Catalyst Switched Port Analyzer (SPAN) Configuratievoorbeeld

Inhoud

Inleiding

In dit document worden de recente functies van de Switched Port Analyzer (SPAN) beschreven

die zijn geïmplementeerd. De SPAN optie, die soms port mirroring of port monitoring wordt genoemd, selecteert netwerkverkeer voor analyse door een netwerkanalyzer. De netwerkanalyzer kan een Cisco SwitchProbe-apparaat of een andere RMON-test (Remote Monitoring) zijn. Eerder was SPAN een relatief basisoptie op de Cisco Catalyst Series-switches. Maar de jongste releases van Catalyst OS (CatOS) heeft grote verbeteringen geïntroduceerd en veel nieuwe mogelijkheden die nu beschikbaar zijn voor de gebruiker. Dit document is niet bedoeld als een alternatieve configuratiehandleiding voor de SPAN-functie. Dit document beantwoordt de meest voorkomende vragen over SPAN, zoals:

- Wat is SPAN en hoe stel je het in?
- Welke functies zijn er beschikbaar (in het bijzonder meerdere, gelijktijdige SPAN-sessies) en welk softwareniveau is er nodig om deze functies te kunnen uitvoeren?
- beïnvloedt SPAN de wisselprestaties?

Voorwaarden

Catalyst-switches die SPAN, RSPAN en ERSPAN ondersteunen

Catalyst-switches	SPAN-ondersteuning	RSPAN-ondersteuning	Ondersteuning van ERSPAN
Catalyst Express versie 500/520 Series	Ja	Nee	Nee
Catalyst 6500/6000 Series-switches	Ja	Ja	Ja supervisor 2T met PFC4, Supervisor 720 met PFC3B of PFC3BXL die Cisco IOS-softwarerelease 12.2(18)SXE of hoger uitvoeren. Supervisor 720 met PFC3A dat hardwareversie 3.2 of hoger heeft en Cisco IOS-softwarerelease 12.2(18)SXE of hoger heeft
Catalyst 5500/5000 Series switch	Ja	Nee	Nee
Catalyst 4900 Series-switches	Ja	Ja	Nee
Catalyst 4500/4000 Series (inclusief 4912G)	Ja	Ja	Nee
Catalyst 3750 Metro Series-switches	Ja	Ja	Nee
Catalyst 3750/3750E/3750X Series-switches	Ja	Ja	Nee
Catalyst 3560/3560E/3650X Series-switches	Ja	Ja	Nee
Catalyst 3550 Series-switches	Ja	Ja	Nee
Catalyst 3500XL	Ja	Nee	Nee

Series switch			
Catalyst 2970 Series-switches	Ja	Ja	Nee
Catalyst 2960 Series-switches	Ja	Ja	Nee
Catalyst 2955 Series switches	Ja	Ja	Nee
Catalyst 2950 Series switches	Ja	Ja	Nee
Catalyst 2940 Series switches	Ja	Nee	Nee
Catalyst 2948G-L3	Nee	Nee	Nee
Catalyst 2948G-L2, 2948G-1 GE-TX, 2980G-A switch	Ja	Ja	Nee
Catalyst 2900XL Series switch	Ja	Nee	Nee
Catalyst 1900 Series switches	Ja	Nee	Nee

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Deze informatie in dit document gebruikt CatOS 5.5 als referentie voor Catalyst 4500/4000, 5500/5000 en 6500/6000 Series-switches. Op de Catalyst 2900XL/3500XL Series-switches wordt Cisco IOS-softwarerelease 12.0(5)XU gebruikt. Hoewel dit document wordt bijgewerkt om de veranderingen in de SPAN weer te geven, raadpleegt u de opmerkingen van de documentatie van het switchplatform voor de laatste ontwikkelingen in de SPAN-functie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

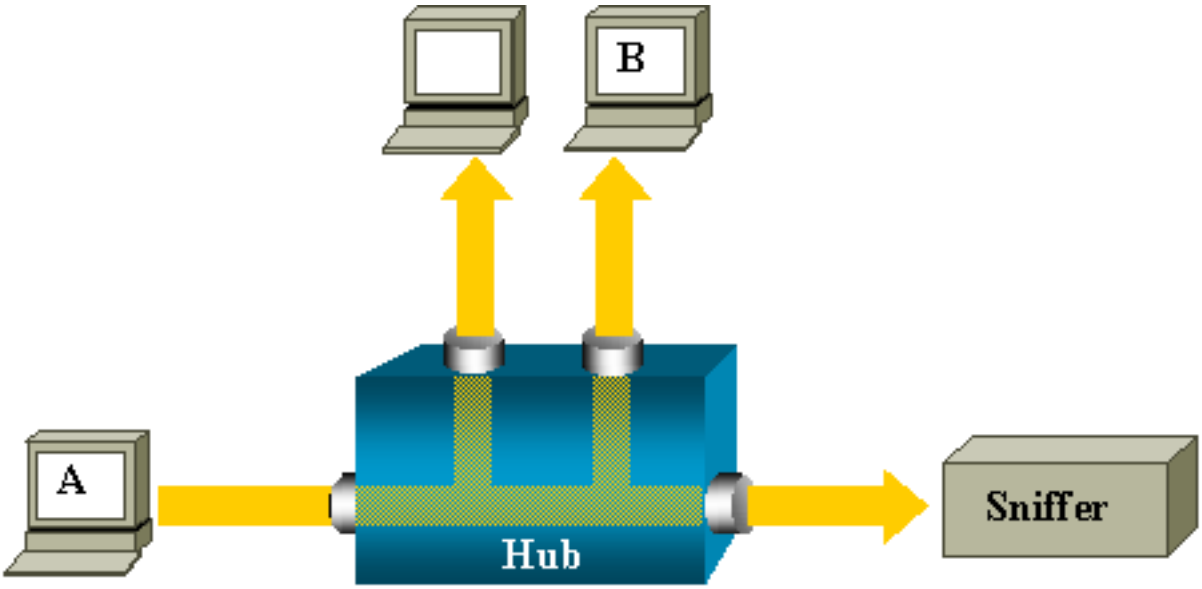
Achtergrondinformatie

Korte beschrijving van de SPAN

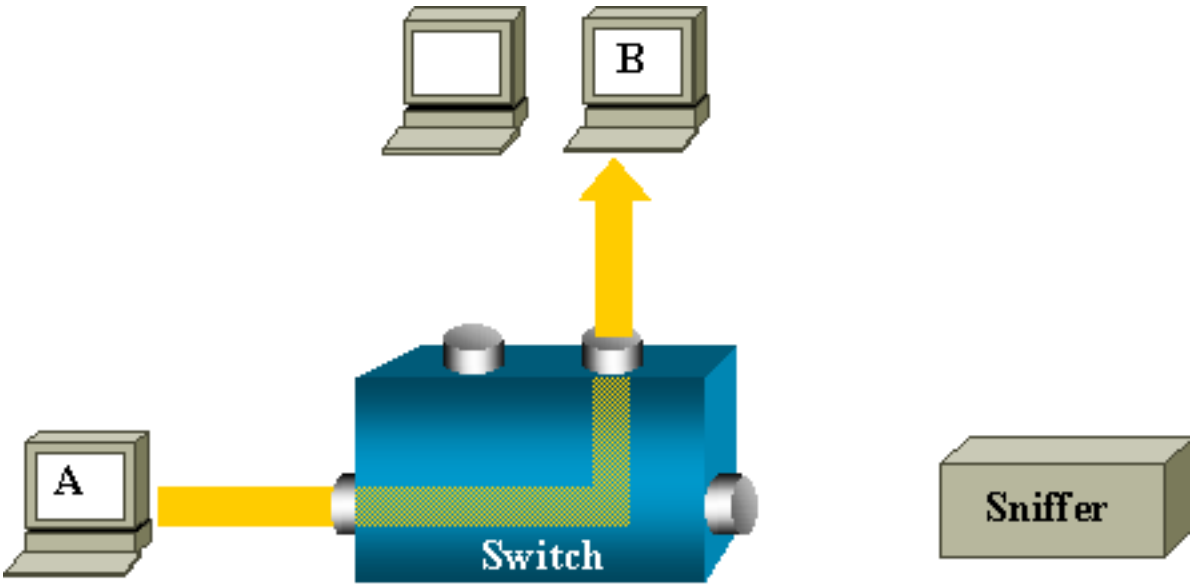
Wat is SPAN en waarom is SPAN nodig? De SPAN optie werd op switches geïntroduceerd vanwege een fundamenteel verschil dat de switches met hubs hebben. Wanneer een hub een pakket op één poort ontvangt, verstuurt de hub een kopie van dat pakket op alle poorten behalve op de poort waar de hub het pakket heeft ontvangen. Na een schakelaar boots, begint het om een Layer 2 die tabel op basis van het bron MAC adres van de verschillende pakketten op te bouwen die de schakelaar ontvangt. Nadat deze verzendtabel is gebouwd, zendt de schakelaar verkeer door dat voor een MAC-adres rechtstreeks naar de corresponderende poort is bestemd.

Bijvoorbeeld, als u Ethernet verkeer wilt vangen dat door host A wordt verzonden om B te

ontvangen, en beiden worden aangesloten op een hub, voeg gewoon een sluipschutter aan deze hub toe. Alle andere poorten zien het verkeer tussen hosts A en B:



Op een switch, nadat het host B MAC-adres is geleerd, wordt het eenastverkeer van A naar B alleen naar de B-poort verzonden. Daarom ziet de sluipschutter dit verkeer niet:

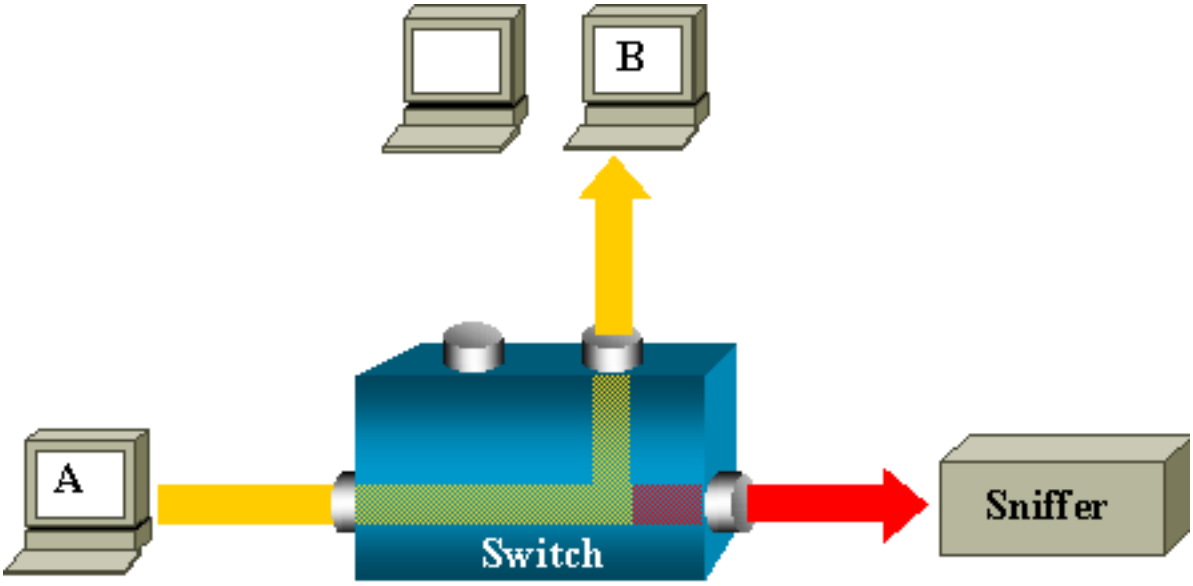


In deze configuratie neemt de sluipschutter alleen verkeer op dat naar alle poorten overstroomt, zoals:

- Breedbandverkeer
- Multicastverkeer met CGMP of Internet Group Management Protocol (IGMP)-snooping uitgeschakeld
- Onbekend eenastverkeer

Unicast overspoelen gebeurt wanneer de schakelaar niet de bestemming MAC in zijn content-adresseerbare geheugen (CAM) tabel heeft. De schakelaar weet niet waar om het verkeer te verzenden. De schakelaar overspoelt de pakketten aan alle havens in het bestemmingsVLAN.

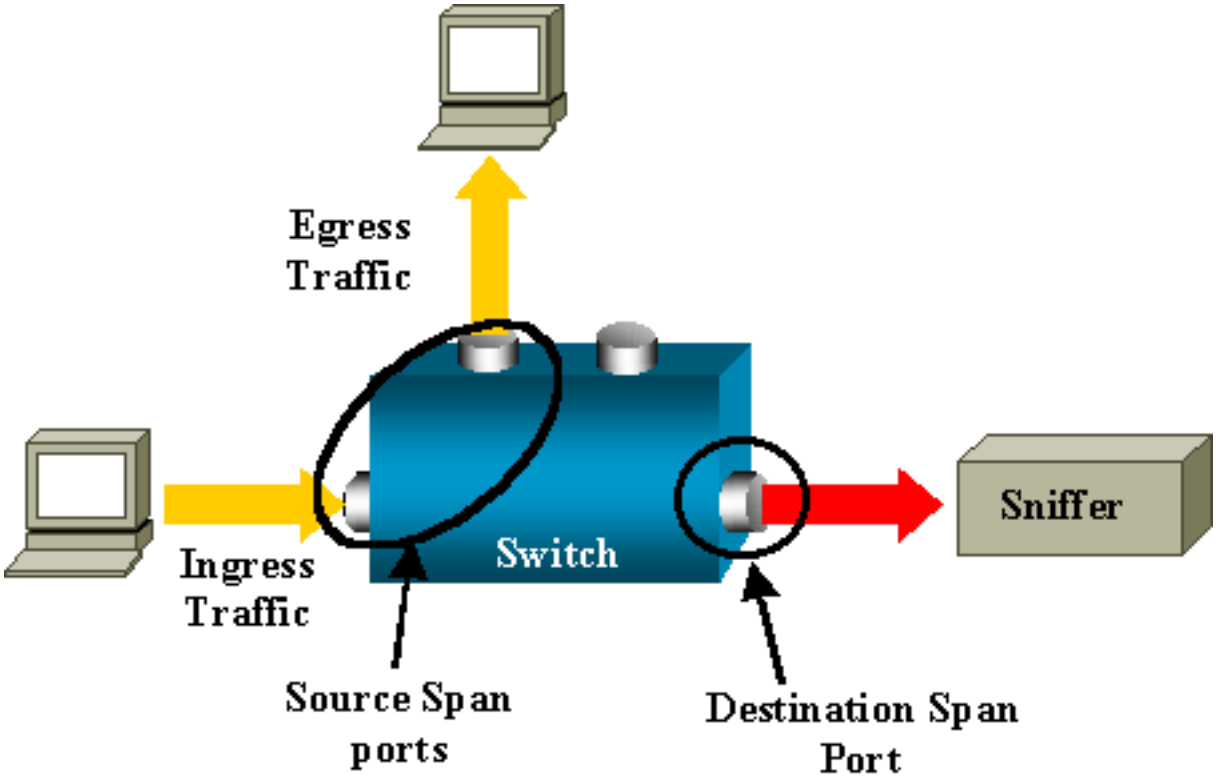
Een extra optie is nodig die kunstmatig eenastpakketten kopieert die A naar de sluippoort sturen:



In dit diagram wordt de sluipschutter aan een haven bevestigd die wordt gevormd om een exemplaar van elk pakket te ontvangen dat A ontvangt. Deze haven wordt een haven van SPAN genoemd. De andere secties van dit document beschrijven hoe u deze optie zeer nauwkeurig kunt aanpassen om meer te doen dan slechts een haven te controleren.

SPAN-terminologie

- **Ingang verkeer**—verkeer dat de schakelaar ingaat.
- **Druk verkeer**—verkeer dat de schakelaar verlaat.
- **Bron (SPAN) poort**-A poort die met gebruik van de SPAN optie wordt gecontroleerd.
- **Bron (SPAN) VLAN**-A VLAN waarvan het verkeer met gebruik van de SPAN optie wordt gecontroleerd.
- **Destination (SPAN) poort**-A poort die bronpoorten controleert, gewoonlijk waar een netwerkanalyzer wordt aangesloten.
- **Verwijs poort**-A poort die pakketten op een RSPAN VLAN kopieert.
- **Monitorpoort**-A is ook een bestemmingspoorts van SPAN in Catalyst 2900XL/3500XL/2950 terminologie.



- **Lokale SPAN**-de SPAN optie is lokaal wanneer de gecontroleerde poorten zich allemaal op dezelfde schakelaar bevinden als de doelpoort. Deze optie contrasteert met Remote SPAN (RSPAN), die ook in deze lijst wordt gedefinieerd.
- **Remote SPAN (RSPAN)** - Sommige bronpoorten bevinden zich niet op dezelfde switch als de doelpoort. RSPAN is een geavanceerde optie die een speciaal VLAN vereist om het verkeer te dragen dat door SPAN tussen switches wordt gecontroleerd. RSPAN wordt niet op alle switches ondersteund. Controleer de respectievelijke opmerkingen en configuratiehandleiding om te zien of u RSPAN kunt gebruiken in de schakelaar die u implementeert.
- **Port-Based SPAN (PSPAN)**-De gebruiker specificeert één of meer bronpoorten op de switch en één doelpoort.
- **VLAN-gebaseerde SPAN (VSPAN)**-Op een bepaalde switch kan de gebruiker ervoor kiezen om alle poorten te controleren die aan een bepaald VLAN behoren in één opdracht.
- **ESPAN**: dit betekent een verbeterde SPAN-versie. Deze term is tijdens de evolutie van de SPAN meerdere malen gebruikt om extra kenmerken te noemen. De term is dan ook niet erg duidelijk. Het gebruik van deze term wordt in dit document vermeden.
- **Administratieve bron**-Een lijst van bronpoorten of VLAN's die zijn geconfigureerd om te worden gevolgd.
- **Operationele bron**: een lijst met poorten die effectief worden gemonitord. Deze lijst van havens kan verschillen van de administratieve bron. Een poort die in shutdown modus is, kan bijvoorbeeld in de administratieve bron verschijnen maar wordt niet effectief gemonitord.

Kenmerken van bronpoort

Een bronpoort, ook genoemd een gecontroleerde haven, is een geschakeld of routed haven die u voor de analyse van het netwerkverkeer controleert. In één lokale SPAN-sessie of RSPAN-bronsessie kunt u bronpoortverkeer controleren, zoals ontvangen (RX), verzonden (TX) of bidirectioneel (beide). De switch ondersteunt elk aantal bronpoorten (tot het maximale aantal beschikbare poorten op de switch) en elk aantal Bron-VLAN's.

Een bronpoort heeft deze kenmerken:

- Het kan elk poorttype zijn, zoals EtherChannel, Fast Ethernet, Gigabit Ethernet, enzovoort.
- Het kan tijdens meerdere SPAN-sessies worden gevolgd.
- Het kan geen doelpoort zijn.
- Elke bronpoort kan worden geconfigureerd met een monitor (ingang, uitgang of beide). Voor EtherChannel-bronnen is de bewaakte richting van toepassing op alle fysieke poorten in de groep.
- Bronpoorten kunnen in hetzelfde of verschillende VLAN's zijn.
- Voor VLAN SPAN-bronnen zijn alle actieve poorten in de bron-VLAN's als bronpoorten opgenomen.

VLAN-filtering

Wanneer u een boomstampoort als bronpoort controleert, worden alle VLANs die op de boomstam actief zijn door standaard gecontroleerd. U kunt VLAN-filtering gebruiken om SPAN-verkeerscontrole op boombronpoorten te beperken tot specifieke VLAN's.

- VLAN-filtering is alleen van toepassing op boompoorten of op spraak-VLAN-poorten.
- VLAN-filtering is alleen van toepassing op poortgebaseerde sessies en is niet toegestaan in sessies met VLAN-bronnen.
- Wanneer een VLAN filterlijst wordt gespecificeerd, worden slechts die VLANs in de lijst gecontroleerd op boomstampoorten of op de toegangspakketten van spraak VLAN.
- SPAN-verkeer dat afkomstig is van andere poorttypen wordt niet beïnvloed door VLAN-filtering, wat betekent dat alle VLAN's op andere poorten zijn toegestaan.
- VLAN-filtering heeft alleen gevolgen voor verkeer dat naar de doelpoort van SPAN wordt doorgestuurd en heeft geen invloed op de switching van normaal verkeer.
- U kunt bronVLAN's en VLAN's niet binnen een sessie combineren. U kunt bron VLAN's of filter VLAN's hebben, maar niet beide tegelijkertijd.

Kenmerken van Bron-VLAN

VSPAN is de bewaking van het netwerkverkeer in een of meer VLAN's. De SPAN of RSPAN bron interface in VSPAN is een VLAN-id en het verkeer wordt op alle poorten voor dat VLAN gecontroleerd.

VSPAN heeft deze kenmerken:

- Alle actieve poorten in de bron-VLAN worden als bronpoorten meegeleverd en kunnen in beide of beide richtingen worden gevolgd.
- Op een bepaalde poort wordt alleen verkeer op het gecontroleerde VLAN naar de doelpoort verzonden.
- Als een doelpoort tot een bron-VLAN behoort, wordt deze van de bronlijst uitgesloten en wordt deze niet gevolgd.
- Als poorten aan de bron VLAN's worden toegevoegd of verwijderd, wordt het verkeer op de bron VLAN dat door deze poorten wordt ontvangen toegevoegd of verwijderd uit de bronnen die worden gecontroleerd.
- U kunt geen filter VLAN's in dezelfde sessie met VLAN-bronnen gebruiken.
- U kunt alleen Ethernet VLAN's controleren.

Kenmerken van de haven van bestemming

Elke lokale SPAN-sessie of RSPAN-doelsessie moet een doelpoort hebben (ook een monitoringpoort genoemd) die een kopie van verkeer van de bronpoorten en VLAN's ontvangt.

Een haven van bestemming heeft deze kenmerken:

- Een doelpoort moet op dezelfde schakelaar als de bronpoort staan (voor een lokale SPAN-sessie).
- Een doelpoort kan elke Ethernet fysieke poort zijn.
- Een doelpoort kan slechts aan één SPAN-sessie tegelijk deelnemen. Een doelpoort in één SPAN-sessie kan geen doelpoort zijn voor een tweede SPAN-sessie.
- Een doelpoort kan geen bronpoort zijn.
- Een doelpoort kan geen EtherChannel-groep zijn.Opmerking: Cisco IOS-softwarerelease 12.2(33)SXH en hoger, kan PortChannel-interface een doelpoort zijn. Destination EtherChannel biedt geen ondersteuning voor de Port Aggregation Control Protocol (PAgP) of Link Aggregation Control Protocol (LACP) EtherChannel-protocollen; alleen de on-modus wordt ondersteund, waarbij alle EtherChannel-protocolondersteuning uitgeschakeld is.Opmerking: Raadpleeg de plaatselijke SPAN-, RSPAN- en ERSPAN-bestemmingen voor meer informatie.
- Een doelpoort kan een fysieke poort zijn die aan een EtherChannel-groep is toegewezen, zelfs als de EtherChannel-groep is gespecificeerd als een SPAN-bron. De poort wordt uit de groep verwijderd terwijl het als een SPAN-doelpoort is ingesteld.
- De poort geeft geen verkeer uit behalve dat verkeer dat vereist is voor de SPAN-sessie tenzij leren is ingeschakeld. Als het leren is ingeschakeld, geeft de poort ook verkeer door dat wordt gericht naar hosts die zijn geleerd op de doelpoort.Opmerking: Raadpleeg de plaatselijke SPAN-, RSPAN- en ERSPAN-bestemmingen voor meer informatie.
- De staat van de bestemmingspoort is omhoog/omlaag door ontwerp. De interface toont de haven in deze staat om duidelijk te maken dat de haven momenteel niet als productiehaven kan worden gebruikt.
- Als het doorsturen van verkeer van de ingangsweg voor een apparaat van de netwerkveiligheid wordt toegelaten. De doelpoort wijst verkeer op Layer 2 door.
- Een doelpoort neemt niet deel aan het overspannen van boom terwijl de SPAN-sessie actief is.
- Wanneer het een doelpoort is, neemt het niet deel aan een van de Layer 2 protocollen (STP, VTP, CDP, DTP, PagP).
- Een doelpoort die tot een bron-VLAN van een SPAN-sessie behoort, wordt niet in de bronlijst opgenomen en wordt niet gevolgd.
- Een doelhaven ontvangt exemplaren van verzonden en ontvangen verkeer voor alle gecontroleerde bronhavens. Als een doelpoort wordt oversubscript, kan deze verstopt raken. Deze congestie kan het doorsturen van verkeer op een of meer bronpoorten beïnvloeden.

Kenmerken van de reflectiepoort

De reflectorpoort is het mechanisme dat pakketten op een RSPAN VLAN kopieert. De reflectorpoort geeft alleen het verkeer door van de RSPAN-bronsessie waarmee het verbonden is. Elk apparaat dat is aangesloten op een poort dat is ingesteld als reflectorpoort verliest connectiviteit tot de RSPAN bronsessie is uitgeschakeld.

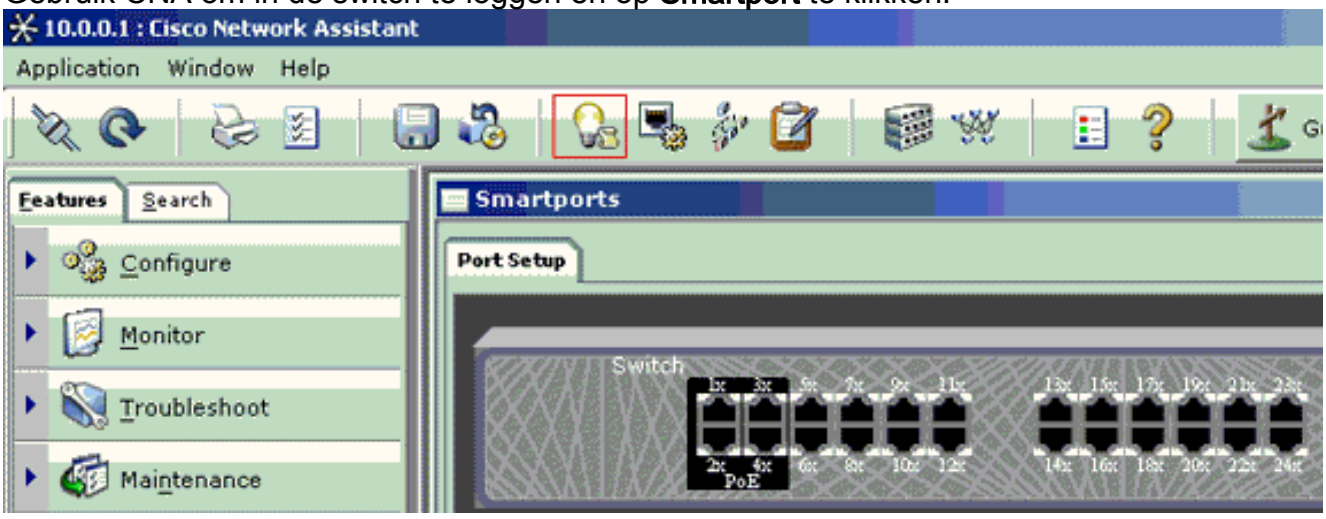
De reflectorpoort heeft deze kenmerken:

- Het is een haven die op loopback is ingesteld.
- Het kan geen EtherChannel-groep zijn, de stam niet en het kan geen protocol filteren.
- Het kan een fysieke poort zijn die aan een EtherChannel-groep wordt toegewezen, zelfs als de EtherChannel-groep als SPAN-bron wordt gespecificeerd. De poort wordt uit de groep verwijderd terwijl deze als reflectorpoort is geconfigureerd.
- Een poort die wordt gebruikt als reflectorpoort kan geen SPAN-bron of doelhaven zijn, en een haven kan geen reflectorhaven voor meer dan één sessie tegelijkertijd zijn.
- Het is onzichtbaar voor alle VLAN's.
- Het inheemse VLAN voor looped-back verkeer op een reflectorhaven is RSPAN VLAN.
- De reflector poort loopt terug untagged verkeer naar de schakelaar. Het verkeer wordt dan op RSPAN VLAN geplaatst en overstroomd naar om het even welke boomhavens die RSPAN VLAN dragen.
- Spanning Tree wordt automatisch uitgeschakeld op een reflectorpoort.
- Een reflectorpoort ontvangt exemplaren van verzonden en ontvangen verkeer voor alle gecontroleerde bronhavens.

SPAN op Catalyst Express versie 500/520

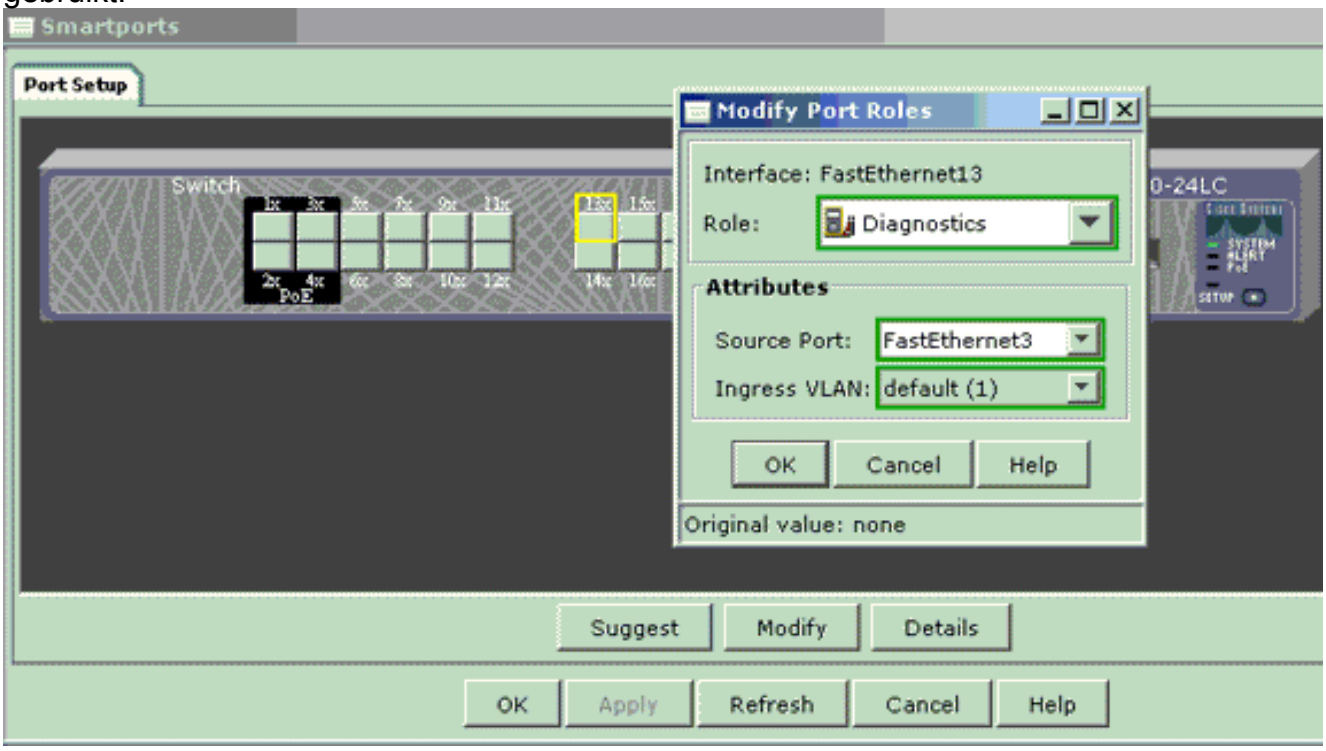
Catalyst Express 5000 of Catalyst Express 520 ondersteunt alleen de SPAN-functie. Catalyst Express 500/520 poorten kunnen alleen voor SPAN worden geconfigureerd met behulp van Cisco Network Assistant (CNA). Volg deze stappen om de SPAN te configureren:

1. Download en installeer CNA op de PC. U kunt CNA downloaden van de pagina Download Software (alleen geregistreerde klanten).
2. Volg de stappen die zijn gezet in het aan de slag gaan met de Guide voor Catalyst Express 500 switches 12.2(25)FY om de switching-instellingen voor Catalyst Express 500 aan te passen. Raadpleeg de Introductiegids voor de Catalyst Express 520 switches voor meer informatie over Catalyst Express 520.
3. Gebruik CNA om in de switch te loggen en op **Smartport** te klikken.



4. Klik op een willekeurige interface waar u de pc wilt aansluiten om de sporen van de sluipschutter op te nemen.
5. Klik op **Wijzigen**. Er verschijnt een kleine pop-up box.
6. Kies de rol **Diagnostiek** voor de poort.
7. Kies de bronpoort en selecteer het VLAN dat u wilt bewaken. Als u geen selecteert, ontvangt

de poort alleen verkeer. Met het Ingrress VLAN kunt de PC die is aangesloten op de Diagnostics-poort gebruiken om pakketten naar het netwerk te verzenden dat VLAN gebruikt.



8. Klik op **OK** om het pop-upvenster te sluiten.
9. Klik op **OK** en **pas** de instellingen **toe**.
10. U kunt Sniffer-software gebruiken om het verkeer te traceren zodra u de diagnostische poort hebt ingesteld.

SPAN op Catalyst 2900XL/3500XL switches

Beschikbare functies en beperkingen

De port monitoring optie is niet erg uitgebreid op Catalyst 2900XL/3500XL. Daarom is deze optie vrij gemakkelijk te begrijpen.

U kunt zoveel lokale PSPAN-sessies maken als nodig. U kunt bijvoorbeeld PSPAN-sessies maken op de configuratiepoort die u als een bestemming-SPAN-poort hebt gekozen. Geef in dit geval de opdracht interface op om een lijst te maken van de bronpoorten die u wilt controleren. Een monitorpoort is een bestemmingSPAN poort in Catalyst 2900XL/3500XL terminologie.

- De belangrijkste beperking is dat alle poorten die betrekking hebben op een bepaalde sessie (of bron of bestemming) tot hetzelfde VLAN moeten behoren.
- Als u de VLAN-interface met een IP-adres configureren controleert de opdracht de **poortmonitor** alleen verkeer dat is bestemd voor dat IP-adres. Het monitort ook het uitzendverkeer dat door de interface van VLAN wordt ontvangen. Maar het vat niet het verkeer op dat in het eigenlijke VLAN zelf stroomt. Als u geen interface in de opdracht **van de havenmonitor** specificeert, worden alle andere poorten die tot hetzelfde VLAN behoren als de interface gecontroleerd.

Deze lijst bevat een aantal beperkingen. Raadpleeg de opdracht verwijzingsgids (Catalyst 2900XL/3500XL) voor meer informatie.

Opmerking: ATM-poorten zijn de enige poorten die geen monitorpoorten kunnen zijn. U kunt echter ATM-poorten bewaken. De beperkingen in deze lijst zijn van toepassing op havens die over de havenbewakingsfunctie beschikken.

- Een monitorpoort kan niet in een Fast EtherChannel of Gigabit EtherChannel poortgroep zijn.
- Een monitor poort kan niet worden ingeschakeld voor poortbeveiliging.
- Een monitorpoort kan geen multi-VLAN poort zijn.
- Een monitor poort moet lid zijn van hetzelfde VLAN als de poort die wordt bewaakt. VLAN-lidmaatschapswijzigingen zijn niet toegestaan op monitoringpoorten en poorten die worden gevolgd.
- Een monitor poort kan geen dynamische toegangspoort zijn of een boomstampoort. Maar een statische-toegangspoort kan een VLAN op een stam, een multi-VLAN, of een dynamische-toegangspoort controleren. Het VLAN dat wordt gecontroleerd is degene die met de statische toegangpoort wordt geassocieerd.
- Poortbewaking werkt niet als zowel de monitorpoort als de haven die wordt bewaakt beschermde havens zijn.

Zorg ervoor dat een poort in de monitor staat niet het Spanning Tree Protocol (STP) uitvoert terwijl de poort nog tot VLAN van de poorten behoort die door deze poort worden spiegeld. De poortmonitor kan deel uitmaken van een lus als u deze bijvoorbeeld aansluit op een hub of een brug en een lus naar een ander deel van het netwerk. In dit geval kunt u eindigen in een catastrofale overbruggingslus omdat STP u niet langer beschermt. Zie de reden waarom de SPAN-sessie een overbruggingslening creëert? deel van dit document, bijvoorbeeld over hoe deze toestand kan gebeuren.

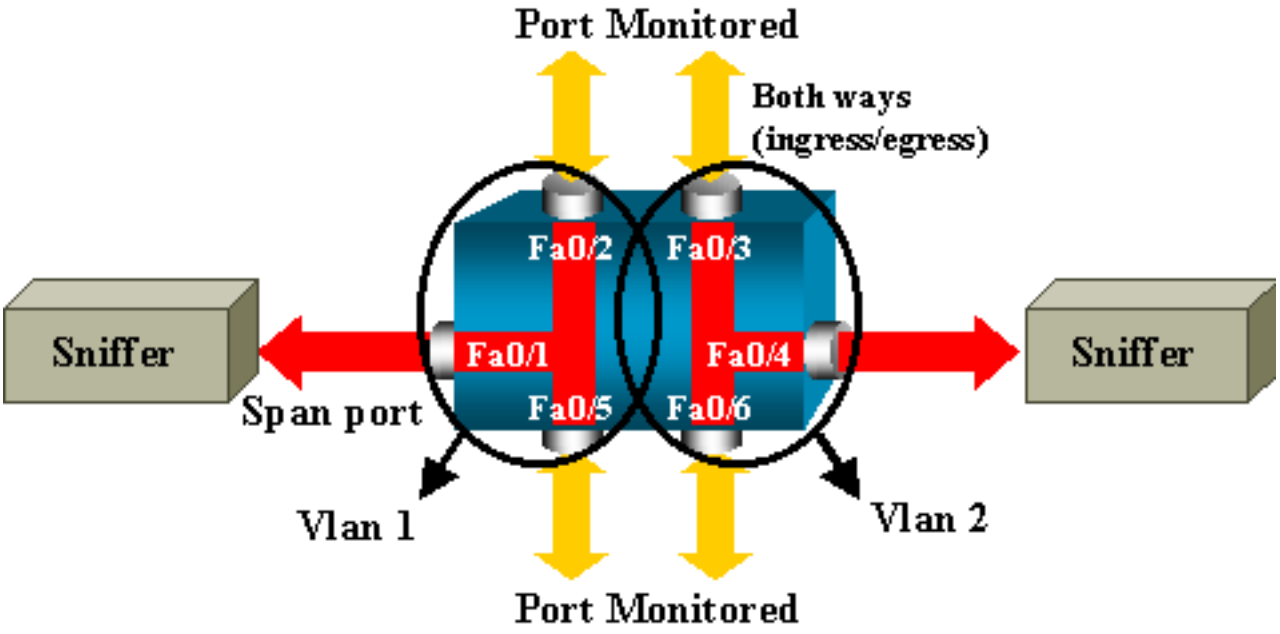
Configuratievoorbeeld

Dit voorbeeld maakt twee gelijktijdige SPAN sessies.

- Port Fast Ethernet 0/1 (Fast Ethernet 0/1) controleert verkeer dat poorten Fa0/2 en Fa0/5 verzenden en ontvangen. Port Fa0/1 controleert ook verkeer naar en van de beheerinterface VLAN 1.
- Port Fa0/4-monitoren poorten Fa0/3 en Fa0/6.

poorten Fa0/3, Fa0/4 en Fa0/6 worden allemaal geconfigureerd in VLAN 2. Andere poorten en de beheerinterface worden geconfigureerd in het standaard VLAN 1.

Netwerkdiagram



Monsterconfiguratie op Catalyst 2900XL/3500XL

2900XL/3500XL SPAN-voorbeeldconfiguratie

```
!--- 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.
```

Configuratiescherm

Om poort Fa0/1 als een doelpoort te configureren selecteert u de bronpoorten Fa0/2 en Fa0/5 en de beheerinterface (VLAN 1), vervolgens selecteert u de interface Fa0/1 in de configuratiemodus:

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

Geef de lijst op van te controleren poorten:

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

Met deze opdracht wordt elk pakje dat deze twee poorten ontvangen of verzenden ook gekopieerd naar poort Fa0/1. Geef een variatie van de opdracht **poortmonitor** uit om de controle voor de administratieve interface te configureren:

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

> Opmerking: Deze opdracht betekent niet dat port Fa0/1 het volledige VLAN 1 controleert. Het **VLAN 1** sleutelwoord verwijst eenvoudig naar de administratieve interface van de schakelaar.

Dit voorbeeldopdracht illustreert dat de monitor van een poort in een verschillend VLAN onmogelijk is:

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

Configureer een andere sessie om de configuratie te voltooien. Gebruik Fa0/4 nu als een bestemming-SPAN-poort:

```
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
```

Geef een **show run-**opdracht op of gebruik de **opdracht show port monitor** om de configuratie te controleren:

```
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
```

> Opmerking: Catalyst 2900XL en 3500XL ondersteunen geen SPAN in de Rx-richting alleen (Rx SPAN of ingress SPAN) of alleen in de Tx-richting (Tx SPAN of egress SPAN). Alle SPAN-poorten zijn ontworpen om zowel Rx- als Tx-verkeer op te nemen.

SPAN op Catalyst 2948G-L3 en 4908G-L3

Catalyst 2948G-L3 en Catalyst 4908G-L3 zijn vaste configuratieswitchrouters of Layer 3-switches.

De SPAN-functie op een Layer 3-schakelaar wordt poortsnooping genoemd. Maar poortsnooping wordt niet op deze switches ondersteund. Raadpleeg het gedeelte *Functies Niet-ondersteunde* onderdelen van de Releaseopmerkingen van document voor Catalyst 2948G-L3 en Catalyst 4908G-L3 voor Cisco IOS release 12.0(10)W5(18g).

SPAN op Catalyst 8500

Een zeer basisoptie van SPAN is beschikbaar op Catalyst 8540 onder de naam port sneoping. Raadpleeg de huidige Catalyst 8540-documentatie voor meer informatie.

Poortsnooping maakt het mogelijk om op transparante wijze verkeer van een of meer bronpoorten naar een doelpoort te spiegelen."

Geef de opdracht van de **snoop uit** om op haven gebaseerd verkeer te spiegelen of te snooping in te stellen. Geef het geen formulier van deze opdracht uit om snooping uit te schakelen:

```
snoop interface source_port direction snoop_direction

no snoop interface source_port
```

De variabele ***source_port*** verwijst naar de poort die wordt gevolgd. De variabele ***snoop_guide*** is de verkeersrichting op de bronpoort of de poorten die worden gecontroleerd: **ontvangen**, **verzenden**, of **beide**.

```
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
```

Dit voorbeeld toont uitvoer van het bevel van de **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)
```

> Opmerking: Deze opdracht wordt niet ondersteund op Ethernet-poorten in een Catalyst 8540 als u een MSR-afbeelding (Multiservice ATM-switchrouter), zoals 8540m-in-mz draait. In plaats daarvan moet u een CSR-beeld (campus Switch Router) gebruiken, zoals 8540c-in-mz.

SPAN op Catalyst 2900, 4500/4000, 5500/5000 en 6500/6000 Series switches die CatOS uitvoeren

Deze sectie is alleen van toepassing op deze Cisco Catalyst 2900 Series switches:

- Cisco Catalyst 2948G-L2 switch
- Cisco Catalyst 2948G-48G-E-TX switch

- Cisco Catalyst 2980G-A switch

Deze sectie is van toepassing op Cisco Catalyst 4000 Series-switches die het volgende omvatten:

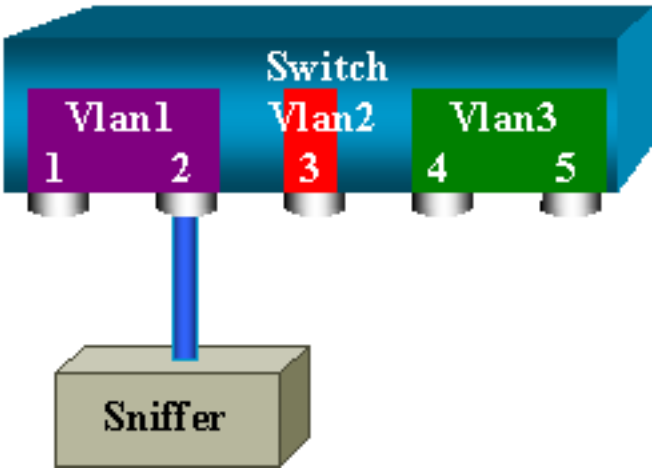
- Modulair chassis switches:Cisco Catalyst 4003 switchCisco Catalyst 4006 switch
- Vaste chassis switch: Cisco Catalyst 4912G switch

Lokale SPAN

SPAN-functies zijn één voor één toegevoegd aan het CatOS-systeem en een SPAN-configuratie bestaat uit één **ingestelde** span-opdracht. Er is nu een breed scala aan opties beschikbaar voor deze opdracht:

```
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 dit netwerkdiagram worden de verschillende SPAN-mogelijkheden geïntroduceerd door het gebruik van variaties:



Dit diagram maakt deel uit van één lijnkaart die in sleuf 6 van een Catalyst 6500/6000 switch bevindt. In dit scenario:

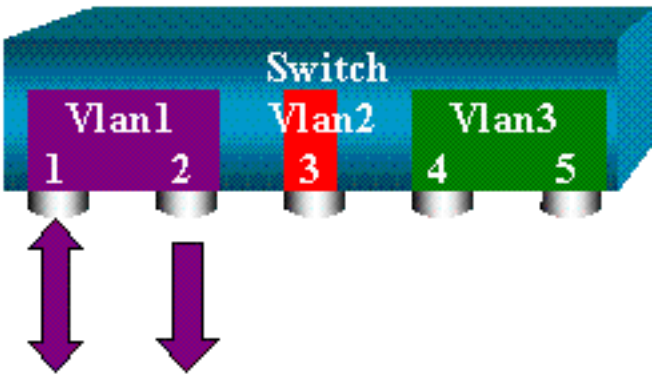
- Poorten 6/1 en 6/2 behoren tot VLAN 1
- Port 6/3 behoort tot VLAN 2
- Poorten 6/4 en 6/5 behoren tot VLAN 3

Sluit een sluipschutter aan op poort 6/2 en gebruik deze in meerdere gevallen als een monitor poort.

PSPAN, VSPAN: Controleer sommige poorten of een heel VLAN

Geef de eenvoudigste vorm van de **set span** opdracht op om één poort te controleren. De syntaxis is is **ingesteld op *source_port target_port*.**

Monitoren van één poort met SPAN

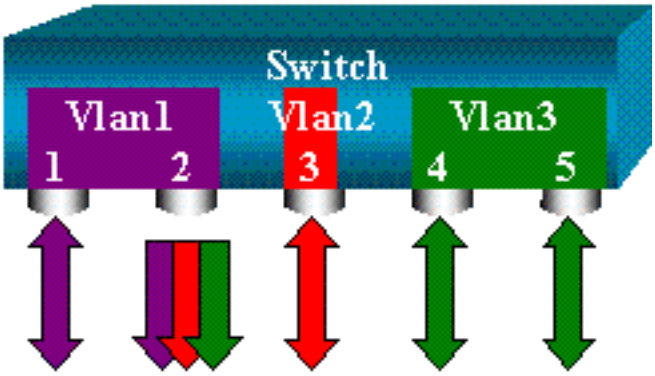



```
switch (enable) set span 6/1 6/2

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
```

Met deze configuratie wordt elk pakje dat per poort 6/1 wordt ontvangen of verzonden gekopieerd op poort 6/2. Een duidelijke beschrijving hiervan verschijnt wanneer u de configuratie ingaat. Geef de **opdracht Show span uit** om een samenvatting van de huidige SPAN-configuratie te ontvangen:

```
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
```

Monitoren van verschillende poorten met SPAN



De **set span** *source_ports* **target_port** opdracht staat de gebruiker toe om meer dan één bronpoort te specificeren. Maak een lijst van alle havens waarop u de SPAN wilt implementeren en maak van de poorten een aparte rij. De opdrachtregel tolk kan ook het koppelteken gebruiken om een bereik poorten te specificeren. Dit voorbeeld illustreert deze mogelijkheid om meer dan één poort te specificeren. In het voorbeeld wordt SPAN gebruikt op poort 6/1 en een bereik van drie poorten, van 6/3 tot 6/5:

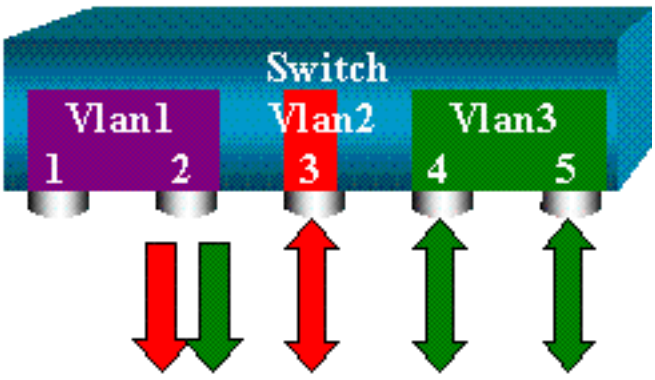
> Opmerking: Er kan maar één bestemming poort zijn. Specificeer altijd de doelpoort na de SPAN-bron.

```
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
```

> Opmerking: In tegenstelling tot Catalyst 2900XL/3500XL switches kan Catalyst 4500/4000, 5500/5000 en 6500/6000 poorten bewaken die behoren tot verschillende VLAN's met CatOS-versies die eerder dan 5.1 zijn. Hier worden de gespiegelde poorten toegewezen aan VLAN's 1, 2 en 3.

Monitor VLAN's met SPAN

Uiteindelijk, staat het **ingestelde spanwijdte** u toe om een haven te vormen om lokaal verkeer voor een volledig VLAN te controleren. De opdracht is **ingesteld op** ***source_VLAN(s) target_port*****.**



Gebruik een lijst van een of meer VLAN's als bron in plaats van een lijst met poorten:

```
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
```

Met deze configuratie wordt elk pakket dat VLAN 2 of 3 invoert of verlaat, gedupliceerd naar poort 6/2.

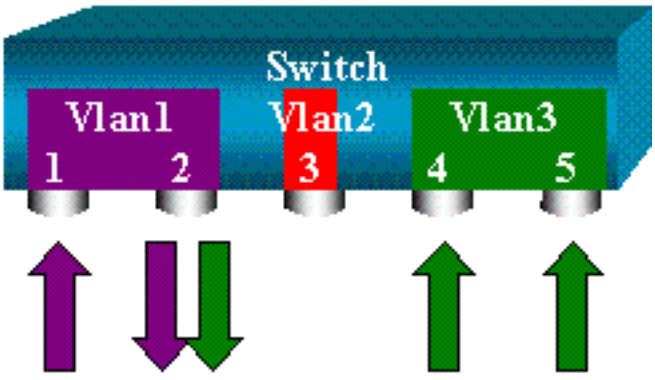
> Opmerking: Het resultaat is precies het zelfde als als als u SPAN afzonderlijk op alle havens uitvoert die aan de VLANs behoren die de opdracht specificeert. Vergelijk het veld `Oper Source` en het veld `Admin Source`. Het veld `Admin Source` maakt een lijst van alle poorten die u voor de SPAN-sessie hebt ingesteld en het veld `Oper Source` maakt een lijst van de poorten die SPAN gebruiken.

SPAN IN HET VUUR/SPAN

In het voorbeeld in de sectie VLAN's van de monitor met sectie SPAN, wordt het verkeer dat de gespecificeerde poorten invoert en verlaat gecontroleerd. De `richting:` Dit wordt weergegeven in het veld `verzenden/ontvangen`. Met Catalyst 4500/4000, 5500/5000 en 6500/6000 Series-switches kunt u alleen progressief (uitgaand) of alleen inbraakverkeer op een bepaalde poort innen. Voeg het **rx** (ontvang) of **tx** (verstuur) sleutelwoord aan het eind van de opdracht toe. De standaardwaarde is **zowel** (tx als rx).

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

In dit voorbeeld neemt de sessie al inkomend verkeer voor VLAN's 1 en 3 op en spiegelt het verkeer aan poort 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
```

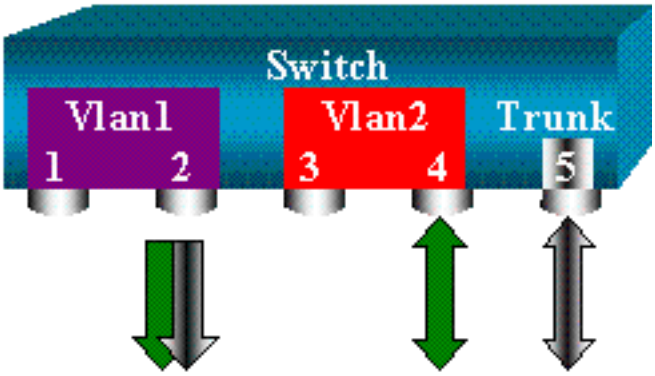
SPAN op een Trunk implementeren

Trunken zijn een speciaal geval in een schakelaar omdat het havens zijn die verscheidene VLAN's dragen. Als een stam als bronpoort wordt geselecteerd, wordt het verkeer voor alle VLANs in deze stam gecontroleerd.

Controleer een subset van VLAN's die tot een Trunk behoren

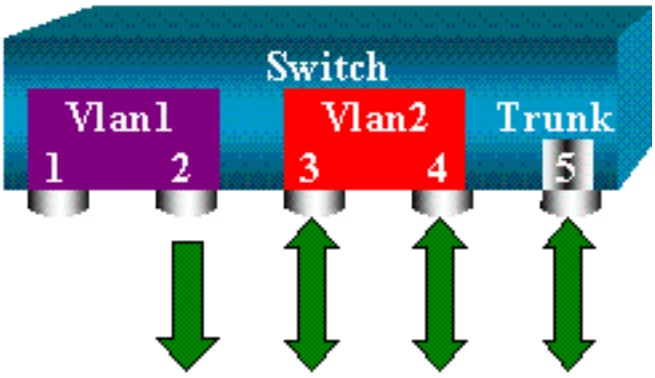
In dit diagram is poort 6/5 nu een stam die alle VLAN's draagt. Stel je voor dat u SPAN op het verkeer in VLAN 2 wilt gebruiken voor poorten 6/4 en 6/5. Geef deze opdracht gewoon uit:

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



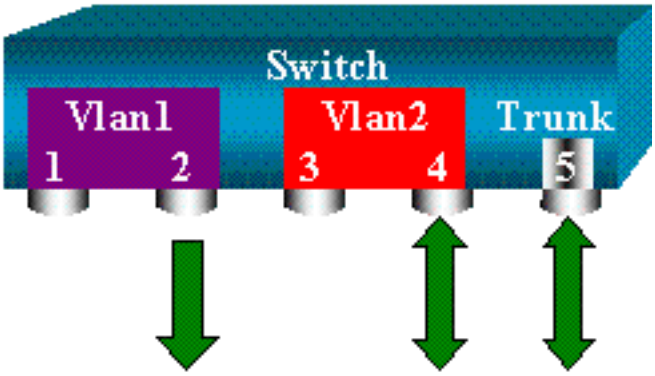
In dit geval, is het verkeer dat op de haven van SPAN wordt ontvangen een mix van het verkeer dat u wilt en alle VLAN's die boomstam 6/5 draagt. Bijvoorbeeld, er is geen manier om op de bestemmingspoort te onderscheiden of een pakket van haven 6/4 in VLAN 2 of haven 6/5 in VLAN 1 komt. Een andere mogelijkheid is SPAN op volledig VLAN 2 te gebruiken:

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



Met deze configuratie, op zijn minst, controleer je alleen verkeer dat tot VLAN 2 van de stam behoort. Het probleem is dat u nu ook verkeer ontvangt dat u niet van poort 6/3 wilt. Het CatOS omvat een ander sleutelwoord dat u toestaat om sommige VLAN's te selecteren om van een boomstam te controleren:

```
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
```



Deze opdracht bereikt het doel omdat u VLAN 2 selecteert op alle stammen die worden gemonitord. U kunt meerdere VLAN's met deze filteroptie instellen.

> Opmerking: Deze filteroptie wordt alleen ondersteund op Catalyst 4500/4000 en Catalyst 6500/6000 switches. Catalyst 5500/5000 biedt geen ondersteuning voor de filteroptie die beschikbaar is onder de opdracht **vaste** breedte.

Trunking op de doelpoort

Als u bronpoorten hebt die aan verschillende VLAN's behoren, of als u SPAN op meerdere VLAN's in een boomstampoort gebruikt, zou u kunnen willen identificeren aan welk VLAN een pakket dat u op de bestemming SPAN poort ontvangt hoort. Deze identificatie is mogelijk als u trunking op de doelpoort toestaat voordat u de poort voor SPAN vormt. Op deze manier worden alle pakketten die naar de sniffer worden verzonden ook getagd met hun respectieve VLAN IDs.

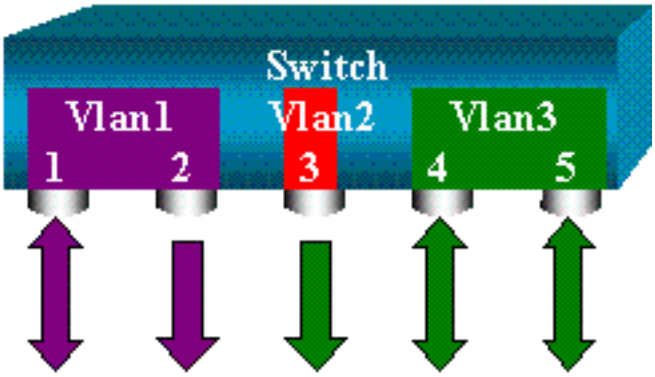
> Opmerking: Uw sluipschutter moet de corresponderende insluiting herkennen.

```
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
```

Meerdere gelijktijdige sessies maken

Tot nu toe is er slechts één SPAN-sessie gemaakt. Elke keer dat u een nieuwe **set span** opdracht geeft, is de vorige configuratie ongeldig. CatOS kan nu meerdere sessies tegelijkertijd uitvoeren, zodat het verschillende doelpoorten tegelijkertijd kan hebben. Geef de **ingestelde *bronbestemming van de* spanwijdte uit creëren** opdracht om een extra SPAN sessie toe te voegen. In deze sessie wordt poort 6/1 tot 6/2 gevolgd en tegelijkertijd wordt VLAN 3 tot poort 6/3 gecontroleerd:




```
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
```

Geef nu de opdracht **Show span op** om te bepalen of u twee sessies tegelijkertijd hebt:

```
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
```

Er worden extra sessies gecreëerd. Je hebt een manier nodig om bepaalde sessies te verwijderen. Deze opdracht is:

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

Omdat er slechts één doelpoort per sessie kan zijn, identificeert de doelpoort een sessie. Verwijdert de eerste sessie die is gemaakt, de sessie die poort 6/2 als bestemming gebruikt:

```
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
```

U kunt nu controleren of er slechts één sessie overblijft:

```
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
```

Geef deze opdracht uit om alle huidige sessies in één stap uit te schakelen:

```
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-opties

De syntaxis voor het **ingestelde** span-opdracht is:

```
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 dit deel worden de opties uiteengezet die in dit document worden besproken:

- **sc0**-U specificeert het **sc0** sleutelwoord in een configuratie van SPAN wanneer u het verkeer naar de interface van het beheer sc0 moet controleren. Deze optie is beschikbaar op Catalyst 5500/5000 en 6500/6000 Switches, codeversie CatOS 5.1 of later.
- **invoer *schakelt/schakelt***-deze optie is uiterst belangrijk. Zoals dit document verklaart, behoort een poort die u als de bestemming van SPAN vormt nog tot zijn origineel VLAN. Packets die op een doelpoort worden ontvangen, gaan dan het VLAN in, alsof deze poort een normale toegangspoort is. Dit gedrag kan gewenst zijn. Als u een PC als snuffer gebruikt, kunt u deze PC volledig met het VLAN verbinden. Niettemin, kan de verbinding gevaarlijk zijn als u de bestemmingspoort op andere netwerkapparatuur aansluit die een lus in het netwerk creëert. De bestemming SPAN poort voert niet STP uit, en u kunt in een gevaarlijke overbruggingslus situatie eindigen. Zie de reden waarom de SPAN-sessie een overbruggingslening creëert? deel van dit document om te begrijpen hoe deze situatie zich kan voordoen. De standaardinstelling voor deze optie is schakelt uit, wat betekent dat de bestemming SPAN poort terugwerpt die de poort ontvangt. Deze teruggooi beschermt de haven tegen overbruggingslijnen. Deze optie verschijnt in CatOS 4.2.
- **leren *schakelt/schakelt***-Met deze optie kunt u leren op de doelpoort uitschakelen. Standaard is het leren ingeschakeld en de bestemmingsppoort leert MAC-adressen van inkomende pakketten die de poort ontvangt. Deze optie verschijnt in CatOS 5.2 op Catalyst 4500/4000 en 5500/5000 en in CatOS 5.3 op Catalyst 6500/6000.
- **multicast *schakelt***-schakelt in/uit-zoals de naam suggereert, staat deze optie u toe om de controle van multicast pakketten in of uit te schakelen. Standaard is deze optie ingeschakeld. Deze optie is beschikbaar op Catalyst 5500/5000, 6500/6000, CatOS 5.1 en hoger.
- **Het overspannen van haven 15/1**-Op Catalyst 6500/6000, kunt u haven 15/1 (of 16/1) als SPAN bron gebruiken. De poort kan het verkeer controleren dat naar de functiekaart voor meerlaagse switch (MSFC) wordt doorgestuurd. De poort vangt verkeer op dat software-routed of gericht aan MSFC is.

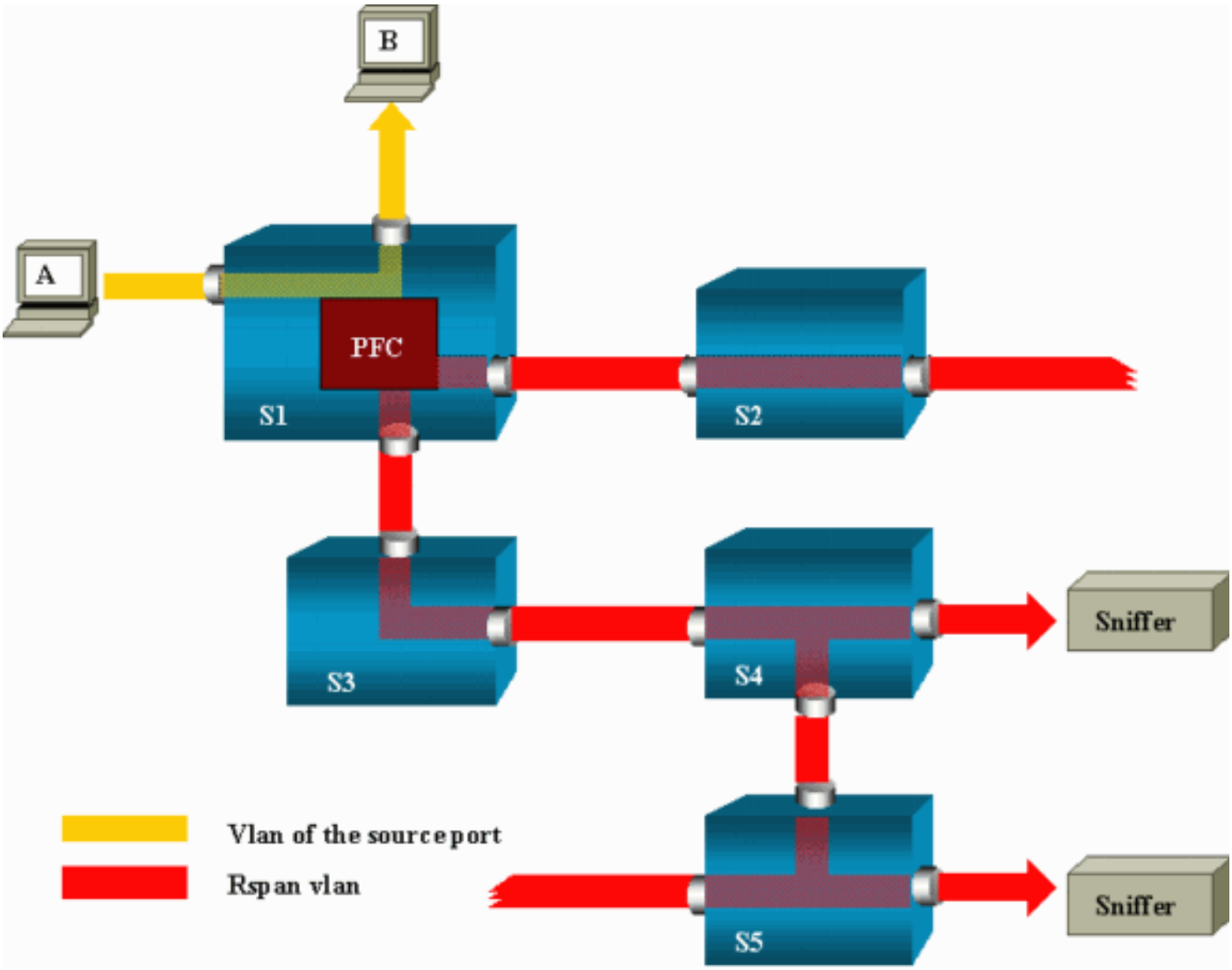
Remote SPAN

RSPAN-Overzicht

RSPAN staat u toe om bronpoorten te controleren die over een geschakeld netwerk worden verspreid, niet alleen lokaal op een schakelaar met SPAN. Deze optie verschijnt in CatOS 5.3 in Catalyst 6500/6000 Series-switches en wordt toegevoegd aan Catalyst 4500/4000 Series-switches in CatOS 6.3 en hoger.

De functionaliteit werkt precies als een reguliere SPAN-sessie. Het verkeer dat door SPAN wordt gecontroleerd wordt niet direct gekopieerd naar de doelpoort, maar overstroomd naar een speciaal RSPAN VLAN. De doelpoort kan dan overal in dit RSPAN VLAN geplaatst worden. Er kunnen zelfs verschillende doelhavens zijn.

In dit schema wordt de structuur van een RSPAN-sessie weergegeven:



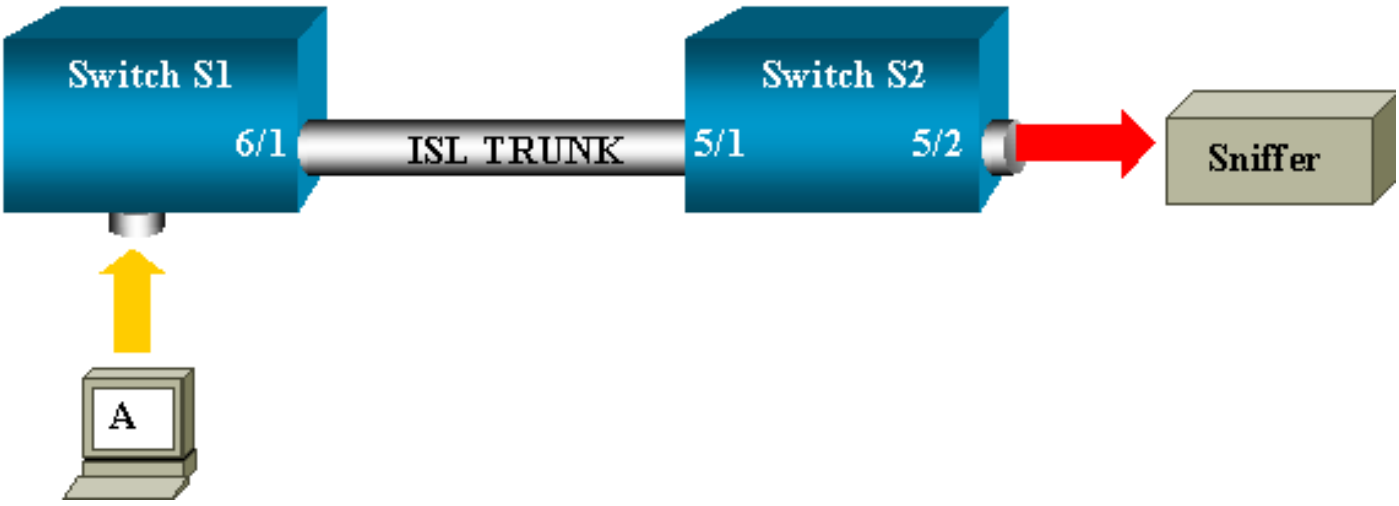
In dit voorbeeld, vormt u RSPAN om verkeer te controleren dat gastheer A verstuurt. Wanneer A een kader genereert dat voor B bestemd is, wordt het pakket gekopieerd door een applicatiespecifiek geïntegreerd circuit (ASIC) van Catalyst 6500/6000 Policy functiekaart (PFC) in een vooraf gedefinieerd RSPAN VLAN. Van daaruit, wordt het pakket overstroomd naar alle andere poorten die aan RSPAN VLAN behoren. Alle koppellijnen die hier worden getekend zijn trunks, wat een vereiste is voor RSPAN. De enige toegangshavens zijn bestemmingspoorten, waar de sluipschutters zijn aangesloten (hier, op S4 en S5).

Dit zijn een paar opmerkingen over dit ontwerp:

- S1 wordt een bronschakelaar genoemd. Packets voeren alleen het RSPAN VLAN in in switches die als RSPAN-bron zijn geconfigureerd. Op dit moment kan een schakelaar alleen de bron zijn voor één RSPAN-sessie, wat betekent dat een bronschakelaar slechts één RSPAN VLAN tegelijkertijd kan voeden.
- S2 en S3 zijn intermediaire switches. Het zijn geen RSPAN-bronnen en geen bestemmingshavens. Een schakelaar kan intermediair zijn voor om het even welk aantal zittingen van RSPAN.
- S4 en S5 zijn bestemmingsswitches. Sommige poorten zijn ingesteld als bestemming voor een RSPAN-sessie. Op dit moment kan Catalyst 6500/6000 tot 24 RSPAN-poorten hebben, voor een of meer verschillende sessies. U kunt ook opmerken dat S4 zowel een bestemming als een tussenschakelaar is.
- U kunt zien dat de pakketten RSPAN in het VLAN worden overstroomd. Zelfs switches die niet op het pad naar een doelpoort zijn, zoals S2, ontvangen het verkeer voor RSPAN VLAN. U kunt het nuttig vinden om dit VLAN op dergelijke S1-S2 links af te drukken.
- Om de overstroming te bereiken, wordt het leren uitgeschakeld aan het RSPAN VLAN.
- Om loops te voorkomen, is STP op RSPAN VLAN gehandhaafd. Daarom kan RSPAN Bridge Protocol Data Units (BPDU's) niet controleren.

Configuratievoorbeeld van RSPAN

De informatie in dit gedeelte illustreert de instelling van deze verschillende elementen met een zeer eenvoudig RSPAN-ontwerp. S1 en S2 zijn twee Catalyst 6500/6000 switches. Om sommige S1 poorten of VLAN's van S2 te controleren, moet u een toegewijd RSPAN VLAN instellen. De rest van de opdrachten heeft een soortgelijke syntaxis als de opdrachten die u in een typische SPAN-sessie gebruikt.



Instellen van de ISL Trunk tussen de twee switches S1 en S2

Om te beginnen, plaats het zelfde VLAN Trunk Protocol (VTP) domein op elke schakelaar en vorm één kant als trunking wenselijk. VTP onderhandeling doet de rest. Geef deze opdracht op S1:

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

Geef deze opdrachten op S2 uit:

```
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
```

Creatie van RSPAN VLAN

Een RSPAN-sessie heeft een specifiek RSPAN VLAN nodig. U moet dit VLAN maken. U kunt een bestaand VLAN niet converteren naar een RSPAN VLAN. Dit voorbeeld gebruikt VLAN 100:

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

Geef deze opdracht uit op één schakelaar die als VTP server is ingesteld. De kennis van RSPAN VLAN 100 wordt automatisch verspreid in het gehele VTP-domein.

Configuratie van poort 5/2 van S2 als RSPAN-bestemming

```
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
```

Configuratie van een RSPAN-bronpoort op S1

In dit voorbeeld wordt het inkomende verkeer dat S1 via poort 6/2 ingaat bewaakt. Deze opdracht geven:

```
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 inkomende pakketten op poort 6/2 worden nu overstroomd op RSPAN VLAN 100 en bereiken de bestemmingspoort die op S1 via de boomstam wordt gevormd.

Controleer de configuratie

De opdracht **Show** span geeft een samenvatting van de huidige RSPAN-configuratie op de schakelaar. Er kan slechts één bron-RSPAN-sessie tegelijk zijn.

```
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
```

Andere configuraties die mogelijk zijn met de ingestelde spanwijdte.

U gebruikt verschillende opdrachtregels om de bron en de bestemming met RSPAN te configureren. Afgezien van dit verschil gedragen SPAN en RSPAN zich werkelijk op dezelfde manier. U kunt RSPAN zelfs lokaal gebruiken, op één schakelaar, als u meerdere poorten van de bestemming SPAN wilt hebben.

Serviceoverzicht en beperkingen

Deze tabel geeft een samenvatting van de verschillende functies die zijn geïntroduceerd en geeft de minimale CatOS-release die nodig is om de functie op het ingestelde platform te kunnen uitvoeren:

Functie	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
optie *in-/uitschakelen*	4.4	4.2	5.1
Meervoudige sessies, poorten in verschillende VLAN's	5.1	5.1	5.1
SC0 optie	—	5.1	5.1
multicast optie *in/uitschakelen*	—	5.1	5.1
optie leren *in/uitschakelen*	5.2	5.2	5.3
RSPAN	6.3	—	5.3

Deze tabel bevat een korte samenvatting van de huidige beperkingen op het aantal mogelijke SPAN-sessies:

Functie	Catalyst 4500/4000 Series switches	Catalyst 5500/5000 Series switches	Catalyst 6500/6000 Series switche
Rx- of beide SPAN-sessies	5	1	2
TX SPAN-sessies	5	4	4

Mini-sessies voor protocolanalyse	Niet ondersteund	Niet ondersteund	1
RX-, TX- of beide RSPAN-bronsessies	5	Niet ondersteund	1 Supervisor Engine 720 ondersteu twee RSPAN-bronsessies.
RSPAN-bestemming	5	Niet ondersteund	24
Totale sessies	5	5	30

Raadpleeg deze documenten voor aanvullende beperkingen en configuratiehandleidingen:

- SPAN EN RSPAN configureren (Catalyst 4500/4000)
- SPAN EN RSPAN configureren (Catalyst 6500/6000)

SPAN op Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 en 3750-E Series switches

Dit zijn richtlijnen voor de configuratie van de SPAN-functie op Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 en 3750-E Series switches ches:

- Catalyst 2950 switches kunnen slechts één SPAN-sessie tegelijkertijd actief hebben en alleen bronpoorten bewaken. Deze switches kunnen VLAN's niet bewaken.
- De Catalyst 2950 en 3550 switches kunnen het verkeer via een doelpoort naar SPAN doorsturen in Cisco IOS-softwarerelease 12.1(13)EA1 en hoger.
- De Catalyst 3550, 3560, en 3750 switches kunnen tot twee SPAN sessies tegelijkertijd ondersteunen en bronpoorten zowel als VLAN's kunnen bewaken.
- De Catalyst 2970, 3560, en 3750 switches vereisen niet de configuratie van een reflectiepoort wanneer u een RSPAN-sessie configureren.
- Catalyst 3750 Switches ondersteunt de sessieconconfiguratie met het gebruik van bron- en doelpoorten die op een van de leden van de switchstack wonen.
- Per SPAN-sessie is slechts één doelpoort toegestaan en dezelfde poort kan geen doelpoort zijn voor meerdere SPAN-sessies. Daarom kunt u geen twee SPAN sessies hebben die dezelfde doelpoort gebruiken.

De opdrachten van de SPAN-functieknop zijn vergelijkbaar op Catalyst 2950 en Catalyst 3550. Catalyst 2950 kan echter niet de VLAN's bewaken. U kunt de SPAN configureren, zoals in dit voorbeeld:

```
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#
```

U kunt een poort ook configureren als een bestemming voor lokale SPAN en RSPAN voor hetzelfde VLAN-verkeer. Om verkeer voor een bepaald VLAN te controleren dat in twee direct aangesloten switches verblijft, moet u deze opdrachten op de switch configureren die de doelpoort heeft. In dit voorbeeld monitoren we verkeer van VLAN 5 dat over twee switches wordt verspreid:

```
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.
```

Gebruik deze configuratie op de afstandsbediening:

```
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
```

In het vorige voorbeeld werd een poort ingesteld als een doelpoort voor zowel de lokale SPAN als RSPAN om verkeer voor hetzelfde VLAN te controleren dat in twee switches verblijft.

> Opmerking: Anders dan de switches van 2900XL en 3500XL Series, Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3755 0-, en 3750-E Series switches ondersteunen SPAN op bronpoortverkeer in de Rx-richting alleen (Rx SPAN of INGress SPAN), alleen in de Tx-richting (Tx SPAN of SPAN) of beide.

> Opmerking: De opdrachten in de configuratie worden niet ondersteund op Catalyst 2950 met Cisco IOS-softwarerelease 12.0(5.2)WC(1) of andere software die eerder is dan Cisco IOS-softwarerelease 12.1(6)EA2. Raadpleeg het gedeelte *InABRICAGE-poortanalyse* van Managed-switches om SPAN op een Catalyst 29 te configureren 50 met software die eerder is dan Cisco IOS-softwarerelease 12.1(6)EA2.

> Opmerking: Catalyst 2950 switches die Cisco IOS-softwarerelease 12.1(9)EA1d en eerdere releases in Cisco IOS-softwarerelease 12.1 gebruiken, ondersteunen SPAN. Alle pakketten die op de SPAN-doelpoort worden gezien (aangesloten op het snuffelapparaat of de PC) hebben echter een IEEE 802.1Q-tag, ook al is de SPAN-bronpoort (gemonitord poort) mogelijk geen 802.1Q.CZK-poort. Als het snuffelapparaat of de interfacekaart van het PC-netwerk (NIC) de pakketten 802.1Q niet begrijpt, kan het apparaat de pakketten laten vallen of problemen hebben aangezien het probeert de pakketten te decoderen. De mogelijkheid om de 802.1Q-gelabelde frames te zien is alleen belangrijk wanneer de SPAN-bronpoort een boompoort is. Met Cisco IOS-softwarerelease 12.1(11)EA1 en hoger kunt u het taggen van de pakketten op de SPAN-doelpoort inschakelen en uitschakelen. Geef de opdracht van de **monitor sessie *sessie_number* bestemmings interface *interface_id* insluitingpunt1q uit** om insluiting van de pakketten in de doelpoort mogelijk te maken. Als u het **insluitingssleutelwoord** niet specificeert, worden de pakketten verzonden untagged, wat de

standaard in Cisco IOS-softwarerelease 12.1(11)EA1 en later is.

Functie	Catalyst 2950/3550
Optie in *-/uitschakelen* (*inches)*	Cisco IOS-softwarerelease 12.1(12c)EA1
RSPAN	Cisco IOS-softwarerelease 12.1(12c)EA1

Functie	Catalyst 2940[1], 2950, 2955, 2960, 2970, 3550, 3560, 3750
Rx- of beide SPAN-sessies	2
TX SPAN-sessies	2
RX-, TX- of beide RSPAN-bronsessies	2
RSPAN-bestemming	2
Totale sessies	2

[1] De Catalyst 2940-switches ondersteunen alleen de lokale SPAN. RSPAN wordt in dit platform niet ondersteund.

Raadpleeg deze configuratiehandleidingen voor meer informatie over de configuratie van SPAN en RSPAN:

- SPAN configureren (Catalyst 2940)
- SPAN en RSPAN configureren (Catalyst 2950 en 2955)
- SPAN en RSPAN configureren (Catalyst 2960)
- SPAN en RSPAN configureren (Catalyst 3550)
- SPAN en RSPAN configureren (Catalyst 3560)
- SPAN en RSPAN configureren (Catalyst 3560-E en 3750-E)
- SPAN en RSPAN configureren (Catalyst 3750)

SPAN op Catalyst 4500/4000 en Catalyst 6500/6000 Series switches die Cisco IOS-systeemsoftware uitvoeren

De SPAN-functie wordt ondersteund op Catalyst 4500/4000 en Catalyst 6500/6000 Series-switches die Cisco IOS-systeemsoftware gebruiken. Beide switchplatforms gebruiken de identieke opdrachtregel-interface (CLI) van en een configuratie die gelijk is aan de configuratie die de SPAN op Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 356 Des voor 0E, 3750 en 3750E Series switches. Raadpleeg deze documenten voor de bijbehorende configuratie:

- SPAN EN RSPAN configureren (Catalyst 6500/6000)
- SPAN EN RSPAN configureren (Catalyst 4500/4000)

Configuratievoorbeeld

U kunt de SPAN configureren, zoals in dit voorbeeld:

```
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#
```

Serviceoverzicht en beperkingen

Deze tabel vat de verschillende functies samen die zijn geïntroduceerd en biedt de minimale Cisco IOS-softwarerelease die nodig is om de functie op het gespecificeerde platform te kunnen uitvoeren:

Functie	Catalyst 4500/4000 (Cisco IOS-software)	Catalyst 6500/6000 (Cisco IOS-software)
Optie in *-/uitschakelen (inches)*	Cisco IOS-softwarerelease 12.1(19)EW	Momenteel niet ondersteund[1]
RSPAN	Cisco IOS-softwarerelease 12.1(20)EW	Cisco IOS-softwarerelease 12.1(1

[1] Deze optie is op dit moment niet beschikbaar en de beschikbaarheid van deze functies wordt normaal gesproken niet gepubliceerd voordat deze worden vrijgegeven.

> **Opmerking**: de SPAN-functie van Cisco Catalyst 6500/6000 Series-switches heeft een beperking met betrekking tot PIM-protocol. Wanneer een switch voor zowel PIM als SPAN is ingesteld, kan de Network Analyzer / Sniffer die aan de SPAN-doelpoort is gekoppeld, PIM-pakketten zien die geen deel uitmaken van de SPAN-bronpoort/VLAN-verkeer. Deze kwestie komt door een beperking in de pakket door verzending architectuur van de switch voor. De SPAN bestemming poort voert geen controle uit om de bron van de pakketten te verifiëren. Dit probleem is ook gedocumenteerd in Cisco bug-ID CSCdy57506 (alleen geregistreerde klanten).

Deze tabel bevat een korte samenvatting van de huidige beperkingen op het aantal mogelijke SPAN- en RSPAN-sessies:

Functie	Catalyst 4500/4000 (Cisco IOS-software)
Rx- of beide SPAN-sessies	2
TX SPAN-sessies	4
RX-, TX- of beide RSPAN-bronsessies	2 (Rx, Tx of beide) en tot 4 voor alleen Tx
RSPAN-bestemming	2
Totale sessies	6

Raadpleeg Lokale SPAN-, RSPAN- en ERSPAN-sessielimieten voor Catalyst 6500/6000 switches die Cisco IOS-software gebruiken.

In Catalyst 6500 Series is het belangrijk om op te merken dat de stress SPAN op de supervisor gebeurt. Hierdoor kan al het verkeer dat aan SPAN is onderworpen, over het weefsel worden verzonden naar de supervisor en vervolgens naar de SPAN-doelpoort, die belangrijke systeemresources kan gebruiken en het gebruikersverkeer kan beïnvloeden. Ingreress SPAN zal worden toegepast op ingress-modules, zodat de SPAN-prestaties de som zouden zijn van alle

deelnemende replicatiemotoren. De prestaties van de SPAN-functie zijn afhankelijk van de pakketgrootte en het type ASIC dat in de replicatiemodule beschikbaar is.

Met releases eerder dan Cisco IOS-softwarerelease 12.2(33)SXH, kan een poortkanaalinterface en EtherChannel geen SPAN-bestemming zijn. Met Cisco IOS-softwarerelease 12.2(33)SXH en hoger kan een EtherChannel een SPAN-bestemming zijn. Destination EtherChannel biedt geen ondersteuning voor de Port Aggregation Control Protocol (PAgP) of Link Aggregation Control Protocol (LACP) EtherChannel-protocollen; alleen de on-modus wordt ondersteund, waarbij alle EtherChannel-protocolondersteuning uitgeschakeld is.

Raadpleeg deze documenten voor aanvullende beperkingen en configuratiehandleidingen:

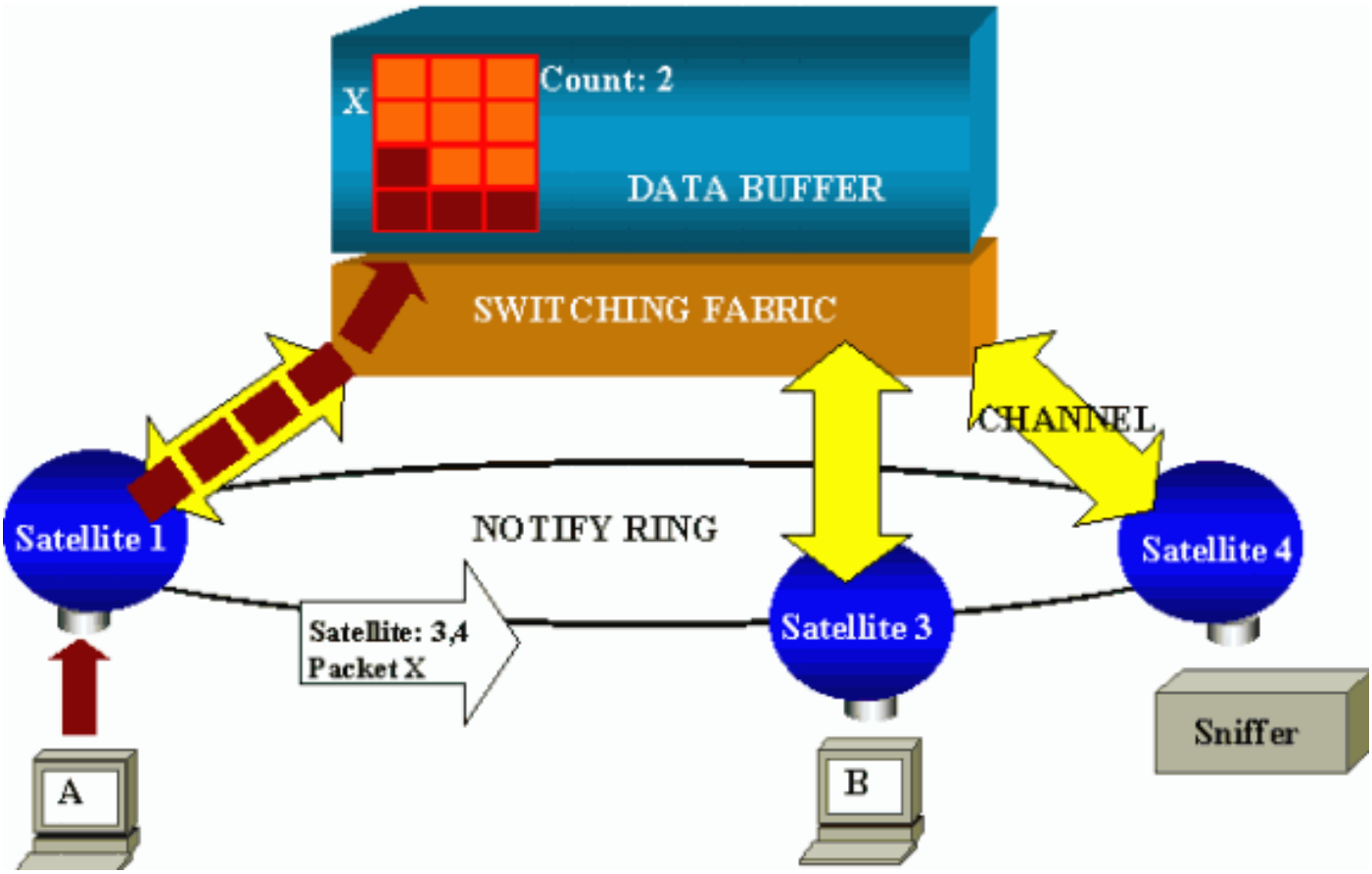
- SPAN en RSPAN configureren (Catalyst 4500/4000)
- Local SPAN, Remote SPAN (RSPAN) en ingesloten RSPAN configureren (Catalyst 6500/6000)

Effect van SPAN op de verschillende Catalyst-platforms

Catalyst 2900XL/3500XL Series switch

Overzicht van architectuur

Dit is een zeer simplistische weergave van de interne architectuur van de 2900XL/3500XL-switches:



De poorten van de schakelaar worden aangesloten op satellieten die via radiaalkanalen op een schakelmateriaal communiceren. Bovenaan zijn alle satellieten onderling verbonden via een

hogesnelheidstreinring die toegewijd is aan signaleringsverkeer.

Wanneer een satelliet een pakje van een poort ontvangt, wordt het pakje in cellen gesplitst en via een of meer kanalen naar de switchfabric verzonden. Het pakket wordt vervolgens opgeslagen in het gedeelde geheugen. Elke satelliet heeft kennis van de havens van bestemming. In het schema in dit deel weet satelliet 1 dat het pakket X door de satellieten 3 en 4 moet worden ontvangen. Satellite 1 stuurt via de kennisgevingsring een bericht naar de andere satellieten. Vervolgens kunnen satellieten 3 en 4 de cellen uit het gedeelde geheugen gaan ophalen via hun radiaalkanalen en uiteindelijk het pakket doorsturen. Omdat de bronsatelliet de bestemming kent, geeft deze satelliet ook een index door die het aantal keren aangeeft dat dit pakket gedownload wordt door de andere satellieten. Telkens een satelliet het pakket uit het gedeelde geheugen herhaalt, wordt deze index bepaald. Wanneer de index 0 bereikt, kan het gedeelde geheugen worden vrijgegeven.

Prestatieimpact

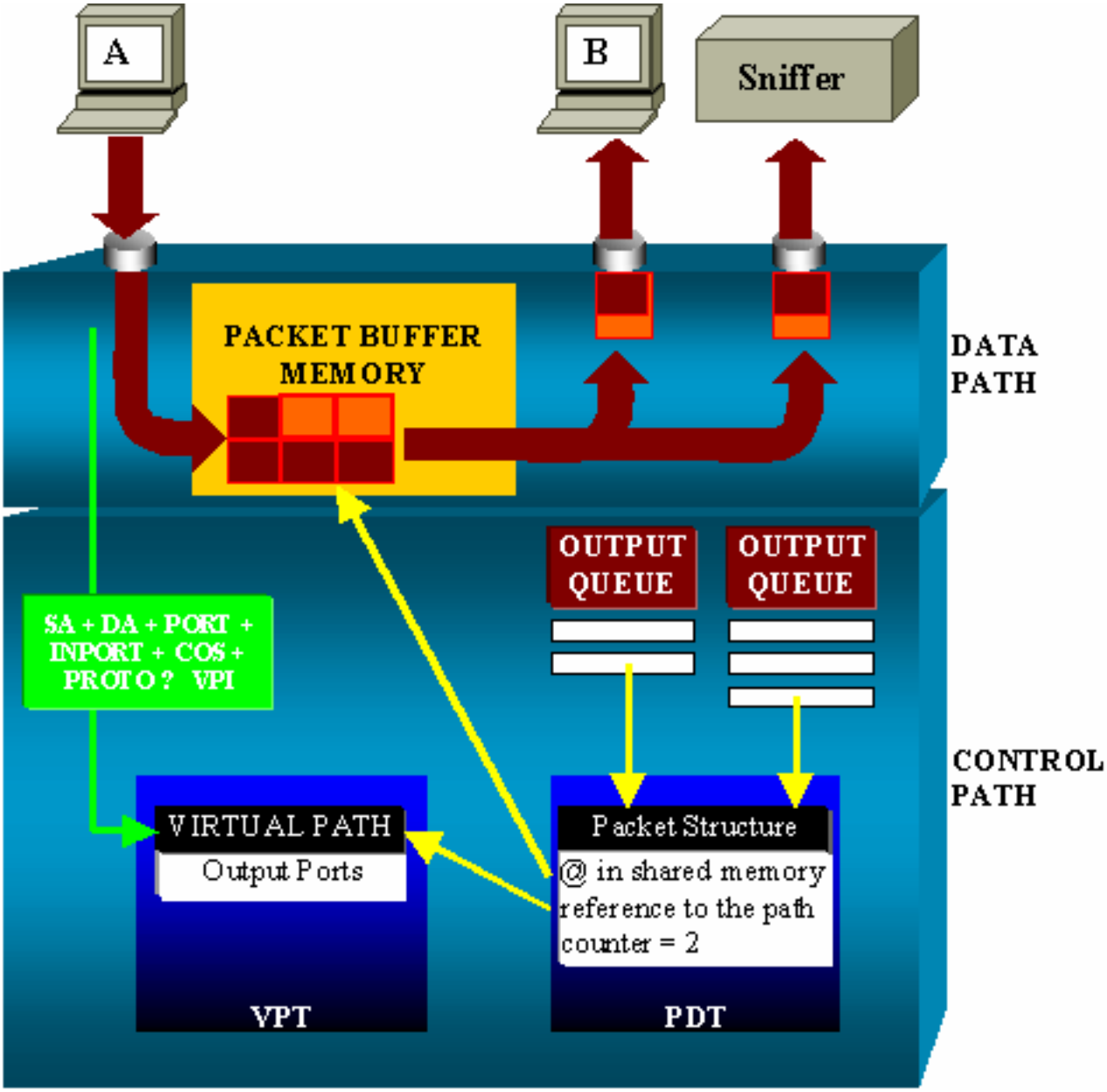
Om sommige poorten met SPAN te kunnen bewaken, moet een pakket van de gegevensbuffer naar een satelliet worden gekopieerd. De impact op de hogesnelheidsswitchfabric is verwaarloosbaar.

De monitoringhaven ontvangt kopieën van verzonden en ontvangen verkeer voor alle gecontroleerde havens. In deze architectuur, wordt een pakket dat voor meerdere bestemmingen bestemd is opgeslagen in geheugen tot alle exemplaren door worden verstuurd. Als de monitoringpoort 50% gedurende een lange periode is overabonneerd, wordt de haven waarschijnlijk geblokkeerd en houdt deze een deel van het gedeelde geheugen vast. Het is mogelijk dat één of meer van de gecontroleerde havens ook een vertraging ondervinden.

Catalyst 4500/4000 Series-switches

Overzicht van architectuur

Catalyst 4500/4000 is gebaseerd op een materiaal met een gedeeld geheugen-switching. Dit diagram is een overzicht op hoog niveau van het pad van een pakje door de schakelaar. De eigenlijke uitvoering is feitelijk veel ingewikkelder:



Op een Catalyst 4500/4000 kunt u het gegevenspad onderscheiden. Het gegevenspad komt overeen met de werkelijke overdracht van gegevens binnen de schakelaar, vanaf het bedieningspaneel, waar alle beslissingen worden genomen.

Wanneer een pakket de schakelaar ingaat, wordt een buffer toegewezen in het Geheugen van de Buffer van het Packet (een gedeeld geheugen). Een pakketstructuur die naar deze buffer wijst, wordt geformatteerd in de Packet Descriptor Tabel (PDT). Terwijl de gegevens in gedeeld geheugen worden gekopieerd, bepaalt het bedieningspaneel waar u het pakket wilt wijzigen. Om deze bepaling te kunnen uitvoeren, wordt aan de hand van deze informatie een hashwaarde berekend:

- Het pakketbronadres
- Bestemmingsadres
- VLAN
- Type protocol
- Invoerpoort
- Serviceklasse (CoS) (IEEE 802.1p of poortstandaard)

Deze waarde wordt gebruikt om de Virtual Path Index (VPI) van een padstructuur in de Virtual Path Tabel (VPT) te vinden. Deze virtuele snijpad in de VPT bevat verschillende velden die op

deze specifieke stroom betrekking hebben. De velden bevatten de doelpoorten. De pakketstructuur in de PDT wordt nu bijgewerkt met een verwijzing naar het virtuele pad en de virtuele teller. In het voorbeeld in deze sectie, moet het pakket naar twee verschillende poorten worden verzonden, zodat de teller op 2 formatteert. Tenslotte wordt de pakketstructuur toegevoegd aan de uitvoerwachtrij van de twee doelpoorten. Van daar af, kopieert de gegevens van het gedeelde geheugen in de uitvoerbuffer van de haven, en de stappen van de pakketstructuur tegen. Wanneer deze 0 bereikt, heft de gedeelde geheugenbuffer op.

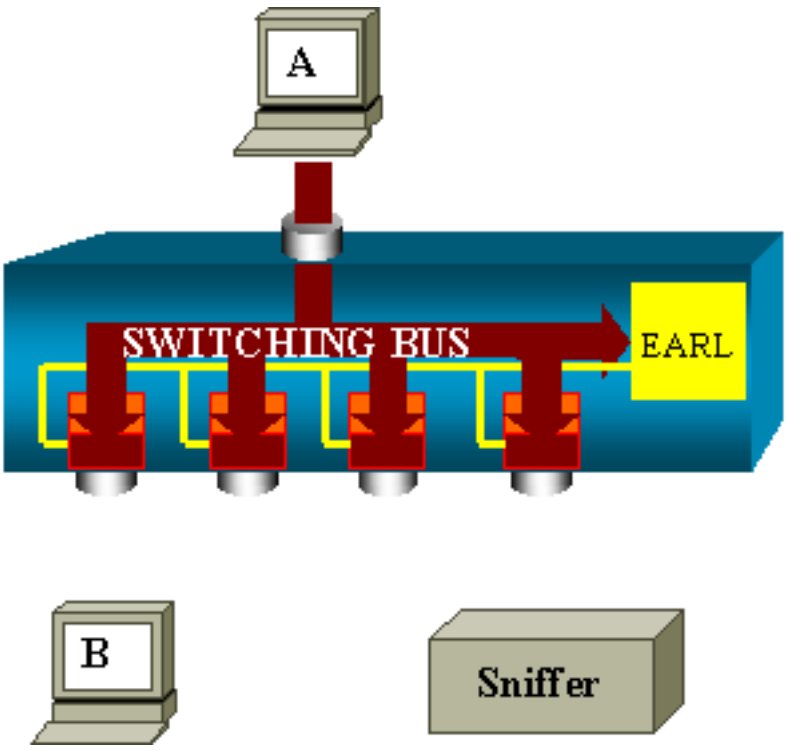
Prestatieimpact

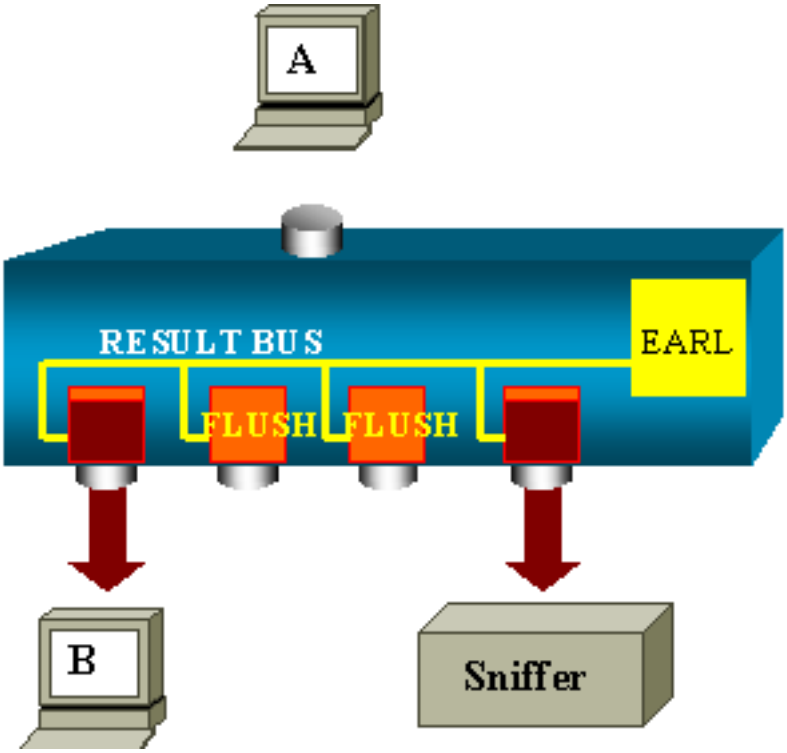
Met gebruik van de SPAN-functie moet een pakket naar twee verschillende poorten worden verzonden, zoals in het voorbeeld in het gedeelte Architecture Overzicht. Het verzenden van het pakket naar twee poorten is geen probleem omdat het switchfabric niet blokkeert. Als de doelpoort van SPAN is geblokkeerd, worden pakketten in de uitvoerwachtrij gedropt en correct vrijgegeven van het gedeelde geheugen. Daarom heeft de wisselwerking geen invloed.

Catalyst 5500/5000 en 6500/6000 Series switch

Overzicht van architectuur

Op Catalyst 5500/5000 en 6500/6000 Series switches wordt een pakket dat op een poort wordt ontvangen, op de interne switchbus verzonden. Elke lijnkaart in de schakelaar begint dit pakket in interne buffers op te slaan. Tegelijkertijd wordt de gecodeerde Address Recognition Logic (EARL) van het pakket voorzien en verwerkt een resultaatindex. EARL stuurt de resultaatindex naar alle lijnkaarten via de resulterende bus. De kennis van deze index stelt de lijnkaart in staat om afzonderlijk te beslissen of het pakje moet doorspoelen of verzenden omdat de lijnkaart het pakje in zijn buffers ontvangt.





Prestatieimpact

Of een of meerdere poorten uiteindelijk het pakket verzenden heeft absoluut geen invloed op de schakelaar bediening. Daarom heeft de SPAN-functie, wanneer je naar deze architectuur kijkt, geen invloed op de prestaties.

Vaak gestelde vragen en vaak voorkomende problemen

Connectiviteitsproblemen door foutieve configuratie van de SPAN

Connectiviteitsproblemen als gevolg van de foutieve configuratie van de SPAN treden vaak op in CatOS-versies die eerder dan 5.1 zijn. Met deze versies is slechts één SPAN-sessie mogelijk. De sessie blijft in de configuratie, zelfs wanneer u SPAN uitschakelt. Wanneer de opdracht is **ingesteld voor** de **instelling**, activeert een gebruiker de opgeslagen SPAN-sessie. De actie komt vaak voor vanwege een typografische fout, bijvoorbeeld, als de gebruiker STP wil inschakelen. Ernstige aansluitingsproblemen kunnen resulteren als de doelpoort wordt gebruikt om gebruikersverkeer door te sturen.

> **Voorzichtig:** Deze kwestie is nog steeds in de huidige implementatie van het CatOS. Wees heel voorzichtig met de poort die u als SPAN-bestemming kiest.

SPAN-doelpoort omhoog/omlaag

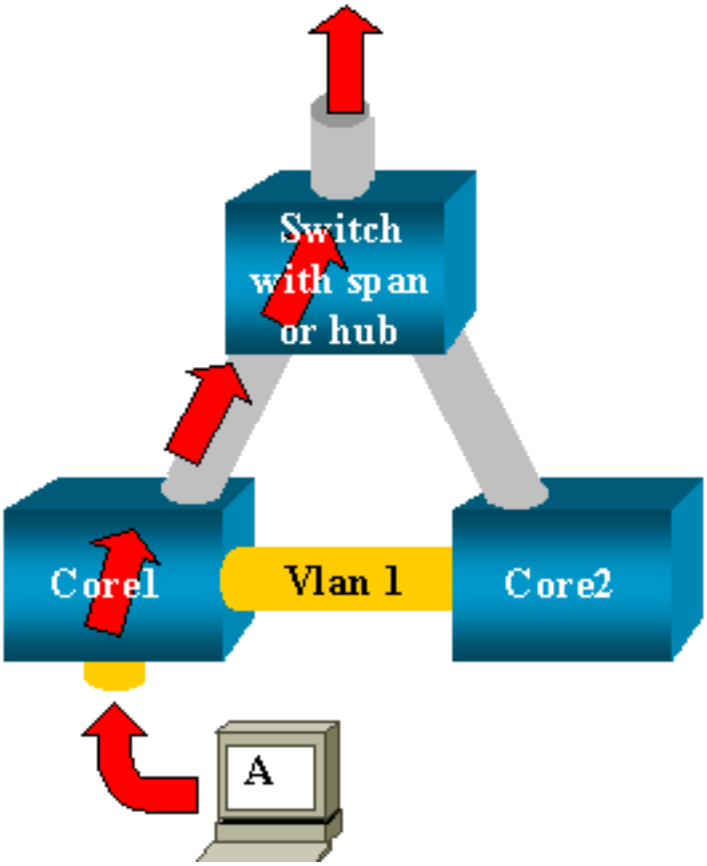
Wanneer havens voor controle worden spandoeken, toont de havenstaat als UP/DOWN.

Wanneer u een SPAN-sessie configureren om de poort te bewaken, toont de doelinterface de status omlaag (controle), door ontwerp. De interface toont de haven in deze staat om duidelijk te maken dat de haven momenteel niet als productiehaven kan worden gebruikt. De haven is normaal als omhoog/omlaag controle.

Waarom creëert de SPAN-sessie een overbruggingslening?

De creatie van een overbruggingslus gebeurt doorgaans wanneer de beheerder de RSPAN-functie negeert. Ook kan een configuratiefout het probleem veroorzaken.

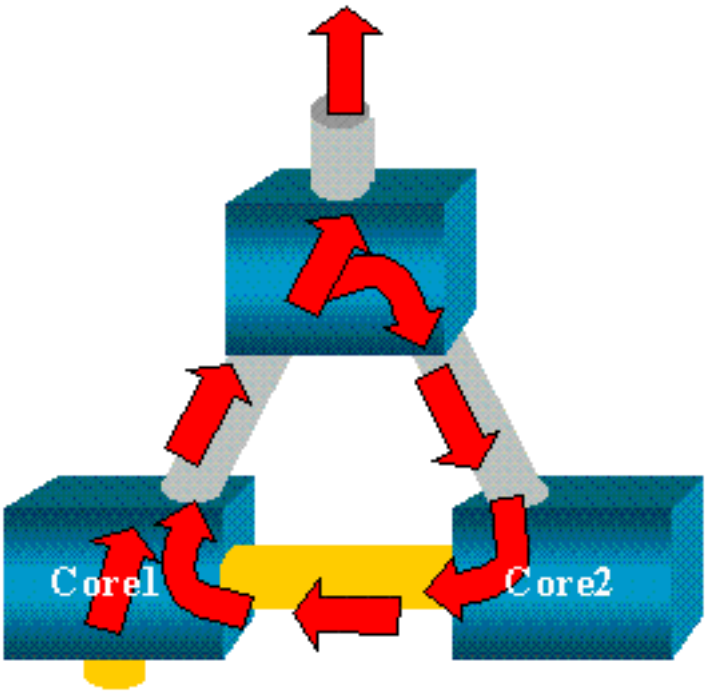
Dit is een voorbeeld van het scenario:



Er zijn twee kernswitches die verbonden zijn door een stam. In dit geval heeft elke switch meerdere servers, klanten of andere bruggen die ermee verbonden zijn. De beheerder wil VLAN 1 controleren, dat op verscheidene bruggen met SPAN verschijnt. De beheerder creëert een SPAN zitting die heel VLAN 1 op elke kernschakelaar controleert, en, om deze twee sessies samen te voegen, sluit de bestemmingspoort aan de zelfde hub (of de zelfde schakelaar, met het gebruik van een andere SPAN zitting).

De beheerder bereikt het doel. Elk pakket dat een kernschakelaar op VLAN 1 ontvangt wordt gedupliceerd op de SPAN poort en naar de hub doorgestuurd. Een sluipschutter vangt uiteindelijk het verkeer.

Het enige probleem is dat het verkeer ook in kern 2 wordt teruggebracht door de bestemming SPAN-poort. De herjectie van het verkeer in kern 2 leidt tot een overbruggingslus in VLAN 1. Vergeet niet dat een bestemmingSPAN poort geen STP voert en niet in staat is om zo een lus te verhinderen.



Opmerking: Vanwege de introductie van de optie Invoerpakketten op CatOS laat een SPAN-doelpoort elk inkomend pakket standaard vallen, waardoor dit mislukkingsscenario wordt voorkomen. Maar het potentiële probleem is nog steeds aanwezig op Catalyst 2900XL/3500XL Series switches.

Opmerking: Zelfs wanneer de optie Inches de lus voorkomt, kan de configuratie die deze sectie toont problemen in het netwerk veroorzaken. Netwerkproblemen kunnen zich voordoen vanwege MAC-adresleerproblemen die worden geassocieerd met leren en die zijn ingeschakeld op de doelpoort.

Voert SPAN-impact prestaties?

Zie deze secties van dit document voor informatie over het prestatieseffect voor de gespecificeerde platforms van de Catalyst:

- Catalyst 2900XL/3500XL Series switch
- Catalyst 4500/4000 Series-switches
- Catalyst 5500/5000 en 6500/6000 Series switch

Kan je de SPAN configureren in een EtherChannel-poort?

Een EtherChannel vormt geen vorm indien een van de havens in de bundel een SPAN-bestemming is. Als u probeert om SPAN in deze situatie te configureren vertelt de schakelaar u:

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

U kunt een poort in een EtherChannel-bundel als een SPAN-bronpoort gebruiken.

Kun je meerdere SPAN sessies tegelijkertijd laten draaien?

Op Catalyst 2900XL/3500XL Series switches is het aantal doelpoorten dat beschikbaar is op de switch de enige limiet voor het aantal SPAN-sessies.

Op Catalyst 2950 Series switches kunt u op elk moment slechts één toegewezen monitor-poort hebben. Als u een andere poort selecteert als de monitor poort, wordt de vorige monitor poort uitgeschakeld en wordt de nieuwe geselecteerde poort de monitor poort.

Op Catalyst 4500/4000, 5500/5000 en 6500/6000 switches met CatOS 5.1 en hoger kunt u meerdere gelijktijdige SPAN-sessies hebben. Zie de secties van dit document voor verschillende gelijktijdige sessies en functieoverzicht en beperkingen.

Fout "% lokale sessielimiet is overschreden"

Dit bericht verschijnt wanneer de toegestane SPAN-sessie de limiet voor de Supervisor Engine overschrijdt:

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

Supervisor Engine heeft een beperking van SPAN sessies. Raadpleeg het gedeelte *Local SPAN, RSPAN en ERSPAN Session Limits* van de Local SPAN, RSPAN en ERSPAN voor meer informatie.

Kan een SPAN-sessie op de VPN-servicemodule niet verwijderen met de fout "% sessie [Sessienummer:] gebruikt door servicemodule"

Met deze kwestie, wordt de Virtual Private Network (VPN) module in het chassis opgenomen, waar al een module van de switchfabric is ingevoegd. De Cisco IOS-software maakt automatisch een SPAN-sessie voor de VPN-servicemodule om het multicast verkeer aan te pakken.

Geef deze opdracht uit om de SPAN-sessie te verwijderen die de software maakt voor de VPN-servicemodule:

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

> Opmerking: Als u de sessie verwijdert, laat de VPN servicemodule het multicast verkeer vallen.

Waarom bent u niet in staat gecorrumpeerde pakketten met SPAN op te nemen?

U kunt geen gecorrumpeerde pakketten met SPAN opnemen vanwege de manier waarop de switches in het algemeen werken. Wanneer een pakje door een schakelaar gaat, komen deze gebeurtenissen voor:

1. Het pakje bereikt de ingangspoort.
2. Het pakje wordt in ten minste één buffer opgeslagen.
3. Het pakket wordt uiteindelijk opnieuw verzonden op de uitgang.

Als de switch een gecorrumpeerd pakket ontvangt, daalt de ingangspoort gewoonlijk het pakket. Daarom ziet u het pakje niet op de uitgang. Een verschuiving is niet volledig transparant met betrekking tot de verkeersopnamen. Op dezelfde manier, wanneer u een gecorrumpeerd pakje op uw sluipschutter in het scenario in deze sectie ziet, weet u dat de fouten bij stap 3 werden gegenereerd op het graafsegment.

Als u denkt dat een apparaat gecorrumpeerde pakketten verstuurt, kunt u ervoor kiezen om de verzendende host en het snifferapparaat op een hub te zetten. De hub voert geen foutcontroles uit. Daarom, in tegenstelling tot de schakelaar, laat de hub de pakketten niet vallen. U kunt de pakketten dus bekijken.

Fout: %-sessie 2 gebruikt door servicemodule

Als bijvoorbeeld een Firewall Service Module (FWSM) later geïnstalleerd en verwijderd werd in de CAT6500, dan heeft deze automatisch de **SPAN Reflector-functie ingeschakeld**. De SPAN Reflector-functie gebruikt één SPAN-sessie in de switch. Als u dit niet langer nodig hebt, zou u de **opdracht** van de **de** module van de **monitor** van de **module** van de **monitor** moeten kunnen invoeren van binnen de configuratie van CAT6500, en dan onmiddellijk de nieuwe gewenste SPAN configuratie ingaan.

Pakketten voor reflector-poortdruppels

Een reflectorpoort ontvangt exemplaren van verzonden en ontvangen verkeer voor alle gecontroleerde bronhavens. Als een reflectorpoort wordt oversubscript, kan dit verstopt raken. Dit kan van invloed zijn op de verkeersdoorgifte op een of meer bronhavens. Als de bandbreedte van de reflectiepoort niet voldoende is voor het verkeersvolume van de corresponderende bronpoorten, worden de overtollige pakketten ingetrokken. Een 10/100 poort wijst op 100 Mbps. Een Gigabit-poort wijst op 1 Gbps.

SPAN-sessie wordt altijd met een FWSM gebruikt in Catalyst 6500-chassis

Wanneer u Supervisor Engine 720 met een FWSM in het chassis gebruikt dat Cisco Native IOS draait, wordt standaard een SPAN-sessie gebruikt. Als u op ongebruikte sessies controleert met de opdracht **monitor**, wordt *sessie 1* gebruikt:

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

Wanneer een firewallmap zich in het Catalyst 6500 chassis bevindt, wordt deze sessie automatisch geïnstalleerd ter ondersteuning van hardware-multicast replicatie omdat een FWSM multicast stromen niet kan repliceren. Als multicast stromen die zich achter FWSM bevinden moeten worden gerepliceerd bij Layer 3 naar meerdere lijnkaarten, kopieert de automatische sessie het verkeer naar de supervisor via een weefselkanaal.

Als u een multicast bron hebt die een multicast stroom van achter de FWSM genereert, hebt u de SPAN reflector nodig. Als u de multicast bron op het externe VLAN plaatst, is de SPAN reflector niet nodig. De SPAN-reflector is niet compatibel met het overbruggen van BPDU's via het FWSM. U kunt de **opdracht** van de **servicemodule voor de monitor niet** gebruiken om de SPAN-reflector uit te schakelen.

Kunnen een SPAN- en een RSPAN-sessie dezelfde ID hebben binnen dezelfde switch?

Nee, het is niet mogelijk om dezelfde sessie-ID te gebruiken voor een reguliere SPAN-sessie en RSPAN-doelsessie. Elke SPAN- en RSPAN-sessie moet een andere sessie-ID hebben.

Kan een RSPAN-sessie over verschillende VTP-domeinen werken?

Ja. Een RSPAN-sessie kan over verschillende VTP-domeinen gaan. Maar zorg ervoor dat RSPAN VLAN in de databases van deze VTP-domeinen aanwezig is. Zorg er ook voor dat er geen Layer 3 apparaat aanwezig is in het pad van sessiebron naar sessiebestemming.

Kan een RSPAN-sessie over WAN of verschillende netwerken werken?

Nr. RSPAN-sessie kan geen Layer 3-apparaat oversteken omdat RSPAN een LAN (Layer 2) functie is. Om verkeer via een WAN of verschillende netwerken te bewaken, gebruikt u de ingekapselde Remote SwitchPort Analyser (ERSPAN). De functie ERSPAN ondersteunt bronpoorten, bron VLAN's en doelpoorten op verschillende switches, die afstandsbediening van meerdere switches via uw netwerk mogelijk maken.

ERSPAN bestaat uit een ERSPAN-bronsessie, routeerbaar ERSPAN GRE-ingekapseld verkeer en een ERSPAN-doelsessie. U vormt afzonderlijk ERSPAN bron sessies en doelsessies op verschillende switches.

Op dit moment wordt de ERSPAN-functie ondersteund in:

- Supervisor 720 met PFC3B of PFC3BXL met Cisco IOS-softwarerelease 12.2(18)SXE of hoger
- Supervisor 720 met PFC3A dat hardwareversie 3.2 of hoger heeft en Cisco IOS-softwarerelease 12.2(18)SXE of hoger heeft

Raadpleeg Local SPAN, Remote SPAN (RSPAN) en Encapsulation RSPAN - Catalyst 6500 Series Cisco IOS-softwareconfiguratie Guide, 12.2SX voor meer informatie over ERSPAN.

Kan een RSPAN-bronsessie en de doelsessie op dezelfde Catalyst-switch bestaan?

Nee. RSPAN werkt niet wanneer de RSPAN-bronsessie en de RSPAN-doelsessie dezelfde schakelaar hebben.

Als een RSPAN-bronsessie wordt geconfigureerd met een bepaald RSPAN VLAN en een RSPAN-doelsessie voor dat RSPAN VLAN is geconfigureerd op dezelfde switch, dan zal de doelpoort van de RSPAN-doelsessie de opgenomen pakketten niet verzenden vanuit de RSPAN-bronsessie vanwege hardwarebeperkingen. Dit wordt niet ondersteund op de 4500 Series- en 3750 Series-switches. Dit probleem is gedocumenteerd in Cisco bug-ID CSCeg08870 (alleen geregistreerde klanten).

Dit is een voorbeeld:

```
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
```

Het idee achter dit systeem is om de reguliere SPAN's te gebruiken.

Network Analyzer/Security-apparaat dat is aangesloten op de SPAN-doelpoort is niet bereikbaar

Het basiskenmerk van een haven van bestemming van SPAN is dat deze geen enkel verkeer doorgeeft, behalve het verkeer dat voor de SPAN-sessie vereist is. Als u de netwerkanalyzer/het security apparaat via de SPAN-doelpoort moet bereiken (IP bereikbaarheid), moet u het doorsturen van toegangsverkeer inschakelen.

Wanneer het binnendringen wordt geactiveerd, aanvaardt de SPAN bestemming binnenkomende pakketten, die potentieel getagd worden dat van de gespecificeerde insluitingsmodus afhangt, en verandert hen normaal. Wanneer u een SPAN-doelpoort vormt, kunt u specificeren of de ingress-functie al dan niet is ingeschakeld en welke VLAN's moeten worden gebruikt om niet-getagde ingangspakketten in te schakelen. De specificatie van een inbraakVLAN is niet vereist wanneer ISL-insluiting wordt ingesteld, omdat alle ISL-ingekapselde pakketten die VLAN-tags hebben, zijn ingesloten. Hoewel de haven STP door het sturen is, neemt het niet aan STP deel, gebruik daarom voorzichtigheid wanneer u deze eigenschap aanpast opdat een overspits-boomlijn in het netwerk wordt geïntroduceerd. Wanneer zowel ingress als een insluiting van de romp op een SPAN-doelpoort worden gespecificeerd, wordt de poort in alle actieve VLAN's verzonden. De configuratie van een niet-bestaand VLAN als ingress VLAN is niet toegestaan.

de *interface van de* bestemmingssessie *sessie_number* [insluiting*]* sl | dot1q}] ingress [vlan *vlan_IDs*]

Dit voorbeeld toont hoe te om een bestemmingspoort met insluiting 802.1q en ingangspakketten met het gebruik van inheems VLAN 7 te vormen.

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

Met deze configuratie wordt verkeer van SPAN-bronnen die bij sessie 1 zijn gekoppeld, gekopieerd van interface Fast Ethernet 5/48, met insluiting van 802.1q. Het inkomende verkeer wordt geaccepteerd en geschakeld, met niet-gelabelde pakketten geclassificeerd in VLAN 7.

Gerelateerde informatie

- Hoe te om SPAN en RSPAN op Cisco Catalyst 4500-switches te configureren die Cisco IOS-software gebruiken
- Een SPAN-doelpoort wordt weergegeven als 'niet aangesloten' en communiceert niet met de rest van het netwerk
- Productondersteuning voor switches
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems