Configureer Catalyst Switched Port Analyzer (SPAN): voorbeeld

Inhoud

Inleiding

In dit document worden de recent geïmplementeerde functies van de Switched Port Analyzer (SPAN) beschreven.

Voorwaarden

Catalyst-Switches die SPAN, RSPAN en ERSPAN ondersteunen

Catalyst-Switches	Ondersteuning van SPAN	RSPAN-ondersteuning	Ondersteuning van ERSPAN
Catalyst Express 5500/5200 Series	Ja	Nee	Nee
Catalyst 6500/6000 Series software	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 die hardwareversie 3.2 of hoger heeft en waarop Cisco IOS-softwarerelease 12.2(18)SXE of

			hoger wordt uitgevoerd
Catalyst 5500/5000 Series software	Ja	Nee	Nee
Catalyst 4900 Series switches	Ja	Ja	Nee
Catalyst 4500/4000 Series (inclusief 4912G)	Ja	Ja	Nee
Catalyst 3750 Metro Series	Ja	Ja	Nee
Catalyst 3750/3750E/3750X Series	Ja	Ja	Nee
Catalyst 3560/3560E/3650X Series	Ja	Ja	Nee
Catalyst 3550 Series software	Ja	Ja	Nee
Catalyst 3500-XL Series	Ja	Nee	Nee
Catalyst 2970 Series software	Ja	Ja	Nee
Catalyst 2960 Series switches	Ja	Ja	Nee
Catalyst 2955 Series software	Ja	Ja	Nee
Catalyst 2950 Series switches	Ja	Ja	Nee
Catalyst 2940 Series software	Ja	Nee	Nee
Catalyst 2948G-L3	Nee	Nee	Nee
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A switch	Ja	Ja	Nee
Catalyst 2900XL Series	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 de Catalyst 4500/4000, 5500/5000 en 6500/6000 Series Switches. Op de Switches van Catalyst 2900XL/3500XL Series wordt Cisco IOS®-softwarerelease 12.0(5)XU gebruikt.

Hoewel dit document wordt bijgewerkt om de wijzigingen in SPAN weer te geven, raadpleegt u de opmerkingen in de documentatie over het platform van de switch voor de meest recente ontwikkelingen met betrekking tot 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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De functie SPAN, die soms poortspiegeling of poortbewaking wordt genoemd, selecteert netwerkverkeer voor analyse door een netwerkanalyzer. De netwerkanalyzer kan een Cisco SwitchProbe-apparaat of andere Remote Monitoring (RMON)-sonde zijn.

Eerder, was SPAN een vrij basiseigenschap op de switches van Cisco Catalyst Series. Echter, de nieuwste releases van Catalyst OS (CatOS) introduceerden grote verbeteringen en veel nieuwe mogelijkheden die nu beschikbaar zijn voor de gebruiker.

Dit document is niet bedoeld als alternatieve configuratiehandleiding voor de functie SPAN. Dit document beantwoordt de meest voorkomende vragen over SPAN, zoals:

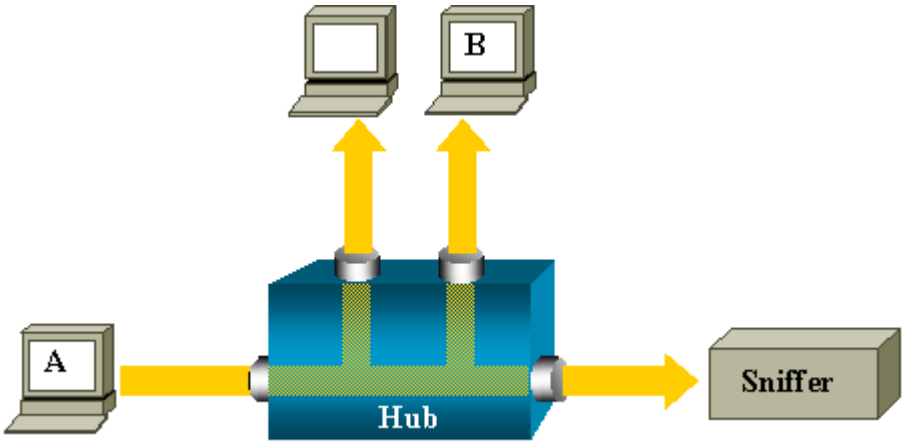
- Wat is SPAN en hoe configureert u het?
- Wat zijn de verschillende beschikbare functies (met name meerdere gelijktijdige SPAN-sessies) en welk softwareniveau is nodig om deze uit te voeren?
- Heeft SPAN invloed op de prestaties van de switch?

Korte beschrijving van SPAN

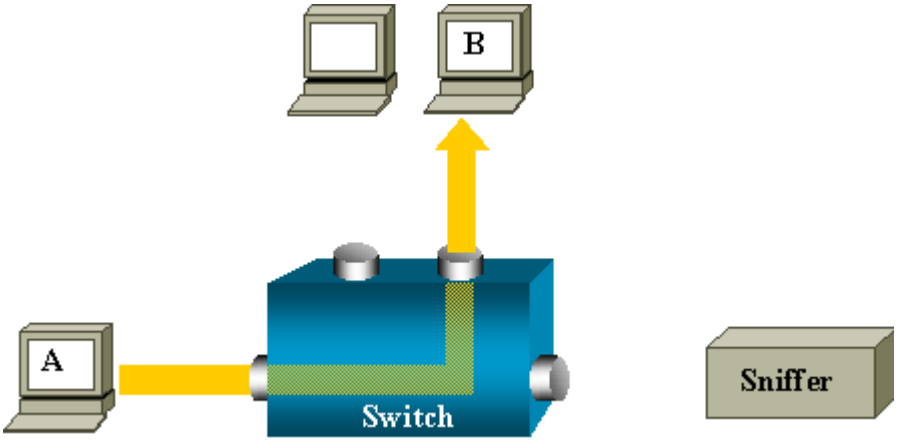
De functie SPAN is op switches geïntroduceerd vanwege een fundamenteel verschil dat switches met hubs hebben. Wanneer een hub een pakket op één poort ontvangt, stuurt de hub een kopie van dat pakket op alle poorten behalve op de poort waar de hub het pakket heeft ontvangen.

Na een switch boots, begint het om een Layer 2 doorsturen tabel op te bouwen op basis van het bron MAC-adres van de verschillende pakketten die de switch ontvangt. Nadat deze doorsturen tabel is gemaakt, wordt het switch voorwaartse verkeer dat is bestemd voor een MAC-adres direct naar de corresponderende poort.

Bijvoorbeeld, om Ethernet verkeer op te nemen dat door gastheer A naar gastheer B wordt verzonden, en allebei met een hub worden verbonden, maak enkel een snuiver aan deze hub vast. Alle andere havens zien het verkeer tussen hosts A en B:



Op een switch, nadat het host B MAC-adres is aangeleerd, wordt unicastverkeer van A naar B alleen doorgestuurd naar de B-poort. Daarom ziet sniffer dit verkeer niet:



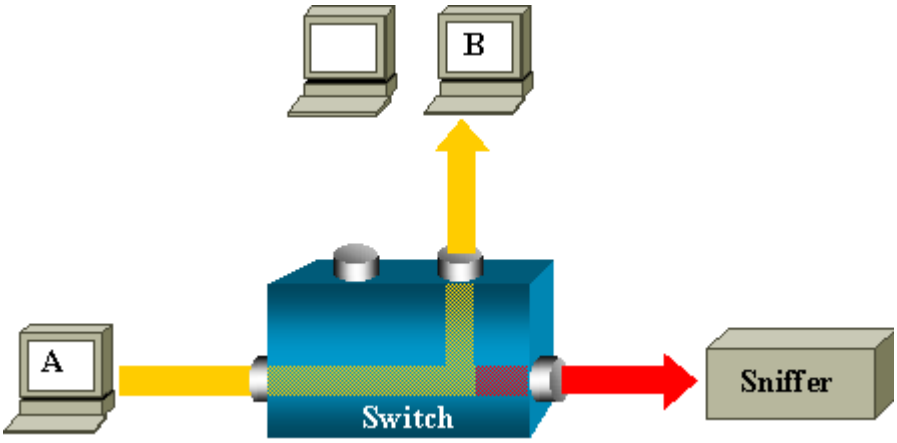
In deze configuratie neemt de snuifschakelaar alleen verkeer op dat naar alle poorten is overstroomd, zoals:

- Uitzendverkeer
- Multicast-verkeer met blokkering van CGMP- of Internet Group Management Protocol (IGMP)-snooping
- Onbekend unicastverkeer

Unicast-overstroming treedt op wanneer de switch niet de doelmap MAC heeft in zijn Content-Adressable Memory (CAM) tabel.

De switch weet niet waar hij het verkeer moet versturen. De switch overspoelt de pakketten naar alle poorten in de doelmap VLAN.

Een extra functie is nodig dat kunstmatig unicastpakketten die host A naar de snifferpoort verzendt:

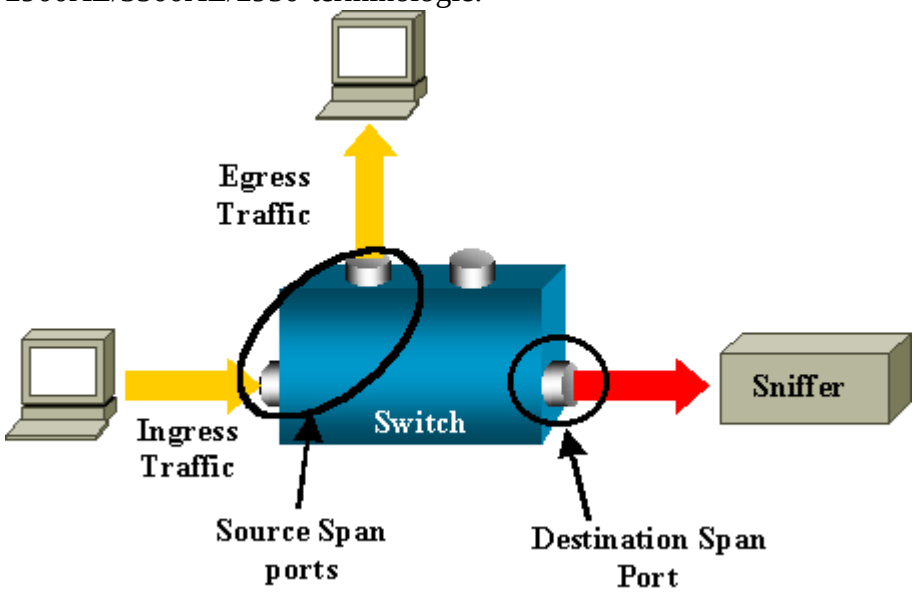


In dit diagram is het snuifje gekoppeld aan een poort die is geconfigureerd om een kopie te ontvangen van elk pakket dat door de host A wordt verzonden. Deze poort wordt een SPAN-poort genoemd.

In de andere delen van dit document wordt beschreven hoe u deze functie zeer nauwkeurig kunt afstemmen om meer te doen dan alleen een poort te bewaken.

SPAN-terminologie

- **Ingress verkeer**â€"verkeer dat de switch ingaat.
- **Uitgaand verkeer**â€"verkeer dat de switch verlaat.
- **Source (SPAN) poort** â€"Een poort die wordt bewaakt met gebruik van de SPAN-functie.
- **Source (SPAN) VLAN** â€"Een VLAN waarvan het verkeer wordt gecontroleerd met gebruik van de SPAN-functie.
- **Bestemming (SPAN) poort** â€"Een poort die bronpoorten bewaakt, meestal waar een netwerkanalyzer is aangesloten.
- **Reflector-poort** â€"een poort die pakketten kopieert naar een RSPAN VLAN.
- **Monitorpoort**â€"Een monitorpoort is ook een bestemmingshaven SPAN in Catalyst 2900XL/3500XL/2950-terminologie.



- **Lokale** SPANâ€”de functie SPAN is lokaal wanneer de bewaakte poorten zich allemaal op dezelfde switch bevinden als de bestemmingshaven. Deze optie is in tegenstelling tot Remote SPAN (RSPAN), dat ook in deze lijst wordt gedefinieerd.

- **Remote SPAN (RSPAN)**â€”Sommige bronpoorten bevinden zich niet op dezelfde switch als de doelpoort.

RSPAN is een geavanceerde functie 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 release opmerkingen of configuratiehandleiding om te zien of u RSPAN kunt gebruiken op de switch die u implementeert.

- **Op poort gebaseerde SPAN (PSPAN)**â€”De gebruiker specificeert een of meer bronpoorten op de switch en een doelpoort.

- **Op VLAN gebaseerde SPAN (VSPAN)**â€”Op een bepaalde switch kan de gebruiker ervoor kiezen alle poorten die tot een bepaald VLAN behoren, in één opdracht te bewaken.

- **ESPAN**â€”Dit betekent een uitgebreide SPAN-versie. Deze term is tijdens de evolutie van de SPAN meerdere malen gebruikt om extra functies te benoemen, daarom is de term niet erg duidelijk en wordt deze in dit document vermeden.

- **Administratieve bron**â€”Een lijst van bronpoorten of VLANâ€™s die zijn geconfigureerd voor bewaking.

- **Operationele bron**-Een lijst van havens die effectief worden gecontroleerd. Deze lijst van poorten kan verschillen van de administratieve bron.

Een poort die zich in de sluitmodus bevindt, kan bijvoorbeeld in de beheerbron verschijnen, maar wordt niet effectief bewaakt.

Kenmerken van bronpoort

Een bronpoort, ook wel een bewaakte poort genoemd, is een switched of routed poort die u bewaakt voor netwerkverkeersanalyse.

In één lokale SPAN-sessie of RSPAN-bronsessie kunt u bronpoortverkeer, zoals ontvangen (Rx), verzonden (Tx) of bidirectioneel (beide), bewaken.

De switch ondersteunt elk aantal bronpoorten (tot het maximale aantal beschikbare poorten op de switch) en elk aantal VLAN-bronpoorten.

Een bronpoort heeft de volgende kenmerken:

- Het kan elk poorttype zijn, zoals EtherChannel, Fast Ethernet, Gigabit Ethernet, enzovoort.

- Het kan in meerdere SPAN-sessies worden gevolgd.

- Het kan geen bestemmingshaven zijn.

- Elke bronpoort kan worden geconfigureerd met een richting (toegang, uitgang of beide) om te monitoren. Voor EtherChannel-bronnen geldt de bewaakte richting voor alle fysieke poorten in de groep.

- De bronpoorten kunnen in hetzelfde of verschillende VLANâ€™s zijn.

- Voor VLAN SPAN-bronnen zijn alle actieve poorten in de bron-VLAN opgenomen als bronpoorten.

VLAN-filtering

Wanneer u een trunkpoort als bronpoort controleert, worden alle VLANâ€™s die actief zijn in de trunk standaard gecontroleerd. U kunt VLAN-filtering gebruiken om de bewaking van SPAN-verkeer op trunkbronpoorten te beperken tot specifieke VLANâ€™s.

- VLAN-filtering is alleen van toepassing op trunkpoorten of 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 is gespecificeerd, worden alleen die VLANâ€™s in de lijst gecontroleerd op trunkpoorten of op spraak-VLAN-toegangspoorten.
- Het SPAN-verkeer dat afkomstig is van andere poorttypen wordt niet beïnvloed door VLAN-filtering, wat betekent dat alle VLANâ€™s zijn toegestaan op andere poorten.
- VLAN-filtering heeft alleen invloed op verkeer dat wordt doorgestuurd naar de bestemmingshaven van SPAN en heeft geen invloed op de switching van normaal verkeer.
- U kunt bron-VLANâ€™s niet combineren met filter-VLANâ€™s binnen een sessie. U kunt bron VLANâ€™s of filter VLANâ€™s hebben, maar niet beide tegelijk.

Kenmerken van Source VLAN

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

VSPAN heeft deze kenmerken:

- Alle actieve poorten in de bron-VLAN zijn opgenomen als bronpoorten en kunnen in beide of beide richtingen worden bewaakt.
- Op een bepaalde poort wordt alleen verkeer op het bewaakte VLAN naar de bestemmingshaven verzonden.
- Als een bestemmingshaven tot een bron VLAN behoort, wordt het uitgesloten van de bronlijst en niet gecontroleerd.
- Als poorten worden toegevoegd aan of verwijderd uit de bron-VLANâ€™s, wordt het verkeer op de bron-VLAN dat door die poorten wordt ontvangen, toegevoegd aan of verwijderd uit de bronnen die worden bewaakt.
- U kunt filter VLANâ€™s niet in dezelfde sessie met VLAN-bronnen gebruiken.
- U kunt alleen Ethernet VLANâ€™s controleren.

Kenmerken van de bestemmingshaven

Elke lokale SPAN-sessie of RSPAN-doelsessie moet een bestemmingshaven hebben (ook een controlepoort genoemd) die een kopie van verkeer ontvangt van de bronpoorten en VLANâ€™s.

Een bestemmingshaven heeft deze kenmerken:

- Een bestemmingshaven moet zich op dezelfde switch bevinden als de bronpoort (voor een lokale SPAN-sessie).
- Een bestemmingshaven kan om het even welke fysieke haven zijn Ethernet.
- Een bestemmingshaven kan slechts aan één SPAN-sessie tegelijkertijd deelnemen. Een bestemmingshaven in één SPAN-sessie kan geen bestemmingshaven zijn voor een tweede SPAN-sessie.
- Een bestemmingshaven kan geen bronpoort zijn.
- Een bestemmingshaven kan geen EtherChannel-groep zijn.

> **Opmerking**: van Cisco IOS-softwarerelease 12.2(33)SRE en hoger kan de PortChannel-interface een doelpoort zijn. Bestemming EtherChannel ondersteunt de EtherChannel-protocollen (Port Aggregation Control Protocol, PAgP) of Link Aggregation Control Protocol (LACP) niet. Alleen de on-modus wordt ondersteund, waarbij alle EtherChannel-protocolondersteuning is uitgeschakeld.

> **Opmerking**: raadpleeg de bestemmingen Local SPAN, RSPAN en ERSPAN voor meer informatie.

- Een bestemmingshaven kan een fysieke poort zijn die aan een EtherChannel-groep is toegewezen, zelfs als de EtherChannel-groep als een SPAN-bron is gespecificeerd. De poort wordt uit de groep verwijderd terwijl deze is geconfigureerd als een SPAN-doelpoort.
- De poort verzendt geen verkeer behalve dat verkeer dat vereist is voor de SPAN-sessie tenzij leren is ingeschakeld. Als het leren wordt toegelaten, brengt de haven ook verkeer over dat aan gastheren wordt geleid die op de bestemmingshaven zijn geleerd.

> **Opmerking**: raadpleeg de bestemmingen Local SPAN, RSPAN en ERSPAN voor meer informatie.

- De staat van de bestemmingshaven is omhoog/omlaag door ontwerp. De interface toont de haven in deze staat om duidelijk te maken dat de haven momenteel niet bruikbaar is als productiehaven.
- Als het doorsturen van toegangsverkeer is ingeschakeld voor een netwerkbeveiligingsapparaat. De bestemmingshaven voorwaarts verkeer bij Layer 2.
- Een bestemmingshaven neemt niet deel aan het overspannen - boom terwijl de zitting van de SPANWIJDTE actief is.
- Wanneer het een bestemmingshaven is, neemt het niet aan om het even welke Layer 2-protocollen deel (STP, VTP, CDP, DTP, PagP).
- Een bestemmingshaven die tot een bron VLAN van om het even welke zitting van de SPAN behoort is uitgesloten van de bronlijst en niet gecontroleerd.
- Een bestemmingshaven ontvangt kopieën van verzonden en ontvangen verkeer voor alle gecontroleerde bronpoorten. Als een bestemmingshaven oversubscribed is, kan het verstopt worden.

Deze congestie kan het doorsturen van verkeer op een of meer van de bronpoorten beïnvloeden.

Kenmerken van Reflectorpoort

De reflectorpoort is het mechanisme waarmee pakketten naar een RSPAN VLAN worden gekopieerd. De reflectorpoort stuurt alleen het verkeer door van de RSPAN-bronsessie waarmee hij is verbonden.

Elk apparaat dat is aangesloten op een poort die is ingesteld als een reflectorpoort, verliest de verbinding totdat de RSPAN-bronsessie is uitgeschakeld.

De reflectorpoort heeft deze kenmerken:

- Het is een poort die is ingesteld op loopback.
- Het kan geen EtherChannel groep zijn, het trunk niet en het kan geen protocolfiltering uitvoeren.
- Het kan een fysieke poort zijn die is toegewezen aan een EtherChannel-groep, zelfs als de EtherChannel-groep is gespecificeerd als een SPAN-bron. 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 bestemmingshaven zijn en een poort kan ook geen reflectorpoort zijn voor meer dan één sessie tegelijk.
- Het is onzichtbaar voor alle VLANâ€™s.
- Het native VLAN voor lusbackverkeer op een reflectorpoort is RSPAN VLAN.
- De reflectorpoort loopt terug untagged verkeer naar de switch. Het verkeer wordt vervolgens op RSPAN VLAN geplaatst en overstroomd naar alle trunkpoorten die RSPAN VLAN dragen.
- Spanning Tree wordt automatisch uitgeschakeld op een reflectorpoort.
- Een reflectorpoort ontvangt kopieën van verzonden en ontvangen verkeer voor alle bewaakte bronpoorten.

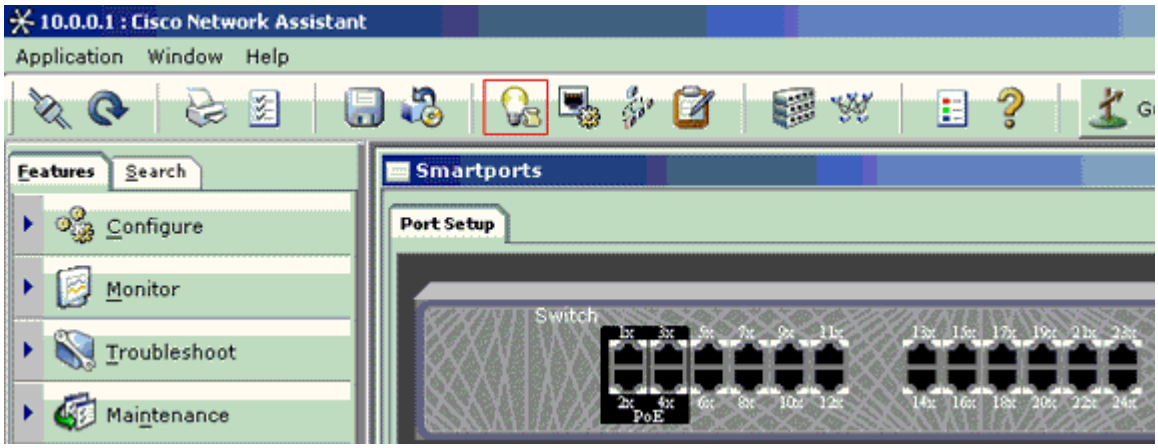
SPAN op Catalyst Express 5500/5200

Catalyst Express 5000 of Catalyst Express 520 ondersteunt alleen de functie SPAN. Catalyst Express 5500/520-poorten kunnen alleen voor SPAN worden geconfigureerd met Cisco Network Assistant (CNA). Voltooi de volgende 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. Voltooi de stappen die zijn gegeven in Getting Started Guide voor Catalyst Express 500 Switches 12.2(25)FY om de switch-instellingen voor Catalyst Express 500 aan te passen. Raadpleeg Getting Started Guide voor de Catalyst Express 520 Switches voor meer informatie over Catalyst Express 520.
3. Gebruik CNA om in te loggen op de switch en klik op **Smartport**.

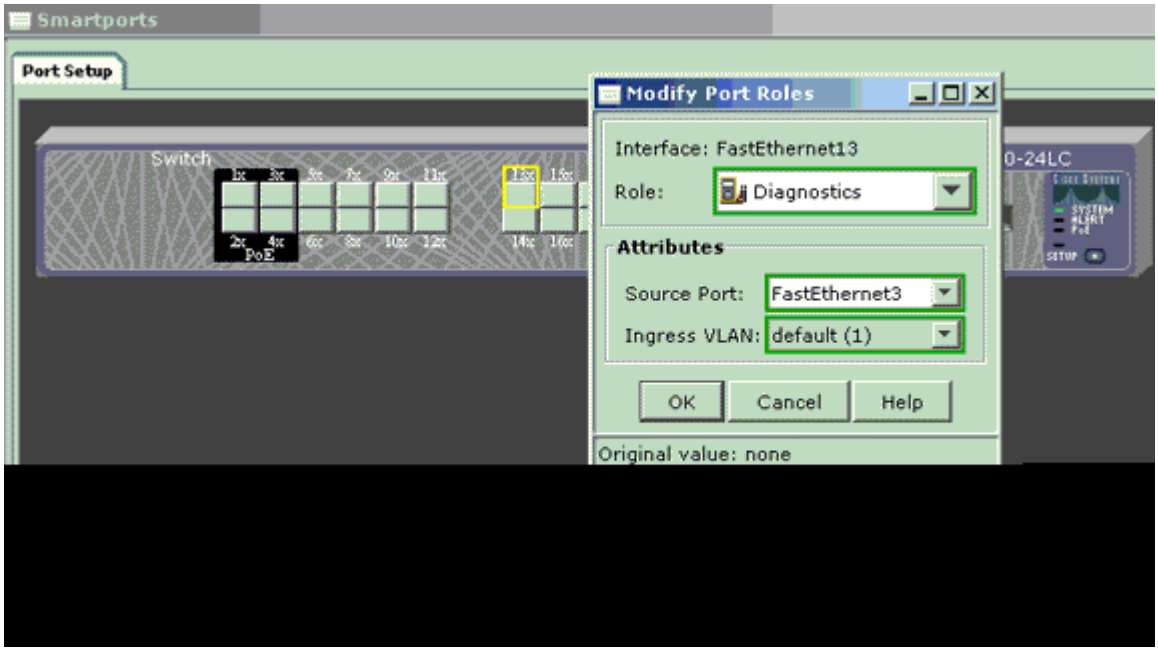


4. Klik op een willekeurige interface waar u de pc wilt aansluiten om de sporen van het snuifapparaat op te nemen.
5. Klik op **Wijzigen**.

   Er verschijnt een klein pop-upvenster.

6. Kies de rol **Diagnostiek** voor de poort.
7. Kies de bronpoort en selecteer het VLAN dat u wilt controleren.

   Als u niets selecteert, ontvangt de poort alleen verkeer. Met het Ingress VLAN kan de pc die is aangesloten op de diagnostische poort pakketten verzenden naar het netwerk dat dat VLAN gebruikt.



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

SPAN op Catalyst 2900XL/3500XL Switches

Functies die beschikbaar en beperkt zijn

De poortbewakingsfunctie is niet erg uitgebreid op Catalyst 2900XL/3500XL. Daarom is deze eigenschap

vrij gemakkelijk te begrijpen.

U kunt zo veel lokale PSPAN-sessies maken als nodig is. U kunt bijvoorbeeld PSPAN-sessies maken op de configuratiepoort die u hebt gekozen als een bestemmings-SPAN-poort. In dit geval, geef het de **interfacebevel** uit van de **havenmonitor** om van de bronhavens een lijst te maken die u wilt controleren. Een monitorpoort is een bestemmings-SPAN-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 configureert, controleert de opdracht **poortmonitor** alleen verkeer dat naar dat IP-adres is bestemd. Het controleert ook het uitzendingsverkeer dat door de interface van VLAN wordt ontvangen. Nochtans, vangt het niet het verkeer dat in het daadwerkelijke VLAN zelf stroomt. Als u geen interface in het bevel van de **poortmonitor** specificeert, worden alle andere poorten die tot hetzelfde VLAN behoren als de interface gecontroleerd.

Deze lijst bevat een aantal beperkingen. Verwijs naar de opdrachtreferentiegids (Catalyst 2900XL/3500XL) voor meer informatie.

Opmerking: ATM-poorten zijn de enige poorten die geen monitorpoorten kunnen zijn. U kunt ATM-poorten echter wel bewaken. De beperkingen in deze lijst zijn van toepassing op poorten die de poortmonitorcapaciteit hebben.

- Een monitorpoort kan niet in een Fast EtherChannel- of Gigabit EtherChannel-poortgroep worden geplaatst.
- Een monitorpoort kan niet worden ingeschakeld voor poortbeveiliging.
- Een monitorpoort kan geen multi-VLAN-poort zijn.
- Een monitorpoort moet lid zijn van hetzelfde VLAN als de poort die wordt bewaakt. VLAN-lidmaatschapswijzigingen zijn niet toegestaan op monitorpoorten en poorten die worden bewaakt.
- Een monitorpoort kan geen poort met dynamische toegang of een trunkpoort zijn. Een poort met statische toegang kan echter een VLAN op een trunk, een multi-VLAN of een poort met dynamische toegang bewaken. VLAN dat wordt gecontroleerd is het VLAN dat met de statisch-toegangspoort is geassocieerd.
- Poortbewaking werkt niet als zowel de monitorpoort als de poort die wordt bewaakt beschermde poorten zijn.

Zorg ervoor dat een poort in de monitorstaat het Spanning Tree Protocol (STP) niet uitvoert, terwijl de poort nog steeds tot het VLAN van de poorten behoort die worden gespiegeld. De poortmonitor kan deel uitmaken van een lus als u deze bijvoorbeeld aansluit op een hub of een brug en op een ander deel van het netwerk. In dit geval, kunt u in een catastrofale overbruggingslijnvoorwaarde eindigen omdat STP u niet meer beschermt. Zie de sectie Waarom maakt de SPAN-sessie een overbruggingslus? van dit document voor een voorbeeld van hoe deze voorwaarde kan gebeuren.

Configuratievoorbeeld

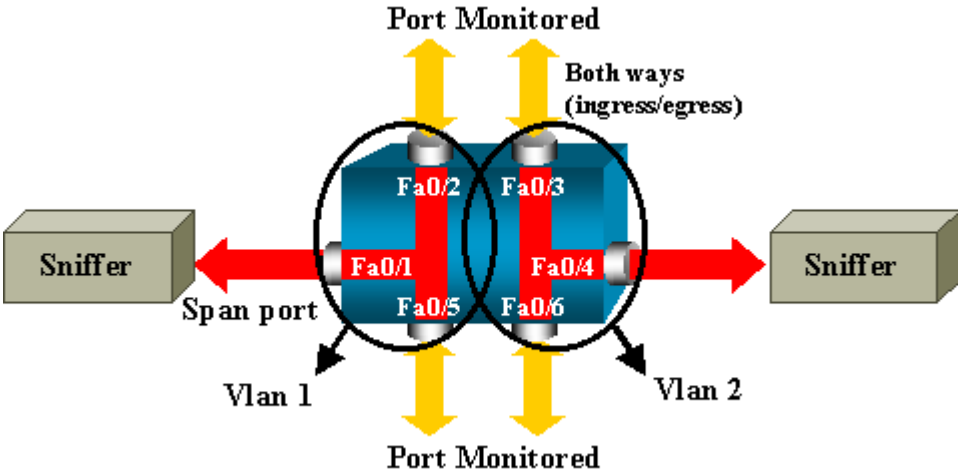
Dit voorbeeld maakt twee gelijktijdige SPAN-sessies.

- Port Fast Ethernet 10/1 (Fa0/1) controleert verkeer dat poorten Fa0/2 en Fa0/5 verzenden en ontvangen. Port Fa0/1 bewaakt 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 zijn alle geconfigureerd in VLAN 2. Andere poorten en de beheerinterface worden geconfigureerd in de 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.
```

Uitleg van configuratiestappen

Om poort Fa0/1 te configureren als een bestemmingshaven, selecteren de bronpoorten Fa0/2 en Fa0/5 en de beheerinterface (VLAN 1) de interface Fa0/1 in de configuratiemodus:

<#root>

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

Geef de lijst op van de poorten die moeten worden bewaakt:

<#root>

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

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

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

<#root>

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

> **Opmerking**: dit commando betekent niet dat poort Fa0/1 het gehele VLAN 1 bewaakt. Het sleutelwoord **VLAN 1** verwijst simpelweg naar de beheerinterface van de switch.

Dit voorbeeldbevel illustreert dat de monitor van een haven in verschillend VLAN onmogelijk is:

<#root>

```
Switch(config-if)#
port monitor fastethernet 0/3

FastEthernet0/1 and FastEthernet0/3 are in different vlan
```

Om de configuratie te voltooien, moet u een andere sessie configureren. Gebruik ditmaal Fa0/4 als een bestemmings-SPAN-poort:

```
<#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
```

Geef een **show running** commando uit of gebruik de **show port monitor** commando om de configuratie te controleren:

```
<#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
```

> **Opmerking**: de Catalyst 2900XL en 3500XL ondersteunen SPAN niet alleen in de Rx-richting (Rx SPAN of Inkomende SPAN) of alleen in de Tx-richting (Tx SPAN of uitgaande 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 switch-routers voor Layer 3-switches. De functie SPAN op een Layer 3-switch wordt poortsnuffelen genoemd.

Port-snooping wordt echter niet ondersteund op deze switches. Raadpleeg het gedeelte *Functies die niet worden ondersteund* van de opmerkingen bij documentrelease voor Catalyst 2948G-L3 en Catalyst 4908G-L3 voor Cisco IOS release 12.0(10)W5(18g).

SPAN op Catalyst 8500

Een zeer fundamentele eigenschap van SPAN is beschikbaar op Catalyst 8540 onder de naampoortsnooping. Raadpleeg de huidige Catalyst 8540-documentatie voor meer informatie.

Met poortsnuffelen kunt u verkeer vanaf een of meer bronpoorten naar een doelpoort transparant spiegelen."

Geef het **snoopbevel uit** om op poort gebaseerde traffic mirroring of snooping in te stellen. Geef **geen** vorm van dit bevel uit om het snooping onbruikbaar te maken:

<#root>

snoop interface source_port direction snoop_direction

no snoop interface source_port

De variabele ***source_port*** verwijst naar de poort die wordt bewaakt. De variabele ***snoop_direction*** is de richting van verkeer op de bronhaven of de havens die worden gecontroleerd: **ontvang**, **breng**, of **allebei over**.

<#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

Dit voorbeeld toont output van het bevel van de **showsnoop**:

<#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)
```

> **Opmerking**: deze opdracht wordt niet ondersteund op Ethernet-poorten in een Catalyst 8540 als u een Multiservice ATM switch Router (MSR)-afbeelding uitvoert, zoals 8540m-in-mz. In plaats daarvan moet u een CSR-afbeelding (campus switch router) gebruiken, zoals 8540c-in-mz.

SPAN op Catalyst 2900, 4500/4000, 5500/5000 en 6500/6000 Series Switches waarop CatOS wordt uitgevoerd

Deze sectie is alleen van toepassing voor deze Cisco Catalyst 2900 Series Switches:

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

Deze sectie is van toepassing voor Cisco Catalyst 4000 Series Switches, waaronder:

- Switches voor modulair chassis:
  - Cisco Catalyst 4003 Switch
  - Cisco Catalyst 4006 Switch
- Switch vast chassis:
  - Cisco Catalyst 4912G Switch

Lokale overloop

SPAN-functies zijn één voor één toegevoegd aan de CatOS, en een SPAN-configuratie bestaat uit één **set span** commando. Er is nu een brede waaier van opties die voor het bevel beschikbaar zijn:

<#root>

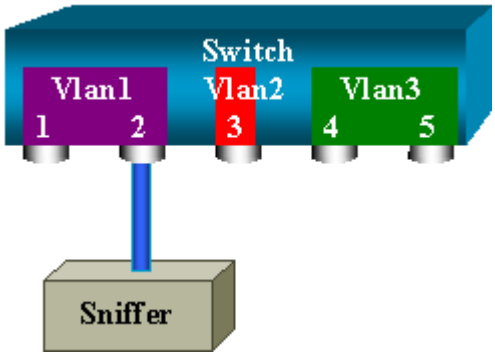
```
switch (enable)
```

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]
```

Dit netwerkdiagram introduceert de verschillende mogelijkheden van het SPAN met het gebruik van variaties:



Dit diagram vertegenwoordigt een deel van één lijnkaart die zich in sleuf 6 van een Catalyst 6500/6000 Switch bevindt. In dit scenario:

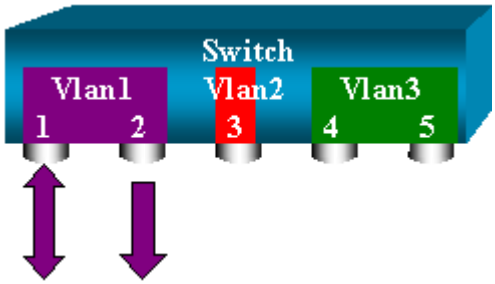
- Poorten 6/1 en 6/2 behoren tot VLAN 1
- Port 6/3 behoort tot VLAN 2
- Poorten 6/4 en 6/5 behoren tot VLAN 3

Sluit een snuffel aan op poort 6/2 en gebruik deze in verschillende gevallen als monitorpoort.

PSPAN, VSPAN: bewaakt bepaalde poorten of een volledig VLAN

Geef de eenvoudigste vorm van het **vastgestelde span**-commando uit om één poort te bewaken. De syntaxis is **ingesteld op span source_port target_port** .

Monitoren van één poort met 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
```

Met deze configuratie wordt elk pakket dat wordt ontvangen of verzonden door poort 6/1 gekopieerd op poort 6/2. Een duidelijke beschrijving van dit komt omhoog wanneer u de configuratie ingaat. Geef het **show span** commando uit om een samenvatting van de huidige SPAN-configuratie te ontvangen:

<#root>

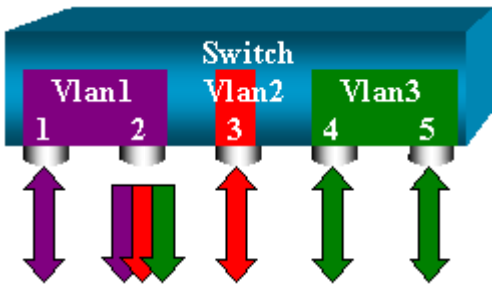
```
switch (enable)
```

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
```

Monitoren van meerdere poorten met SPAN



De **ingestelde span source_ports bestemmings_port** opdracht staat de gebruiker toe om meer dan één bronpoort te specificeren. Vermeld gewoon alle poorten waarop u de SPAN wilt implementeren en scheid de poorten met komma's.

Met de opdrachtregeltolk kunt u ook het koppelteken gebruiken om een reeks poorten te specificeren.

Dit voorbeeld illustreert dit vermogen om meer dan één poort te specificeren. In het voorbeeld wordt SPAN op poort 6/1 en een bereik van drie poorten, van 6/3 tot 6/5 gebruikt:

Opmerking: er kan maar één bestemmingshaven zijn. Specificeer altijd de bestemmingshaven na de bron van de SPAN.

<#root>

```
switch (enable)
```

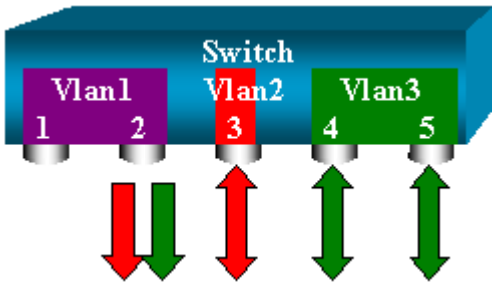
```
set span 6/1,6/3-5 6/2
```

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

Opmerking: in tegenstelling tot Catalyst 2900XL/3500XL Switches, kunnen Catalyst 4500/4000, 5500/5000 en 6500/6000 poorten controleren die behoren tot verschillende VLANâ€™s met CatOS-versies die eerder zijn dan 5.1. Hier worden de gespiegelde poorten toegewezen aan VLANâ€™s 1, 2 en 3.

Monitor VLANâ€™s met SPAN

Uiteindelijk kunt u met de **ingestelde** opdracht **span** een poort configureren om lokaal verkeer voor een volledig VLAN te bewaken. De opdracht is **ingesteld op span source_VLAN(s) target_port** .



Gebruik een lijst van één of meerdere VLANâ€™s als bron in plaats van een lijst met poorten:

<#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
```

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

> **Opmerking**: het resultaat is precies hetzelfde als wanneer u SPAN afzonderlijk implementeert op alle poorten die tot de VLANâ€™s behoren die door de opdracht worden gespecificeerd. Vergelijk het veld `Bron openen` en het veld `Bron beheren`. Het veld `Admin Source` beschrijft in principe alle poorten die u hebt geconfigureerd voor de SPAN-sessie en het veld `Open Source` toont de poorten die SPAN gebruiken.

Ingress/uitgaande SPAN

In het voorbeeld in de Monitor VLANâ€™s met SPAN-sectie wordt verkeer dat de opgegeven poorten invoert en verlaat, bewaakt.

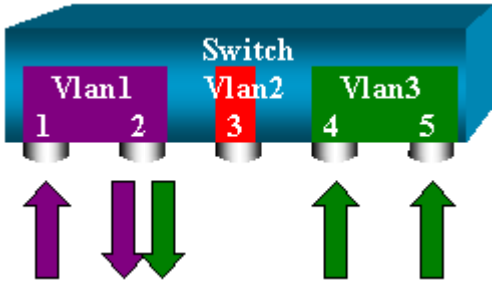
De veld `Richting: verzenden/ontvangen` toont dit. Met de Switches Catalyst 4500/4000, 5500/5000 en 6500/6000 Series kunt u alleen uitgaand verkeer of alleen inkomend verkeer op een bepaalde poort verzamelen.

Voeg het trefwoord **rx** (**ontvangstl**) of **tx** (zend) toe aan het einde van de opdracht. De standaardwaarde is **zowel** tx als rx.

<#root>

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

In dit voorbeeld, vangt de zitting al inkomend verkeer voor VLANs 1 en 3 en spiegelt het verkeer aan haven 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
```

Voer SPAN op een Trunk uit

Trunks zijn een speciaal geval in een switch omdat ze poorten zijn die verschillende VLANâ€™s dragen. Als een trunk is geselecteerd als een bronpoort, wordt het verkeer voor alle VLANâ€™s op deze trunk gecontroleerd.

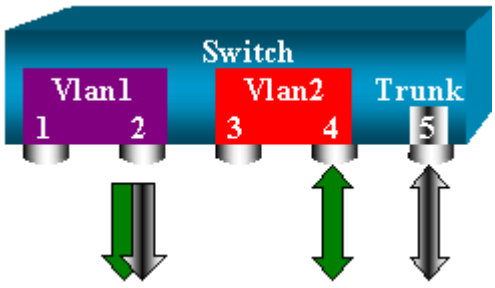
Controleer een subset van VLANâ€™s die tot een trunk behoren

In dit diagram is poort 6/5 nu een trunk die alle VLANâ€™s draagt. Stel u voor dat u SPAN wilt gebruiken op het verkeer in VLAN 2 voor poorten 6/4 en 6/5. Geef dit commando simpelweg uit:

<#root>

```
switch (enable)
```

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



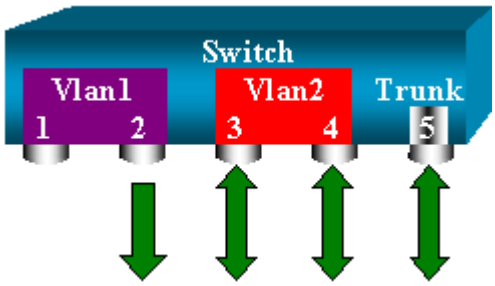
In dit geval is het verkeer dat op de SPAN-poort wordt ontvangen een mengeling van het verkeer dat u wilt en alle VLANâ€™s die trunk 6/5 draagt.

Bijvoorbeeld, is er geen manier om op de bestemmingshaven te onderscheiden of een pakket van haven 6/4 in VLAN 2 of haven 6/5 in VLAN 1 komt. Een andere mogelijkheid is het gebruik van SPAN op het gehele VLAN 2:

<#root>

```
switch (enable)
```

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



Met deze configuratie, minstens, controleert u slechts verkeer dat tot VLAN 2 van de boomstam behoort. Het probleem is dat u nu ook verkeer ontvangt dat u niet van haven 6/3 wilde.

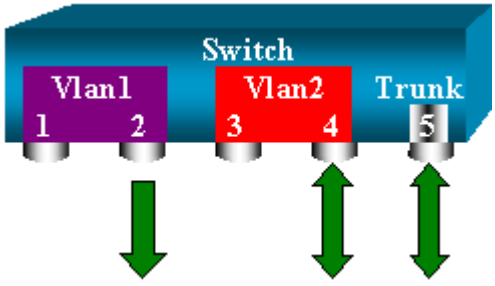
De CatOS bevat een ander trefwoord dat u in staat stelt bepaalde VLANâ€™s te selecteren om te monitoren vanuit een trunk:

<#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
```



Deze opdracht bereikt het doel omdat u VLAN 2 selecteert op alle trunks die worden bewaakt. U kunt met deze filteroptie meerdere VLANâ€™s instellen.

Opmerking: deze filteroptie wordt alleen ondersteund op Switches van Catalyst 4500/4000 en Catalyst 6500/6000. Catalyst 5500/5000 ondersteunt de filteroptie die beschikbaar is met de **ingestelde** opdracht **voor** de **reeks**.

Trunking op de doelpoort

Als u bronpoorten hebt die tot meerdere verschillende VLANâ€™s behoren, of als u SPAN op meerdere VLANâ€™s op een trunkpoort gebruikt, kunt u zich misschien afvragen tot welk VLAN een pakket behoort dat u op de bestemmingshaven van SPAN ontvangt.

Deze identificatie is mogelijk als u trunking op de bestemmingshaven inschakelt voordat u de poort voor SPAN configureert. Op deze manier worden alle pakketten die worden doorgestuurd naar de sniffer ook gelabeld met hun respectievelijke VLAN-IDâ€™s.

Opmerking: uw sniffer moet de bijbehorende inkapseling herkennen.

<#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)
```

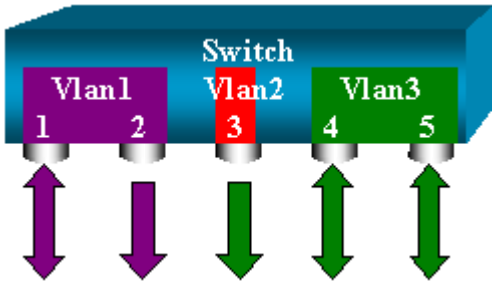
set span 6/4-5 6/2

```
      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
```

Meerdere gelijktijdige sessies maken

Tot dusver is slechts één SPAN-sessie ingesteld. Elke keer dat u een nieuwe **set span** commando uitgeeft, wordt de vorige configuratie ongeldig gemaakt. De CatOS heeft nu de mogelijkheid om meerdere sessies tegelijkertijd uit te voeren, zodat het verschillende bestemmingspoorten op hetzelfde moment kan hebben.

Geef de **vastgestelde spanwijdte bronbestemming uit creeer** bevel om een extra zitting van de SPAN toe te voegen. In deze sessie wordt poort 6/1 tot en met 6/2 bewaakt en tegelijkertijd wordt VLAN 3 tot poort 6/3 bewaakt:



<#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
```

Nu, geef het bevel van de **showspanwijdte** uit om te bepalen als u twee zittingen tezelfdertijd hebt:

<#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
```

Er worden extra sessies gemaakt. U hebt een manier nodig om bepaalde sessies te verwijderen. De opdracht is:

<#root>

set span disable {all | destination_port}

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

<#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
```

U kunt nu controleren of er nog maar één sessie over is:

<#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
```

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

<#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
```

Andere opties voor SPAN

De syntaxis van de **ingestelde** opdracht **span** is:

<#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 dit gedeelte worden de opties die in dit document worden besproken, kort beschreven:

- **sc0**â€”U specificeert het **sc0-**trefwoord in een SPAN-configuratie wanneer u het verkeer naar de beheerinterface sc0 moet bewaken. Deze functie is beschikbaar op de Catalyst 5500/5000 en Catalyst 6500/6000 Switches, codeversie CatOS 5.1 of hoger.
- **De** optie Inpkts ***Enable/deactiveren/deactiveren*** is zeer belangrijk. Zoals dit document verklaart, behoort een poort die u als SPAN-bestemming configureert nog steeds tot het oorspronkelijke VLAN. Pakketten die op een bestemmingshaven worden ontvangen gaan dan VLAN in, alsof deze haven een normale toegangshaven was. Dit gedrag kan gewenst zijn. Als u een PC als snuffelaar gebruikt, zou u deze PC volledig met VLAN kunnen willen worden verbonden. Desalniettemin kan de verbinding gevaarlijk zijn als u de bestemmingshaven aansluit op andere netwerkapparatuur die een lus in het netwerk creëert. De bestemmings-SPAN-poort voert de STP niet uit en u kunt in een gevaarlijke

overbruggingslussituatie belanden. Zie de sectie Waarom maakt de SPAN-sessie een overbruggingslus? van dit document om te begrijpen hoe deze situatie kan ontstaan. De standaardinstelling voor deze optie is uit te schakelen, wat betekent dat de bestemmings-SPAN-poort pakketten weggooit die de poort ontvangt. Deze verwerping beschermt de poort tegen overbruggingslijnen. Deze optie wordt weergegeven in CatOS 4.2.

- **leren *in-/uitschakelen*** â€"Met deze optie kunt u het leren op de bestemmingshaven uitschakelen. Door gebrek, wordt het leren toegelaten en de bestemmingshaven leert de adressen van MAC van inkomende pakketten die de haven ontvangt. Deze functie wordt weergegeven in CatOS 5.2 op Catalyst 4500/4000 en 5500/5000 en in CatOS 5.3 op Catalyst 6500/6000.

- **multicast *inschakelen/uitschakelen*** â€"Zoals de naam al aangeeft, kunt u met deze optie de controle van multicast-pakketten in- of uitschakelen. De standaardinstelling is ingeschakeld. Deze optie is beschikbaar op Catalyst 5500/5000 en Catalyst 6500/6000, CatOS 5.1 en hoger.

- **via poort 15/1**â€"Op Catalyst 6500/6000 kunt u poort 15/1 (of 16/1) gebruiken als een SPAN-bron. De poort kan het verkeer bewaken dat wordt doorgestuurd naar de Multilayer Switch Feature Card (MSFC). De poort neemt verkeer op dat softwarerouted of doorgestuurd is naar MSFC.

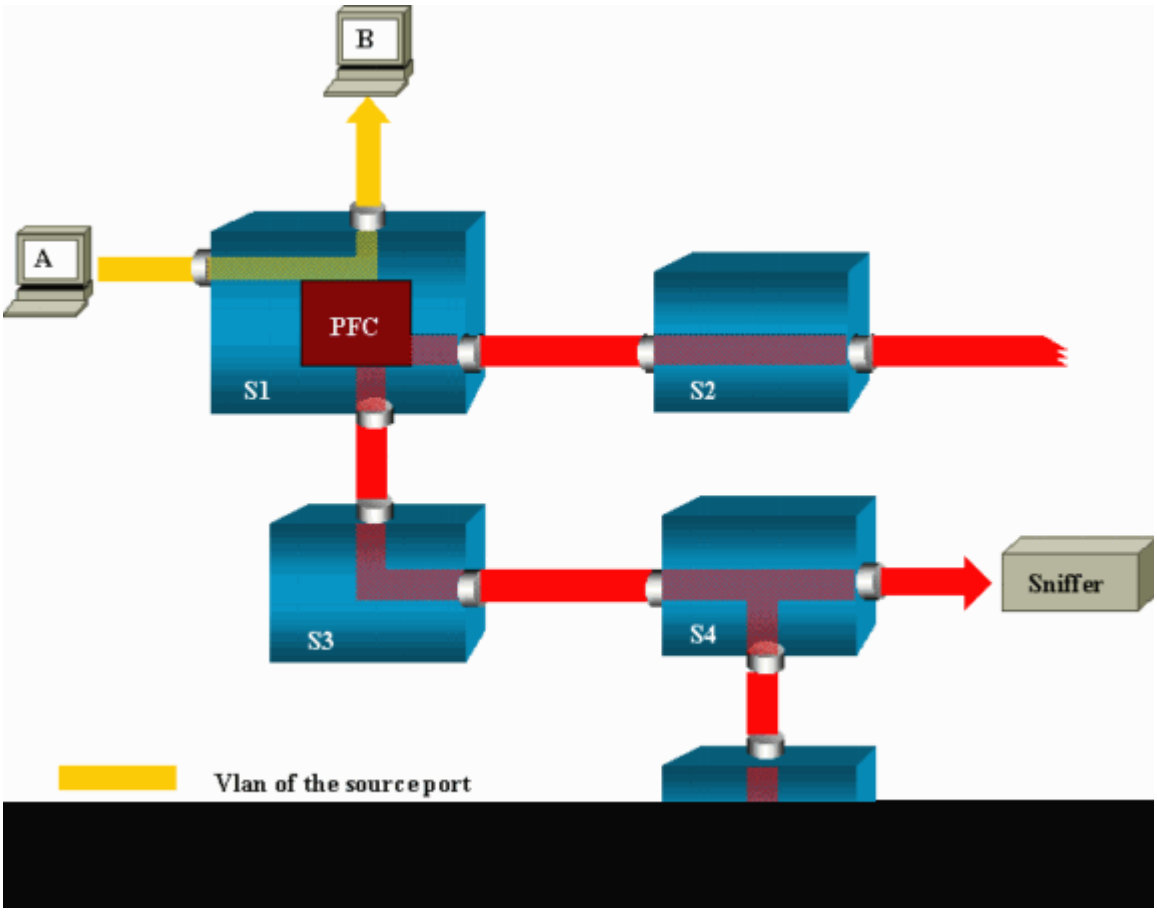
Remote SPAN

RSPAN - Overzicht

RSPAN stelt u in staat bronpoorten te bewaken die over een switched netwerk worden verspreid, en niet alleen lokaal op een switch met SPAN. Deze functie wordt weergegeven in CatOS 5.3 in de Catalyst 6500/6000 Series Switches en wordt toegevoegd in 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 bestemmingshaven, maar overstroomd in een speciale RSPAN VLAN. De bestemmingshaven kan dan overal in dit RSPAN VLAN worden gevestigd. Er kunnen zelfs verschillende bestemmingshavens zijn.

Dit diagram illustreert de structuur van een RSPAN-sessie:



In dit voorbeeld, vormt u RSPAN om verkeer te controleren dat gastheer A verzendt. Wanneer u een frame genereert dat voor B bestemd is, wordt het pakket gekopieerd door een toepassingsspecifieke geïntegreerde schakeling (ASIC) van Catalyst 6500/6000 beleidsfunctiekaart (PFC) naar een vooraf gedefinieerd RSPAN-VLAN. Van daar, wordt het pakket overstroomd aan alle andere havens die tot RSPAN VLAN behoren. Alle interswitchkoppelingen die hier worden getekend zijn trunks, wat een vereiste is voor RSPAN. De enige toegangshavens zijn bestemmingspoorten, waar de snuivers zijn aangesloten (hier, op S4 en S5).

Dit zijn een paar opmerkingen over dit ontwerp:

- S1 wordt een source switch genoemd. Packets voeren alleen het RSPAN VLAN in in switches die als RSPAN-bron zijn geconfigureerd. Momenteel kan een switch slechts de bron zijn voor één RSPAN-sessie, wat betekent dat een bron-switch slechts één RSPAN VLAN tegelijk kan voeden.

- S2 en S3 zijn intermediaire switches. Zij zijn geen bronnen van RSPAN en hebben geen bestemmingspoorten. Een switch kan intermediair zijn voor elk aantal RSPAN-sessies.

- S4 en S5 zijn bestemmings switches. Sommige poorten zijn ingesteld als bestemming voor een RSPAN-sessie. Op dit moment kan een Catalyst 6500/6000 maximaal 24 RSPAN-bestemmingspoorten hebben, voor een of meer verschillende sessies. U kunt ook opmerken dat S4 zowel een bestemming als een tussenliggende switch is.

- U kunt zien dat RSPAN-pakketten worden overspoeld naar RSPAN VLAN. Zelfs switches die niet op het pad naar een bestemmingshaven liggen, zoals S2, ontvangen het verkeer voor RSPAN VLAN. U kunt het nuttig vinden om dit VLAN op dergelijke S1-S2-koppelingen te snoeien.

- Om de overstroming te bereiken, wordt het leren op RSPAN VLAN uitgeschakeld.

- Om lijnen te voorkomen, is STP onderhouden op RSPAN VLAN. Daarom kan RSPAN Bridge Protocol Data Units (BPDUâ€™s) niet bewaken.

Voorbeeld van RSPAN-configuratie

De informatie in deze sectie illustreert de opstelling van deze verschillende elementen met een zeer eenvoudig ontwerp RSPAN. S1 en S2 zijn twee Catalyst 6500/6000 Switches. Om bepaalde S1-poorten of VLANâ€™s vanaf S2 te kunnen bewaken, moet u een speciaal 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

Zet om te beginnen hetzelfde VLAN Trunk Protocol (VTP)-domein op elke switch en configureer een kant als trunking wenselijk. VTP-onderhandeling doet de rest. Geef deze opdracht op S1:

<#root>

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

      VTP domain cisco modified
```

Geef deze opdrachten uit op S2:

<#root>

```
S2> (enable)
set vtp domain cisco

      VTP domain cisco modified
      S2> (enable)
set trunk 5/1 desirable

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

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. In dit voorbeeld wordt VLAN 100 gebruikt:

<#root>

```
S2> (enable)
```

`set vlan 100 rspan`

```
      Vlan 100 configuration successful
```

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

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

<#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
```

Configuratie van een RSPAN-bronpoort op S1

In dit voorbeeld wordt inkomend verkeer dat S1 via poort 6/2 ingaat, bewaakt. Voer de volgende opdracht uit:

<#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 inkomende pakketten op poort 6/2 worden nu overstroomd op de RSPAN VLAN 100 en bereiken de bestemmingshaven die op S1 via de trunk is geconfigureerd.

De configuratie verifiëren

Het **show rspan** commando geeft een overzicht van de huidige RSPAN configuratie op de switch. Opnieuw, kan er slechts één bron RSPAN zitting in één keer zijn.

<#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
```

Andere configuraties die mogelijk zijn met de ingestelde opdracht span

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 switch, als u meerdere bestemmings-SPAN-poorten wilt hebben.

Samenvatting en beperkingen van functies

Deze tabel geeft een overzicht van de verschillende functies die zijn geïntroduceerd en biedt de minimale CatOS-release die nodig is om de functie op het gespecificeerde platform uit te voeren:

Feature	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000

optie ***Inputs in/uit zetten***	4.4	4.2	5.1
Meervoudige sessies, poorten in verschillende VLANâ€™s	5.1	5.1	5.1
SC0-optie	â€”	5.1	5.1
optie **multicast *in-/uitschakelen***	â€”	5.1	5.1
optie ***Inschakelen/uitschakelen* leren**	5.2	5.2	5.3
RSPAN	6.3	â€”	5.3

Deze tabel geeft een korte samenvatting van de huidige beperkingen ten aanzien van het aantal mogelijke SPAN-sessies:

Feature	Catalyst 4500/4000 reeks Switches	Catalyst 5500/5000 reeks Switches	Catalyst 6500/6000 reeks Switches
Rx- of beide SPAN-sessies	5	1	2
Sessies van Tx SPAN	5	4	4
Sessies voor Mini Protocol Analyzer	Niet ondersteund	Niet ondersteund	1
RX, Tx of beide RSPAN-bronsessies	5	Niet ondersteund	1 Supervisor Engine 720 ondersteunt twee RSPAN-bronsessies.
RSPAN-bestemming	5	Niet ondersteund	24
Totaal aantal sessies	5	5	30

Raadpleeg deze documenten voor aanvullende beperkingen en configuratierichtlijnen:

- 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 de Switches van Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 en 3750-E Series:

- Catalyst 2950 Switches kan slechts één SPAN-sessie tegelijk actief hebben en kan alleen bronpoorten bewaken. Deze switches kunnen VLANâ€™s niet controleren.
- De Catalyst 2950 en 3550 Switches kunnen verkeer doorsturen op een bestemmingshaven van SPAN in Cisco IOS-softwarerelease 12.1(13)EA1 en hoger.
- De Switches Catalyst 3550, 3560 en 3750 kunnen maximaal twee SPAN-sessies tegelijkertijd ondersteunen en kunnen zowel bronpoorten als VLANâ€™s controleren.
- Voor de Switches Catalyst 2970, 3560 en 3750 is de configuratie van een reflectorpoort niet vereist wanneer u een RSPAN-sessie configureert.
- De Catalyst 3750 Switches ondersteunen sessieconfiguratie met het gebruik van bron- en doelpoorten die zich op een van de leden van de switch-stack bevinden.

- Per SPAN-sessie is slechts één bestemmingshaven toegestaan en dezelfde poort kan geen bestemmingshaven zijn voor meerdere SPAN-sessies. Daarom kunt u geen twee SPAN-sessies hebben die dezelfde bestemmingshaven gebruiken.

De opdrachten voor de SPAN-functieconfiguratie zijn vergelijkbaar voor Catalyst 2950 en Catalyst 3550. Catalyst 2950 kan de VLANâ€™s echter niet bewaken. U kunt de SPAN configureren, zoals in dit voorbeeld:

<#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#
```

U kunt een poort ook configureren als een bestemming voor lokaal SPAN en RSPAN voor hetzelfde VLAN-verkeer. Om verkeer voor een bepaald VLAN te controleren dat in twee direct aangesloten switches verblijft, vorm deze bevelen op de switch die de bestemmingshaven heeft. In dit voorbeeld, controleren wij verkeer van VLAN 5 dat over twee switches wordt uitgespreid:

<#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.
```

Gebruik op de switch op afstand deze configuratie:

<#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
```

In het vorige voorbeeld werd een poort ingesteld als een bestemmingshaven voor zowel lokale SPAN als RSPAN om verkeer te bewaken voor hetzelfde VLAN dat zich in twee switches bevindt.

Opmerking: in tegenstelling tot de Switches 2900XL en 3500XL Series, ondersteunen de Switches Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 en 3750-E Series alleen SPAN op bronpoortverkeer in de richting Rx (Rx SPAN of instress SPAN) in de richting Tx (Tx SPAN of uitgaande 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 op software die ouder is dan Cisco IOS-softwarerelease 12.1(6)EA2. Raadpleeg het gedeelte *Enabled Switch Port Analyzer* van Managing Switches om SPAN op een Catalyst 2950 te configureren 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 ondersteunen SPAN. Alle pakketten die worden gezien op de bestemmingshaven van de SPAN (aangesloten op het snuffelapparaat of de PC) hebben echter een IEEE 802.1Q-tag, ook al is de SPAN-bronpoort (bewaakte poort) mogelijk geen 802.1Q-trunkpoort.

Als het snuffelapparaat of de het netwerkinterfacekaart van PC (NIC) 802.1Q-Gelabelde pakketten niet begrijpt, kan het apparaat de pakketten laten vallen of moeilijkheid hebben aangezien het probeert om de pakketten te decoderen. De mogelijkheid om de 802.1Q-gelabelde frames te zien is alleen belangrijk wanneer de SPAN-bronpoort een trunkpoort is. Met Cisco IOS-softwarerelease 12.1(11)EA1 en hoger kunt u tagging van de pakketten inschakelen en uitschakelen op de SPAN-doelpoort. Geef de **monitorsessie sessie_number bestemmingsinterface interface_id inkapselingsdot1q** bevel uit om inkapseling van de pakketten bij de bestemmingshaven toe te laten. Als u het trefwoord voor de **inkapseling** niet specificeert, worden de pakketten zonder label verzonden, wat het standaard is in Cisco IOS-softwarerelease 12.1(11)EA1 en hoger.

Feature	Catalyst 2950/3550
Ingress (inpkts) *schakelt* optie *in/uit*	Cisco IOS-softwarerelease 12.1(12c)EA1
RSPAN	Cisco IOS-softwarerelease 12.1(12c)EA1

Feature	Catalyst 2940[1], 2950, 2955, 2960, 2970, 3550, 3560, 3750
Rx- of beide SPAN-sessies	2
Sessies van Tx SPAN	2
RX, Tx of beide RSPAN-bronsessies	2
RSPAN-bestemming	2
Totaal aantal sessies	2

[1] Catalyst 2940 Switches ondersteunen alleen lokale SPAN. RSPAN wordt niet ondersteund op dit platform.

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 waarop Cisco IOS-systeemsoftware wordt uitgevoerd

De SPAN-functie wordt ondersteund op de Switches van Catalyst 4500/4000 en Catalyst 6500/6000 Series die Cisco IOS-systeemsoftware uitvoeren. Beide switch-platforms gebruiken de identieke opdrachtregelinterface (CLI) van en een configuratie die vergelijkbaar is met de configuratie die de SPAN op de sectie Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560E, 3750 en 3750E Series Switches dekt. 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:

```
<#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#
```

Samenvatting en beperkingen van functies

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 uit te voeren:

Feature	Catalyst 4500/4000 (Cisco IOS-software)	Catalyst 6500/6000 (Cisco IOS-software)
Ingress (inpkts) *schakelt* optie *in/uit*	Cisco IOS-softwarerelease 12.1(19)EW	Momenteel niet ondersteund[1]
RSPAN	Cisco IOS-softwarerelease 12.1(20)EW	Cisco IOS-softwarerelease 12.1(13)E

[1] Deze optie is momenteel niet beschikbaar en de beschikbaarheid van deze functies wordt doorgaans pas

gepubliceerd na de release.

> **Opmerking**: de functie SPAN van Cisco Catalyst 6500/6000 Series Switches heeft een beperking ten opzichte van PIM-protocol. Wanneer een switch voor zowel PIM als SPAN is geconfigureerd, kan de Network Analyzer/Sniffer die is aangesloten op de SPAN-doelpoort PIM-pakketten zien die geen deel uitmaken van het SPAN-bronpoort/VLAN-verkeer. Deze kwestie doet zich voor als gevolg van een beperking in de pakketdoorstuurarchitectuur van de switch. De bestemmingshaven van de SPAN voert geen controle uit om de bron van de pakketten te verifiëren. Dit probleem is ook gedocumenteerd in Cisco bug-id CSC57506 (alleen geregistreerde klanten).

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

Feature	Catalyst 4500/4000 (Cisco IOS-software)
Rx- of beide SPAN-sessies	2
Sessies van Tx SPAN	4
RX, Tx of beide RSPAN-bronsessies	2 (Rx, Tx of beide) en tot 4 (alleen Tx)
RSPAN-bestemming	2
Totaal aantal sessies	6

Raadpleeg de lokale SPAN-, RSPAN- en ERSPAN-sessielimieten voor Catalyst 6500/6000 switches waarop Cisco IOS-software wordt uitgevoerd.

In Catalyst 6500 Series is het belangrijk om op te merken dat uitgaande SPAN op de supervisor wordt uitgevoerd. Hierdoor kan al het verkeer dat onderhevig is aan uitgaande SPAN worden verzonden over de fabric naar de supervisor en vervolgens naar de SPAN-bestemmingshaven, die aanzienlijke systeembronnen kan gebruiken en gebruikersverkeer kan beïnvloeden. Ingress SPAN zal worden gedaan op toegangsmodules zodat de prestaties SPAN de som van alle deelnemende replicatiemotoren zou zijn. De prestaties van de functie SPAN zijn afhankelijk van de pakketgrootte en het type ASIC dat beschikbaar is in de replicatie-engine.

Met releases eerder dan Cisco IOS-softwarerelease 12.2(33)SXH kan een poortkanaals interface, een EtherChannel, geen SPAN-bestemming zijn. Met Cisco IOS-softwarerelease 12.2(33)SRE en hoger kan een EtherChannel een SPAN-bestemming zijn. Bestemming EtherChannel ondersteunt de EtherChannel-protocollen (Port Aggregation Control Protocol, PAgP) of Link Aggregation Control Protocol (LACP) niet. Alleen de on-modus wordt ondersteund, waarbij alle EtherChannel-protocolondersteuning is uitgeschakeld.

Raadpleeg deze documenten voor aanvullende beperkingen en configuratierichtlijnen:

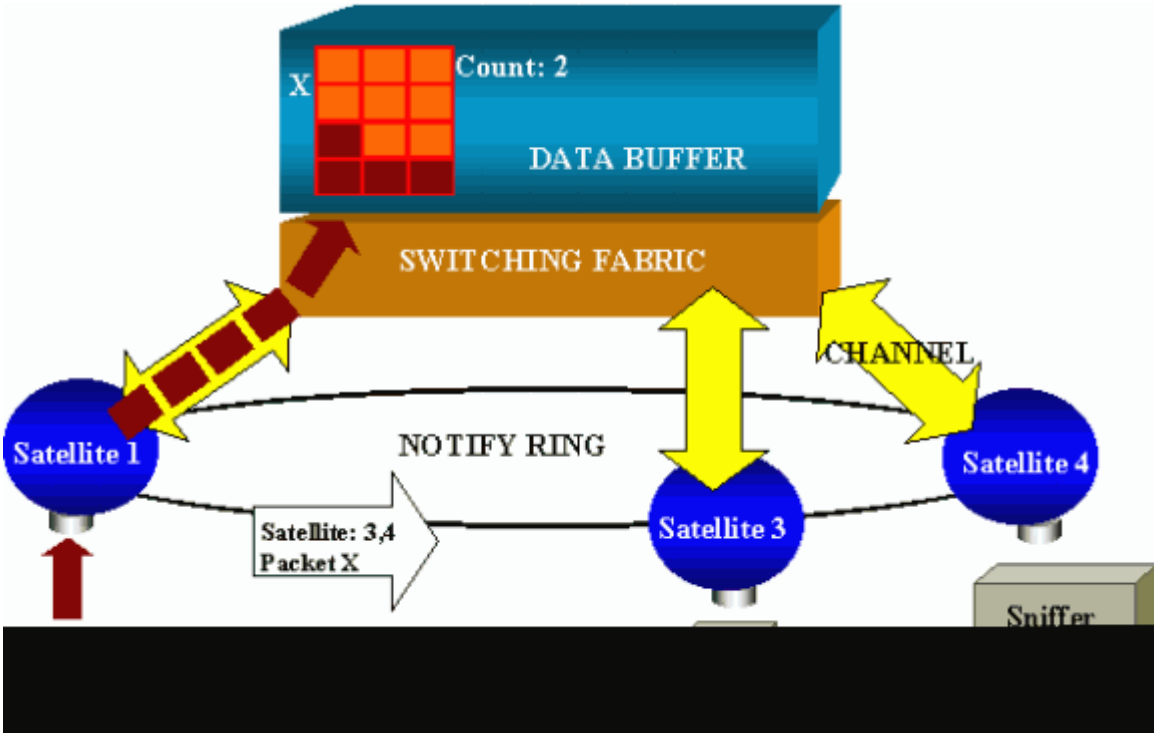
- SPAN en RSPAN configureren (Catalyst 4500/4000)
- Lokale SPAN, externe SPAN (RSPAN) en ingesloten RSPAN configureren (Catalyst 6500/6000)

Effect van prestaties van SPAN op de verschillende Catalyst platforms

Catalyst 2900XL/3500XL Series

Overzicht van architectuur

Dit is een zeer simplistische kijk op de 2900XL/3500XL Switches binnenarchitectuur:



De poorten van de switch zijn aangesloten op satellieten die via radiale kanalen communiceren met een schakelmateriaal. Bovenaan zijn alle satellieten onderling verbonden via een snelle waarschuwingsring die is gewijd aan signaleringsverkeer.

Wanneer een satelliet een pakket van een haven ontvangt, wordt het pakket verdeeld in cellen en naar de omschakelingsstof via één of meerdere kanalen verzonden. Het pakket wordt vervolgens opgeslagen in het gedeelde geheugen. Elke satelliet heeft kennis van de bestemmingspoorten. In het diagram in deze sectie weet satelliet 1 dat het pakket X door satellieten 3 en 4 moet worden ontvangen. Satelliet 1 stuurt een bericht naar de andere satellieten via de meldring. Dan kunnen satellieten 3 en 4 beginnen met het ophalen van de cellen uit het gedeelde geheugen via hun radiale kanalen en kunnen uiteindelijk het pakket doorsturen. Omdat de bronsatelliet de bestemming kent, stuurt deze satelliet ook een index die het aantal tijden aangeeft dat dit pakket wordt gedownload door de andere satellieten. Telkens wanneer een satelliet het pakket van het gedeelde geheugen terugwint, is deze index decremented. Wanneer de index 0 bereikt, kan het gedeelde geheugen worden vrijgegeven.

Effect op prestaties

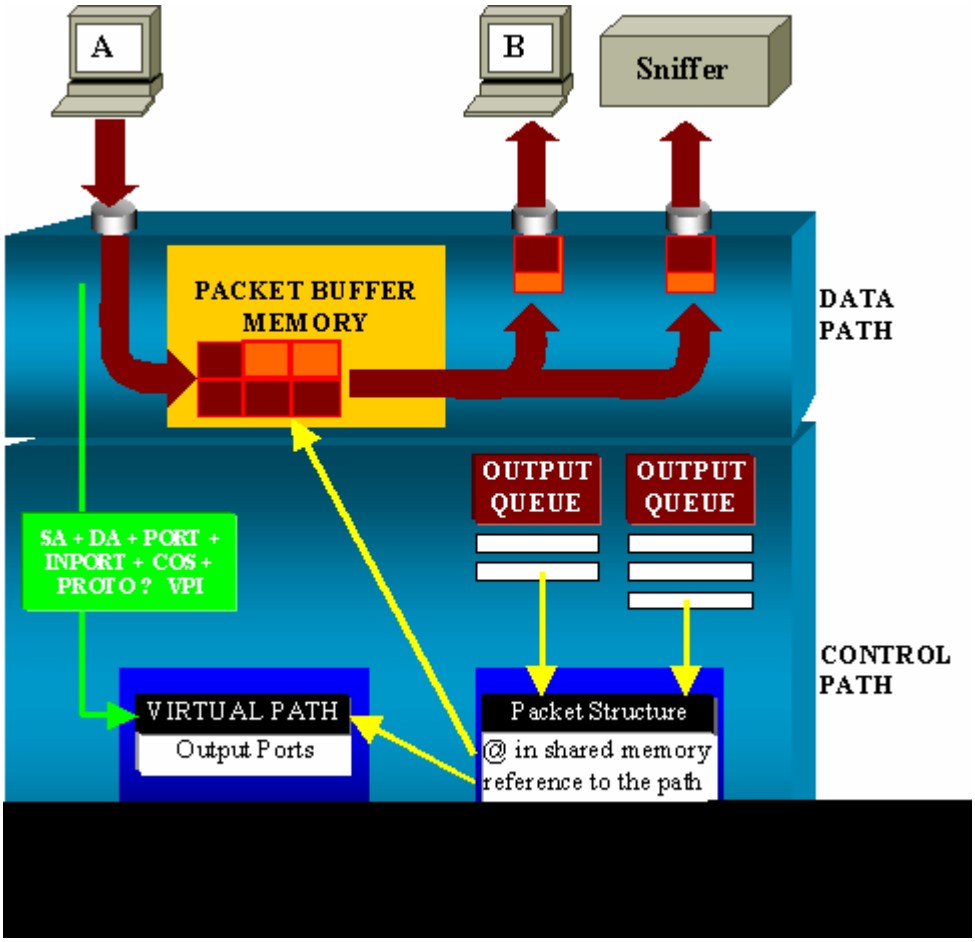
Om sommige poorten met SPAN te kunnen bewaken, moet een pakket van de gegevensbuffer naar een satelliet en extra tijd worden gekopieerd. Het effect op de snelle schakelstof is verwaarloosbaar.

De controlehaven ontvangt kopieën van verzonden en ontvangen verkeer voor alle gecontroleerde havens. In deze architectuur wordt een pakket dat bestemd is voor meerdere bestemmingen opgeslagen in het geheugen totdat alle kopieën worden doorgestuurd. Als de controlepoort gedurende langere tijd voor 50 procent overgeabonneerd is, raakt de poort waarschijnlijk verstopt en houdt deze een deel van het gedeelde geheugen in. Het is mogelijk dat een of meer van de gecontroleerde havens ook een vertraging doormaken.

Catalyst 4500/4000 Series software

Overzicht van architectuur

Catalyst 4500/4000 is gebaseerd op een stof voor gedeelde geheugenswitching. Dit diagram is een overzicht op hoog niveau van het pad van een pakket door de switch. De feitelijke tenuitvoerlegging is namelijk veel ingewikkelder:



Op een Catalyst 4500/4000 kunt u het gegevenspad onderscheiden. Het gegevenspad komt overeen met de werkelijke gegevensoverdracht binnen de switch, vanaf het controlepad, waar alle beslissingen worden genomen.

Wanneer een pakket in de switch wordt ingevoerd, wordt er een buffer toegewezen in het Packet Buffer Memory (een gedeeld geheugen).

Een pakketstructuur die naar deze buffer wijst, wordt geïnitialiseerd in de Packet Descriptor Table (PDT).

Terwijl de gegevens in gedeeld geheugen worden gekopieerd, bepaalt de controleweg waar te om het pakket te switches. Om dit te kunnen bepalen, wordt een hashwaarde berekend aan de hand van deze informatie:

- Het pakketbronadres
- Bestemmingsadres
- VLAN
- Protocoltype
- Invoerpoort
- Serviceklasse (CoS) (IEEE 802.1p-tag of poortstandaard)

Deze waarde wordt gebruikt om de Virtual Path Index (VPI) van een padstructuur in de Virtual Path Table

(VPT) te vinden. Deze virtuele pad-ingang in de VPT bevat verschillende velden die betrekking hebben op deze specifieke stroom.

De velden bevatten de bestemmingspoorten. De pakketstructuur in de PDT wordt nu bijgewerkt met een verwijzing naar het virtuele pad en de teller.

In het voorbeeld in deze sectie moet het pakket worden verzonden naar twee verschillende poorten, dus de teller initialiseert naar 2. Tot slot wordt de pakketstructuur toegevoegd aan de uitvoerwachtrij van de twee doelpoorten.

Van daar, de gegevenskopieën van het gedeelde geheugen in de outputbuffer van de poort, en de pakketstructuur tegendecreten. Wanneer 0 wordt bereikt, komt de gedeelde geheugenbuffer vrij.

Effect op prestaties

Met gebruik van de functie SPAN moet een pakket naar twee verschillende poorten worden verzonden, zoals in het voorbeeld in het gedeelte Architectuur - overzicht.

Het verzenden van het pakket naar twee poorten is geen probleem, omdat de switchingstof niet blokkeert.

Als de bestemmingsSPAN haven verstopt is, worden de pakketten gelaten vallen in de outputrij en correct van het gedeelde geheugen vrijgegeven. T

De switch ondervindt dus geen gevolgen.

Catalyst 5500/5000 en 6500/6000 Series

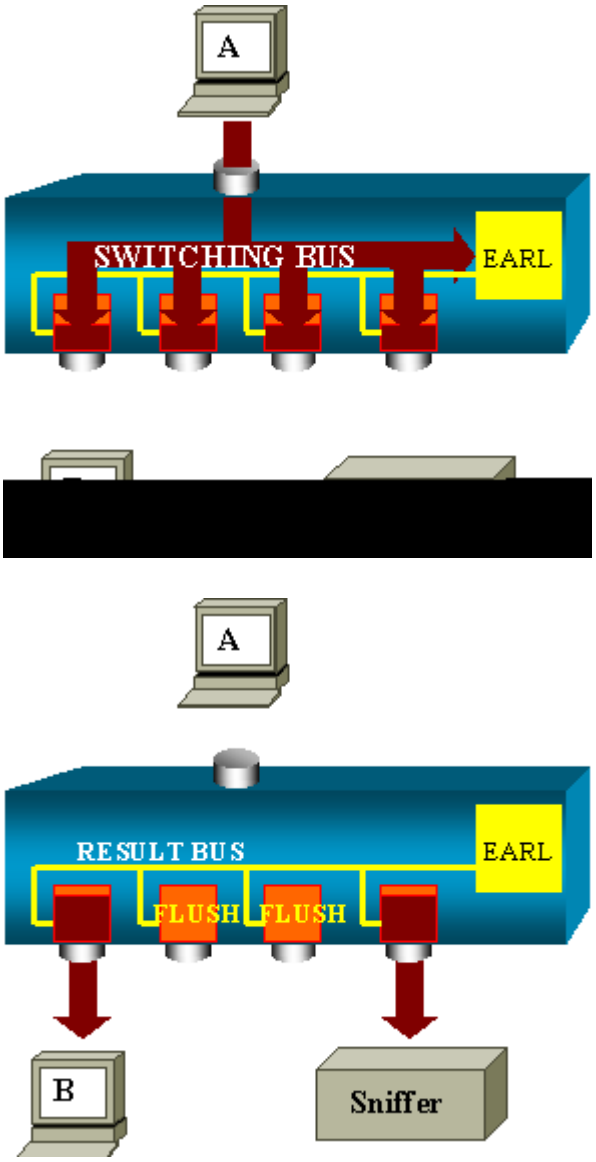
Overzicht van architectuur

Op de Switches van Catalyst 5500/5000 en 6500/6000 Series wordt een pakket dat op een poort wordt ontvangen, verzonden over de interne switchingbus.

Elke lijnkaart in de switch begint dit pakket in interne buffers op te slaan.

Tegelijkertijd ontvangt de Encoded Address Recognition Logic (EARL) de header van het pakket en wordt een resultaatindex berekend. EARL stuurt de resultaatindex via de resultaatbus naar alle lijnkaarten.

De kennis van deze index staat de lijnkaart toe om individueel te beslissen of het het pakket zou moeten spoelen of overbrengen aangezien de lijnkaart het pakket in zijn buffers ontvangt.



Effect op prestaties

Of één of meerdere poorten uiteindelijk het pakket overbrengen heeft absoluut geen invloed op de switch operatie. Daarom wanneer u deze architectuur overweegt, heeft de functie SPAN geen invloed op de prestaties.

Vaak gestelde vragen en vaak voorkomende problemen

Connectiviteitsproblemen als gevolg van verkeerde configuratie van de SPAN

Connectiviteitsproblemen als gevolg van de verkeerde configuratie van SPAN komen vaak voor in CatOS-versies die eerder zijn dan 5.1. Met deze versies is slechts één SPAN-sessie mogelijk.

De sessie blijft in de configuratie, zelfs wanneer u SPAN uitschakelt. Wanneer de **ingestelde span** commando **inschakelt**, activeert een gebruiker de opgeslagen SPAN-sessie.

De actie komt vaak voor als gevolg van een typografische fout, bijvoorbeeld, als de gebruiker STP wil inschakelen. Ernstige connectiviteitsproblemen kunnen resulteren als de bestemmingshaven wordt gebruikt om gebruikersverkeer door te sturen.

Waarschuwing: dit probleem is nog steeds in de huidige implementatie van de CatOS. Wees heel voorzichtig met de poort die u als SPAN-bestemming kiest.

SPAN-doelpoort naar boven/beneden

Wanneer poorten voor bewaking worden geijkt, wordt de poortstatus UP/DOWN weergegeven.

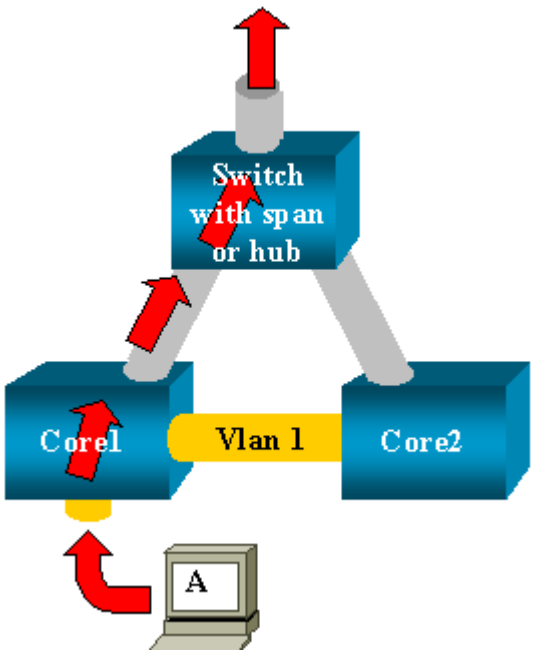
Wanneer u een SPAN-sessie configureert om de poort te bewaken, wordt de toestand door de doelinterface weergegeven (bewaking), op basis van het ontwerp.

De interface toont de haven in deze staat om duidelijk te maken dat de haven momenteel niet bruikbaar is als productiehaven. De poort voor het bewaken van de omhoog/omlaag is normaal.

Waarom maakt de SPAN-sessie een overbruggingslus?

De creatie van een overbruggingslijn komt typisch voor wanneer de beheerder probeert om de eigenschap RSPAN te vervalsen. Ook kan een configuratiefout het probleem veroorzaken.

Dit is een voorbeeld van het scenario:



Er zijn twee switches die met elkaar verbonden zijn door een stam. In dit geval heeft elke switch meerdere servers, clients of andere bruggen die erop zijn aangesloten.

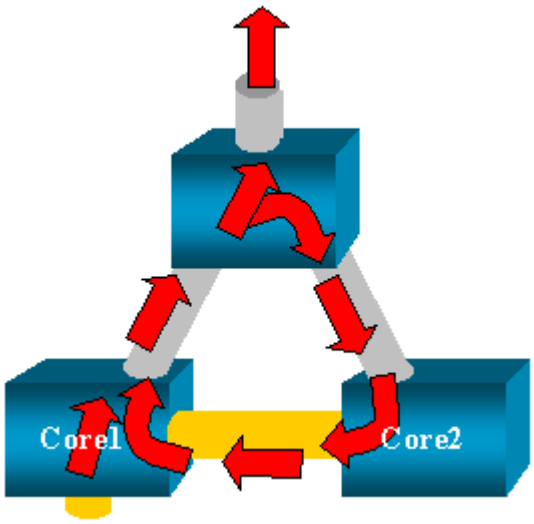
De beheerder wil VLAN 1 controleren, dat op verscheidene bruggen met SPAN verschijnt.

De beheerder maakt een SPAN-sessie die het gehele VLAN 1 op elke core switch controleert, en die, om deze twee sessies samen te voegen, de bestemmingshaven met dezelfde hub (of dezelfde switch, met het gebruik van een andere SPAN-sessie) verbindt.

De beheerder bereikt het doel. Elk enkelvoudig pakket dat een core switch op VLAN 1 ontvangt, wordt gedupliceerd op de SPAN-poort en naar boven doorgestuurd naar de hub. Uiteindelijk neemt een snuffelaar het verkeer op.

Het enige probleem is dat het verkeer ook opnieuw in kern 2 door de haven van het bestemmingsSPAN wordt geïnjecteerd.

De herinjectie van het verkeer in kern 2 leidt tot een overbruggingslijn in VLAN 1. Herinner dat een haven van het bestemmingsSPAN geen STP in werking stelt en niet dergelijk een lijn kan verhinderen.



Opmerking: vanwege de introductie van de inputpakketten (invoerpakketten) optie op de CatOS, een SPAN-bestemmingspoort laat elk inkomend pakket standaard vallen, wat dit storingsscenario voorkomt. Maar het potentiële probleem is nog steeds aanwezig op de Catalyst 2900XL/3500XL Series Switches.

Opmerking: zelfs wanneer de inputoptie de lus voorkomt, kan de configuratie die deze sectie laat zien problemen in het netwerk veroorzaken. Netwerkproblemen kunnen optreden vanwege MAC-adresleerproblemen die zijn gekoppeld aan leren dat is ingeschakeld op de doelpoort.

Prestaties van de gevolgen van SPAN?

Zie deze secties van dit document voor informatie over het effect van prestaties voor de gespecificeerde Catalyst-platforms:

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

Kunt u SPAN op een EtherChannel-poort configureren?

Een EtherChannel vormt zich niet als een van de poorten in de bundel een SPAN-bestemmingshaven is. Als u in deze situatie probeert SPAN te configureren, vertelt de switch u:

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

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

Kunt u meerdere SPAN-sessies tegelijkertijd laten uitvoeren?

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

Op de Catalyst 2950 Series Switches kunt u slechts één toegewezen monitorpoort op elk moment hebben.

Als u een andere poort selecteert als de monitorpoort, wordt de vorige monitorpoort uitgeschakeld en wordt de nieuwe geselecteerde poort de monitorpoort.

Op de 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 Meerdere gelijktijdige sessies en functieoverzicht en beperkingen van dit document maken.

Fout "% lokale sessielimiet is overschreden"

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

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

Supervisor Engines hebben een beperking van SPAN-sessies. Raadpleeg het gedeelte *Local SPAN, RSPAN en ERSPAN Session Limits* van Configuration Local SPAN, RSPAN en ERSPAN voor meer informatie.

Kan een SPAN-sessie op de VPN-servicemodule niet verwijderen, met de fout "% sessie [Session No:] used by Service Module"

Bij dit probleem wordt de Virtual Private Network (VPN)-module in de switch geplaatst, waar al een chassisfabric-module is ingebracht.

De Cisco IOS-software maakt automatisch een SPAN-sessie voor de VPN-servicemodule om het multicast-verkeer te verwerken.

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

```
<#root>

Switch(config)#

no monitor session session_number service-module
```

> **Opmerking**: als u de sessie verwijdert, wordt het multicastverkeer door de VPN-servicemodule verbroken.

Waarom kunt u geen gecorrumpeerde pakketten met SPAN opnemen?

U kunt geen beschadigde pakketten met SPAN vastleggen vanwege de manier waarop switches in het algemeen werken. Wanneer een pakket door een switch gaat, komen deze gebeurtenissen voor:

1. Het pakket bereikt de toegangspoort.
2. Het pakket wordt opgeslagen in minstens één buffer.
3. Het pakket wordt uiteindelijk opnieuw verzonden op de uitgang poort.

Als de switch een beschadigd pakket ontvangt, laat de toegangspoort het pakket gewoonlijk vallen. Daarom ziet u het pakket niet op de uitgang poort.

Een switch is niet helemaal doorzichtig als het gaat om het afvangen van verkeer.

Op dezelfde manier wanneer u een beschadigd pakket op uw snuffel in het scenario in deze sectie ziet, weet u dat de fouten bij stap 3, op het uitgangssegment werden geproduceerd.

Als u denkt dat een apparaat corrupte pakketten verstuurt, kunt u ervoor kiezen om de verzendende host en het snuifapparaat op een hub te plaatsen. De hub voert geen foutcontroles uit.

In tegenstelling tot de switch laat de hub de pakketten daarom niet vallen. Op deze manier kunt u de pakketten bekijken.

Fout: % sessie 2 gebruikt door servicemodule

Als een Firewall Service Module (FWSM) is geïnstalleerd, bijvoorbeeld, later geïnstalleerd en verwijderd, in de CAT6500, dan heeft deze automatisch de **functie SPAN Reflector** ingeschakeld.

De functie SPAN-reflector gebruikt één SPAN-sessie in de Switch.

Als u dit niet meer nodig hebt, moet u de opdracht **Geen monitorsessiesemodule** kunnen invoeren vanuit de configuratiemodus van CAT6500 en vervolgens onmiddellijk de nieuwe gewenste SPAN-configuratie invoeren.

Reflector-poortdruppels voor pakketten

Een reflectorpoort ontvangt kopieën van verzonden en ontvangen verkeer voor alle bewaakte bronpoorten. Als een reflectorpoort te veel is geabonneerd, kan deze verstopt raken.

Dit kan van invloed zijn op het doorsturen van verkeer op een of meer van de bronpoorten.

Als de bandbreedte van de reflectorpoort niet voldoende is voor het verkeersvolume van de corresponderende bronpoorten, worden de overtollige pakketten weggelaten.

Een 10/100-poort reflecteert op 100 Mbps. Een Gigabit-poort reflecteert op 1 Gbps.

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

Wanneer u Supervisor Engine 720 gebruikt met een FWSM in het chassis dat Cisco Native IOS uitvoert,

wordt standaard een SPAN-sessie gebruikt. Als u met de opdracht **monitor** ongebruikte sessies controleert, wordt *sessie 1* gebruikt:

```
<#root>

Cat6K#

show monitor


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

Wanneer een firewallblad in het Catalyst 6500-chassis is geïnstalleerd, wordt deze sessie automatisch geïnstalleerd voor ondersteuning van hardware-multicast replicatie omdat een FWSM geen multicast-stromen kan repliceren.

Als multicast stromen die achter FWSM zijn afkomstig moeten bij Layer 3 worden gerepliceerd naar meerdere lijnkaarten, kopieert de automatische sessie het verkeer naar de supervisor via een fabric-kanaal.

Als u een multicastbron hebt die een multicaststroom van achter FWSM genereert, hebt u de SPAN-reflector nodig.

Als u de multicastbron op het buitenste VLAN plaatst, is de SPAN-reflector niet nodig. De SPAN-reflector is niet compatibel met het overbruggen van BPDU's door het FWSM.

U kunt de opdracht **servicemodule zonder monitor** gebruiken om de SPAN-reflector uit te schakelen.

Kan 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 aanwezig is in de databases van deze VTP-domeinen.

Zorg er ook voor dat er geen Layer 3-apparaat aanwezig is in het pad van de sessiebron naar de sessiebestemming.

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

Nee. RSPAN-sessie kan geen Layer 3-apparaat kruisen, aangezien RSPAN een LAN (Layer 2)-functie is.

Gebruik Encapsulated Remote Switch Port Analyzer (ERSPAN) om verkeer via een WAN of andere netwerken te controleren.

De ERSPAN-functie ondersteunt bronpoorten, bron-VLANâ€™s en doelpoorten op verschillende switches, waardoor controle op afstand van meerdere switches via uw netwerk mogelijk is.

ERSPAN bestaat uit een ERSPAN-bronsessie, routable ERSPAN GRE-ingekapseld verkeer en een

ERSPAN-bestemmingssessie.

U configureert ERSPAN-bronsessies en doelsessies afzonderlijk op verschillende switches.

Op dit moment wordt de functie ERSPAN ondersteund in:

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

Raadpleeg Configureren van lokale span, externe span (RSPAN) en ingesloten RSPAN - Catalyst 6500 Series Cisco IOS-softwareconfiguratiegids, 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 op dezelfde switch staan.

Als een RSPAN-bronsessie is geconfigureerd met een bepaald RSPAN VLAN en een RSPAN-doelsessie voor dat RSPAN VLAN op dezelfde switch is geconfigureerd, zal de bestemmingshaven van de RSPAN-doelsessie de opgenomen pakketten niet vanuit de RSPAN-bronsessie verzenden vanwege hardwarebeperkingen. Dit wordt niet ondersteund op de 4500 Series en 3750 Series Switches.

Dit probleem is gedocumenteerd in Cisco bug-id CSC08870 (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
```

De tijdelijke oplossing voor dit probleem is het gebruik van de normale SPAN.

Netwerkanalyzer/beveiligingsapparaat dat is aangesloten op de SPAN-doelpoort is niet bereikbaar

Het basiskenmerk van een SPAN-bestemmingshaven is dat deze geen verkeer verzendt behalve het verkeer dat voor de SPAN-sessie vereist is.

Als u (IP-bereikbaarheid) de netwerkanalyzer/het beveiligingsapparaat moet bereiken via de SPAN-bestemmingshaven, moet u toegangsverkeer doorsturen inschakelen.

Wanneer toegang is ingeschakeld, accepteert de SPAN-bestemmingshaven inkomende pakketten die potentieel zijn gelabeld en afhankelijk zijn van de opgegeven inkapselingsmodus, en maakt deze normaal switches.

Wanneer u een SPAN-bestemmingshaven configureert, kunt u specificeren of de toegangsfunctie is ingeschakeld en welk VLAN moet worden gebruikt om niet-gelabelde toegangspakketten te switches.

De specificatie van een toegang VLAN is niet vereist wanneer ISL-insluiting is geconfigureerd, zoals alle

ISL-ingekapselde pakketten die VLAN-tags hebben.

Hoewel de poort STP-doorsturen is, neemt deze niet deel aan STP, dus gebruik voorzichtigheid wanneer u deze optie configureert, zodat er geen overspannende-boomlus in het netwerk geïntroduceerd wordt.

Wanneer zowel toegang als een trunkinsluiting op een SPAN-bestemmingshaven zijn gespecificeerd, gaat de poort door:sturen in alle actieve VLANâ€™s.

De configuratie van een niet-bestaand VLAN als toegang tot VLAN is niet toegestaan.

monitor sessie sessie_nummer doelinterface-interface [inkapseling {ISL | dot1q}] toegang [VLAN vlan_IDs]

Dit voorbeeld toont hoe u een bestemmingshaven met 802.1q inkapseling en ingangspakketten kunt configureren met het gebruik van het native VLAN 7.

<#root>

```
Switch(config)#
```

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

Met deze configuratie wordt verkeer van SPAN-bronnen die aan sessie 1 zijn gekoppeld, gekopieerd van interface Fast Ethernet 5/48 met 802.1q-insluiting.

Inkomend verkeer wordt geaccepteerd en geschakeld, met untagged pakketten die geclassificeerd zijn in VLAN 7.

Gerelateerde informatie

- **Hoe u SPAN en RSPAN kunt configureren op Cisco Catalyst 4500-switches waarop Cisco IOS-software wordt uitgevoerd**
- **Een SPAN-doelpoort wordt weergegeven als "niet verbonden" en communiceert niet met de rest van het netwerk**
- **Productondersteuning voor switches**
- **Ondersteuning voor LAN-switching technologie**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.