auch einen Port als Ziel für lokalen SPAN und RSPAN für denselben VLAN-Datenverkehr konfigurieren. Um den Datenverkehr für ein bestimmtes VLAN zu überwachen, das sich in zwei direkt verbundenen Switches befindet, konfigurieren Sie diese Befehle auf dem Switch, der über den Zielport verfügt. In diesem Beispiel wird der Datenverkehr von VLAN 5 überwacht, der auf zwei Switches verteilt ist:

```
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.
```

Verwenden Sie auf dem Remote-Switch folgende Konfiguration:

```
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
```

Im vorherigen Beispiel wurde ein Port als Zielport für das lokale SPAN und das RSPAN konfiguriert, um den Datenverkehr für dasselbe VLAN zu überwachen, das sich in zwei Switches befindet.

> **Hinweis**: Im Gegensatz zu den Switches der Serien 2900XL und 3500XL bieten die Catalyst Switches der Serien 2940, 2950, 2955, 2960, 2970, 3550, 3560, 350-E Die Switches der Serien 50 und 3750-E unterstützen SPAN für Quellport-Datenverkehr nur in Rx-Richtung (Rx SPAN oder Eingangs-SPAN), nur in Tx-Richtung (Tx SPAN oder Ausgangs-SPAN) oder beides.

> **Hinweis**: Die Befehle in der Konfiguration werden vom Catalyst 2950 mit Cisco IOS Software Release 12.0(5.2)WC(1) oder einer früheren Software als die Cisco IOS Software Release 12.1(6)EA2 nicht unterstützt. Im Abschnitt *Enabling Switch Port Analyzer* unter Managing Switches können Sie SPAN auf einem Catalyst 2950 mit Software konfigurieren, die älter ist als die Cisco IOS Software Release 12.1(6)EA2.

> **Hinweis**: Catalyst Switches der Serie 2950, die die Cisco IOS Software Version 12.1.(9)EA1d und frühere Versionen der Cisco IOS Software Release 12.1 Train unterstützen SPAN. Alle Pakete, die auf dem SPAN-Zielport (verbunden mit dem Sniffing-Gerät oder PC) gesehen werden, haben jedoch ein IEEE 802.1Q-Tag, obwohl der SPAN-Quellport (überwachter Port) möglicherweise kein 802.1Q-Trunk-Port ist. Wenn das Sniffing-Gerät oder die PC-Netzwerkschnittstellenkarte (NIC) 802.1Q-getaggte Pakete nicht versteht, kann das Gerät die Pakete verwerfen oder Schwierigkeiten haben, wenn es versucht, die Pakete zu dekodieren. Die Anzeige der 802.1Q-markierten Frames ist nur dann wichtig, wenn der SPAN-Quellport ein Trunk-Port ist. Mit der Cisco IOS Softwareversion 12.1(11)EA1 und höher können Sie das Tagging der Pakete am SPAN-Zielport aktivieren und deaktivieren. Geben Sie den Befehl **monitor session *session_number* destination interface_id encapsulation dot1q** ein, um die Kapselung der Pakete am Zielport zu aktivieren. Wenn Sie das **Encapsulation**-Schlüsselwort nicht angeben, werden die Pakete unmarkiert gesendet. Dies ist die Standardeinstellung in Cisco IOS Software Release 12.1(11)EA1 und höher.

Funktion	**Catalyst 2950/3550**
Aktivieren/Deaktivieren der Option Ingress (Ingress*, Inpkts)*	Cisco IOS Softwareversion 12.1(12c)EA1
RSPAN	Cisco IOS Softwareversion 12.1(12c)EA1

Funktion	**Catalyst 2940[1], 2950, 2955, 2960, 2970, 3550, 3560, 3750**
Rx- oder beide SPAN-Sitzungen	2

Tx SPAN-Sitzungen	2
Rx-, Tx- oder beide RSPAN-Quellsitzungen	2
RSPAN-Ziel	2
Gesamtsitzungen	2

[1] Die Catalyst Switches der Serie 2940 unterstützen nur das lokale SPAN. RSPAN wird von dieser Plattform nicht unterstützt.

Weitere Informationen zur Konfiguration von SPAN und RSPAN finden Sie in diesen Konfigurationsleitfäden:

- SPAN konfigurieren (Catalyst 2940)
- Konfigurieren von SPAN und RSPAN (Catalyst 2950 und 2955)
- Konfigurieren von SPAN und RSPAN (Catalyst 2960)
- Konfigurieren von SPAN und RSPAN (Catalyst 3550)
- Konfigurieren von SPAN und RSPAN (Catalyst 3560)
- Konfigurieren von SPAN und RSPAN (Catalyst 3560-E und 3750-E)
- Konfigurieren von SPAN und RSPAN (Catalyst 3750)

SPAN auf Catalyst Switches der Serien 4500/4000 und 6500/6000, die Cisco IOS-Systemsoftware ausführen

Die SPAN-Funktion wird von den Catalyst Switches der Serien 4500/4000 und 6500/6000 unterstützt, auf denen Cisco IOS-Systemsoftware ausgeführt wird. Beide Switch-Plattformen verwenden die identische Kommandozeilenschnittstelle (CLI) und eine Konfiguration, die der Konfiguration des SPAN auf den Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 350 ähnelt. Abschnitt zu Switches der Serien 60E, 3750 und 3750E. Informationen zur entsprechenden Konfiguration finden Sie in den folgenden Dokumenten:

- Konfigurieren von SPAN und RSPAN (Catalyst 6500/6000)
- Konfigurieren von SPAN und RSPAN (Catalyst 4500/4000)

Konfigurationsbeispiel

Sie können das SPAN wie in diesem Beispiel konfigurieren:

```
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#
```

Funktionsübersicht und Einschränkungen

In dieser Tabelle sind die verschiedenen Funktionen zusammengefasst, die eingeführt wurden, und es wird die Cisco IOS Software-Mindestversion bereitgestellt, die zur Ausführung der Funktion auf der angegebenen Plattform erforderlich ist:

Funktion	Catalyst 4500/4000 (Cisco IOS Software)	Catalyst 6500/6000 (Cisco Software)
Aktivieren/Deaktivieren der Option Ingress (Ingress*, Inpkts)*	Cisco IOS Softwareversion 12.1(19)EW	Derzeit nicht unterstützt[1]
RSPAN	Cisco IOS Software Release 12.1(20)EW	Cisco IOS Softwareversio 12.1(13)E

[1] Die Funktion ist derzeit nicht verfügbar, und die Verfügbarkeit dieser Funktionen wird in der Regel erst nach ihrer Veröffentlichung veröffentlicht.

> **Hinweis**: Die SPAN-Funktion der Cisco Catalyst Switches der Serien 6500 und 6000 beschränkt sich auf das PIM-Protokoll. Wenn ein Switch für PIM und SPAN konfiguriert ist, kann der mit dem SPAN-Zielport verbundene Network Analyzer/Sniffer PIM-Pakete sehen, die nicht Teil des SPAN-Quellports/VLAN-Datenverkehrs sind. Dieses Problem tritt aufgrund einer Einschränkung der Paketweiterleitungsarchitektur des Switches auf. Der SPAN-Zielport führt keine Überprüfung durch, um die Quelle der Pakete zu überprüfen. Dieses Problem ist auch in der Cisco Bug-ID CSCdy57506 dokumentiert (nur registrierte Kunden).

Diese Tabelle enthält eine kurze Zusammenfassung der aktuellen Einschränkungen hinsichtlich der Anzahl möglicher SPAN- und RSPAN-Sitzungen:

Funktion	Catalyst 4500/4000 (Cisco IOS Software)
Rx- oder beide SPAN-Sitzungen	2
Tx SPAN-Sitzungen	4
Rx-, Tx- oder beide RSPAN-Quellsitzungen	2 (Rx, Tx oder beide) und bis zu 4 nur für Tx
RSPAN-Ziel	2
Gesamtsitzungen	6

Informationen zu den Local SPAN-, RSPAN- und ERSPAN Session Limits für Catalyst 6500/6000-Switches mit Cisco IOS-Software finden Sie unter Local SPAN.

Bei der Catalyst Serie 6500 ist zu beachten, dass der Ausgangs-SPAN auf dem Supervisor ausgeführt wird. Auf diese Weise kann der gesamte Datenverkehr, der einem Ausgangs-SPAN unterliegt, über die Fabric an den Supervisor und anschließend an den SPAN-Zielport gesendet werden, der erhebliche Systemressourcen nutzen und den Benutzerdatenverkehr beeinflussen kann. Eingangs-SPAN wird auf Eingangs-Modulen durchgeführt, sodass die SPAN-Leistung der Summe aller teilnehmenden Replikations-Engines entspricht. Die Leistung der SPAN-Funktion hängt von der Paketgröße und dem ASIC-Typ ab, der in der Replikations-Engine verfügbar ist.

Bei Versionen vor der Cisco IOS-Softwareversion 12.2(33)SXH kann eine Port-Channel-Schnittstelle, ein EtherChannel, kein SPAN-Ziel sein. Mit der Cisco IOS Software Release 12.2(33)SXH und höher kann ein EtherChannel ein SPAN-Ziel sein. Ziel-EtherChannels

unterstützen die PAgP- (Port Aggregation Control Protocol) oder LACP-EtherChannel-Protokolle (Link Aggregation Control Protocol) nicht. Es wird nur der On-Modus unterstützt, wobei alle EtherChannel-Protokolle deaktiviert sind.

Weitere Einschränkungen und Konfigurationsrichtlinien finden Sie in diesen Dokumenten:

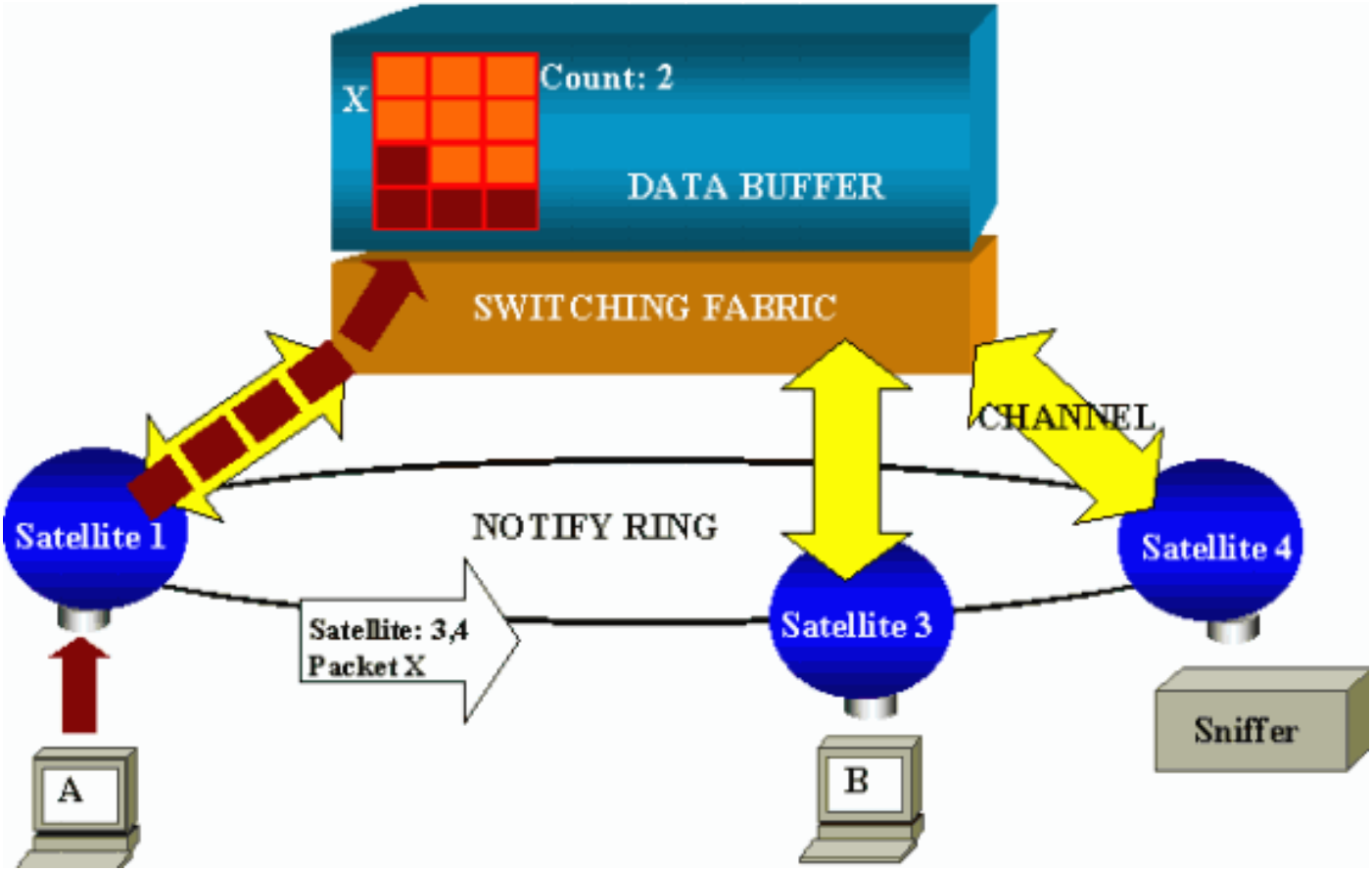
- Konfigurieren von SPAN und RSPAN (Catalyst 4500/4000)
- Konfigurieren des lokalen SPAN, des Remote-SPAN (RSPAN) und des gekapselten RSPAN (Catalyst 6500/6000)

Performance Impact des SPAN auf die verschiedenen Catalyst-Plattformen

Catalyst Serie 2900XL/3500XL

Architekturübersicht

Dies ist eine sehr einfache Ansicht der internen Architektur der 2900XL/3500XL-Switches:



Die Ports des Switches sind an Satelliten angeschlossen, die über Radialkanäle mit einer Switching-Fabric kommunizieren. Oben sind alle Satelliten über einen Hochgeschwindigkeits-Benachrichtigungsring verbunden, der für den Signalisierungsverkehr vorgesehen ist.

Wenn ein Satellit ein Paket von einem Port empfängt, wird das Paket in Zellen aufgeteilt und über einen oder mehrere Kanäle an die Switching Fabric gesendet. Das Paket wird dann im gemeinsam genutzten Speicher gespeichert. Jeder Satellit kennt die Zielports. Im Diagramm in diesem Abschnitt weiß Satellit 1, dass das Paket X von den Satelliten 3 und 4 empfangen werden

soll. Satellit 1 sendet eine Nachricht über den Benachrichtigungsring an die anderen Satelliten. Anschließend können die Satelliten 3 und 4 anfangen, die Zellen über ihre Radialkanäle aus dem gemeinsamen Speicher abzurufen und das Paket schließlich weiterleiten. Da der Quellsatellit das Ziel kennt, überträgt dieser Satellit auch einen Index, der angibt, wie oft dieses Paket von den anderen Satelliten heruntergeladen wird. Jedes Mal, wenn ein Satellit das Paket aus dem freigegebenen Speicher abruft, wird dieser Index reduziert. Wenn der Index 0 erreicht, kann der freigegebene Speicher freigegeben werden.

Performance-Auswirkungen

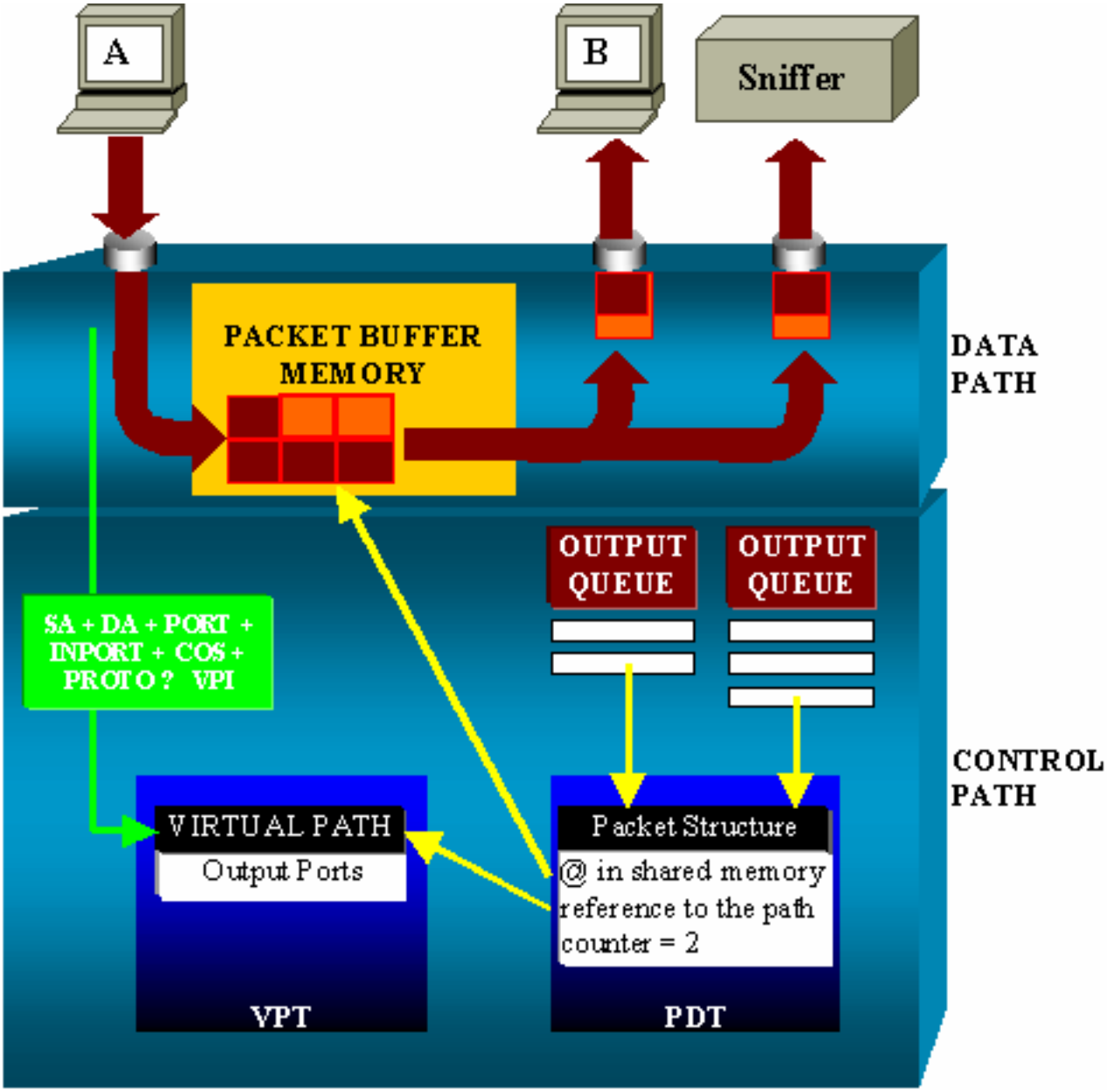
Um einige Ports mit SPAN zu überwachen, muss ein Paket zusätzlich aus dem Datenpuffer in einen Satelliten kopiert werden. Die Auswirkungen auf die Hochgeschwindigkeits-Switching-Fabric sind unerheblich.

Der Überwachungsport empfängt Kopien des übertragenen und empfangenen Datenverkehrs für alle überwachten Ports. In dieser Architektur wird ein für mehrere Ziele bestimmtes Paket im Speicher gespeichert, bis alle Kopien weitergeleitet werden. Wenn der Überwachungsport über einen längeren Zeitraum zu 50 % überbelegt ist, wird der Port wahrscheinlich überlastet und hält einen Teil des gemeinsam genutzten Speichers. Es besteht die Möglichkeit, dass mindestens einer der überwachten Ports auch langsamer wird.

Catalyst Serie 4500/4000

Architekturübersicht

Der Catalyst 4500/4000 basiert auf einer Switching-Fabric mit gemeinsamem Speicher. Dieses Diagramm bietet eine allgemeine Übersicht über den Pfad eines Pakets durch den Switch. Die tatsächliche Umsetzung ist in der Tat viel komplexer:



Auf einem Catalyst 4500/4000 können Sie den Datenpfad unterscheiden. Der Datenpfad entspricht der tatsächlichen Datenübertragung innerhalb des Switches vom Steuerpfad, wo alle Entscheidungen getroffen werden.

Wenn ein Paket in den Switch gelangt, wird im Paketpuffer-Speicher (einem gemeinsam genutzten Speicher) ein Puffer zugewiesen. Eine Paketstruktur, die auf diesen Puffer zeigt, wird in der Packet Descriptor Table (PDT) initialisiert. Während die Daten in den gemeinsam genutzten Speicher kopiert werden, bestimmt der Steuerungspfad, wo das Paket gewechselt werden soll. Um diese Bestimmung vorzunehmen, wird ein Hashwert anhand der folgenden Informationen berechnet:

- Die Paketquellen-Adresse
- Zieladresse
- VLAN
- Protokolltyp
- Eingangsport
- Class of Service (CoS) (entweder IEEE 802.1p-Tag oder Port-Standard)

Dieser Wert wird verwendet, um den Virtual Path Index (VPI) einer Pfadstruktur in der Virtual Path Table (VPT) zu finden. Dieser Eintrag für virtuelle Pfade im VPT enthält mehrere Felder, die sich

auf diesen bestimmten Fluss beziehen. Die Felder enthalten die Zielports. Die Paketstruktur im PDT wird nun mit einem Verweis auf den virtuellen Pfad und Zähler aktualisiert. Im Beispiel in diesem Abschnitt soll das Paket an zwei verschiedene Ports übertragen werden. Der Zähler initialisiert sich also auf 2. Schließlich wird die Paketstruktur der Ausgabewarteschlange der beiden Zielports hinzugefügt. Von dort werden die Daten aus dem freigegebenen Speicher in den Ausgabepuffer des Ports kopiert, und der Zähler der Paketstruktur nimmt ab. Wenn der Puffer 0 erreicht, wird er freigegeben.

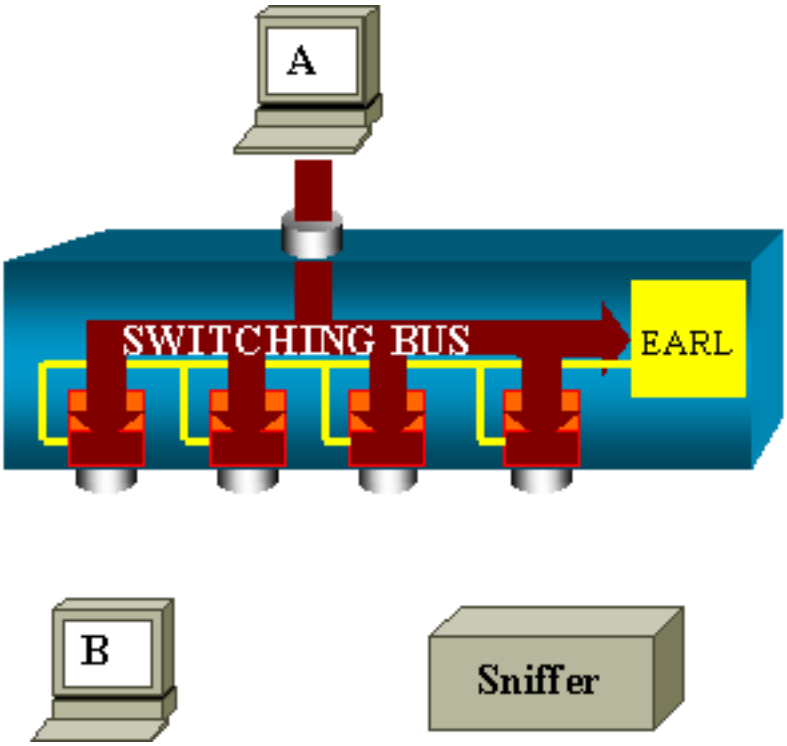
Performance-Auswirkungen

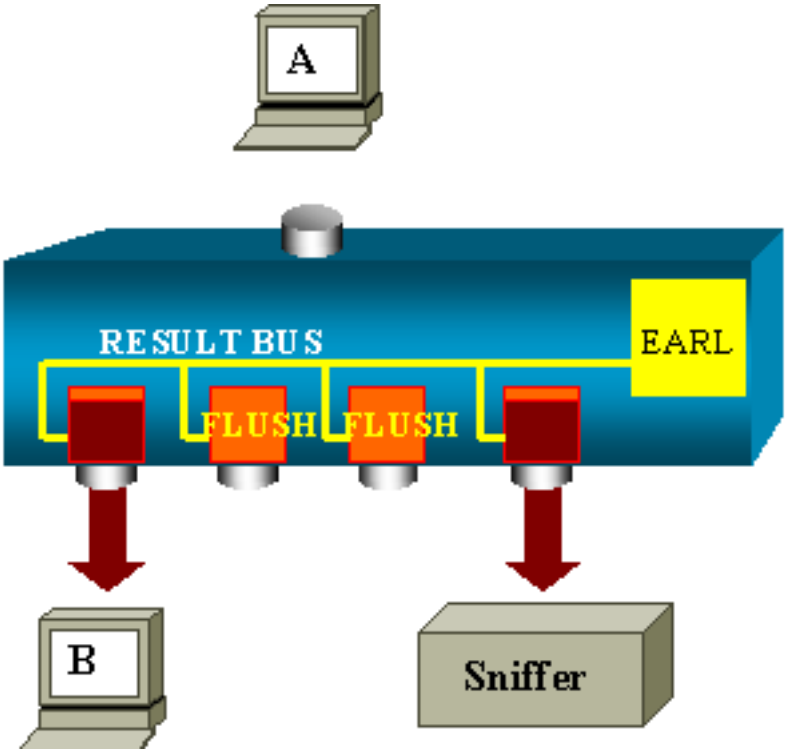
Bei Verwendung der SPAN-Funktion muss ein Paket an zwei verschiedene Ports gesendet werden, wie im Beispiel im Abschnitt "Architecture Overview" (Architekturübersicht) beschrieben. Das Senden des Pakets an zwei Ports ist kein Problem, da die Switching-Fabric nicht blockiert. Wenn der Ziel-SPAN-Port überlastet ist, werden Pakete in der Ausgabewarteschlange verworfen und korrekt aus dem gemeinsam genutzten Speicher freigegeben. Daher wird der Switch-Betrieb nicht beeinträchtigt.

Catalyst Serien 5500/500 und 6500/6000

Architekturübersicht

Auf den Catalyst Switches der Serien 5500/5000 und 6500/6000 wird ein Paket, das auf einem Port empfangen wird, über den internen Switching-Bus übertragen. Jede Linecard im Switch speichert dieses Paket in internen Puffern. Gleichzeitig empfängt die Encoded Address Recognition Logic (EARL) den Header des Pakets und berechnet einen Ergebnisindex. EARL sendet den Ergebnisindex über den Ergebnisbus an alle Linecards. Die Kenntnis dieses Index ermöglicht es der Linecard, einzeln zu entscheiden, ob sie das Paket leeren oder übertragen soll, wenn die Linecard das Paket in ihren Puffern empfängt.





Performance-Auswirkungen

Ob ein oder mehrere Ports das Paket schließlich übertragen, hat keinerlei Einfluss auf den Switch-Betrieb. Wenn Sie diese Architektur betrachten, hat die SPAN-Funktion daher keine Auswirkungen auf die Leistung.

Häufig gestellte Fragen und häufige Probleme

Verbindungsprobleme aufgrund fehlerhafter SPAN-Konfiguration

Verbindungsprobleme aufgrund der fehlerhaften Konfiguration von SPAN treten häufig in CatOS-Versionen vor 5.1 auf. Bei diesen Versionen ist nur eine SPAN-Sitzung möglich. Die Sitzung verbleibt in der Konfiguration, selbst wenn Sie SPAN deaktivieren. Bei der Frage des Befehls **set span enable** aktiviert ein Benutzer die gespeicherte SPAN-Sitzung. Die Aktion tritt häufig aufgrund eines typografischen Fehlers auf, z. B. wenn der Benutzer STP aktivieren möchte. Schwere Verbindungsprobleme können auftreten, wenn der Zielport zum Weiterleiten von Benutzerdatenverkehr verwendet wird.

> **Vorsicht**: Dieses Problem befindet sich noch in der aktuellen Implementierung von CatOS. Achten Sie auf den Port, den Sie als SPAN-Ziel auswählen.

SPAN-Zielport - Nach oben/Nach unten

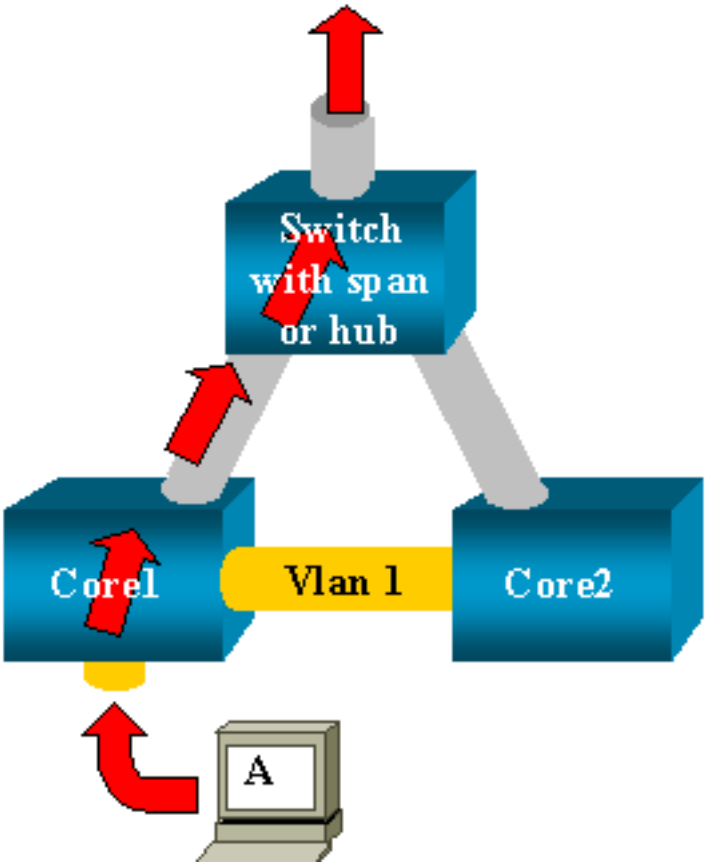
Wenn Ports für die Überwachung angepasst sind, wird der Portstatus als UP/DOWN angezeigt.

Wenn Sie eine SPAN-Sitzung für die Überwachung des Ports konfigurieren, zeigt die Zielschnittstelle den Status "down" (Überwachung) planmäßig an. Die Schnittstelle zeigt den Port in diesem Zustand an, um sicherzustellen, dass der Port derzeit nicht als Produktionsport verwendbar ist. Die Überwachung des Ports auf/ab ist normal.

Warum erstellt die SPAN-Sitzung eine Bridging-Schleife?

Die Erstellung einer Bridging-Schleife erfolgt in der Regel, wenn der Administrator versucht, die RSPAN-Funktion zu manipulieren. Außerdem kann ein Konfigurationsfehler das Problem verursachen.

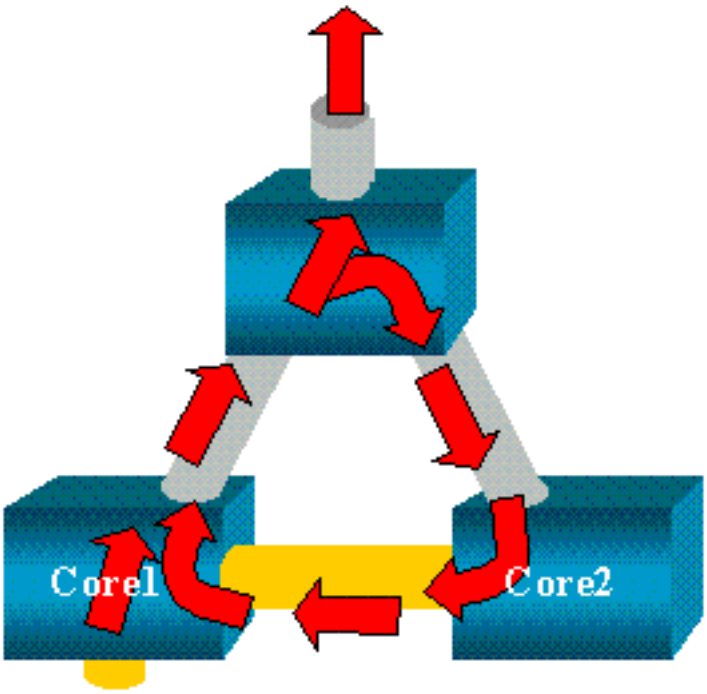
Dies ist ein Beispiel für das Szenario:



Es gibt zwei Core-Switches, die durch einen Trunk verbunden sind. In diesem Fall ist jeder Switch mit mehreren Servern, Clients oder anderen Bridges verbunden. Der Administrator möchte VLAN 1 überwachen, das auf mehreren Bridges mit SPAN angezeigt wird. Der Administrator erstellt eine SPAN-Sitzung, die das gesamte VLAN 1 auf jedem Core-Switch überwacht und zum Zusammenführen dieser beiden Sitzungen den Ziel-Port mit demselben Hub (oder demselben Switch, unter Verwendung einer anderen SPAN-Sitzung) verbindet.

Der Administrator erreicht das Ziel. Jedes einzelne Paket, das ein Core-Switch in VLAN 1 empfängt, wird auf dem SPAN-Port dupliziert und nach oben an den Hub weitergeleitet. Ein Sniffer fängt schließlich den Datenverkehr ein.

Das einzige Problem besteht darin, dass der Datenverkehr über den Ziel-SPAN-Port auch in Core 2 zurückgeleitet wird. Durch die Wiedereinspeisung des Datenverkehrs in Core 2 entsteht eine Bridging-Schleife in VLAN 1. Beachten Sie, dass ein Ziel-SPAN-Port STP nicht ausführt und eine solche Schleife nicht verhindern kann.



Hinweis: Aufgrund der Einführung der Option "inpkts" (Eingabepakete) im CatOS verwirft ein SPAN-Zielport standardmäßig alle eingehenden Pakete, wodurch dieses Fehlerszenario verhindert wird. Das potenzielle Problem besteht jedoch weiterhin bei den Catalyst Switches der Serien 2900XL/3500XL.

Hinweis: Selbst wenn die Option inpkts die Schleife verhindert, kann die in diesem Abschnitt angezeigte Konfiguration einige Probleme im Netzwerk verursachen. Netzwerkprobleme können aufgrund von Lernproblemen mit MAC-Adressen auftreten, die mit dem auf dem Zielport aktivierten Lernen verbunden sind.

Wirkt sich SPAN auf die Leistung aus?

In den folgenden Abschnitten dieses Dokuments finden Sie Informationen zu den Auswirkungen auf die Leistung für die angegebenen Catalyst-Plattformen:

- Catalyst Serie 2900XL/3500XL
- Catalyst Serie 4500/4000
- Catalyst Serien 5500/500 und 6500/6000

Können Sie SPAN auf einem EtherChannel-Port konfigurieren?

Ein EtherChannel bildet sich nicht, wenn einer der Ports im Paket ein SPAN-Zielport ist. Wenn Sie in dieser Situation versuchen, SPAN zu konfigurieren, teilt Ihnen der Switch Folgendes mit:

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

Sie können einen Port in einem EtherChannel-Paket als SPAN-Quellport verwenden.

Können mehrere SPAN-Sitzungen gleichzeitig ausgeführt werden?

Auf den Catalyst Switches der Serien 2900XL/3500XL ist die Anzahl der Zielports, die auf dem Switch verfügbar sind, die einzige Grenze für die Anzahl der SPAN-Sitzungen.

Auf den Catalyst Switches der Serie 2950 kann jeweils nur ein Überwachungsport zugewiesen sein. Wenn Sie einen anderen Port als Monitorport auswählen, ist der vorherige Monitorport deaktiviert, und der neu ausgewählte Port wird zum Monitorport.

Auf Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 mit CatOS 5.1 und höher können Sie mehrere SPAN-Sitzungen gleichzeitig abhalten. Weitere Informationen finden Sie im Abschnitt Erstellen mehrerer gleichzeitiger Sitzungen und Zusammenfassung der Funktionen und Einschränkungen dieses Dokuments.

Fehler "% Lokaler Sitzungsgrenzwert wurde überschritten"

Diese Meldung wird angezeigt, wenn die zulässige SPAN-Sitzung den Grenzwert für die Supervisor Engine überschreitet:

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

Die Supervisor Engines begrenzen die Anzahl der SPAN-Sitzungen. Weitere Informationen finden Sie im Abschnitt zur Konfiguration des lokalen SPAN, RSPAN und ERSPAN-Session Limits unter Konfiguration lokaler SPAN-, RSPAN- und ERSPAN-Sitzungen.

SPAN-Sitzungen können im VPN-Servicemodul nicht gelöscht werden. Fehler: "% Sitzung [Sitzung Nr.:] Wird vom Servicemodul verwendet"

Bei diesem Problem wird das VPN-Modul (Virtual Private Network) in das Chassis eingesetzt, in das bereits ein Switch-Fabric-Modul eingesetzt wurde. Die Cisco IOS-Software erstellt automatisch eine SPAN-Sitzung für das VPN-Servicemodul, um den Multicast-Datenverkehr zu verarbeiten.

Führen Sie diesen Befehl aus, um die von der Software für das VPN-Dienstmodul erstellte SPAN-Sitzung zu löschen:

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

> **Hinweis**: Wenn Sie die Sitzung löschen, verwirft das VPN-Servicemodul den Multicast-Verkehr.

Warum können Sie beschädigte Pakete mit SPAN nicht erfassen?

Sie können beschädigte Pakete nicht mit SPAN erfassen, da die Switches im Allgemeinen arbeiten. Wenn ein Paket einen Switch durchläuft, treten folgende Ereignisse auf:

1. Das Paket erreicht den Eingangsport.
2. Das Paket wird in mindestens einem Puffer gespeichert.
3. Das Paket wird schließlich auf dem Ausgangsport erneut übertragen.

Wenn der Switch ein beschädigtes Paket empfängt, verwirft der Eingangsport das Paket in der Regel. Daher wird das Paket nicht auf dem Ausgangsport angezeigt. Ein Switch ist hinsichtlich der Erfassung von Datenverkehr nicht vollständig transparent. Wenn Sie im Szenario in diesem Abschnitt ein beschädigtes Paket auf Ihrem Sniffer sehen, wissen Sie, dass die Fehler in Schritt 3 im Ausgangs-Segment generiert wurden.

Wenn Sie glauben, dass ein Gerät beschädigte Pakete sendet, können Sie den sendenden Host und das Sniffer-Gerät auf einen Hub legen. Der Hub führt keine Fehlerprüfungen durch. Im Gegensatz zum Switch verwirft der Hub daher keine Pakete. Auf diese Weise können Sie die Pakete anzeigen.

Fehler: % Sitzung 2 verwendet durch Servicemodul

Wenn z. B. ein Firewall Service Module (FWSM) auf dem CAT6500 installiert und später entfernt wurde, dann wurde die **SPAN Reflector-Funktion** automatisch aktiviert. Die SPAN-Reflektorfunktion verwendet eine SPAN-Sitzung im Switch. Wenn Sie dies nicht mehr benötigen, müssen Sie den Befehl **no monitor session session service module** im Konfigurationsmodus von CAT6500 eingeben und sofort die gewünschte SPAN-Konfiguration eingeben.

Reflektor-Port-Drops-Pakete

Ein Reflektorport empfängt Kopien von gesendetem und empfangenem Datenverkehr für alle überwachten Quell-Ports. Wenn ein Reflektor-Port überbelegt ist, kann er überlastet werden. Dies kann die Weiterleitung des Datenverkehrs an einem oder mehreren der Quell-Ports beeinträchtigen. Wenn die Bandbreite des Reflektorports für das Datenverkehrsvolumen der entsprechenden Quell-Ports nicht ausreicht, werden die überzähligen Pakete verworfen. Ein 10/100-Port spiegelt 100 Mbit/s wider. Ein Gigabit-Port reflektiert 1 Gbit/s.

Die SPAN-Sitzung wird immer mit einem FWSM im Catalyst 6500-Chassis verwendet.

Wenn Sie die Supervisor Engine 720 mit einem FWSM im Chassis verwenden, das Cisco Native IOS ausführt, wird standardmäßig eine SPAN-Sitzung verwendet. Wenn Sie mit dem Befehl **show monitor** nach nicht verwendeten Sitzungen suchen, wird *Sitzung 1* verwendet:

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

Befindet sich ein Firewall-Blade im Catalyst 6500-Chassis, wird diese Sitzung automatisch installiert, um die Hardware-Multicast-Replikation zu unterstützen, da ein FWSM Multicast-Streams nicht replizieren kann. Wenn Multicast-Streams, die im FWSM eingehen, auf Layer 3 auf mehrere Linecards repliziert werden müssen, kopiert die automatische Sitzung den Datenverkehr über einen Fabric-Kanal an den Supervisor.

Wenn Sie über eine Multicast-Quelle verfügen, die einen Multicast-Stream hinter dem FWSM generiert, benötigen Sie den SPAN-Reflektor. Wenn Sie die Multicast-Quelle im externen VLAN platzieren, ist der SPAN-Reflektor nicht erforderlich. Der SPAN-Reflektor ist nicht mit dem Bridging von BPDUs über das FWSM kompatibel. Sie können den Befehl **no monitor session service module** verwenden, um den SPAN-Reflektor zu deaktivieren.

Können ein SPAN und eine RSPAN-Sitzung dieselbe ID innerhalb desselben Switches haben?

Nein, es ist nicht möglich, dieselbe Sitzungs-ID für eine reguläre SPAN-Sitzung und eine RSPAN-Zielsitzung zu verwenden. Jede SPAN- und RSPAN-Sitzung muss eine andere Sitzungs-ID haben.

Kann eine RSPAN-Sitzung über verschiedene VTP-Domänen hinweg ausgeführt werden?

Ja. Eine RSPAN-Sitzung kann sich über verschiedene VTP-Domänen erstrecken. Stellen Sie jedoch sicher, dass das RSPAN-VLAN in den Datenbanken dieser VTP-Domänen vorhanden ist. Stellen Sie außerdem sicher, dass im Pfad der Sitzungsquelle zum Sitzungsziel kein Layer-3-Gerät vorhanden ist.

Kann eine RSPAN-Sitzung über das WAN oder verschiedene Netzwerke hinweg ausgeführt werden?

Nein. RSPAN-Sitzungen können kein Layer-3-Gerät überqueren, da RSPAN eine LAN-Funktion (Layer 2) ist. Um den Datenverkehr über ein WAN oder verschiedene Netzwerke zu überwachen, verwenden Sie den Encapsulated Remote SwitchPort Analyser (ERSPAN). Die ERSPAN-Funktion unterstützt Quellports, Quell-VLANs und Ziel-Ports auf verschiedenen Switches und ermöglicht so die Remote-Überwachung mehrerer Switches im Netzwerk.

ERSPAN besteht aus einer ERSPAN-Quellsitzung, routingfähigem GRE-gekapselten ERSPAN-Datenverkehr und einer ERSPAN-Zielsitzung. Sie konfigurieren die ERSPAN-Quell- und Zielsitzungen separat auf verschiedenen Switches.

Derzeit wird die ERSPAN-Funktion in folgenden Ländern unterstützt:

- Supervisor 720 mit PFC3B oder PFC3BXL mit Cisco IOS Software Release 12.2(18)SXE oder höher
- Supervisor 720 mit PFC3A mit Hardwareversion 3.2 oder höher und Cisco IOS Software Release 12.2(18)SXE oder höher

Weitere Informationen zu ERSPAN finden Sie im Konfigurationshandbuch zur Cisco IOS-Software 12.2SX unter Konfiguration des lokalen SPAN, des Remote SPAN (RSPAN) und des gekapselten RSPAN - Catalyst 6500 Series.

Können auf demselben Catalyst Switch eine RSPAN-Quellsitzung und eine Zielsitzung vorhanden sein?

Nein. RSPAN funktioniert nicht, wenn sich die RSPAN-Quellsitzung und die RSPAN-Zielsitzung auf demselben Switch befinden.

Wenn eine RSPAN-Quellsitzung mit einem bestimmten RSPAN-VLAN konfiguriert und eine RSPAN-Zielsitzung für dieses RSPAN-VLAN auf demselben Switch konfiguriert ist, werden die erfassten Pakete aus der RSPAN-Quellsitzung aufgrund von Hardwareeinschränkungen nicht vom Zielport der RSPAN-Zielsitzung übertragen. Dies wird von den Switches der Serien 4500 und 3750 nicht unterstützt. Dieses Problem ist in der Cisco Bug-ID CSCeg08870 dokumentiert (nur registrierte Kunden).

Dies ist ein Beispiel:

```
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
```

Die Problemumgehung bei diesem Problem besteht in der Verwendung des regulären SPAN.

Mit dem SPAN-Zielport verbundenes Netzwerkanalysegerät/Sicherheitsgerät ist nicht erreichbar

Das grundlegende Merkmal eines SPAN-Zielports besteht darin, dass er außer dem für die SPAN-Sitzung erforderlichen Datenverkehr keinen Datenverkehr überträgt. Wenn Sie den Netzwerkanalysator bzw. das Sicherheitsgerät über den SPAN-Zielport erreichen (IP-Erreichbarkeit) müssen, müssen Sie die Weiterleitung des eingehenden Datenverkehrs aktivieren.

Wenn der Eingang aktiviert ist, akzeptiert der SPAN-Zielport eingehende Pakete, die entsprechend dem angegebenen Kapselungsmodus möglicherweise mit Tags versehen sind, und schaltet sie normal. Wenn Sie einen SPAN-Zielport konfigurieren, können Sie angeben, ob die Eingangsfunktion aktiviert ist und welches VLAN zum Umschalten nicht getaggter Eingangspakete verwendet werden soll. Die Spezifikation eines Eingangs-VLANs ist bei der Konfiguration der ISL-Kapselung nicht erforderlich, da alle gekapselten ISL-Pakete VLAN-Tags aufweisen. Obwohl der Port STP-Forwarding ist, ist er nicht am STP beteiligt. Seien Sie daher vorsichtig, wenn Sie diese Funktion konfigurieren, damit im Netzwerk eine Spanning-Tree-Schleife eingeführt wird. Wenn sowohl Eingangs- als auch Trunk-Kapselung auf einem SPAN-Zielport angegeben sind, leitet der Port alle aktiven VLANs weiter. Die Konfiguration eines nicht vorhandenen VLANs als Eingangs-VLAN ist nicht zulässig.

monitor session *session_number* destination interface *interface* [Kapselung {isl | dot1q}] Ingress [vlan *vlan_IDs*]

In diesem Beispiel wird veranschaulicht, wie ein Zielport mithilfe von 802.1q-Kapselung und Eingangspaketen mithilfe des nativen VLAN 7 konfiguriert wird.

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

Bei dieser Konfiguration wird Datenverkehr aus SPAN-Quellen, der mit Session 1 verknüpft ist, mithilfe von 802.1q-Kapselung aus der Fast Ethernet 5/48-Schnittstelle kopiert. Eingehender Datenverkehr wird angenommen und geswitcht, Pakete ohne Tags werden in VLAN 7 klassifiziert.

Zugehörige Informationen

- Konfigurieren von SPAN und RSPAN auf Cisco Catalyst Switches der Serie 4500, auf denen

die Cisco IOS Software ausgeführt wird
- Ein SPAN-Zielport wird als "nicht verbunden" angezeigt und kommuniziert nicht mit dem Rest des Netzwerks
- Produktsupport für Switches
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems