Konfigurieren von Catalyst Switched Port Analyzer (SPAN): Beispiel

Inhalt

Einleitung

In diesem Dokument werden die neuesten implementierten Funktionen von Switched Port Analyzer (SPAN) beschrieben.

Voraussetzungen

Catalyst Switches mit Unterstützung für SPAN, RSPAN und ERSPAN

Catalyst-Switches	SPAN-Unterstützung	RSPAN-Unterstützung	ERSPAN-Unterstützung
Catalyst Express der Serie 500/520	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 Hardware-Version 3.2 oder höher und Cisco IOS Software-Version 12.2(18)SXE oder höher

Catalyst Serie 5500/5000	Ja	Nein	Nein
Catalyst Serie 4900	Ja	Ja	Nein
Catalyst Serie 4500/4000 (einschl. 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

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

In diesem Dokument wird CatOS 5.5 als Referenz für die Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 verwendet. Für die Catalyst Switches der Serien 2900XL/3500XL wird Cisco IOS® Softwareversion 12.0(5)XU verwendet.

Obwohl dieses Dokument aktualisiert wird, um die Änderungen an SPAN zu berücksichtigen, finden Sie in den Versionshinweisen der Switch-Plattform die neuesten Entwicklungen für die SPAN-Funktion.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die SPAN-Funktion, die manchmal auch als Portspiegelung oder Portüberwachung bezeichnet wird, wählt

den Netzwerkverkehr zur Analyse durch einen Netzwerkanalysator aus. Der Netzwerkanalysator kann ein Cisco SwitchProbe-Gerät oder ein anderer Remote Monitoring (RMON)-Sensor sein.

In der Vergangenheit war SPAN bei den Cisco Catalyst Switches eine relativ einfache Funktion. Mit den neuesten Versionen von Catalyst OS (CatOS) wurden jedoch großartige Verbesserungen eingeführt und zahlreiche neue Möglichkeiten eröffnet, die dem Benutzer nun zur Verfügung stehen.

Dieses Dokument ist nicht als alternative Konfigurationsanleitung für die SPAN-Funktion gedacht. In diesem Dokument werden die häufigsten Fragen zu SPAN beantwortet, z. B.:

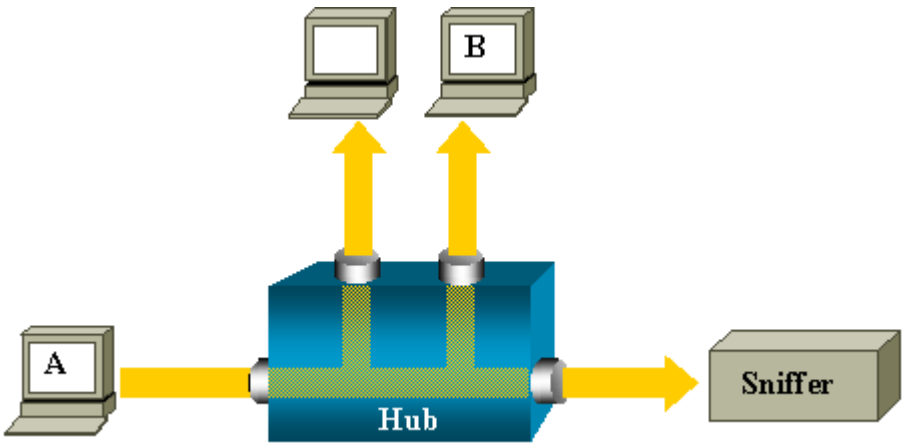
- Was ist SPAN und wie wird es konfiguriert?
- Welche verschiedenen Funktionen stehen zur Verfügung (insbesondere mehrere, gleichzeitige SPAN-Sitzungen), und welche Softwareebene ist erforderlich, um diese auszuführen?
- Beeinträchtigt SPAN die Switch-Leistung?

Kurze Beschreibung von SPAN

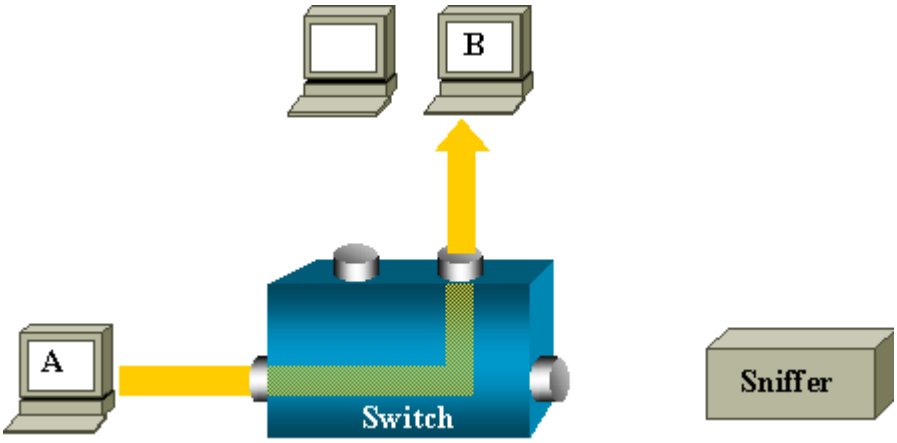
Die SPAN-Funktion wurde für Switches eingeführt, da sich Switches grundlegend von Hubs unterscheiden. Wenn ein Hub ein Paket auf einem Port empfängt, sendet er eine Kopie dieses Pakets an alle Ports mit Ausnahme des Ports, an dem der Hub das Paket empfangen hat.

Nach dem Hochfahren des Switches beginnt dieser, eine Layer-2-Weiterleitungstabelle auf Basis der Quell-MAC-Adresse der verschiedenen Pakete zu erstellen, 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.

Um beispielsweise den Ethernet-Datenverkehr zu erfassen, 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 Hosts A und B:



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



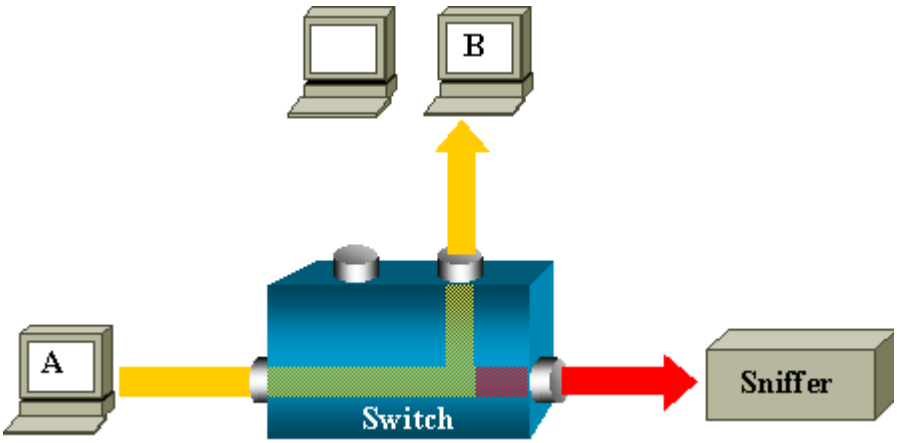
In dieser Konfiguration erfasst der Sniffer nur Datenverkehr, der an alle Ports geleitet wird, wie z. B.:

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

Unicast-Flooding tritt auf, wenn die Ziel-MAC-Adresse des Switches nicht in der CAM-Tabelle (Content-Addressable Memory) enthalten ist.

Der Switch weiß nicht, wohin der Datenverkehr gesendet werden soll. Der Switch flutet die Pakete an alle Ports im Ziel-VLAN.

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



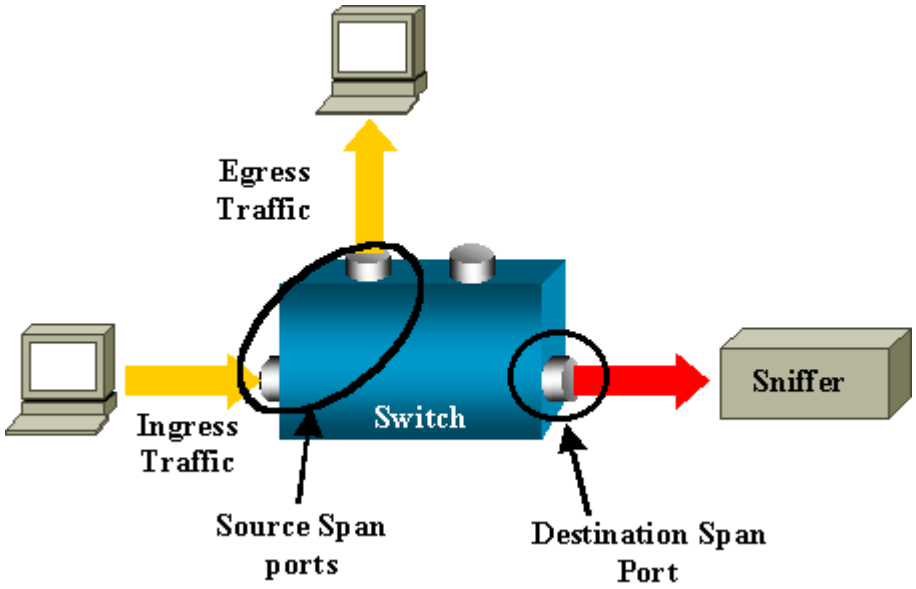
In diesem Diagramm ist der Sniffer an einen Port angeschlossen, der so konfiguriert ist, dass er eine Kopie jedes Pakets empfängt, das Host A sendet. Dieser Port wird als SPAN-Port bezeichnet.

In den anderen Abschnitten dieses Dokuments wird beschrieben, wie Sie diese Funktion sehr genau abstimmen können, um mehr als nur die Überwachung eines Ports zu erreichen.

SPAN-Terminologie

- **Eingehender Datenverkehr** - Datenverkehr, der auf dem Switch eingeht.
- **Ausgehender Datenverkehr** - Datenverkehr, der den Switch verlässt.

- **Source (SPAN) port** - Ein Port, der unter Verwendung der SPAN-Funktion überwacht wird.
- **Source (SPAN) VLAN (Quell-VLAN**): Ein VLAN, dessen Datenverkehr unter Verwendung der SPAN-Funktion überwacht wird.
- **Destination (SPAN)-Port** - Ein Port, der Quell-Ports überwacht, in der Regel dort, wo ein Netzwerkanalysator angeschlossen ist.
- **Reflector Port** - Ein Port, der Pakete in ein RSPAN-VLAN kopiert.
- **Monitor-Port** - Ein Monitor-Port ist in der Terminologie für Catalyst 2900XL/3500XL/2950 auch ein Ziel-SPAN-Port.



- **Local SPAN (Lokales 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. Lesen Sie die jeweiligen Versionshinweise oder das Konfigurationsleitfaden, um zu sehen, ob Sie RSPAN auf dem bereitgestellten Switch verwenden können.

- **Port-based SPAN (PSPAN)**: Der Benutzer gibt einen oder mehrere Quellports auf dem Switch und einen Zielport an.
- **VLAN-basiertes SPAN (VSPAN)** - Auf einem bestimmten Switch kann der Benutzer mit einem einzigen Befehl alle Ports überwachen, die zu einem bestimmten VLAN gehören.
- **ESPAN**: Dies bedeutet eine erweiterte SPAN-Version. Dieser Begriff wurde in der Entwicklung des SPAN mehrmals verwendet, um zusätzliche Funktionen zu benennen. Daher ist der Begriff nicht sehr klar und wird in diesem Dokument vermieden.
- **Administrative Quelle**: Eine Liste der Quellports oder VLANs, die für die Überwachung konfiguriert wurden.

- **Betriebsquelle:** Eine Liste der Ports, die effektiv überwacht werden. Diese Portliste kann sich von der administrativen Quelle unterscheiden.

Beispielsweise kann ein Port, der sich im heruntergefahrenen Modus befindet, in der administrativen Quelle erscheinen, wird aber nicht effektiv überwacht.

Merkmale des Quellports

Ein Quell-Port, auch Überwachter Port genannt, ist ein geswitchter oder gerouteter Port, den Sie zur Analyse des Netzwerkverkehrs überwachen.

In einer einzelnen lokalen SPAN-Sitzung oder RSPAN-Quellsitzung können Sie den Quell-Port-Datenverkehr, z. B. den empfangenen (Rx), übertragenen (Tx) oder bidirektionalen (beide) Datenverkehr, überwachen.

Der Switch unterstützt eine beliebige Anzahl von Quell-Ports (bis zur maximalen Anzahl verfügbarer Ports auf dem Switch) und Quell-VLANs.

Ein Quellport hat folgende Eigenschaften:

- 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 kann sich nicht um einen Zielport handeln.
- Jeder Quellport kann mit einer Überwachungsrichtung (Eingang, Ausgang oder beide) konfiguriert werden. Bei EtherChannel-Quellen gilt die überwachte Richtung für alle physischen Ports in der Gruppe.
- Quellports können sich im selben oder in verschiedenen VLANs befinden.
- Bei VLAN-SPAN-Quellen sind alle aktiven Ports im Quell-VLAN als Quell-Ports enthalten.

VLAN-Filterung

Wenn Sie einen Trunk-Port als Quell-Port überwachen, werden standardmäßig alle auf dem Trunk aktiven VLANs überwacht. Sie können die VLAN-Filterung verwenden, um die SPAN-Datenverkehrsüberwachung an den 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 ist, werden nur die VLANs in der Liste an den Trunk-Ports oder an den Sprach-VLAN-Access-Ports überwacht.
- SPAN-Datenverkehr, der von anderen Port-Typen stammt, wird von der VLAN-Filterung nicht beeinflusst, d. h. alle VLANs sind an anderen Ports zulässig.
- Die VLAN-Filterung wirkt sich nur auf den Datenverkehr aus, der an den Ziel-SPAN-Port weitergeleitet wird, und nicht auf das Switching für den normalen Datenverkehr.
- Sie können Quell-VLANs nicht mischen und VLANs innerhalb einer Sitzung filtern. Sie können

Quell-VLANs einrichten oder VLANs filtern, aber nicht beides 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 an allen Ports für dieses VLAN überwacht.

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 der Datenverkehr des überwachten VLAN an den Zielport gesendet.
- Wenn ein Zielport zu einem Quell-VLAN gehört, wird er aus der Quellenliste ausgeschlossen und nicht überwacht.
- Wenn den Quell-VLANs Ports hinzugefügt oder daraus entfernt werden, wird der von diesen Ports empfangene Datenverkehr im Quell-VLAN den überwachten Quellen hinzugefügt oder daraus entfernt.
- Sie können in derselben Sitzung keine Filter-VLANs mit VLAN-Quellen verwenden.
- Sie können nur Ethernet-VLANs überwachen.

Merkmale des Zielhafens

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

Ein Zielport hat folgende Eigenschaften:

- Ein Zielport muss sich auf demselben Switch wie der Quellport (für eine lokale SPAN-Sitzung) befinden.
- Ein Zielport kann ein beliebiger physischer Ethernet-Port sein.
- Ein Zielport kann jeweils nur an einer SPAN-Sitzung teilnehmen. Ein Zielport in einer SPAN-Sitzung kann kein Zielport für eine zweite SPAN-Sitzung sein.
- Ein Zielport kann kein Quellport sein.
- Ein Zielport kann keine EtherChannel-Gruppe sein.

Hinweis: Ab Version 12.2(33)SXH der Cisco IOS-Software kann die PortChannel-Schnittstelle ein Zielport sein. Ziel-EtherChannels unterstützen die EtherChannel-Protokolle PAgP (Port Aggregation Control Protocol) und LACP (Link Aggregation Control Protocol) nicht. Es wird nur der Ein-Modus unterstützt, wobei die Unterstützung für alle EtherChannel-Protokolle deaktiviert ist.

Hinweis: Weitere Informationen finden Sie unter Lokale SPAN-, RSPAN- und ERSPAN-Ziele.

- Ein Zielport kann ein physischer Port sein, der einer EtherChannel-Gruppe zugewiesen ist, 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 überträgt keinen Datenverkehr mit Ausnahme des Datenverkehrs, der für die SPAN-Sitzung erforderlich ist, es sei denn, die Lernfunktion ist aktiviert. Wenn Learning aktiviert ist, überträgt der Port auch Datenverkehr, der an Hosts gerichtet ist, die vom Zielport erfasst wurden.

Hinweis: Weitere Informationen finden Sie unter Lokale SPAN-, RSPAN- und ERSPAN-Ziele.

- Der Status des Zielports lautet "up/down" (aktiv/inaktiv). Die Schnittstelle zeigt den Port in diesem Zustand an, um deutlich zu machen, dass der Port derzeit nicht als Produktions-Port 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 an keines der Layer-2-Protokolle (STP, VTP, CDP, DTP, PagP) gebunden.
- Ein Zielport, der zu einem Quell-VLAN einer SPAN-Sitzung gehört, wird aus der Quellliste ausgeschlossen und nicht überwacht.
- Ein Zielport empfängt Kopien des gesendeten und empfangenen Datenverkehrs für alle überwachten Quellports. Wenn ein Zielport überbelegt ist, kann es zu Überlastungen kommen. Diese Überlastung kann die Weiterleitung des Datenverkehrs an einen oder mehrere Quellports beeinträchtigen.

Merkmale des Reflektoranschlusses

Der Reflektor-Port ist der Mechanismus, der Pakete in ein RSPAN-VLAN kopiert. Der Reflektor-Port leitet nur den Datenverkehr der RSPAN-Quellsitzung weiter, der er angehört.

Jedes Gerät, das an einen als Reflektor-Port festgelegten Port angeschlossen ist, verliert die Verbindung, bis die RSPAN-Quellsitzung deaktiviert wird.

Der Reflektoranschluss hat folgende Eigenschaften:

- Es handelt sich um einen Port, der auf Loopback festgelegt ist.
- Dabei kann es sich nicht um eine EtherChannel-Gruppe handeln, es ist kein Trunk vorhanden, und es ist keine Protokollfilterung möglich.
- Dabei kann es sich um einen physischen Port handeln, der einer EtherChannel-Gruppe zugewiesen ist, auch wenn die EtherChannel-Gruppe als SPAN-Quelle angegeben ist. Der Port wird aus der Gruppe entfernt, während er als Reflektor-Port konfiguriert ist.
- Ein Port, der als Reflektor-Port verwendet wird, kann weder ein SPAN-Quell- noch ein Ziel-Port sein, noch kann ein Port gleichzeitig ein Reflektor-Port für mehr als eine Sitzung sein.
- Sie ist für alle VLANs unsichtbar.
- Das native VLAN für Looped-Back-Datenverkehr an einem Reflektor-Port ist das RSPAN-VLAN.

- Der Reflektor-Port leitet nicht getaggten Datenverkehr über eine Schleife an den Switch zurück. Der Datenverkehr wird dann auf das RSPAN-VLAN übertragen und an alle Trunk-Ports geleitet, die das RSPAN-VLAN übertragen.
- Spanning Tree wird auf einem Reflektor-Port automatisch deaktiviert.
- Ein Reflektor-Port empfängt Kopien des gesendeten und empfangenen Datenverkehrs für alle überwachten Quellports.

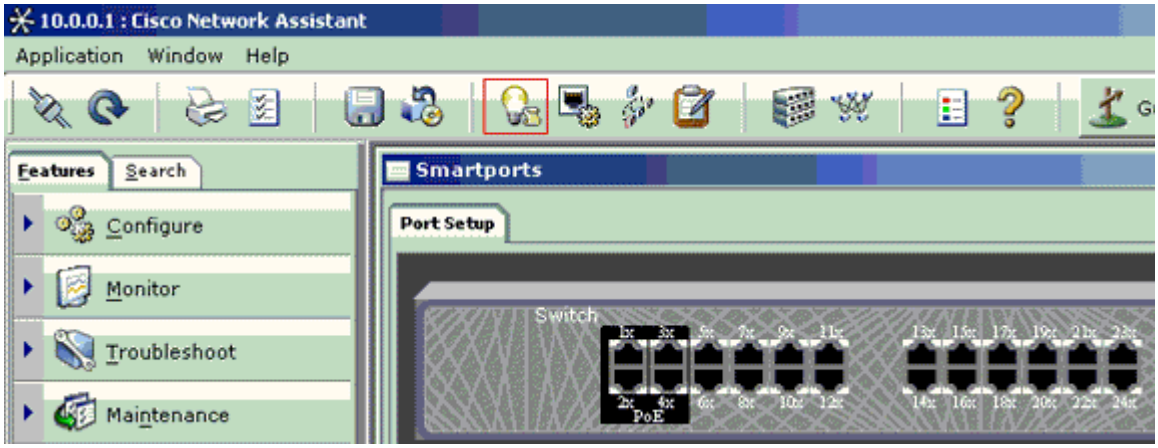
SPAN bei Catalyst Express 500/520

Catalyst Express 500 oder Catalyst Express 520 unterstützt nur die SPAN-Funktion. Catalyst Express 500/520-Ports können nur mithilfe des Cisco Network Assistant (CNA) für SPAN konfiguriert werden. Führen Sie die folgenden Schritte aus, um das SPAN zu konfigurieren:

1. Herunterladen und Installieren von CNA auf dem PC

   Sie können CNA von der Seite Download Software (nur registrierte Kunden) herunterladen.

2. Führen Sie die Schritte aus, die im Handbuch "Erste Schritte" für Catalyst Express 500 Switches 12.2(25)FY beschrieben sind, um die Switch-Einstellungen für Catalyst Express 500 anzupassen. Weitere Informationen zu Catalyst Express 520 finden Sie im Handbuch "Erste Schritte" für Catalyst Express 520.
3. Melden Sie sich mit CNA beim Switch an, und klicken Sie auf **SmartPort**.

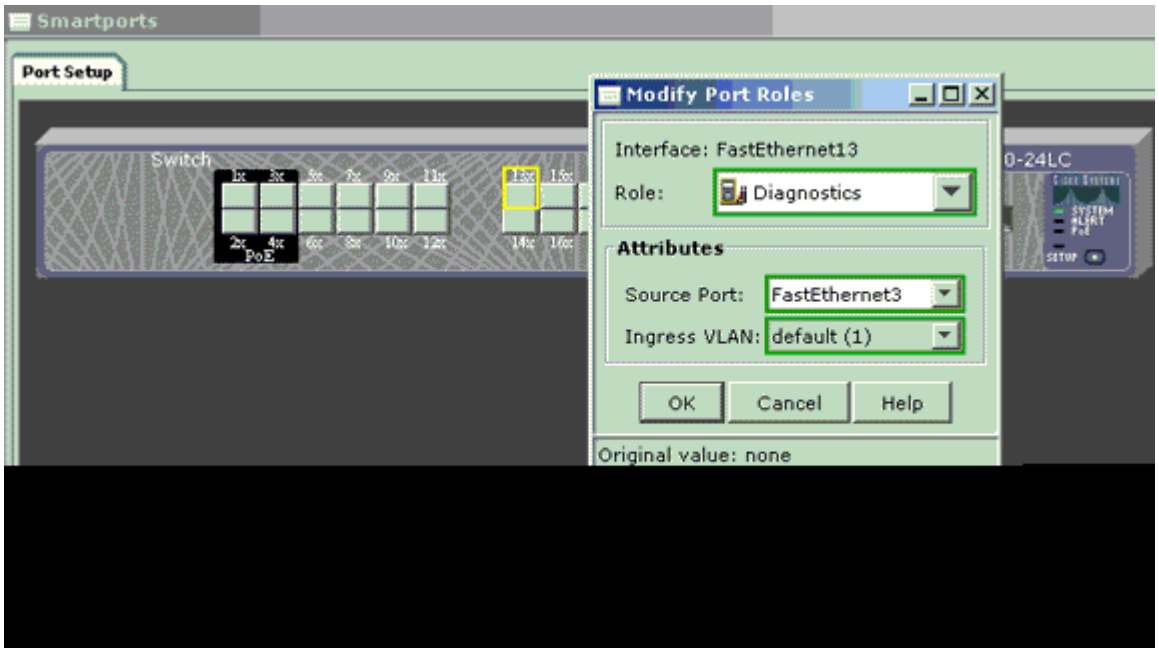


4. Klicken Sie auf eine beliebige Schnittstelle, an der Sie den PC anschließen möchten, um die Sniffer-Spuren zu erfassen.
5. Klicken Sie auf **Ändern**.

   Ein kleines Popup-Fenster wird angezeigt.

6. Wählen Sie die **Diagnosefunktion** für den Port aus.
7. Wählen Sie den Quell-Port und das VLAN aus, das Sie überwachen möchten.

   Wenn Sie None (Keines) auswählen, empfängt der Port nur Datenverkehr. Über das Eingangs-VLAN kann der mit dem Diagnoseport verbundene PC Pakete an das Netzwerk senden, das dieses VLAN verwendet.



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

SPAN bei Catalyst Switches der Serien 2900XL/3500XL

Verfügbare Funktionen und Einschränkungen

Die Portüberwachungsfunktion des Catalyst 2900XL/3500XL ist nicht sehr umfangreich. Diese Funktion ist daher relativ leicht zu verstehen.

Sie können so viele lokale PSPAN-Sitzungen wie nötig erstellen. Sie können beispielsweise PSPAN-Sitzungen auf dem Konfigurations-Port erstellen, den Sie als Ziel-SPAN-Port ausgewählt haben. Führen Sie in diesem Fall den Befehl **port monitor interface** aus, um die zu überwachenden Quellports aufzulisten. Ein Monitor-Port ist ein Ziel-SPAN-Port in der Catalyst 2900XL/3500XL-Terminologie.

- Die Haupteinschränkung besteht darin, dass alle Ports, die sich auf eine bestimmte Sitzung beziehen (Quelle oder Ziel), zum gleichen VLAN gehören müssen.
- Wenn Sie die VLAN-Schnittstelle mit einer IP-Adresse konfigurieren, überwacht der Befehl **port monitor** nur den Datenverkehr, der an diese IP-Adresse gerichtet ist. Darüber hinaus überwacht er den Broadcast-Datenverkehr, der von der VLAN-Schnittstelle empfangen wird. Er erfasst jedoch nicht den Datenverkehr, der im eigentlichen VLAN fließt. Wenn Sie im Befehl **port monitor** keine Schnittstelle angeben, werden alle anderen Ports überwacht, die zum gleichen VLAN gehören wie die Schnittstelle.

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

Hinweis: ATM-Ports sind die einzigen Ports, die nicht überwacht werden können. Sie können jedoch ATM-Ports überwachen. Die Einschränkungen in dieser Liste gelten für Ports, die die Funktion "port-monitor" aufweisen.

- Ein Monitorport kann sich nicht in einer Fast EtherChannel- oder Gigabit EtherChannel-Portgruppe befinden.
- Ein Monitorport kann nicht für die Portsicherheit aktiviert werden.
- Ein Monitorport kann kein Multi-VLAN-Port sein.
- Ein Überwachungsport muss zu demselben VLAN gehören wie der überwachte Port. Änderungen der VLAN-Mitgliedschaft sind auf überwachten Ports und Ports nicht zulässig.
- Ein Monitorport kann kein dynamischer Zugriffsport oder Trunk-Port sein. Ein Port für statischen Zugriff kann jedoch ein VLAN auf einem Trunk, einem Multi-VLAN oder einem Port für dynamischen Zugriff überwachen. Das überwachte VLAN ist mit dem Port für statischen Zugriff verknüpft.
- Die Portüberwachung funktioniert nicht, wenn sowohl der Monitorport als auch der überwachte Port geschützte Ports sind.

Achten Sie darauf, dass auf einem Port im Überwachungsstatus das Spanning Tree Protocol (STP) nicht ausgeführt wird, während der Port weiterhin zum VLAN der gespiegelten Ports gehört. 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 einen katastrophalen Bridging-Loop-Zustand geraten, da STP Sie nicht mehr schützt. Im Abschnitt Why Does the SPAN Session Create a Bridging Loop? (Warum erstellt die SPAN-Sitzung eine Bridging-Schleife?) dieses Dokuments finden Sie ein Beispiel, wie dieser Zustand auftreten kann.

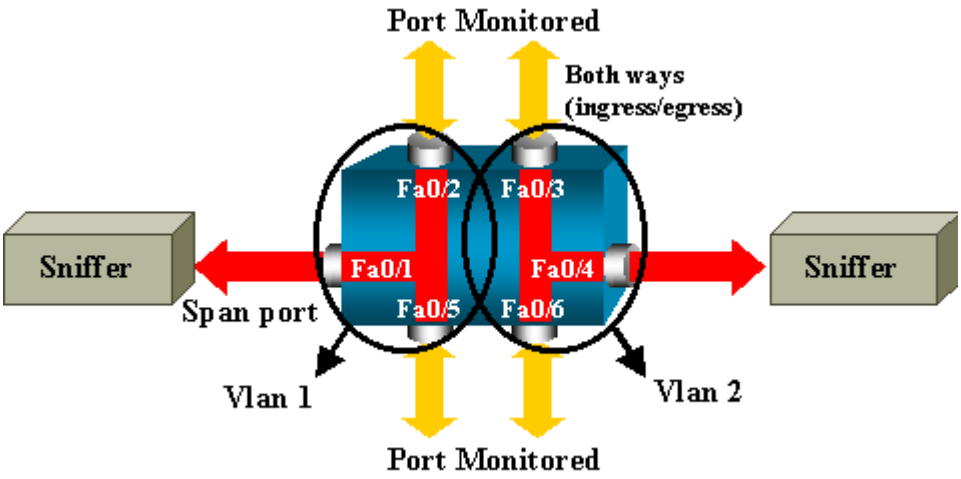
Konfigurationsbeispiel

In diesem Beispiel werden zwei gleichzeitige SPAN-Sitzungen erstellt.

- Port Fast Ethernet 0/1 (Fa0/1) überwacht den Datenverkehr, den die Ports Fa0/2 und Fa0/5 senden und empfangen. Port Fa0/1 überwacht auch den Datenverkehr von und zu 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. Weitere Ports und die Management-Schnittstelle werden im Standard-VLAN 1 konfiguriert.

Netzwerkdiagramm



Beispielkonfiguration für den 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 den Port Fa0/1 als Zielport, die Quellports Fa0/2 und Fa0/5 sowie die Managementschnittstelle (VLAN 1) zu konfigurieren, wählen Sie im Konfigurationsmodus die Schnittstelle Fa0/1 aus:

<#root>

```
Switch(config)#
```

interface fastethernet 0/1

Geben Sie die Liste der zu überwachenden Ports ein:

<#root>

```
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, auch an Port Fa0/1 kopiert. Geben Sie eine Variante des Befehls **port monitor** ein, um die Überwachung für die Verwaltungsschnittstelle zu konfigurieren:

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

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

Dieser Beispielbefehl veranschaulicht, dass die Überwachung eines Ports in einem anderen VLAN nicht möglich ist:

```
<#root>
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. Verwenden Sie dieses Mal Fa0/4 als Ziel-SPAN-Port:

```
<#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
```

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

<#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
```

> **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 für die Erfassung von Rx- und Tx-Datenverkehr ausgelegt.

SPAN beim Catalyst 2948G-L3 und 4908G-L3

Catalyst 2948G-L3 und Catalyst 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* der Versionshinweise für Catalyst 2948G-L3 und Catalyst 4908G-L3 für Cisco IOS Release 12.0(10)W5(18g).

SPAN beim 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 Catalyst 8540-Dokumentation.

Port Snooping ermöglicht die transparente Spiegelung des Datenverkehrs von einem oder mehreren Quell-Ports auf einen Ziel-Port."

Führen Sie den Befehl **snoop** aus, um eine portbasierte Datenverkehrsspiegelung bzw. Snooping einzurichten. Geben Sie **no** (**keine** Form) dieses Befehls ein, um Snooping zu deaktivieren:

<#root>

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*** gibt die Richtung des Datenverkehrs auf dem Quellport bzw. den überwachten Ports an: **Receive**, **Transmit** oder **Both (Beide)**.

```
<#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
```

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

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

SPAN bei Catalyst Switches der Serien 2900, 4500/4000, 5500/5000 und 6500/6000 mit CatOS

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

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

Dieser Abschnitt gilt für Cisco Catalyst Switches der Serie 4000. Er umfasst:

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

Lokales SPAN

SPAN-Funktionen wurden der CatOS-Software einzeln hinzugefügt, und eine SPAN-Konfiguration besteht aus einem einzelnen **set span**-Befehl. Für den Befehl stehen jetzt eine Reihe von Optionen zur Verfügung:

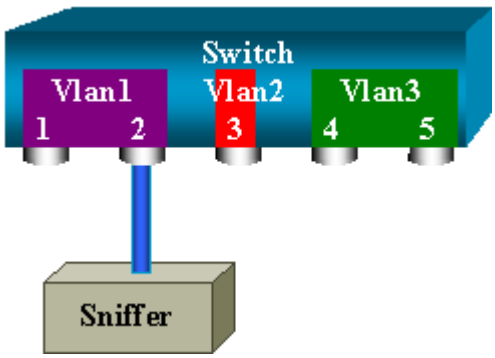
<#root>

```
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]
```

In diesem Netzwerkdiagramm werden die verschiedenen SPAN-Möglichkeiten anhand von Varianten vorgestellt:



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

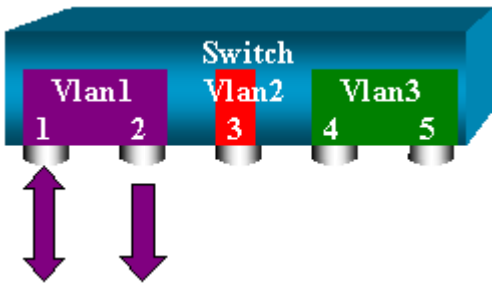
- Ports 6/1 und 6/2 gehören zu VLAN 1
- Port 6/3 gehört zu VLAN 2
- Ports 6/4 und 6/5 gehören zu VLAN 3

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

PSPAN, VSPAN: Überwachung einiger Ports oder eines gesamten VLAN

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

Überwachung eines einzelnen Ports mit 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
```

Bei dieser Konfiguration wird jedes von Port 6/1 empfangene oder gesendete Paket auf Port 6/2 kopiert. Eine klare Beschreibung wird angezeigt, wenn Sie die Konfiguration eingeben. Führen Sie den Befehl **show span** aus, um eine Zusammenfassung der aktuellen SPAN-Konfiguration zu erhalten:

<#root>

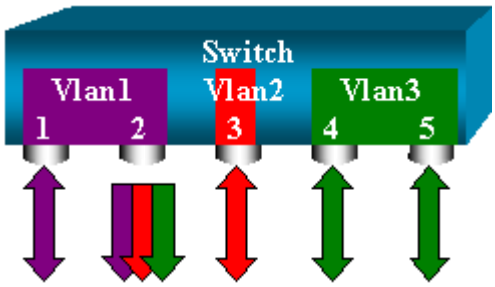
```
switch (enable)
```

```
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
```

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 Portbereich anzugeben.

Dieses Beispiel zeigt die Möglichkeit, mehr als einen Port anzugeben. Im Beispiel wird SPAN an Port 6/1 und ein Bereich von drei Ports (6/3 bis 6/5) verwendet:

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

<#root>

```
switch (enable)
```

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

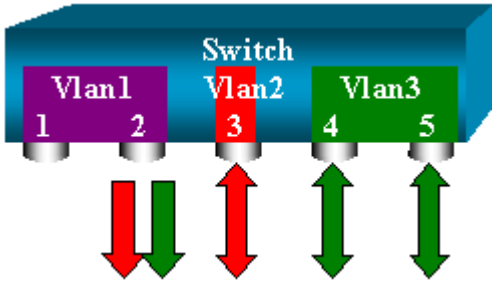
```
2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
       for destination port 6/2
       Destination : Port 6/2
       Admin Source : Port 6/1,6/3-5
       Oper Source : Port 6/1,6/3-5
       Direction : transmit/receive
       Incoming Packets: disabled
       Learning : enabled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

Hinweis: Im Gegensatz zu Catalyst Switches der Serien 2900XL/3500XL können Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 Ports überwachen, die zu mehreren verschiedenen VLANs gehören. atOS-Versionen, die älter als 5.1 sind. Hier werden die gespiegelten Ports den VLANs 1, 2 und 3 zugewiesen.

Überwachung von VLANs mit SPAN

Schließlich ermöglicht Ihnen der Befehl **set span**, einen Port zur Überwachung des lokalen Datenverkehrs für ein gesamtes VLAN zu konfigurieren. Der Befehl lautet **set span source_vlan(s) destination_port** .



Verwendung einer Liste mit einem oder mehreren VLANs als Quelle anstelle einer Liste mit Ports:

<#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
```

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

Hinweis: Das Ergebnis ist genau dasselbe, als ob Sie SPAN einzeln auf allen Ports implementieren würden, die zu den VLANs gehören, die der Befehl angibt. Vergleichen Sie die Felder `Operative` und `Admin`. Im Feld `Admin Source (Admin-Quelle)` werden im Wesentlichen alle Ports aufgeführt, die Sie für die SPAN-Sitzung konfiguriert haben. Im Feld `Oper Source` (Oper-Quelle) werden die Ports aufgeführt, die SPAN verwenden.

Eingangs-/Ausgangs-SPAN

Im Beispiel im Abschnitt VLANs mit SPAN überwachen wird der Datenverkehr, der zu den angegebenen Ports gelangt und diese verlässt, überwacht.

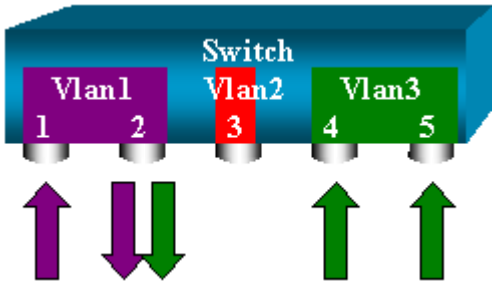
Das Feld `Richtung: Senden/Empfangen` zeigt dies an. Mit den Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 können Sie an einem bestimmten Port nur ausgehenden oder eingehenden Datenverkehr sammeln.

Fügen Sie das Schlüsselwort **rx** (Receive) oder **tx** (Transmit) am Ende des Befehls hinzu. Der Standardwert ist **sowohl (**tx als auch rx).

<#root>

```
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 an Port 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
```

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 Quell-Port ausgewählt wird, wird der Datenverkehr für alle VLANs auf diesem Trunk überwacht.

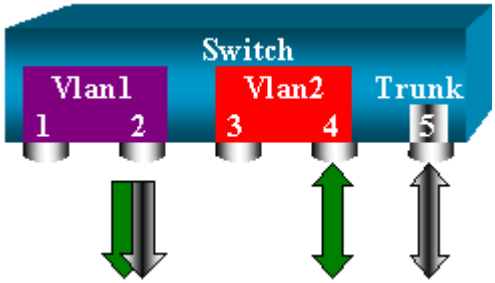
Überwachen einer Untergruppe von VLANs, die zu einem Trunk gehören

In diesem Diagramm ist Port 6/5 jetzt 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:

<#root>

```
switch (enable)
```

```
set span 6/4-5 6/2
```



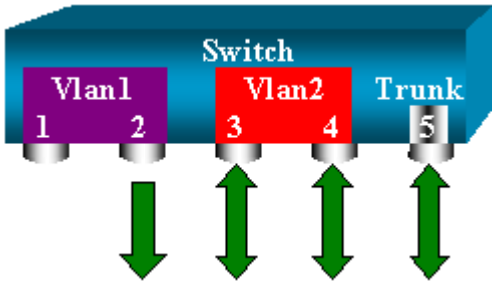
In diesem Fall ist der Datenverkehr, der über den SPAN-Port empfangen wird, eine Mischung aus dem gewünschten Datenverkehr und allen VLANs, die der Trunk 6/5 überträgt.

Beispielsweise kann auf dem Zielport nicht unterschieden werden, ob ein Paket von Port 6/4 in VLAN 2 oder Port 6/5 in VLAN 1 stammt. Eine weitere Möglichkeit besteht in der Verwendung von SPAN im gesamten VLAN 2:

<#root>

```
switch (enable)
```

```
set span 2 6/2
```



Mit dieser Konfiguration überwachen Sie zumindest nur den Verkehr vom Trunk, der zu VLAN 2 gehört. Das Problem ist, dass Sie jetzt auch Datenverkehr erhalten, den Sie von Port 6/3 nicht wünschen.

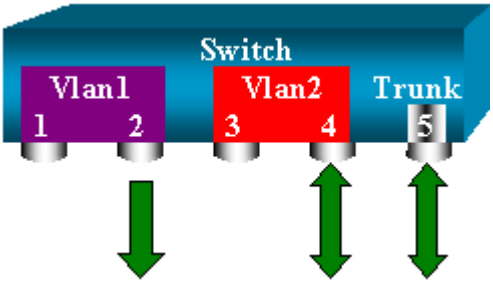
CatOS enthält ein weiteres Schlüsselwort, mit dem Sie einige VLANs auswählen können, die von einem Trunk aus überwacht werden sollen:

<#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
```



Mit diesem Befehl wird dieses Ziel erreicht, da Sie VLAN 2 auf allen überwachten Trunks auswählen. Mit dieser Filteroption können Sie mehrere VLANs angeben.

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

Trunking am Zielport

Wenn Sie Quell-Ports haben, die zu mehreren verschiedenen VLANs gehören, oder wenn Sie SPAN auf mehreren VLANs an einem Trunk-Port verwenden, möchten Sie möglicherweise identifizieren, 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, ebenfalls mit ihren jeweiligen VLAN-IDs markiert.

> **Hinweis**: Ihr Sniffer muss die entsprechende Kapselung erkennen.

<#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`

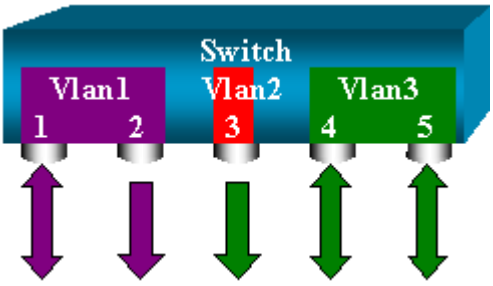
```
      Port(s) 6/2 trunk mode set to nonegotiate.
      Port(s) 6/2 trunk type set to isl.
      switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become
        isl trunk
      switch (enable)
```

`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
```

Mehrere gleichzeitige Sitzungen erstellen

Bisher wurde nur eine SPAN-Sitzung erstellt. Jedes Mal, wenn Sie einen neuen **set span**-Befehl eingeben, wird die vorherige Konfiguration ungültig. CatOS kann jetzt mehrere Sitzungen gleichzeitig ausführen, sodass es über verschiedene Ziel-Ports gleichzeitig verfügen kann. Führen Sie den Befehl **set span source destination create** aus, um eine zusätzliche SPAN-Sitzung hinzuzufügen. In dieser Sitzung wird Port 6/1 bis 6/2 überwacht, und gleichzeitig wird VLAN 3 bis Port 6/3 überwacht:



<#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
```

Führen Sie nun den Befehl **show span** aus, um festzustellen, ob zwei Sitzungen gleichzeitig stattfinden:

<#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
```

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

<#root>

set span disable {all | destination_port}

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

<#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
```

Sie können nun prüfen, ob nur noch eine Sitzung übrig bleibt:

<#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
```

Führen Sie diesen Befehl aus, um alle aktuellen Sitzungen in einem Schritt zu deaktivieren:

<#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
```

Weitere SPAN-Optionen

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

<#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

]

[learning

]

[multicast

]

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

In diesem Abschnitt werden die in diesem Dokument beschriebenen Optionen kurz vorgestellt:

- **sc0:** Sie geben das **sc0**-Schlüsselwort in einer SPAN-Konfiguration an, wenn Sie den Datenverkehr zur Verwaltungsschnittstelle sc0 überwachen müssen. Diese Funktion ist für Catalyst Switches der Serien 5500/5000 und 6500/6000 verfügbar, Codeversion CatOS 5.1 oder höher.

- **inpkts *enable/disable*** - Diese Option ist äußerst wichtig. Wie in diesem Dokument angegeben, gehört ein Port, den Sie als SPAN-Ziel konfigurieren, weiterhin zum ursprünglichen VLAN. Pakete, die auf einem Zielport empfangen werden, treten dann in das VLAN ein, als handele es sich bei diesem Port um einen normalen Zugriffsport. Dieses Verhalten kann gewünscht werden. Wenn Sie einen PC als Sniffer verwenden, möchten Sie möglicherweise, dass dieser PC vollständig mit dem VLAN verbunden ist. Dennoch kann die Verbindung gefährlich sein, wenn Sie den Zielport mit anderen Netzwerkgeräten verbinden, die eine Schleife im Netzwerk erstellen. Der SPAN-Zielport führt STP nicht aus, und Sie können in eine gefährliche Bridging-Loop-Situation geraten. Im Abschnitt Why Does the SPAN Session Create a Bridging Loop? (Warum erstellt die SPAN-Sitzung eine Bridging-Schleife?) dieses Dokuments erfahren Sie, 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. Dieser Ausschuss schützt den Port vor Bridge-Schleifen. Diese Option wird in CatOS 4.2 angezeigt.

- learning ***enable/disable*** - Mit dieser Option können Sie das Lernen auf dem Zielport deaktivieren. Standardmäßig ist Lernen aktiviert, und der Zielport bezieht MAC-Adressen von eingehenden Paketen, die der Port empfängt. Diese Funktion wird in CatOS 5.2 auf dem Catalyst 4500/4000 und 5500/5000 sowie in CatOS 5.3 auf dem Catalyst 6500/6000 angezeigt.

- **Multicast *enable/disable*** - Wie der Name schon sagt, können Sie mit dieser Option die Überwachung von Multicast-Paketen aktivieren oder deaktivieren. Standardmäßig ist diese Option aktiviert. Diese Funktion ist für Catalyst 5500/5000 und 6500/6000 sowie CatOS 5.1 und höher verfügbar.

- **spanning port 15/1** - Beim 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 über die Software geleitet oder an die MSFC weitergeleitet wird.

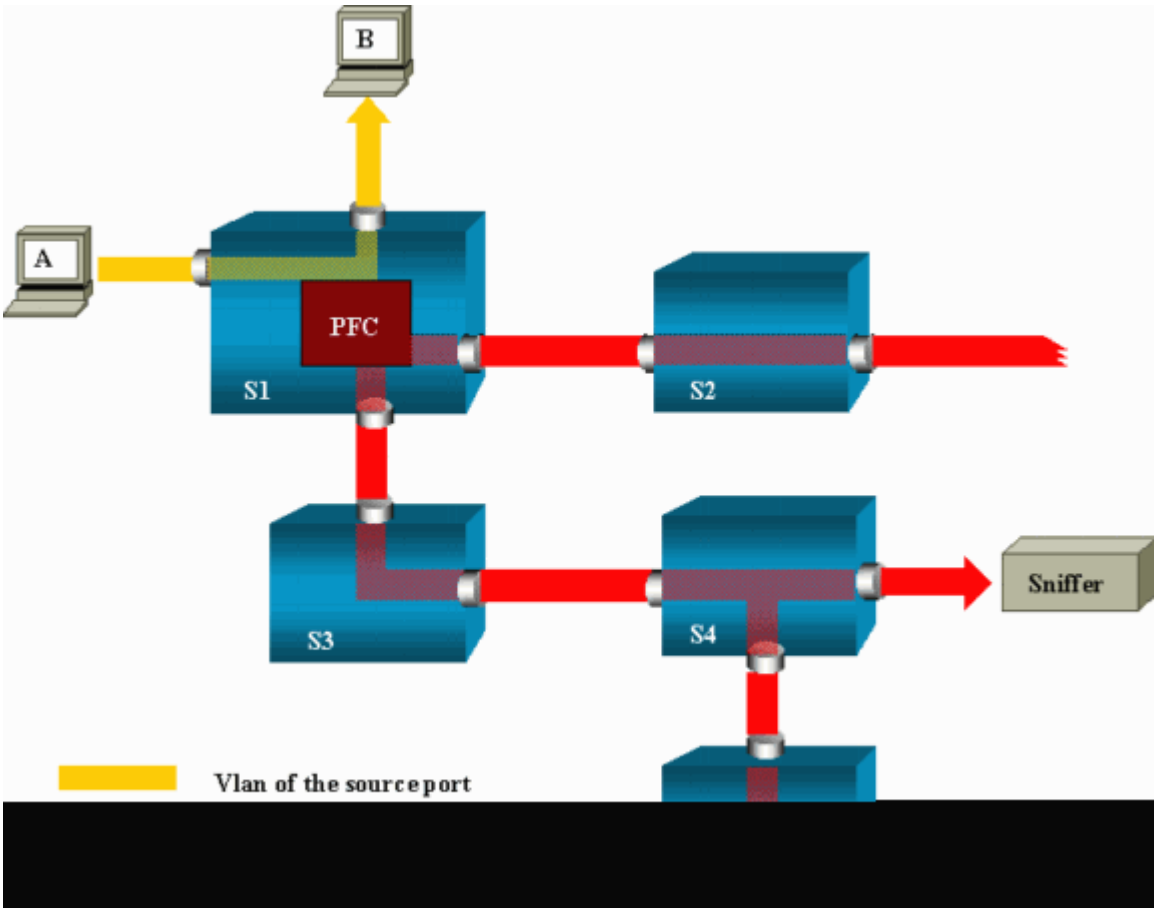
Remote-SPAN

RSPAN - Überblick

RSPAN ermöglicht Ihnen die Überwachung von Quell-Ports, die über ein Switch-Netzwerk verteilt sind, nicht nur lokal auf einem Switch mit SPAN. Diese Funktion wird in CatOS 5.3 in den Catalyst Switches der Serien 6500/6000 angezeigt und in den Catalyst Switches der Serien 4500/4000 in CatOS 6.3 und höher hinzugefügt.

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

Dieses Diagramm veranschaulicht den Aufbau einer RSPAN-Sitzung:



In diesem Beispiel konfigurieren Sie RSPAN so, dass der von Host A gesendete Datenverkehr überwacht wird. Wenn A einen Frame generiert, der für B bestimmt ist, wird das Paket von einem ASIC (Application-Specific Integrated Circuit) der Catalyst 6500/6000 Policy Feature Card (PFC) in ein vordefiniertes RSPAN-VLAN kopiert. Von dort wird das Paket an alle anderen Ports geflutet, die zum RSPAN-VLAN gehören. Alle hier gezeigten Interswitch-Verbindungen sind Trunks, was für RSPAN erforderlich ist. Die einzigen Zugangsports sind Zielports, an denen die Sniffer angeschlossen sind (hier auf S4 und S5).

Dies sind einige Anmerkungen zu diesem Design:

- S1 wird als Quellswitch bezeichnet. Pakete gelangen nur in Switches, die als RSPAN-Quelle konfiguriert sind, in das RSPAN-VLAN. Derzeit kann ein Switch nur die Quelle für eine RSPAN-Sitzung sein, d. h., ein Source-Switch kann jeweils nur ein RSPAN-VLAN versorgen.

- S2 und S3 sind Zwischenschalter. Sie sind keine RSPAN-Quellen und verfügen über keine Ziel-Ports. Ein Switch kann für eine beliebige Anzahl von RSPAN-Sitzungen zwischengeschaltet sein.

- S4 und S5 sind Ziel-Switches. Einige ihrer Ports sind als Ziel für eine RSPAN-Sitzung konfiguriert.

Derzeit kann ein Catalyst 6500/6000 über bis zu 24 RSPAN-Zielports für eine oder mehrere verschiedene Sitzungen verfügen. Sie können auch feststellen, dass S4 sowohl ein Ziel- als auch ein Zwischenswitch ist.

- Sie können sehen, dass RSPAN-Pakete in das RSPAN-VLAN geleitet werden. Selbst Switches, die sich nicht auf dem Pfad zu einem Zielport befinden, wie S2, empfangen den Datenverkehr für das RSPAN-VLAN. Sie können es nützlich finden, dieses VLAN auf solchen S1-S2-Verbindungen zu bereinigen.
- Um die Überflutung zu erreichen, wird das Lernen im RSPAN-VLAN deaktiviert.
- Zur Vermeidung von Schleifen wurde STP im RSPAN-VLAN beibehalten. Daher kann RSPAN Bridge Protocol Data Units (BPDUs) nicht 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 Syntax der übrigen Befehle ähnelt der in einer typischen SPAN-Sitzung.

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

Platzieren Sie zunächst dieselbe VTP-Domäne (VLAN Trunk Protocol) auf jedem Switch, und konfigurieren Sie eine Seite als wünschenswertes Trunking. Die VTP-Verhandlung erledigt den Rest. Geben Sie den folgenden Befehl auf S1 ein:

```
<#root>

S1> (enable)

set vtp domain cisco

      VTP domain cisco modified
```

Führen Sie auf S2 die folgenden Befehle aus:

```
<#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
```

Erstellung des RSPAN-VLANs

Für eine RSPAN-Sitzung ist ein bestimmtes RSPAN-VLAN erforderlich. Sie müssen dieses VLAN erstellen. Sie können ein vorhandenes VLAN nicht in ein RSPAN-VLAN konvertieren. In diesem Beispiel wird VLAN 100 verwendet:

<#root>

```
S2> (enable)
```

set vlan 100 rspan

```
      Vlan 100 configuration successful
```

Führen Sie diesen Befehl auf einem Switch aus, der als VTP-Server konfiguriert ist. Die Kenntnis des RSPAN VLAN 100 wird automatisch auf die gesamte VTP-Domäne verteilt.

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

<#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
```

Konfiguration eines RSPAN-Quell-Ports auf S1

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

<#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
```

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

Überprüfen der Konfiguration

Der Befehl **show** rspan gibt eine Übersicht über die aktuelle RSPAN-Konfiguration auf dem Switch. Auch hier kann immer nur eine RSPAN-Quellsitzung gleichzeitig stattfinden.

<#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
```

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 in der Tat gleich. Sie können RSPAN sogar lokal auf einem einzelnen Switch verwenden, wenn Sie mehrere Ziel-SPAN-Ports haben möchten.

Funktionsübersicht und Einschränkungen

In dieser Tabelle werden die verschiedenen Funktionen zusammengefasst, die eingeführt wurden, und es wird die erforderliche CatOS-Mindestversion angegeben, um die Funktion auf der angegebenen Plattform auszuführen:

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	â€”	5.1	5.1
Option ***zum Aktivieren/Deaktivieren von* Multicast**	â€”	5.1	5.1
Learning *Aktivieren/Deaktivieren*-Option	5.2	5.2	5.3
RSPAN	6.3	â€”	5.3

Diese Tabelle bietet eine kurze Zusammenfassung der aktuellen Beschränkungen hinsichtlich der Anzahl möglicher SPAN-Sitzungen:

Funktion	Catalyst Switches der Serien 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
Sitzungen gesamt	5	5	30

Weitere Einschränkungen und Konfigurationsrichtlinien finden Sie in den folgenden Dokumenten:

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

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

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

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

Die SPAN-Funktionskonfigurationsbefehle sind bei Catalyst 2950 und Catalyst 3550 ähnlich. Catalyst 2950 kann die VLANs jedoch nicht überwachen. Sie können das SPAN wie in diesem Beispiel konfigurieren:

```
<#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#
```

Sie können auch einen Port als Ziel für lokales SPAN und RSPAN für den gleichen VLAN-Datenverkehr konfigurieren. Um den Datenverkehr für ein bestimmtes VLAN zu überwachen, das sich auf 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 über zwei Switches verteilt ist:

<#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.

Verwenden Sie auf dem Remote-Switch die folgende Konfiguration:

<#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

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 auf zwei Switches befindet.

Hinweis: Im Gegensatz zu den Switches der Serien 2900XL und 3500XL bietet der Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-1 Die Switches der Serien E, 3750 und 3750-E unterstützen SPAN beim Quell-Port-Datenverkehr nur in Rx-Richtung (Rx SPAN oder Eingangs-SPAN), nur in Tx-Richtung (Tx SPAN oder Ausgangs-SPAN) oder in beiden.

Hinweis: Die Befehle in der Konfiguration werden von Catalyst 2950 mit Version 12.0(5.2)WC(1) der Cisco IOS-Software oder von Software, die älter ist als Version 12.1(6)EA2 der Cisco IOS-Software, nicht unterstützt. Um SPAN auf einem Catalyst 2950 mit einer Software zu konfigurieren, die älter ist als die Cisco IOS Software Version 12.1(6)EA2, lesen Sie den Abschnitt *Enabling Switch Port Analyzer (Aktivieren* des Switch-Port-*Analyzers)* unter Managing Switches.

Hinweis: Catalyst 2950 Switches, die Cisco IOS Software Release 12.1.(9)EA1d und frühere Versionen im Cisco IOS Software Release 12.1 verwenden, unterstützen SPAN. Alle Pakete, die auf dem SPAN-Zielport (verbunden mit dem Sniffing-Gerät oder PC) angezeigt werden, weisen jedoch ein IEEE 802.1Q-Tag auf, obwohl es sich bei dem SPAN-Quellport (überwachter Port) möglicherweise nicht um einen 802.1Q-Trunk-Port handelt. Wenn das Sniffing-Gerät oder die Netzwerkkarte (NIC) des PCs Pakete mit 802.1Q-Tags nicht versteht, kann das Gerät Pakete verwerfen oder Probleme beim Decodieren der Pakete haben. Die Möglichkeit, die mit 802.1Q gekennzeichneten Frames anzuzeigen, ist nur wichtig, wenn der SPAN-Quellport ein Trunk-Port ist. Mit Cisco IOS Software, Version 12.1(11)EA1 und höher, können Sie das Tagging der Pakete am SPAN-Zielport aktivieren und deaktivieren. Führen Sie den Befehl **monitor session session_number destination interface interface_id encapsulation dot1q aus**, um die Kapselung der Pakete am Zielport zu aktivieren. Wenn Sie das **Kapselungsschlüsselwort** nicht angeben, werden die Pakete ohne Tags gesendet. Dies ist die Standardeinstellung in Version 12.1(11)EA1 und höher der Cisco IOS-Software.

Funktion	Catalyst 2950/3550
Option zum *Aktivieren/Deaktivieren* des Eingangs (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
Sitzungen gesamt	2

[1] Die Catalyst 2940 Switches unterstützen nur lokales SPAN. RSPAN wird auf dieser Plattform nicht unterstützt.

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

- Konfigurieren von SPAN (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 bei Switches der Serien Catalyst 4500/4000 und Catalyst 6500/6000 mit Cisco IOS System-Software

Die SPAN-Funktion wird von den Catalyst Switches der Serien 4500/4000 und 6500/6000 unterstützt, auf denen die Cisco IOS-Systemsoftware ausgeführt wird. Beide Switch-Plattformen verwenden die gleiche Befehlszeilenschnittstelle (CLI) wie SPAN auf Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560 und 3565. Siehe Abschnitt zu den Switches der Serien 60E, 3750 und 3750E. Weitere 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:

<#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#
```

Funktionsübersicht und Einschränkungen

In dieser Tabelle werden die verschiedenen Funktionen zusammengefasst, die eingeführt wurden, und die erforderliche Mindestversion der Cisco IOS Software bereitgestellt, um die Funktion auf der angegebenen Plattform auszuführen:

Funktion	Catalyst 4500/4000 (Cisco IOS Software)	Catalyst 6500/6000 (Cisco IOS Software)
Option zum *Aktivieren/Deaktivieren* des Eingangs (Inpkts)	Cisco IOS Software-Version 12.1(19)EW	Derzeit nicht unterstützt[1]
RSPAN	Cisco IOS Software-Version 12.1(20)EW	Cisco IOS Software-Version 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 6500/6000 unterliegt einer Einschränkung in Bezug auf das PIM-Protokoll. Wenn ein Switch sowohl für PIM als auch für SPAN konfiguriert ist, kann der an den SPAN-Zielport angeschlossene Network Analyzer/Sniffer PIM-Pakete erkennen, die nicht Teil des SPAN-Quellports/VLAN-Verkehrs sind. Dieses Problem tritt aufgrund einer Beschränkung in der Paketweiterleitungsarchitektur des Switches auf. Der SPAN-Zielport führt keine Überprüfung der Paketquelle durch. Dieses Problem ist auch in der Cisco Bug-ID CSCdy57506 dokumentiert (nur für registrierte Kunden).

Diese Tabelle bietet 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
Sitzungen gesamt	6

Weitere Informationen finden Sie unter Local SPAN, RSPAN, and ERSPAN Session Limits for Catalyst 6500/6000 switches running Cisco IOS software.

Bei der Catalyst Serie 6500 ist zu beachten, dass das Ausgangs-SPAN auf dem Supervisor erfolgt. Auf diese Weise kann der gesamte Datenverkehr, der dem Egress-SPAN unterliegt, über die Fabric zum Supervisor und dann zum SPAN-Zielport gesendet werden, wodurch erhebliche Systemressourcen genutzt und der Benutzerdatenverkehr beeinträchtigt werden kann. Eingangs-SPAN wird für Eingangsmodule ausgeführt, sodass die SPAN-Leistung die Summe aller teilnehmenden Replikations-Engines ist. Die Performance der SPAN-Funktion hängt von der Paketgröße und dem in der Replikations-Engine verfügbaren ASIC-Typ ab.

Bei älteren Versionen als Cisco IOS Software, Version 12.2(33)SXH, kann eine Port-Channel-Schnittstelle,

ein EtherChannel, kein SPAN-Ziel sein. Mit Cisco IOS Software, Version 12.2(33)SXH und höher, kann ein EtherChannel als SPAN-Ziel verwendet werden. Ziel-EtherChannels unterstützen die EtherChannel-Protokolle PAgP (Port Aggregation Control Protocol) und LACP (Link Aggregation Control Protocol) nicht. Es wird nur der Ein-Modus unterstützt, wobei die Unterstützung für alle EtherChannel-Protokolle deaktiviert ist.

Weitere Einschränkungen und Konfigurationsrichtlinien finden Sie in den folgenden Dokumenten:

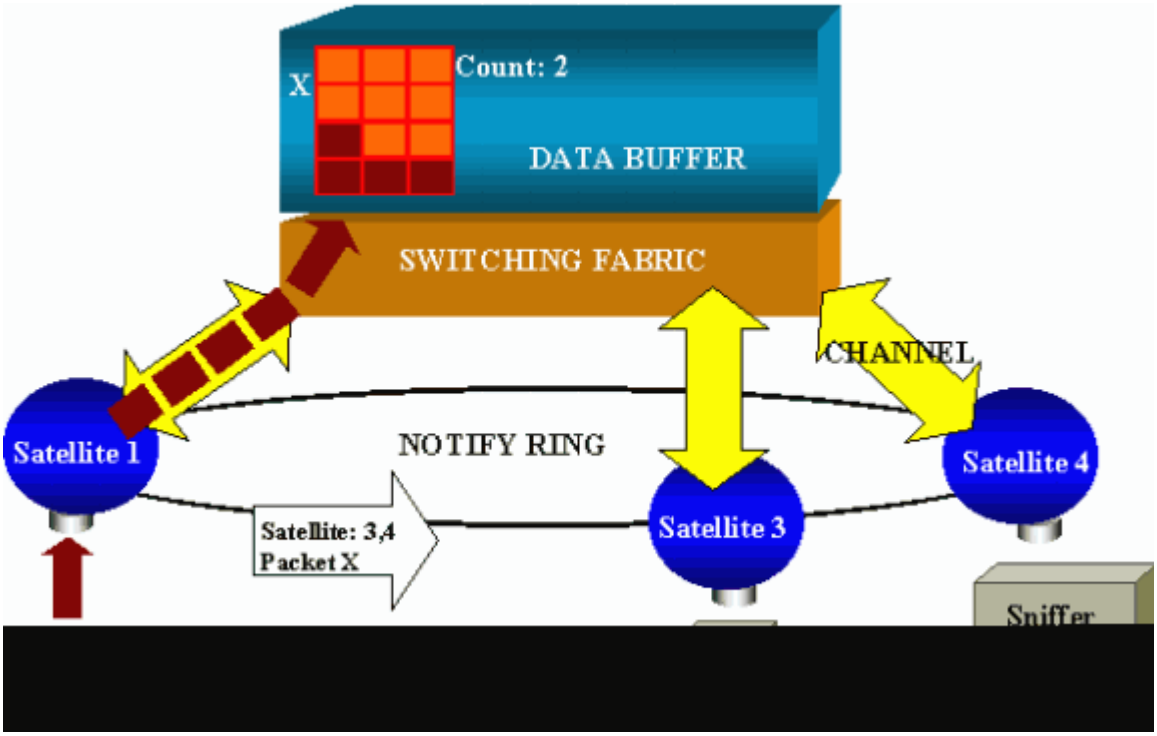
- Konfigurieren von SPAN und RSPAN (Catalyst 4500/4000)
- Konfigurieren von lokalem SPAN, Remote SPAN (RSPAN) und gekapseltem RSPAN (Catalyst 6500/6000)

Auswirkungen von SPAN auf die Leistung der verschiedenen Catalyst-Plattformen

Catalyst Serie 2900XL/3500XL

Architektur-Übersicht

Dies ist eine sehr vereinfachte Ansicht der internen Architektur der Switches der Serien 2900XL/3500XL:



Die Ports des Switches sind mit Satelliten verbunden, die über radiale Kanäle mit einer Switching Fabric kommunizieren. Oben sind alle Satelliten über einen speziellen Hochgeschwindigkeitsring für den Signalisierungsverkehr miteinander verbunden.

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 Zielhäfen. In dem Diagramm in diesem Abschnitt weiß Satellit 1, dass das Paket X von den Satelliten 3 und 4 empfangen werden soll. Satellit 1 sendet über den Benachrichtigungsring eine Nachricht an die anderen Satelliten. Anschließend können die Satelliten 3 und 4 über ihre radialen Kanäle die Zellen aus dem gemeinsamen Speicher abrufen und das Paket schließlich

weiterleiten. Da der Quellsatellit das Ziel kennt, sendet 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 gemeinsam genutzten Speicher abruft, wird dieser Index dekrementiert. Wenn der Index 0 erreicht, kann der freigegebene Speicher freigegeben werden.

Auswirkungen auf die Leistung

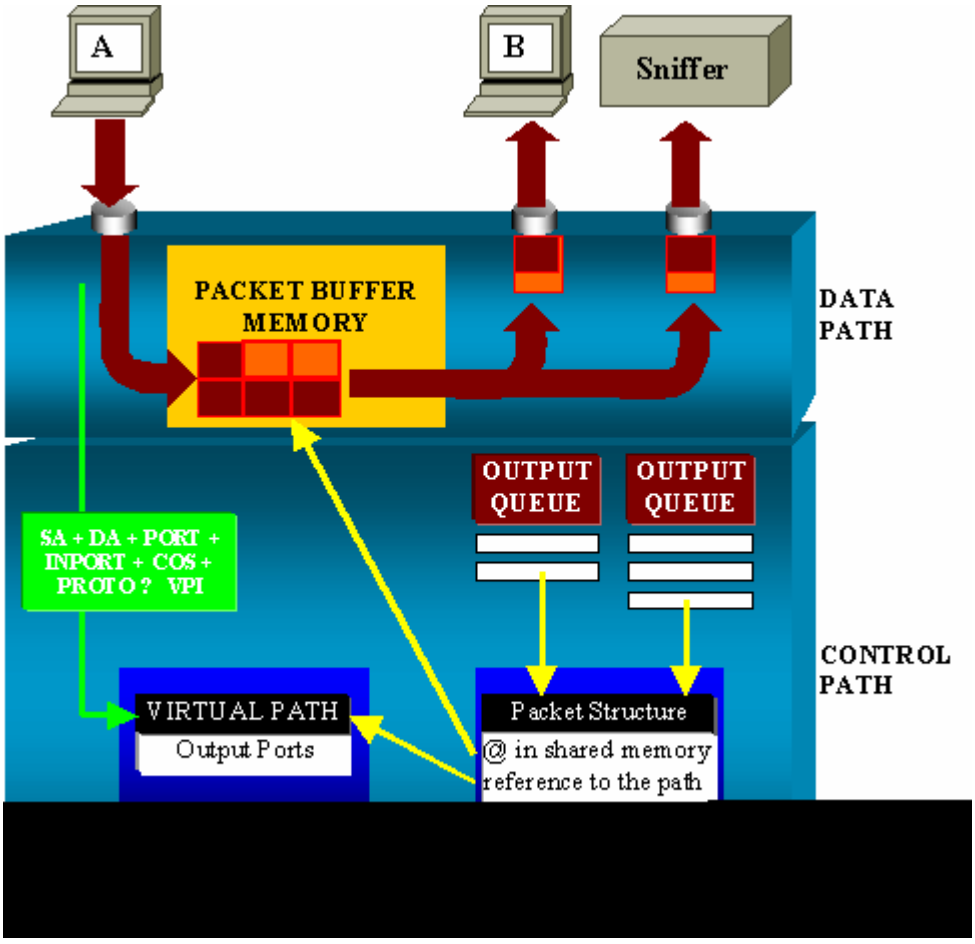
Um einige Ports mit SPAN zu überwachen, muss ein Paket eine zusätzliche Zeit lang aus dem Datenpuffer in einen Satelliten kopiert werden. Die Auswirkungen auf die Hochgeschwindigkeits-Switching-Fabric sind vernachlässigbar.

Der Überwachungs-Port empfängt Kopien des übertragenen und empfangenen Datenverkehrs für alle überwachten Ports. Bei dieser Architektur wird ein Paket, das für mehrere Ziele bestimmt ist, im Speicher gespeichert, bis alle Kopien weitergeleitet werden. Wenn der Überwachungsport für einen längeren Zeitraum zu 50 % überbelegt ist, ist dieser wahrscheinlich überlastet und nimmt einen Teil des gemeinsam genutzten Speichers ein. Es besteht die Möglichkeit, dass sich einer oder mehrere der überwachten Ports ebenfalls verlangsamen.

Catalyst Serie 4500/4000

Architektur-Übersicht

Der Catalyst 4500/4000 basiert auf einer Switching-Fabric für gemeinsam genutzten Speicher. Dieses Diagramm bietet einen allgemeinen Überblick 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 dem

realen Datentransfer innerhalb des Switches, vom Steuerpfad, wo alle Entscheidungen getroffen werden.

Wenn ein Paket auf den Switch zugreift, wird ein Puffer im Paketpufferspeicher (einem gemeinsam genutzten Speicher) zugewiesen.

Eine Paketstruktur, die auf diesen Puffer verweist, wird in der PDT (Packet Descriptor Table) initialisiert.

Während die Daten in den gemeinsam genutzten Speicher kopiert werden, bestimmt der Steuerungspfad, wohin das Paket weitergeleitet wird. Für diese Bestimmung wird aus den folgenden Informationen ein Hashwert berechnet:

- Die Adresse der Paketquelle
- 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 den virtuellen Pfad im VPT enthält mehrere Felder, die sich auf diesen bestimmten Datenfluss beziehen.

Die Felder enthalten die Zielports. Die Paketstruktur in der 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, sodass der Zähler auf 2 initialisiert wird. Schließlich wird die Paketstruktur der Ausgabewarteschlange der beiden Zielports hinzugefügt.

Von dort werden die Daten aus dem gemeinsam genutzten Speicher in den Ausgangspuffer des Ports kopiert, und der Paketstrukturzähler wird dekrementiert. Wenn 0 erreicht ist, wird der Puffer des gemeinsamen Speichers freigegeben.

Auswirkungen auf die Leistung

Bei Verwendung der SPAN-Funktion muss ein Paket an zwei verschiedene Ports gesendet werden, wie im Beispiel im Abschnitt Architekturübersicht gezeigt.

Das Senden des Pakets an zwei Ports ist kein Problem, da die Switching-Fabric nicht blockiert.

Wenn der SPAN-Zielport überlastet ist, werden Pakete in der Ausgabewarteschlange verworfen und korrekt aus dem gemeinsam genutzten Speicher freigegeben. T

Der Betrieb des Switches wird daher nicht beeinträchtigt.

Catalyst Serien 5500/5000 und 6500/6000

Architektur-Übersicht

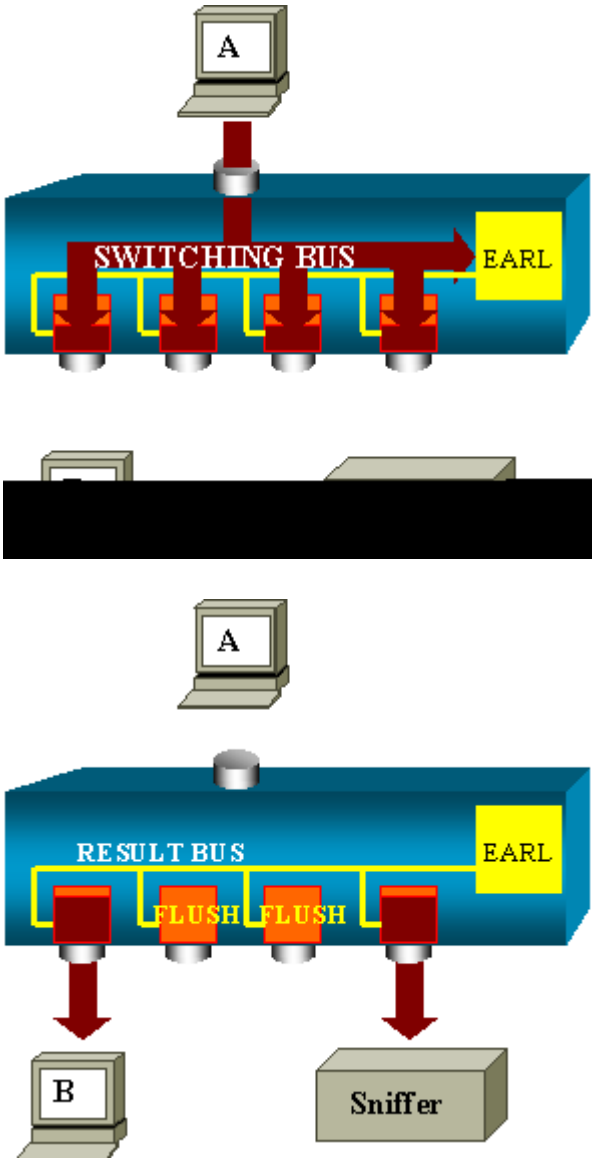
Auf den Catalyst Switches der Serien 5500/5000 und 6500/6000 wird ein an einem Port empfangenes Paket

auf dem internen Switching-Bus übertragen.

Jede Linecard im Switch beginnt, dieses Paket in internen Puffern zu speichern.

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 Indexes ermöglicht es der Linecard, individuell zu entscheiden, ob sie das Paket leeren oder übertragen soll, wenn die Linecard das Paket in ihren Puffern empfängt.



Auswirkungen auf die Leistung

Ob ein oder mehrere Ports das Paket letztendlich übertragen, hat absolut keinen Einfluss auf den Switch-Betrieb. Aus diesem Grund hat die SPAN-Funktion keine Auswirkungen auf die Leistung, wenn Sie diese Architektur in Betracht ziehen.

Häufig gestellte Fragen und häufige Probleme

Verbindungsprobleme aufgrund einer fehlerhaften SPAN-Konfiguration

Verbindungsprobleme aufgrund der falschen SPAN-Konfiguration treten häufig bei CatOS-Versionen vor 5.1 auf. Bei diesen Versionen ist nur eine SPAN-Sitzung möglich.

Die Sitzung bleibt in der Konfiguration, auch wenn Sie SPAN deaktivieren. Mit dem Befehl **set span enable** wird die gespeicherte SPAN-Sitzung erneut aktiviert.

Die Aktion tritt häufig aufgrund eines Tippfehlers 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 besteht noch in der aktuellen Implementierung von CatOS. Achten Sie sehr sorgfältig auf den Port, den Sie als SPAN-Ziel auswählen.

SPAN-Ziel-Port aktiv/inaktiv

Wenn Ports zur Überwachung über mehrere Spanns verteilt werden, wird der Port-Status als UP/DOWN angezeigt.

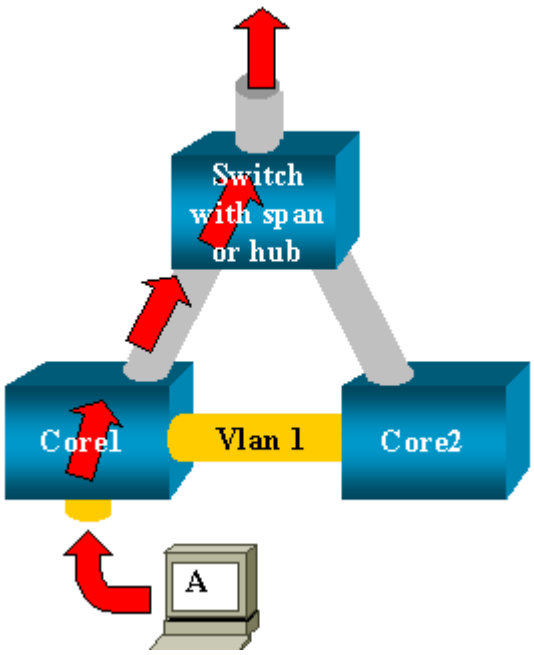
Wenn Sie eine SPAN-Sitzung zur Überwachung des Ports konfigurieren, zeigt die Zielschnittstelle standardmäßig den Status "Down" (Überwachung) an.

Die Schnittstelle zeigt den Port in diesem Zustand an, um deutlich zu machen, dass der Port derzeit nicht als Produktions-Port verwendbar ist. Die Überwachung des Ports nach oben/unten ist normal.

Warum erzeugt die SPAN-Sitzung eine Bridging-Schleife?

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

Dies ist ein Beispiel für das Szenario:



Es gibt zwei Core-Switches, die über einen Trunk verbunden sind. In diesem Fall sind mit jedem Switch mehrere Server, Clients oder andere Bridges verbunden.

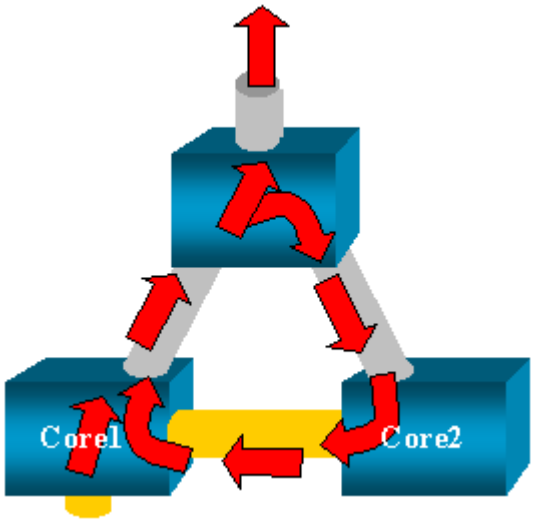
Der Administrator möchte VLAN 1 überwachen, das auf mehreren Brücken mit SPAN angezeigt wird.

Der Administrator erstellt eine SPAN-Sitzung, die das gesamte VLAN 1 auf jedem Core-Switch überwacht. Um diese beiden Sitzungen zusammenzuführen, verbindet er den Zielport mit demselben Hub (oder demselben Switch unter Verwendung einer anderen SPAN-Sitzung).

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

Das einzige Problem besteht darin, dass der Datenverkehr über den Ziel-SPAN-Port ebenfalls wieder in den Core 2 eingespeist wird.

Die erneute Einspeisung des Datenverkehrs in Core 2 erzeugt eine Bridging-Schleife in VLAN 1. Denken Sie daran, dass auf einem SPAN-Zielport STP nicht ausgeführt wird und eine solche Schleife nicht verhindert werden kann.



Hinweis: Aufgrund der Einführung der Option "inpkts (input packages)" (Eingabepakete) in 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: Auch wenn die Option inpkts den Loop verhindert, kann die in diesem Abschnitt gezeigte Konfiguration zu Problemen im Netzwerk führen. Netzwerkprobleme können aufgrund von MAC-Adressen-Lernproblemen auftreten, die mit dem auf dem Zielport aktivierten Lernen verknüpft sind.

Beeinträchtigt SPAN die Leistung?

Informationen zu den Leistungseinbußen für die angegebenen Catalyst Plattformen finden Sie in den folgenden Abschnitten dieses Dokuments:

- Catalyst Serie 2900XL/3500XL
- Catalyst Serie 4500/4000
- Catalyst Serien 5500/5000 und 6500/6000

Können Sie SPAN auf einem EtherChannel-Port konfigurieren?

Es bildet sich kein EtherChannel, wenn einer der Ports im Paket ein SPAN-Zielport ist. Wenn Sie in dieser Situation versuchen, SPAN zu konfigurieren, werden Sie vom Switch wie folgt informiert:

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

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

Können mehrere SPAN-Sitzungen gleichzeitig ausgeführt werden?

Bei Catalyst Switches der Serien 2900XL/3500XL stellt die Anzahl der auf dem Switch verfügbaren Zielports die einzige Beschränkung für die Anzahl der SPAN-Sitzungen dar.

Den Catalyst Switches der Serie 2950 kann jeweils nur ein Überwachungsport zugewiesen werden.

Wenn Sie einen anderen Port als Monitorport auswählen, wird 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 mehrere SPAN-Sitzungen gleichzeitig stattfinden.

Weitere Informationen finden Sie in den Abschnitten Mehrere gleichzeitige Sitzungen erstellen sowie Funktionsübersicht und -einschränkungen dieses Dokuments.

Fehler "% Limit für lokale Sitzung überschritten"

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

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

Supervisor Engines unterliegen einer Beschränkung von SPAN-Sitzungen. Weitere Informationen finden Sie im Abschnitt *Local SPAN, RSPAN, and ERSPAN Session Limits* (*Lokale SPAN-, RSPAN- und ERSPAN-Sitzungslimits*) unter Configuring Local SPAN, RSPAN, and ERSPAN (Konfigurieren von lokalem SPAN, RSPAN und ERSPAN).

Eine SPAN-Sitzung auf dem VPN-Servicemodul kann nicht gelöscht werden. Fehler: "% Session [Session No:] Used by Service Module"

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-Servicemodul erstellte SPAN-Sitzung

zu löschen:

<#root>

```
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?

Beschädigte Pakete können mit SPAN aufgrund der allgemeinen Funktionsweise der Switches nicht erfasst werden. Wenn ein Paket einen Switch durchläuft, treten die folgenden Ereignisse auf:

1. Das Paket erreicht den Eingangsport.
2. Das Paket wird in mindestens einem Puffer gespeichert.
3. Das Paket wird schließlich am Ausgangs-Port erneut übertragen.

Wenn der Switch ein beschädigtes Paket empfängt, verwirft der Eingangsport das Paket in der Regel. Daher wird das Paket am Ausgangsport nicht angezeigt.

Ein Switch ist hinsichtlich der Erfassung des Datenverkehrs nicht vollständig transparent.

Wenn Sie ein beschädigtes Paket in Ihrem Sniffer im Szenario in diesem Abschnitt sehen, wissen Sie ebenfalls, dass die Fehler in Schritt 3 im Ausgangssegment generiert wurden.

Wenn Sie der Meinung sind, dass ein Gerät beschädigte Pakete sendet, können Sie den sendenden Host und das Sniffer-Gerät auf einem Hub platzieren. 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 vom Dienstmodul verwendet

Wenn beispielsweise ein Firewall Service Module (FWSM) installiert und später aus dem CAT6500 entfernt wurde, wurde automatisch die **SPAN-Reflektorfunktion** aktiviert.

Die SPAN-Reflektorfunktion verwendet eine SPAN-Sitzung im Switch.

Wenn Sie dies nicht mehr benötigen, müssen Sie den Befehl **no monitor session service module** im Konfigurationsmodus von CAT6500 eingeben können und dann sofort die neue gewünschte SPAN-Konfiguration eingeben.

Reflektor-Port verwirft Pakete

Ein Reflektor-Port empfängt Kopien des gesendeten und empfangenen Datenverkehrs für alle überwachten Quellports. Wenn ein Reflektor-Port überbelegt ist, kann es zu Überlastungen kommen.

Dies kann die Weiterleitung des Datenverkehrs an einen oder mehrere Quellports beeinträchtigen.

Wenn die Bandbreite des Reflektor-Ports nicht für das Datenverkehrsvolumen der entsprechenden Quell-Ports ausreicht, werden die überschüssigen Pakete verworfen.

Ein 10/100-Port reflektiert bei 100 Mbit/s. Ein Gigabit-Port reflektiert mit 1 Gbit/s.

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

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

<#root>

```
Cat6K#
```

```
show monitor
```

```
Session 1
---------
Type : Service Module Session
```

Wenn sich ein Firewall-Blade im Catalyst 6500-Chassis befindet, wird diese Sitzung automatisch installiert, um die Hardware-Multicast-Replikation zu unterstützen, da ein FWSM keine Multicast-Streams replizieren kann.

Wenn Multicast-Streams, die von FWSM generiert werden, auf Layer 3 auf mehrere Linecards repliziert werden müssen, kopiert die automatische Sitzung den Datenverkehr über einen Fabric-Channel an den Supervisor.

Wenn Sie eine Multicast-Quelle haben, die einen Multicast-Stream hinter dem FWSM generiert, benötigen Sie den SPAN-Reflektor.

Wenn Sie die Multicast-Quelle in das externe VLAN platzieren, ist der SPAN-Reflektor nicht erforderlich. Der SPAN-Reflektor ist nicht mit Bridging-BPDUs über FWSM kompatibel.

Sie können den Befehl **no monitor session service module** verwenden, um den SPAN-Reflektor zu deaktivieren.

Können eine 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 funktionieren?

Ja. Eine RSPAN-Sitzung kann über verschiedene VTP-Domänen hinweg stattfinden. Stellen Sie jedoch sicher, dass das RSPAN-VLAN in den Datenbanken dieser VTP-Domänen vorhanden ist.

Stellen Sie außerdem sicher, dass im Pfad von Sitzungsquelle zu Sitzungsziel kein Layer-3-Gerät vorhanden ist.

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

Nein. Die RSPAN-Sitzung kann kein Layer-3-Gerät durchlaufen, da es sich bei dem RSPAN um eine LAN-Funktion (Layer 2) handelt.

Um den Datenverkehr über ein WAN oder verschiedene Netzwerke zu überwachen, verwenden Sie Encapsulated Remote SwitchPort Analyzer (ERSPAN).

Die ERSPAN-Funktion unterstützt Quell-Ports, 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, ERSPAN GRE-gekapseltem Datenverkehr und einer ERSPAN-Zielsitzung.

Sie können die ERSPAN-Quell- und -Zielsitzungen auf verschiedenen Switches separat konfigurieren.

Derzeit wird die ERSPAN-Funktion in folgenden Bereichen unterstützt:

- Supervisor 720 mit PFC3B oder PFC3BXL mit Cisco IOS Software, Version 12.2(18)SXE oder höher
- Supervisor 720 mit PFC3A mit Hardware-Version 3.2 oder höher und Cisco IOS Software-Version 12.2(18)SXE oder höher

Weitere Informationen zu ERSPAN finden Sie im Configuring Local SPAN, Remote SPAN (RSPAN) und Encapsulated RSPAN - Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX.

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

Nein. RSPAN funktioniert nicht, wenn sich die RSPAN-Quell- 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, überträgt der Zielport der RSPAN-Zielsitzung die erfassten Pakete der RSPAN-Quellsitzung aufgrund von Hardwarebeschränkungen nicht. Dies wird von den Switches der Serien 4500 und 3750 nicht unterstützt.

Dieses Problem ist dokumentiert in Cisco Bug-ID CSCeg08870 (nur registrierte Kunden) .

Hier 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 besteht in der Verwendung des regulären SPAN.

Das mit dem SPAN-Zielport verbundene Netzwerkanalyse-/Sicherheitsgerät ist nicht erreichbar.

Das grundlegende Merkmal eines SPAN-Ziel-Ports besteht darin, dass er außer dem für die SPAN-Sitzung erforderlichen Datenverkehr keinen Datenverkehr überträgt.

Wenn Sie das Netzwerkanalyse-/Sicherheitsgerät über den SPAN-Zielport erreichen (IP-Erreichbarkeit) müssen Sie die Weiterleitung des eingehenden Datenverkehrs aktivieren.

Wenn der Eingang aktiviert ist, akzeptiert der SPAN-Zielport eingehende Pakete, die je nach angegebenem Kapselungsmodus markiert werden können, und schaltet sie normal um.

Wenn Sie einen SPAN-Zielport konfigurieren, können Sie angeben, ob die Eingangsfunktion aktiviert ist und welches VLAN zum Umschalten nicht markierter Eingangspakete verwendet werden soll.

Die Angabe eines Eingangs-VLAN ist bei der Konfiguration der ISL-Kapselung nicht erforderlich, da alle ISL-gekapselten Pakete VLAN-Tags aufweisen.

Obwohl der Port STP Forwarding ist, ist er nicht Teil des STP. Verwenden Sie daher bei der Konfiguration dieser Funktion Vorsicht, damit im Netzwerk keine Spanning-Tree-Schleife eingeführt wird.

Wenn auf einem SPAN-Zielport sowohl eine Eingangs- als auch eine Trunk-Kapselung angegeben wird, geht der Port in allen aktiven VLANs zur Weiterleitung über.

Die Konfiguration eines nicht vorhandenen VLANs als Eingangs-VLAN ist nicht zulässig.

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

In diesem Beispiel wird gezeigt, wie ein Zielport mit 802.1q-Kapselung und Eingangspaketen unter Verwendung des nativen VLAN 7 konfiguriert wird.

<#root>

```
Switch(config)#

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

Bei dieser Konfiguration wird der Datenverkehr von SPAN-Quellen für Sitzung 1 aus der Fast Ethernet 5/48-Schnittstelle mit 802.1q-Kapselung kopiert.

Eingehender Datenverkehr wird akzeptiert und weitergeleitet, wobei Pakete ohne Tags in VLAN 7 klassifiziert werden.

Zugehörige Informationen

- **Konfigurieren von SPAN und RSPAN auf Cisco Catalyst 4500 Switches mit Cisco IOS Software**
- **Ein SPAN-Zielport wird als "nicht verbunden" angezeigt und kommuniziert nicht mit dem Rest des Netzwerks.**
- **Produkt-Support für Switches**

- **Support für LAN-Switching-Technologie**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.