Configuration de l'analyseur de port commuté (SPAN) Catalyst : exemple

Table des matières

Introduction

Le présent document décrit les fonctionnalités récentes de Switched Port Analyzer (SPAN) qui ont

été mises en œuvre.

Conditions préalables

Commutateurs Catalyst qui prennent en charge la fonctionnalité SPAN, RSPAN et ERSPAN

Commutateurs Catalyst	Prise en charge de la fonctionnalité SPAN	Prise en charge de la fonctionnalité RSPAN	Prise en charge de la fonctionnalité ERSPAN
Gamme Catalyst Express 500/520	Oui	Non	Non
Gamme Catalyst 6500/6000	Oui	Oui	Oui, Supervisor 2T avec PFC4, Supervisor 720 avec PFC3B ou PFC3BXL exécutant le logiciel Cisco IOS version 12.2(18)SXE ou ultérieure. Supervisor 720 avec PFC3A disposant de la version de matériel 3.2 ou ultérieures et exécutant le logiciel Cisco IOS Version 12.2(18)SXE ou ultérieures
Gamme Catalyst 5500/5000	Oui	Non	Non
Gamme Catalyst 4900	Oui	Oui	Non
Gamme Catalyst 4500/4000 (inclut 4912G)	Oui	Oui	Non
Gamme Catalyst 3750 Metro	Oui	Oui	Non
Gamme Catalyst 3750 / 3750E / 3750X	Oui	Oui	Non
Gamme Catalyst 3560 / 3560E / 3650X	Oui	Oui	Non
Gamme Catalyst 3550	Oui	Oui	Non
Gamme Catalyst 3500 XL	Oui	Non	Non
Gamme Catalyst 2970	Oui	Oui	Non
Gamme Catalyst	Oui	Oui	Non

2960			
Gamme Catalyst 2955	Oui	Oui	Non
Gamme Catalyst 2950	Oui	Oui	Non
Gamme Catalyst 2940	Oui	Non	Non
Catalyst 2948G-L3	Non	Non	Non
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A	Oui	Oui	Non
Gamme Catalyst 2900XL	Oui	Non	Non
Gamme Catalyst 1900	Oui	Non	Non

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ces informations dans ce document utilisent CatOS 5.5 comme référence pour les commutateurs de la gamme Catalyst 4500/4000, 5500/5000 et 6500/6000. Sur les commutateurs de la gamme Catalyst 2900XL/3500XL, le logiciel Cisco IOS® Version 12.0(5)XU est utilisée.

Bien que ce document soit mis à jour pour refléter les modifications apportées à la fonctionnalité SPAN, reportez-vous aux notes de publication de la documentation des plates-formes de commutation pour connaître les derniers développements relatifs à la fonctionnalité SPAN.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La fonctionnalité SPAN, parfois appelée mise en miroir des ports ou surveillance des ports, sélectionne le trafic réseau à analyser par un analyseur de réseau. L'analyseur réseau peut être un périphérique Cisco SwitchProbe ou toute autre sonde de surveillance à distance (RMON).

Auparavant, SPAN était une fonctionnalité relativement basique sur les commutateurs de la gamme Cisco Catalyst. Cependant, les dernières versions de CatOS (Catalyst OS) ont introduit d'importantes améliorations et beaucoup de nouvelles possibilités qui sont à présent disponibles pour l'utilisateur.

Ce document n'est pas destiné à être un autre guide de configuration pour la fonctionnalité SPAN. Ce document répond à la plupart des questions courantes relatives à la fonctionnalité SPAN, par exemple :

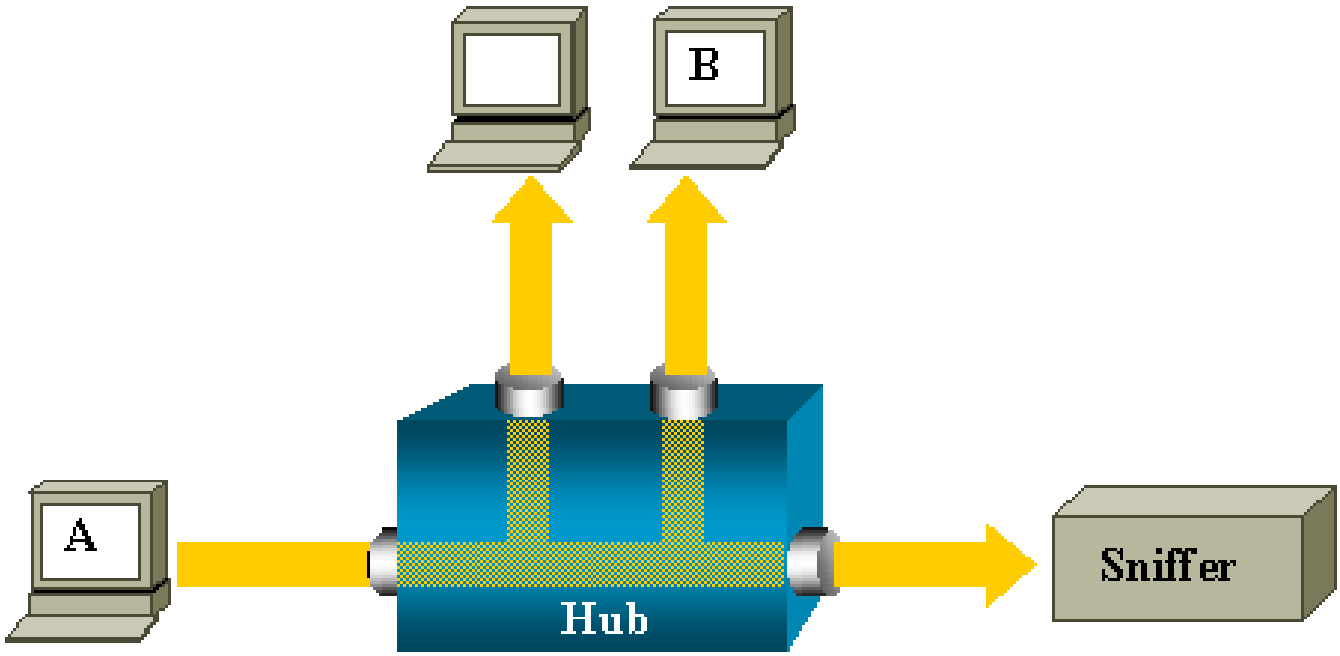
- Qu'est-ce que la fonctionnalité SPAN et comment la configurez-vous ?
- Quelles sont les différentes fonctionnalités disponibles (en particulier plusieurs sessions SPAN simultanées), et quel niveau de logiciel est nécessaire pour les exécuter ?
- La fonctionnalité SPAN affecte-t-elle les performances du commutateur ?

Brève description de la fonctionnalité SPAN

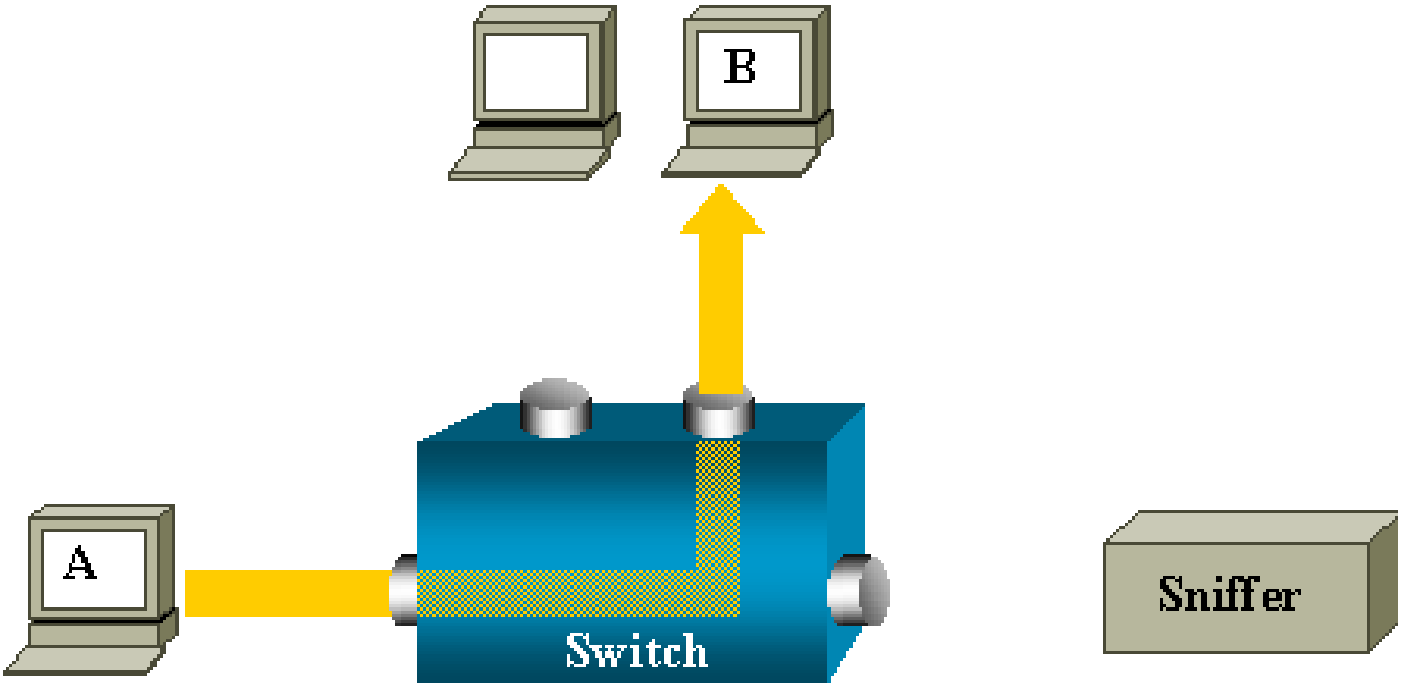
La fonctionnalité SPAN a été introduite sur les commutateurs en raison d'une différence fondamentale qu'ont les commutateurs par rapport aux concentrateurs. Lorsqu'un concentrateur reçoit un paquet sur un port, il envoie une copie de ce paquet sur tous les ports excepté sur celui où le concentrateur a reçu le paquet.

Une fois démarré, un commutateur commence à créer une table de transfert de couche 2 sur la base de l'adresse MAC source des différents paquets reçus par le commutateur. Une fois cette table de transfert créée, le commutateur transfère le trafic qui est destiné à une adresse MAC directement au port correspondant.

Par exemple, pour capturer le trafic Ethernet qui est envoyé par l'hôte A à l'hôte B et qui sont tous deux connectés à un concentrateur, il suffit de connecter un analyseur à ce concentrateur. Tous les autres ports voient le trafic entre les hôtes A et B :



Sur un commutateur, une fois l'adresse MAC de l'hôte B apprise, le trafic de monodiffusion de A à B est uniquement transféré au port de B. Par conséquent, le renifleur ne voit pas ce trafic :



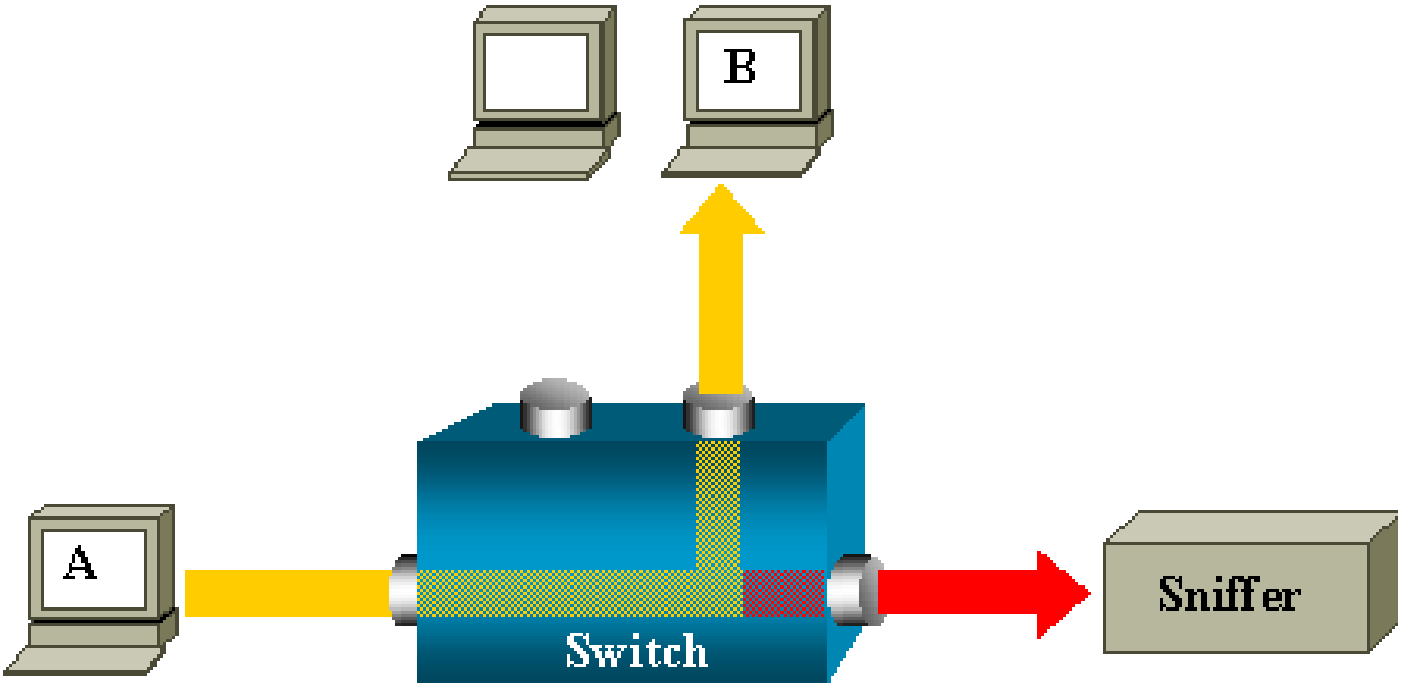
Dans cette configuration, le renifleur capture le trafic qui est propagé vers tous les ports, par exemple :

- Le trafic de diffusion
- Le trafic de multidiffusion avec CGMP ou IGMP (Internet Group Management Protocol) Snooping désactivé
- Le trafic de monodiffusion inconnu

La propagation monodiffusion se produit quand le commutateur n'a pas l'adresse MAC de destination dans sa table de mémoire de contenu adressable (CAM, Content-Addressable Memory).

Le commutateur ne sait pas où envoyer le trafic. Le commutateur propage les paquets vers tous les ports dans le VLAN de destination.

Une fonctionnalité supplémentaire qui copie artificiellement les paquets de monodiffusion que l'hôte A envoie au port du renifleur est nécessaire :

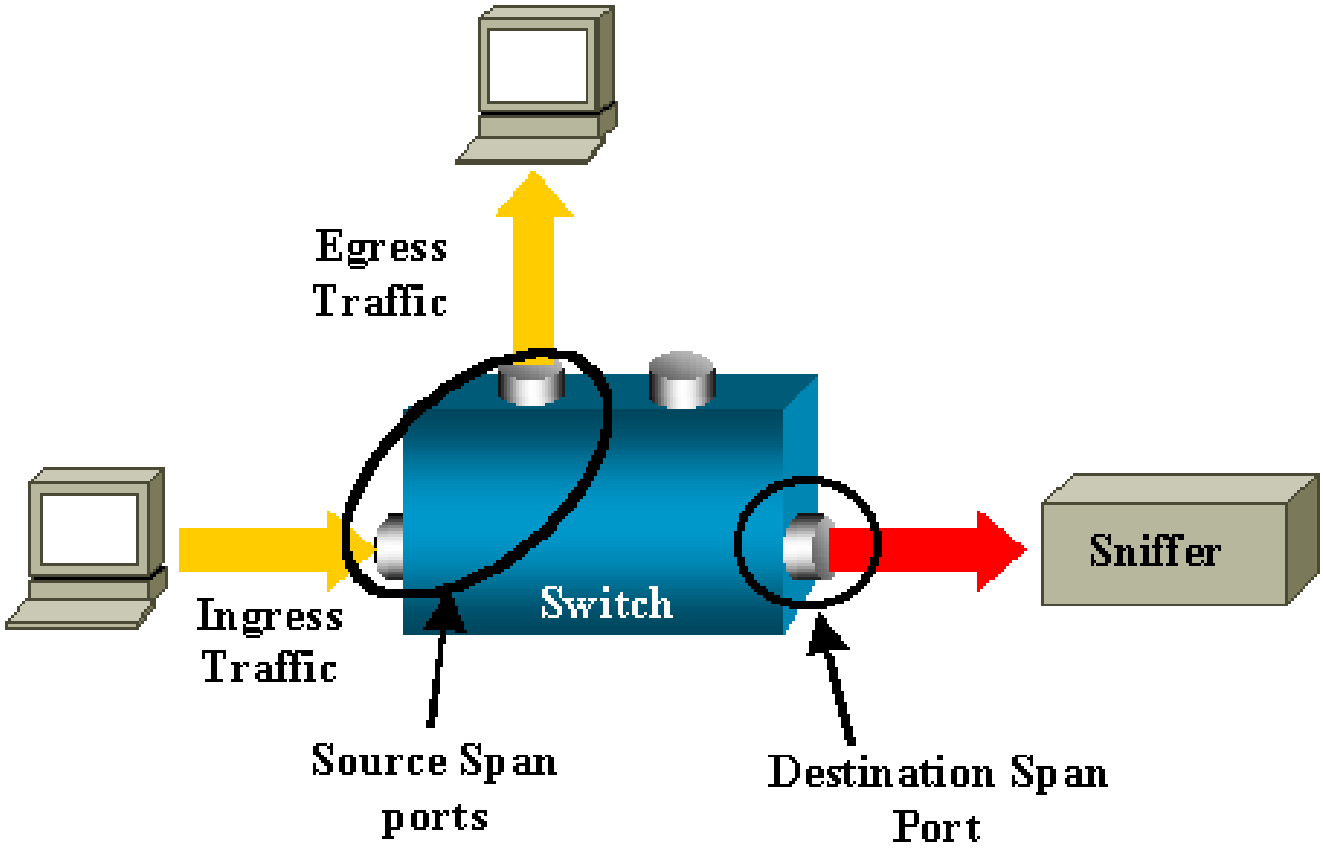


Dans ce diagramme, le renifleur est attaché à un port qui est configuré pour recevoir une copie de chaque paquet envoyé par l'hôte A. Ce port est appelé port SPAN.

Les autres sections de ce document expliquent comment vous pouvez optimiser cette fonctionnalité avec beaucoup de précision afin de faire plus que surveiller un port.

Terminologie relative à la fonctionnalité SPAN

- Trafic entrant : Trafic qui entre dans le commutateur.
- Trafic sortant : Trafic qui quitte le commutateur.
- Port (SPAN) source : Port qui est surveillé à l'aide de la fonctionnalité SPAN.
- VLAN (SPAN) source : VLAN dont le trafic est surveillé à l'aide de la fonctionnalité SPAN.
- Port (SPAN) de destination : Port qui surveille les ports sources, généralement là où un analyseur réseau est connecté.
- Port de réflecteur : Port qui copie les paquets sur un VLAN RSPAN.
- Port de surveillance : Un port de surveillance est également un port SPAN de destination dans la terminologie relative à Catalyst 2900XL/3500XL/2950.



- Fonctionnalité SPAN locale : La fonctionnalité SPAN est locale quand tous les ports surveillés se trouvent sur le même commutateur que le port de destination. Cette fonctionnalité s'oppose à la fonctionnalité Remote SPAN (RSPAN), également définie dans cette liste.
- Fonctionnalité Remote SPAN (RSPAN) : Certains ports sources ne se trouvent pas sur le même commutateur que le port de destination.

RSPAN est une fonctionnalité avancée qui requiert un VLAN spécial pour transporter le trafic qui est surveillé par la fonctionnalité SPAN entre les commutateurs.

La fonctionnalité RSPAN n'est pas prise en charge sur tous les commutateurs. Vérifiez les notes de publication ou le guide de configuration correspondants pour voir si vous pouvez utiliser RSPAN sur le commutateur que vous déployez.

- Fonctionnalité SPAN basée sur les ports (PSPAN) : L'utilisateur spécifie un ou plusieurs ports sources sur le commutateur et un port de destination.
- Fonctionnalité SPAN basée sur le VLAN (VSPAN) : Sur un commutateur particulier, l'utilisateur peut choisir, dans une seule commande, de surveiller tous les ports qui appartiennent à un VLAN particulier.
- ESPAN : il s'agit de la version Enhanced SPAN. Ce terme a été utilisé plusieurs fois au cours de l'évolution de la fonctionnalité SPAN afin de nommer des fonctionnalités supplémentaires. Par conséquent, le terme n'est pas très clair et est évité dans ce document.

- Source administrative : Liste de ports ou de VLAN sources qui ont été configurés pour être surveillés.
- Source opérationnelle : Liste de ports qui sont effectivement surveillés. Cette liste de ports peut être différente de la source administrative.

Par exemple, un port qui est en mode d'arrêt peut figurer dans la source administrative, mais il n'est pas effectivement surveillé.

Caractéristiques du port source

Un port source, également appelé « port surveillé », est un port commuté ou routé que vous surveillé pour l'analyse du trafic réseau.

Dans une session SPAN locale unique ou une session source RSPAN, vous pouvez surveiller le trafic du port source, tel que le trafic reçu (Rx), transmis (Tx) ou bidirectionnel (both).

Le commutateur prend en charge un certain nombre de ports sources (au maximum le nombre de ports disponibles sur le commutateur) et un certain nombre de VLAN sources.

Un port source a les caractéristiques suivantes :

- Ce peut être n'importe quel type de port, par exemple EtherChannel, Fast Ethernet, Gigabit Ethernet, etc.
- Il peut être surveillé dans plusieurs sessions SPAN.
- Il ne peut pas être un port de destination.
- Chaque port source peut être configuré avec une direction (entrée, sortie, ou les deux) à surveiller. Pour les sources EtherChannel, la direction surveillée s'applique à tous les ports physiques du groupe.
- Les ports sources peuvent se trouver dans les mêmes VLAN ou dans des VLAN différents.
- Pour les sources SPAN de VLAN, tous les ports actifs dans le VLAN source sont inclus comme ports sources.

Filtrage des VLAN

Lorsque vous surveillez un port de jonction comme port source, tous les VLAN actifs sur la jonction sont surveillés par défaut. Vous pouvez utiliser le filtrage des VLAN pour limiter la surveillance du trafic SPAN sur les ports sources de jonction à des VLAN spécifiques.

- Le filtrage des VLAN s'applique uniquement aux ports de jonction ou aux ports VLAN voix.
- Le filtrage des VLAN s'applique uniquement aux sessions basées sur les ports et n'est pas autorisé dans des sessions avec des sources de VLAN.
- Lorsqu'une liste de filtrage des VLAN est spécifiée, seuls les VLAN figurant dans la liste sont

surveillés sur des ports de tronc ou sur les ports d'accès aux VLAN voix.

- Le trafic SPAN en provenance d'autres types de ports n'est pas affecté par le filtrage des VLAN ; par conséquent, tous les VLAN sont autorisés sur les autres ports.
- Le filtrage des VLAN affecte uniquement le trafic transféré au port SPAN de destination et n'affecte pas la commutation du trafic normal.
- Vous ne pouvez pas combiner des VLAN sources et des VLAN de filtre dans une session. Vous pouvez avoir des VLAN sources ou des VLAN de filtre, mais pas les deux en même temps.

Caractéristiques du VLAN source

La fonctionnalité VSPAN est la surveillance du trafic réseau dans un ou plusieurs VLAN. L'interface source de la fonctionnalité SPAN ou RSPAN dans la fonctionnalité VSPAN est un ID de VLAN, et le trafic est surveillé sur tous les ports pour ce VLAN.

La fonctionnalité VSPAN a les caractéristiques suivantes :

- Tous les ports actifs dans le VLAN source sont inclus comme ports sources et peuvent être surveillés dans l'un ou l'autre des directions, ou dans les deux.
- Sur un port donné, seul le trafic sur le VLAN surveillé est envoyé au port de destination.
- Si un port de destination appartient à un VLAN source, il est exclu de la liste des sources et n'est pas surveillé.
- Si des ports sont ajoutés ou supprimés dans des VLAN sources, le trafic sur le VLAN source reçu par ces ports est ajouté ou supprimé dans les sources qui sont surveillées.
- Vous ne pouvez pas utiliser, dans une même session, des VLAN de filtre avec des sources de VLAN.
- Vous pouvez surveiller uniquement les VLAN Ethernet.

Caractéristiques du port de destination

Chaque session SPAN locale ou session de destination RSPAN doit avoir un port de destination (également appelé « port de surveillance ») qui reçoit une copie du trafic en provenance des ports et VLAN sources.

Un port de destination a les caractéristiques suivantes :

- Un port de destination doit résider sur le même commutateur que le port source (pour une session SPAN locale).
- Un port de destination peut être n'importe quel port physique Ethernet.
- Un port de destination ne peut participer qu'à une seule session SPAN à la fois. Un port de

destination dans une session SPAN ne peut pas être un port de destination pour une deuxième session SPAN.

- Un port de destination ne peut pas être un port source.
- Un port de destination ne peut pas être un groupe EtherChannel.

> Remarque : à partir de la version 12.2(33)SXH du logiciel Cisco IOS, l'interface PortChannel peut être un port de destination. Les EtherChannels de destination ne prennent pas en charge les protocoles EtherChannel PAgP (Port Aggregation Control Protocol) ou LACP (Link Aggregation Control Protocol) ; seul le mode on est pris en charge, avec la prise en charge de tous les protocoles EtherChannel désactivée.

> Remarque : reportez-vous aux Destinations SPAN, RSPAN et ERSPAN locales pour plus d'informations.

- Un port de destination peut être un port physique qui est affecté à un groupe EtherChannel, même si ce groupe EtherChannel a été spécifié comme source de la fonctionnalité SPAN. Le port est supprimé du groupe pendant sa configuration comme port de destination de la fonctionnalité SPAN.
- Le port ne transmet aucun trafic excepté le trafic requis pour la session SPAN sauf si l'apprentissage est activé. Dans ce cas, le port transmet également le trafic destiné aux hôtes qui ont été appris sur le port de destination.

> Remarque : reportez-vous aux Destinations SPAN, RSPAN et ERSPAN locales pour plus d'informations.

- Par conception, l'état du port de destination est actif/inactif. L'interface montre le port dans cet état pour indiquer clairement qu'il n'est actuellement pas utilisable comme port de production.
- Si le transfert du trafic entrant est activé pour un périphérique de sécurité du réseau, le port de destination transfère le trafic à la couche 2.
- Un port de destination ne participe pas à l'arborescence fractionnée pendant que la session SPAN est active.
- Quand il est un port de destination, il ne participe à aucun des protocoles de couche 2 (STP, VTP, CDP, DTP, PagP).
- Un port de destination qui appartient à un VLAN source d'une session SPAN est exclu de la liste des sources et n'est pas surveillé.
- Un port de destination reçoit des copies du trafic envoyé et reçu pour tous les ports sources surveillés. Si un port de destination est surabonné, il peut devenir saturé. Cet encombrement

peut affecter le transfert du trafic sur un ou plusieurs des ports sources.

Caractéristiques du port de réflecteur

Le port de réflecteur est le mécanisme qui copie les paquets sur un VLAN RSPAN. Le port de réflecteur transfère uniquement le trafic en provenance de la session source RSPAN à laquelle il est affilié.

Tout périphérique connecté à un port défini comme port de réflecteur perd la connectivité jusqu'à ce que la session source RSPAN soit désactivée.

Le port de réflecteur a les caractéristiques suivantes :

- C'est un port défini pour effectuer un retour en boucle.
- Ce ne peut pas être un groupe EtherChannel, il n'est pas un tronc, et il ne peut pas effectuer de filtrage de protocoles.
- Cela peut être un port physique qui est affecté à un groupe EtherChannel, même si le groupe EtherChannel est spécifié comme source de la fonctionnalité SPAN. Le port est supprimé du groupe pendant sa configuration comme port de réflecteur.
- Un port utilisé comme port de réflecteur ne peut pas être une source de la fonctionnalité SPAN ou un port de destination. Un port ne peut pas non plus être un port de réflecteur pour plusieurs sessions à la fois.
- Il est invisible pour tous les VLAN.
- Le VLAN natif pour le trafic retourné en boucle sur un port de réflecteur est le VLAN RSPAN.
- Le port de réflecteur retourne en boucle le trafic sans balise au commutateur. Le trafic est alors placé sur le VLAN RSPAN et propagé aux ports de jonction qui comportent le VLAN RSPAN.
- L'arborescence fractionnée est automatiquement désactivée sur un port de réflecteur.
- Un port de réflecteur reçoit des copies du trafic envoyé et reçu pour tous les ports sources surveillés.

Fonctionnalité SPAN sur Catalyst Express 500/520

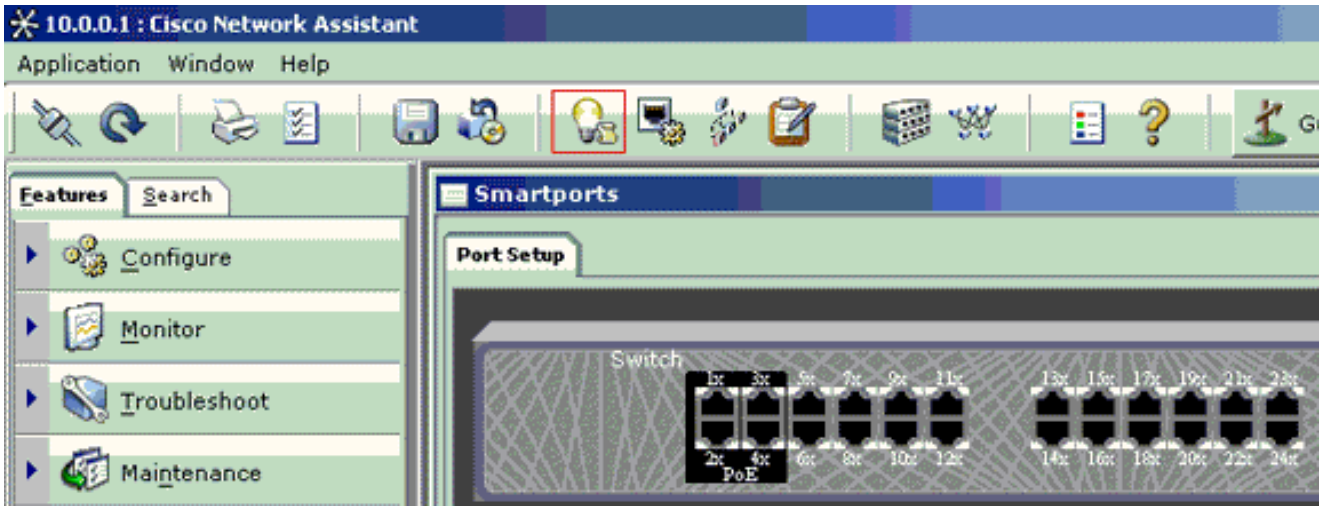
Catalyst Express 500 ou Catalyst Express 520 prend en charge uniquement la fonctionnalité SPAN. Les ports Catalyst Express 500/520 peuvent être configurés pour la fonctionnalité SPAN uniquement à l'aide de Cisco Network Assistant (CNA). Pour configurer la fonctionnalité SPAN, exécutez les étapes suivantes :

1. Téléchargez et installez CNA sur le PC.

   Vous pouvez télécharger CNA à partir de la page Download Software (clients enregistrés

seulement).

2. Exécutez les étapes mentionnées dans le Guide de mise en route pour les commutateurs Catalyst Express 500 12.2(25)FY pour personnaliser les paramètres de commutateur pour Catalyst Express 500. Pour plus d'informations sur Catalyst Express 520, reportez-vous au Guide de mise en route pour les commutateurs Catalyst Express 520.
3. Utilisez CNA pour vous connecter au commutateur, puis cliquez sur Smartport.

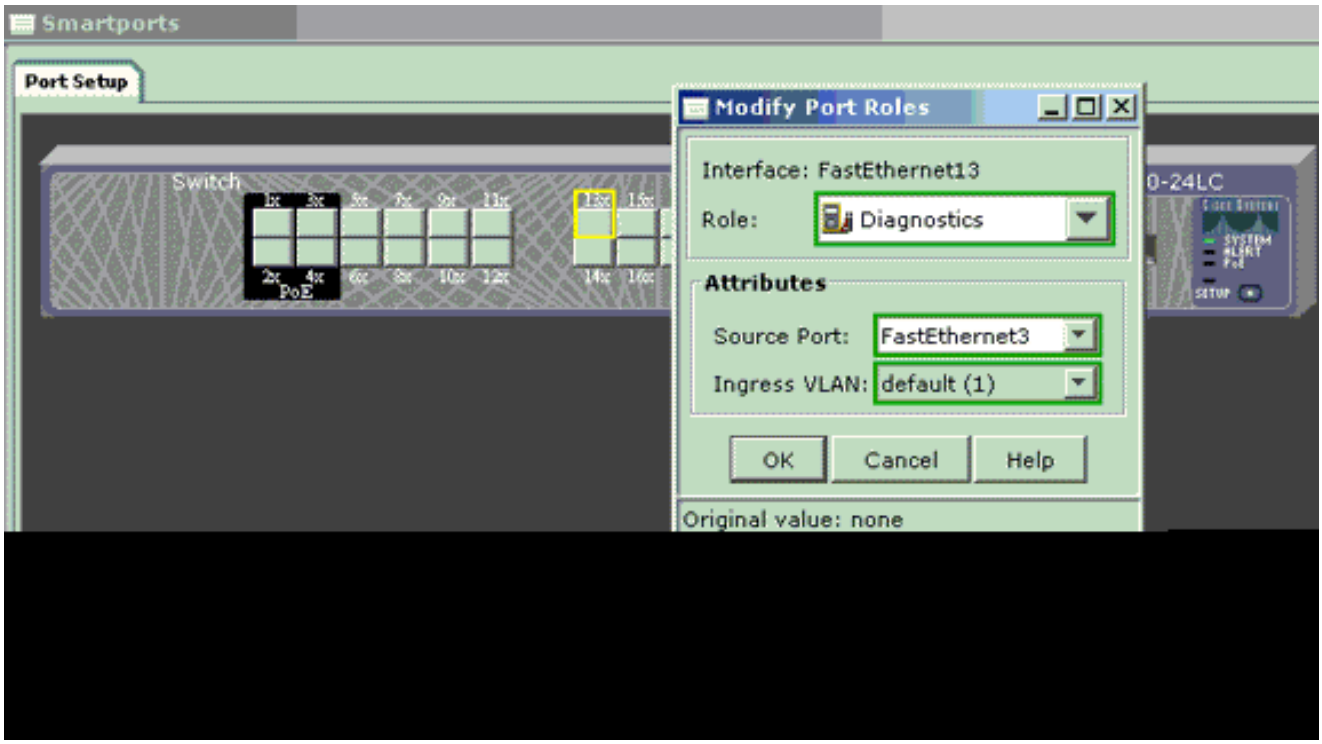


4. Cliquez sur une interface où vous envisagez de connecter le PC afin de capturer les traces du renifleur.
5. Cliquez sur Modify.

   Une petite zone contextuelle s'affiche.

6. Choisissez le rôle Diagnostics pour le port.
7. Choisissez le port source et sélectionnez le VLAN que vous envisagez de surveiller.

   Si vous n'en sélectionnez aucun, le port reçoit seulement le trafic. Le VLAN d'entrée permet au PC connecté au port Diagnostics d'envoyer les paquets au réseau qui utilise ce VLAN.



8. Cliquez sur OK pour fermer la zone contextuelle.
9. Cliquez sur OK, puis sur Apply pour appliquer les paramètres.
10. Vous pouvez utiliser n'importe quel logiciel renifleur pour suivre le trafic une fois le port de diagnostic défini.

Fonctionnalité SPAN sur les commutateurs Catalyst 2900XL/3500XL

Fonctionnalités disponibles et restrictions

La fonctionnalité de surveillance de port n'est pas très étendue sur Catalyst 2900XL/3500XL. Par conséquent, elle est relativement simple à comprendre.

Vous pouvez créer autant de sessions PSPAN locales que nécessaires. Par exemple, vous pouvez créer des sessions PSPAN sur le port de configuration que vous avez choisi pour être un port SPAN de destination. Dans ce cas, émettez l'interface port monitor afin d'afficher la liste des ports sources que vous souhaitez surveiller. Un port de surveillance est un port SPAN de destination dans la terminologie relative à Catalyst 2900XL/3500XL.

- La principale restriction est que tous les ports qui sont associés à une session particulière (source ou de destination) doivent appartenir au même VLAN.
- Si vous configurez l'interface de VLAN avec une adresse IP, la commande port monitor surveille le trafic destiné à cette adresse IP uniquement. Elle surveille également le trafic de diffusion qui est reçu par l'interface de VLAN. Cependant, elle ne capture pas le trafic qui passe dans le VLAN réel lui-même. Si vous ne spécifiez pas d'interface dans la commande port monitor, tous les autres ports qui appartiennent au même VLAN que l'interface sont surveillés.

Cette liste fournit certaines restrictions. Référez-vous au guide de référence des commandes (Catalyst 2900XL/3500XL) pour plus d'informations.

Remarque : les ports ATM sont les seuls ports qui ne peuvent pas être des ports de surveillance. Cependant, vous pouvez surveiller les ports ATM. Les restrictions de cette liste s'appliquent aux ports qui ont la capacité de port de surveillance.

- Un port de surveillance ne peut pas se trouver dans un groupe de ports Fast EtherChannel ou Gigabit EtherChannel.
- Un port de surveillance ne peut pas être activé pour la sécurité de port.
- Un port de surveillance ne peut pas être un port à VLAN multiple.
- Un port de surveillance doit être membre du même VLAN que le port qui est surveillé. Des modifications d'appartenance aux VLAN ne sont pas autorisées sur les ports de surveillance et les ports qui sont surveillés.
- Un port de surveillance ne peut pas être un port d'accès dynamique ou un port de jonction. Cependant, un port d'accès statique peut surveiller un VLAN sur un port de tronc, un port à VLAN multiple ou un port d'accès dynamique. Le VLAN qui est surveillé est celui qui est associé au port d'accès statique.
- La surveillance de port ne fonctionne pas si le port de surveillance et le port qui est surveillé sont des ports protégés.

Faites attention qu'un port dans l'état de surveillance n'exécute pas le protocole STP (Spanning Tree Protocol) alors qu'il appartient encore au VLAN des ports qu'il met en miroir. La surveillance de port peut faire partie d'une boucle si, par exemple, vous le connectez à un concentrateur ou un pont et que vous effectuez une boucle sur une autre partie du réseau. Dans ce cas, vous pouvez terminer dans une condition de boucle de pontage catastrophique car STP ne vous protège plus. Consultez la section Pourquoi la session SPAN crée-t-elle une boucle de pontage ? de ce document pour un exemple de la façon dont cette condition peut se produire.

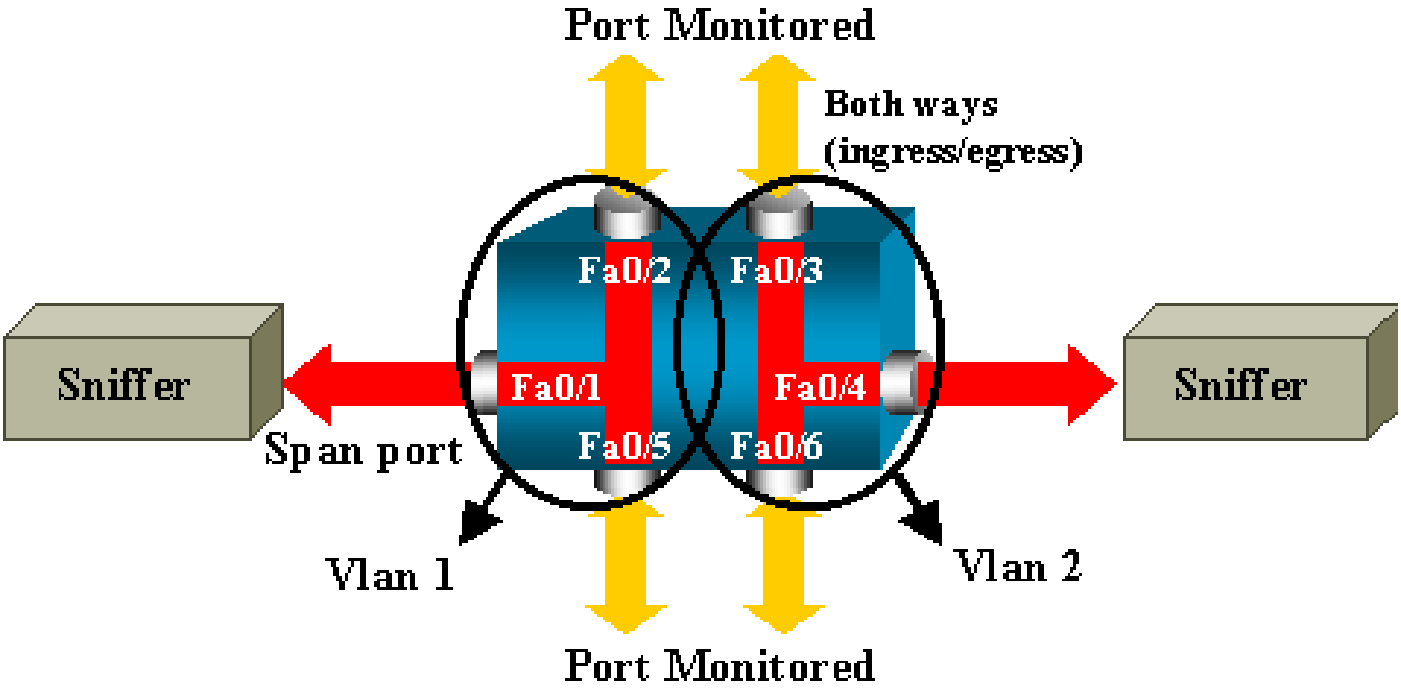
Exemple de configuration

Cet exemple crée deux sessions SPAN simultanées.

- Le port Fast Ethernet 0/1 (Fa0/1) surveille le trafic que les ports Fa0/2 et Fa0/5 envoient et reçoivent. Le port Fa0/1 surveille également le trafic vers et en provenance de l'interface de gestion VLAN 1.
- Le port Fa0/4 surveille les ports Fa0/3 et Fa0/6.

Les ports Fa0/3, Fa0/4 et Fa0/6 sont tous configurés dans VLAN 2. Les autres ports et l'interface de gestion sont configurés dans le VLAN par défaut VLAN 1.

Diagramme du réseau



Exemple de configuration sur Catalyst 2900XL/3500XL

Exemple de configuration SPAN 2900XL/3500XL

```
!--- Output suppressed.
!
interface FastEthernet0/1
port monitor FastEthernet0/2
 port monitor FastEthernet0/5
 port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
 port monitor FastEthernet0/3
 port monitor FastEthernet0/6
 switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 2
!
!--- Output suppressed.
!
interface VLAN1
 ip address 10.200.8.136 255.255.252.0
 no ip directed-broadcast
 no ip route-cache
!
!--- Output suppressed.
```

Explication des étapes de configuration

Pour configurer le port Fa0/1 comme port de destination, les ports sources Fa0/2 et Fa0/5, ainsi que l'interface de gestion (VLAN 1), sélectionnez l'interface Fa0/1 dans le mode de configuration :

<#root>

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

Entrez la liste de ports à surveiller :

<#root>

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

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

Avec cette commande, chaque paquet que ces deux ports reçoivent ou transmettent est également copié vers le port Fa0/1. Pour configurer la surveillance pour l'interface d'administration, émettez une variation de la commande port monitor :

<#root>

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

Remarque : cette commande ne signifie pas que le port Fa0/1 surveille l'ensemble du VLAN 1. Le mot clé VLAN 1 fait simplement référence à l'interface d'administration du commutateur.

Cet exemple de commande montre que la surveillance d'un port dans un autre VLAN est impossible :

<#root>

```
Switch(config-if)#
```

```
port monitor fastethernet 0/3

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

Pour terminer la configuration, configurez une autre session. Cette fois-ci, utilisez Fa0/4 comme port SPAN de destination :

```
<#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
```

Pour contrôler la configuration, émettez la commande show running, ou utilisez la commande show port monitor :

```
<#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
```

Remarque : les Catalyst 2900XL et 3500XL ne prennent pas en charge la fonctionnalité SPAN dans la direction Rx uniquement (Rx SPAN ou SPAN d'entrée) ou dans la direction Tx uniquement (Tx SPAN ou SPAN de sortie). Tous les ports SPAN sont conçus pour capturer à la fois le trafic Rx et le trafic Tx.

Fonctionnalité SPAN sur Catalyst 2948G-L3 et 4908G-L3

Catalyst 2948G-L3 et Catalyst 4908G-L3 sont des commutateurs-routeurs à configuration fixe ou des commutateurs de couche 3. La fonctionnalité SPAN sur un commutateur de couche 3 s'appelle « espionnage de port ».

Cependant, l'espionnage de port n'est pas pris en charge sur ces commutateurs. Reportez-vous à la section Fonctionnalités non prises en charge du document Notes de publication relatives à Catalyst 2948G-L3 et Catalyst 4908G-L3 pour Cisco IOS Version 12.0(10)W5(18g).

Fonctionnalité SPAN sur Catalyst 8500

Une fonctionnalité SPAN très basique est disponible sur Catalyst 8540 sous le nom « espionnage de port ». Pour plus d'informations, reportez-vous à la documentation actuelle de Catalyst 8540 .

La surveillance des ports vous permet de mettre en miroir de manière transparente le trafic d'un ou plusieurs ports source vers un port de destination."

Pour configurer la mise en miroir du trafic basé sur les ports, ou espionnage, émettez la commande snoop. Pour désactiver l'espionnage, émettez la forme no de cette commande :

<#root>

snoop interface source_port direction snoop_direction

no snoop interface source_port

La variable source_port fait référence au port qui est surveillé. La variable snoop_direction est la direction du trafic sur le ou les ports source qui sont surveillés : receive, transmit, ou both.

<#root>

8500CSR#

configure terminal

8500CSR(config)#

interface fastethernet 12/0/15

8500CSR(config-if)#

shutdown

```
8500CSR(config-if)#
snoop interface fastethernet 0/0/1 direction both

8500CSR(config-if)#
no shutdown
```

Cet exemple montre la sortie de la commande show snoop :

```
<#root>
8500CSR#
show snoop

Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option:         (configured=enabled)(actual=enabled)
Snoop direction:      (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```

Remarque : cette commande n'est pas prise en charge sur les ports Ethernet d'un Catalyst 8540 si vous exécutez une image de routeur de commutation ATM multiservice (MSR), telle que 8540m-in-mz. Au lieu de cela, vous devez utiliser une image de commutateur-routeur Campus (CSR), telle que 8540c-in-mz.

Fonctionnalité SPAN sur les commutateurs de la gamme Catalyst 2900, 4500/4000, 5500/5000 et 6500/6000 qui exécutent CatOS

Cette section s'applique uniquement aux commutateurs de la gamme Cisco Catalyst 2900 suivants :

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

Cette section s'applique aux commutateurs de la gamme Cisco Catalyst 4000, lesquels incluent :

- Commutateurs à châssis modulaire :
  - Commutateur Cisco Catalyst 4003
  - Commutateur Cisco Catalyst 4006

- Commutateur à châssis fixe :
    - Commutateur Cisco Catalyst 4912G

Fonctionnalité SPAN locale

Les fonctionnalités SPAN ont été ajoutées une par une à CatOS, et une configuration SPAN se compose d'une seule commande set span. Il existe désormais un large éventail d'options disponibles pour la commande :

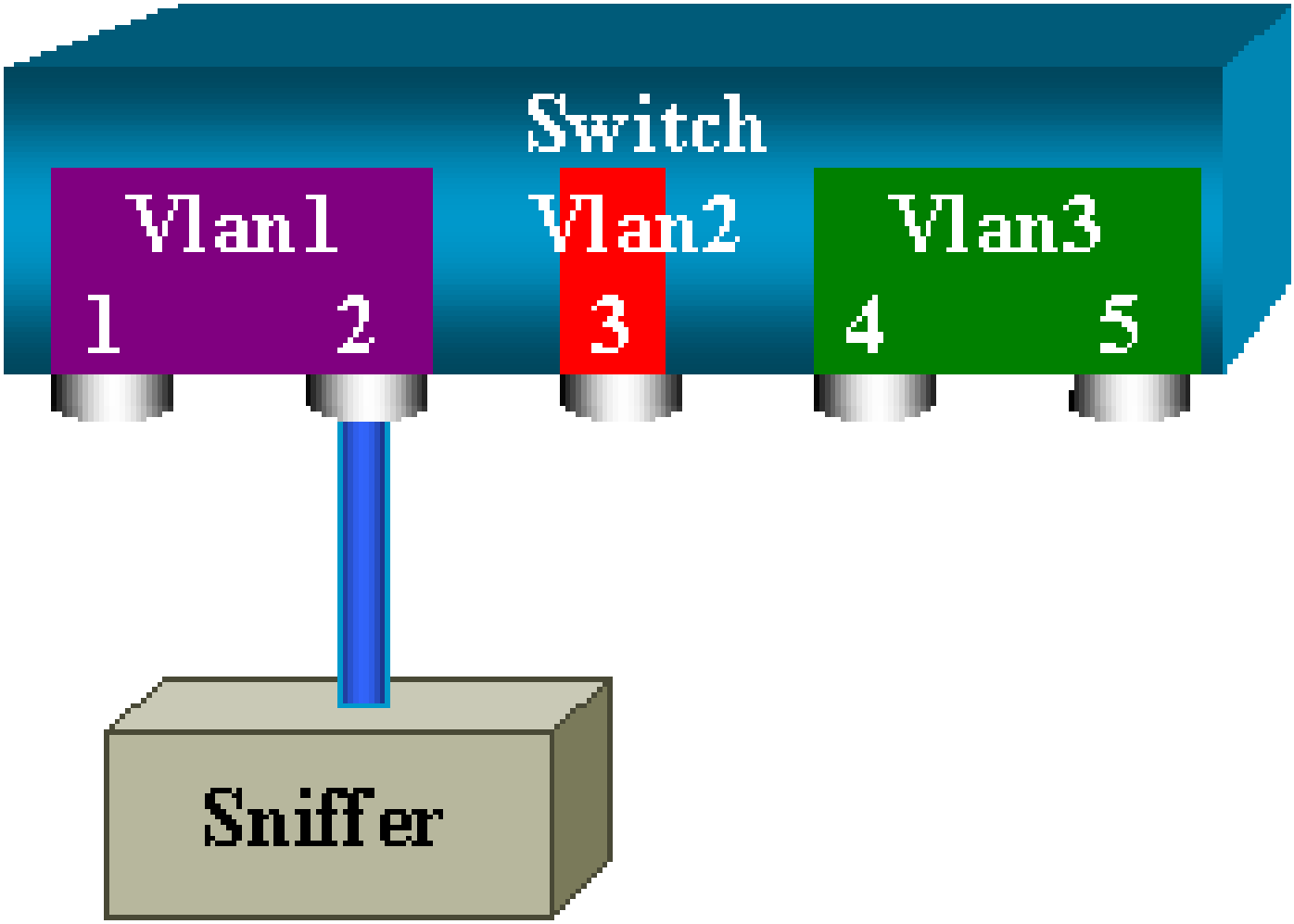
<#root>

```
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]
```

Ce diagramme de réseau présente les différentes possibilités de fonctionnalité SPAN avec utilisation de variations :



Ce diagramme représente une partie d'une carte de ligne unique qui se trouve dans l'emplacement 6 d'un commutateur Catalyst 6500/6000. Dans ce scénario :

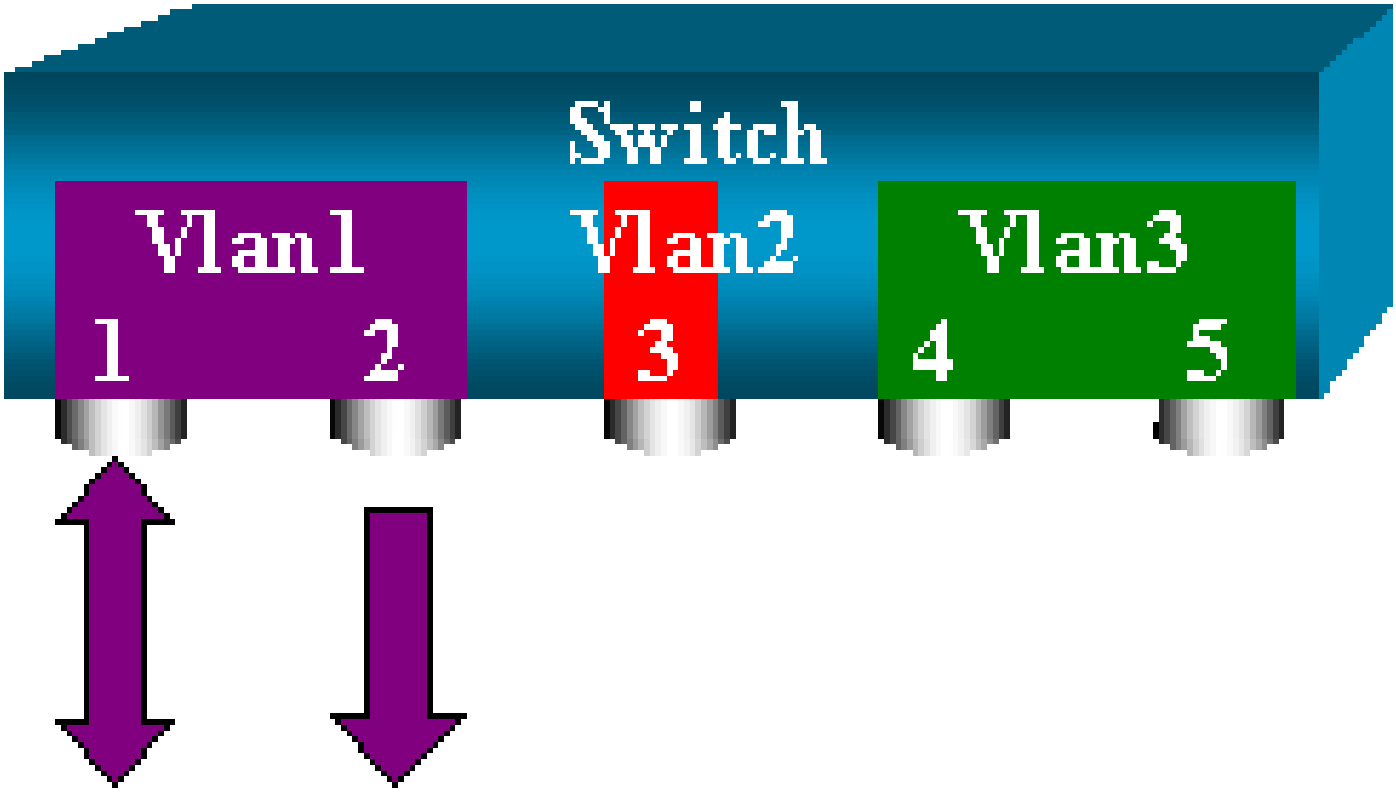
- Les ports 6/1 et 6/2 appartiennent à VLAN 1
- Le port 6/3 appartient à VLAN 2
- Les ports 6/4 et 6/5 appartiennent à VLAN 3

Connectez un renifleur au port 6/2 et utilisez-le comme port de surveillance dans plusieurs cas différents.

PSPAN, VSPAN : surveillance de certains ports ou d'un VLAN entier

Pour surveiller un seul port, émettez la forme la plus simple de la commande set span. La syntaxe est set span source_port dest_modination.

Surveiller un seul port avec la fonctionnalité 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
```

Avec cette configuration, chaque paquet qui est reçu ou envoyé par le port 6/1 est copié sur le port 6/2. Une description claire de cela apparaît lorsque vous entrez la configuration. Pour recevoir un résumé de la configuration SPAN actuelle, émettez la commande show span :

<#root>

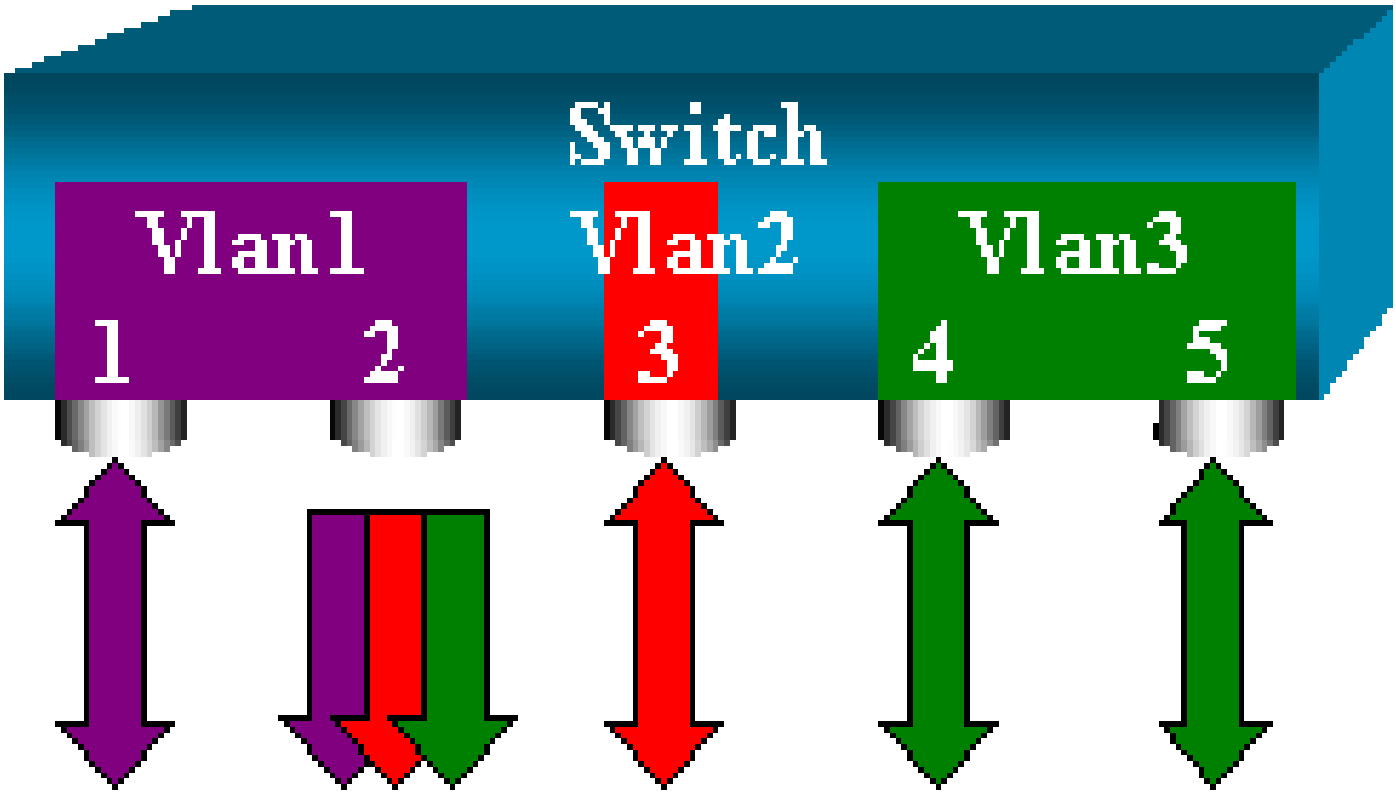
```
switch (enable)
```

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
```

Surveiller plusieurs ports avec la fonctionnalité SPAN



La commande set span source_ports destination_port permet à l'utilisateur de spécifier plusieurs ports sources. Répertoriez simplement tous les ports sur lesquels vous voulez implémenter la fonctionnalité SPAN, en séparant les ports avec des virgules.

L'interprète de ligne de commande vous permet également d'utiliser le trait d'union pour spécifier une plage de ports.

L'exemple suivant illustre cette possibilité pour spécifier plusieurs ports. Il utilise la fonctionnalité SPAN sur le port 6/1 et une plage de trois ports, de 6/3 à 6/5 :

Remarque : il ne peut y avoir qu'un seul port de destination. Spécifiez toujours le port de destination après la source de la fonctionnalité SPAN.

<#root>

```
switch (enable)
```

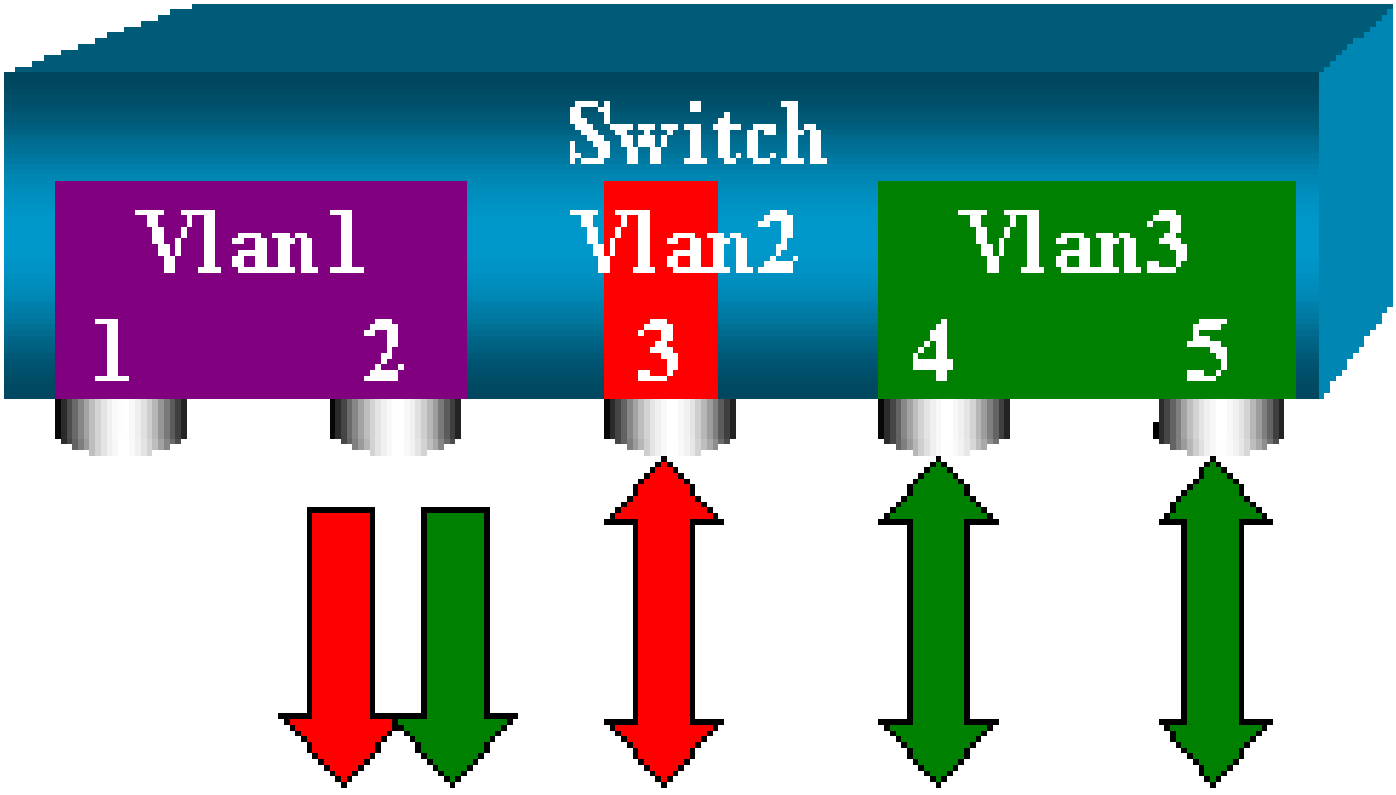
`set span 6/1,6/3-5 6/2`

```
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
```

Remarque : contrairement aux commutateurs Catalyst 2900XL/3500XL, les commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000 peuvent surveiller les ports qui appartiennent à plusieurs VLAN différents avec des versions de CatOS antérieures à 5.1. Ici, les ports mis en miroir sont affectés aux VLAN 1, 2 et 3.

Surveiller des VLAN avec la fonctionnalité SPAN

En définitive, la commande set span vous permet de configurer un port pour surveiller le trafic local pour la totalité d'un VLAN. La commande est set span source_vlan(s) destination_port .



Utilisez une liste d'un ou de plusieurs VLAN comme source, au lieu d'une liste de ports :

<#root>

```
switch (enable)
```

set span 2,3 6/2

```
2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 2-3
Oper Source : Port 6/3-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

Avec cette configuration, chaque paquet qui entre dans VLAN 2 ou 3 ou qui en sort est dupliqué sur le port 6/2.

Remarque : le résultat est exactement le même que si vous implémentez la fonctionnalité SPAN individuellement sur tous les ports qui appartiennent aux VLAN spécifiés par la commande. Comparez le champ `Oper Source` et le champ `Admin Source`. Le champ `Admin Source` répertorie essentiellement tous les ports que vous avez configurés pour la session SPAN, et le champ `Oper Source` répertorie les ports qui utilisent la fonctionnalité SPAN.

SPAN d'entrée/de sortie

Dans l'exemple figurant dans la section Surveiller des VLAN avec la fonctionnalité SPAN, le trafic qui entre dans les ports spécifiés et qui en sort est surveillé.

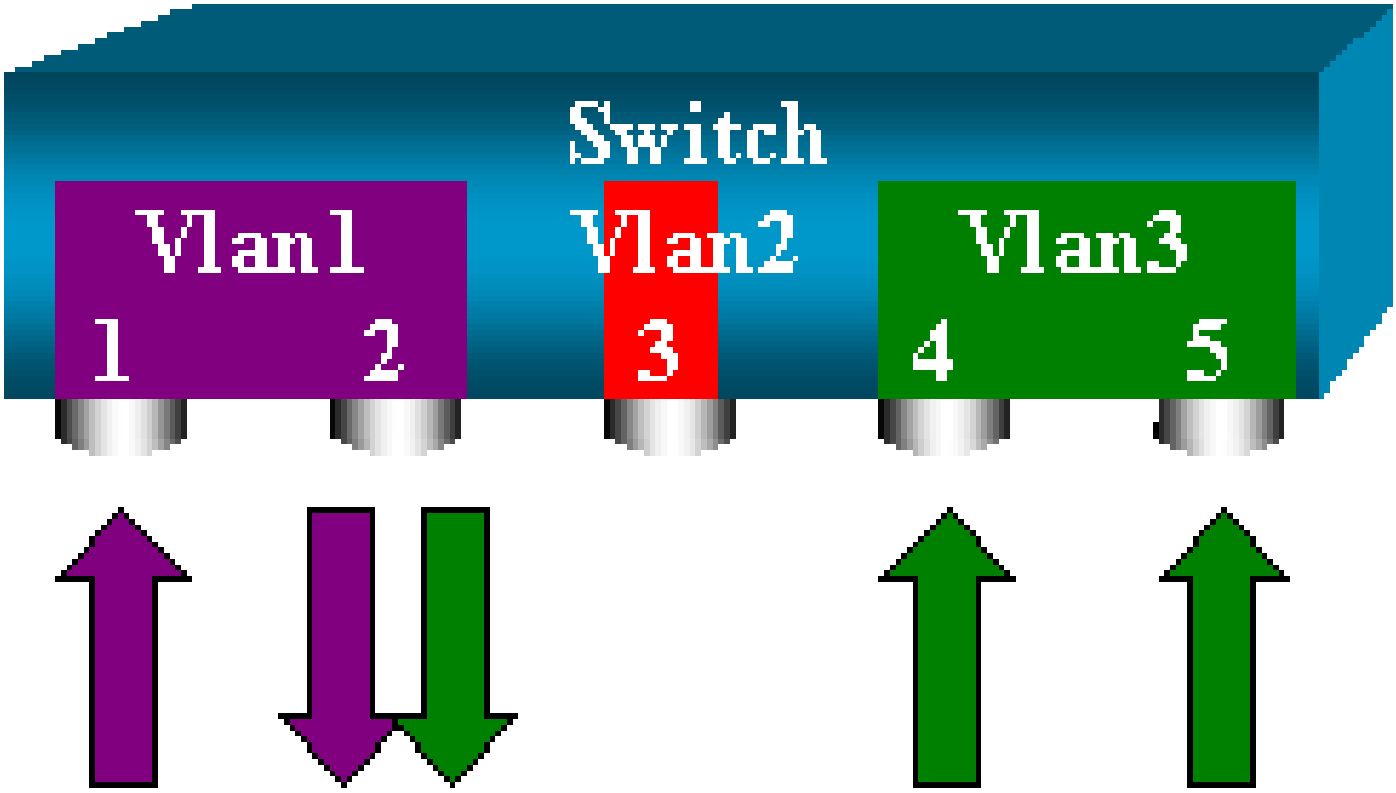
Le champ `Direction : transmit/receive` le montre. Les commutateurs de la gamme Catalyst 4500/4000, 5500/5000 et 6500/6000 vous permettent de collecter uniquement le trafic de sortie ou d'entrée sur un port particulier.

Ajoutez le mot clé rx (recevoir) ou tx (transmettre) à la fin de la commande. La valeur par défaut est both (tx et rx).

<#root>

set span source_port destination_port [rx | tx | both]

Dans cet exemple, la session capture tout le trafic entrant pour les VLAN 1 et 3, et met en miroir le trafic vers le port 6/2 :



<#root>

```
switch (enable)
```

set span 1,3 6/2 rx

```
2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 1,3
Oper Source : Port 1/1,6/1,6/4-5,15/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

Implémenter la fonctionnalité SPAN sur une jonction

Les jonctions sont un cas particulier dans un commutateur, car ce sont des ports qui comportent plusieurs VLAN. Si une jonction est sélectionnée comme port source, le trafic de tous les VLAN sur cette jonction est surveillé.

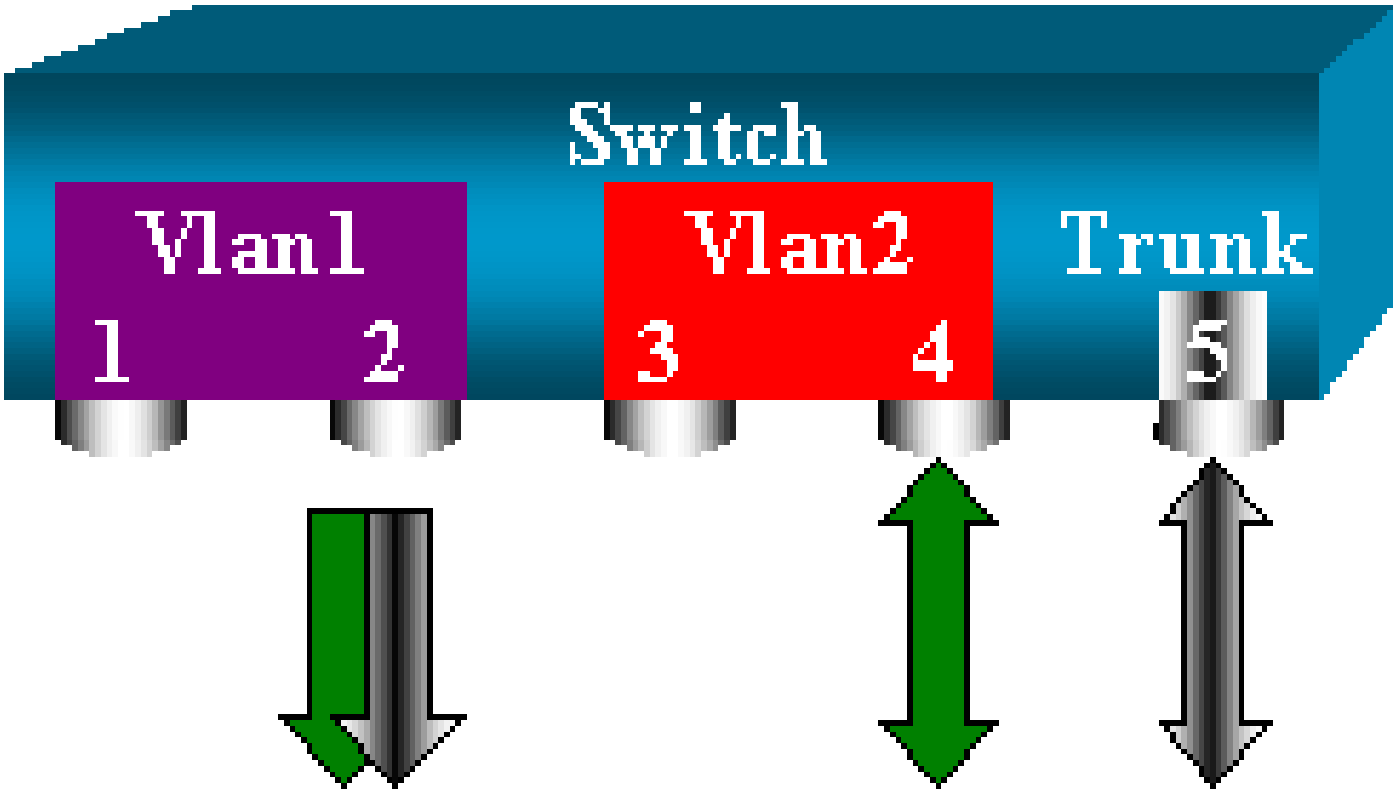
Surveiller un sous-ensemble de VLAN qui appartiennent à une jonction

Dans ce diagramme, le port 6/5 est maintenant une jonction qui comporte tous les VLAN. Imaginez que vous voulez utiliser la fonctionnalité SPAN sur le trafic dans VLAN 2 pour les ports 6/4 et 6/5. Émettez simplement la commande suivante :

<#root>

```
switch (enable)
```

set span 6/4-5 6/2



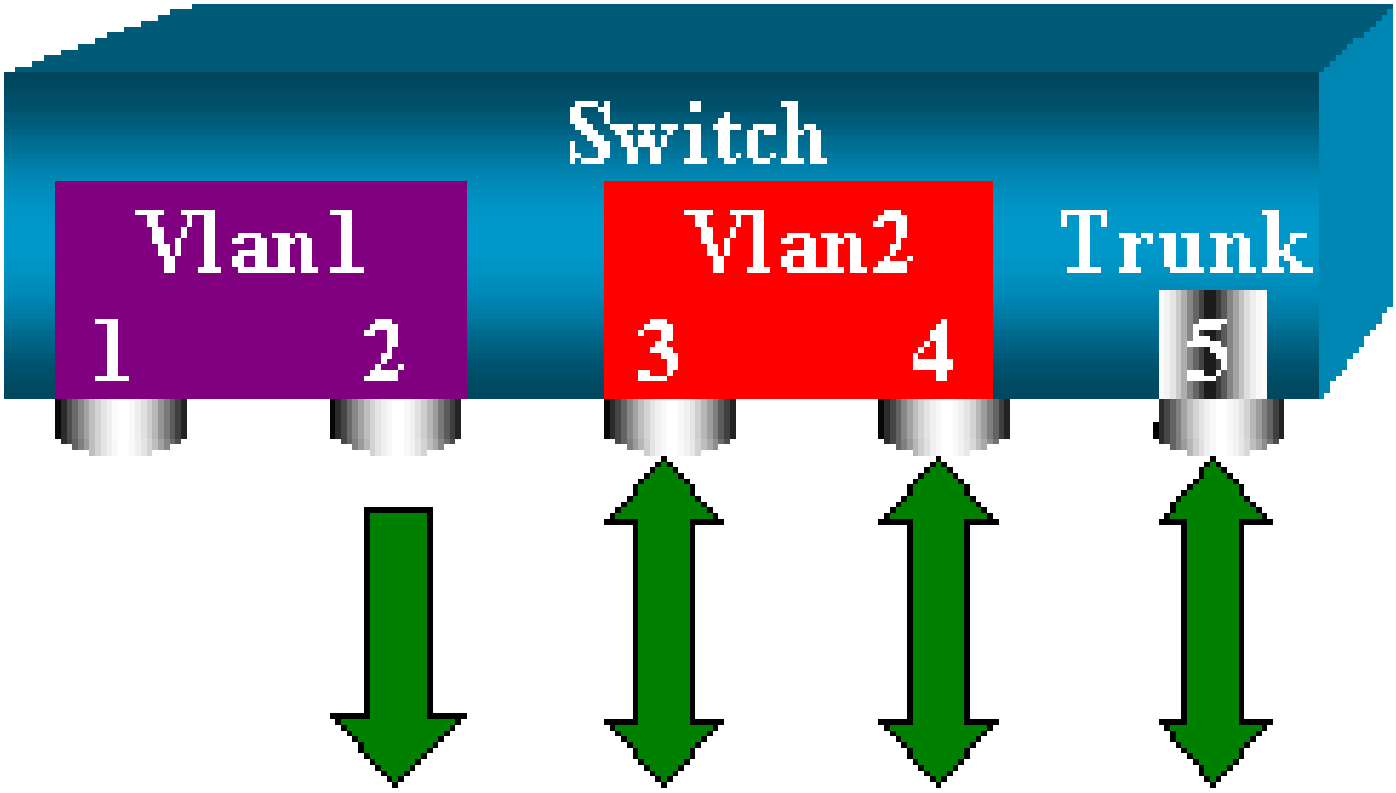
Dans le cas présent, le trafic qui est reçu sur le port SPAN est une combinaison du trafic que vous voulez et de tous les VLAN que le tronc 6/5 comporte.

Par exemple, il n'y a aucune façon de distinguer, sur le port de destination, si un paquet provient du port 6/4 dans VLAN 2 ou du port 6/5 dans VLAN 1. Une autre possibilité consiste à utiliser la fonctionnalité SPAN sur la totalité de VLAN 2 :

<#root>

```
switch (enable)
```

set span 2 6/2



Avec cette configuration, au moins, vous surveillez uniquement le trafic qui appartient à VLAN 2 en provenance de la jonction. Le problème est que, maintenant, vous recevez également le trafic que vous ne vouliez pas en provenance du port 6/3.

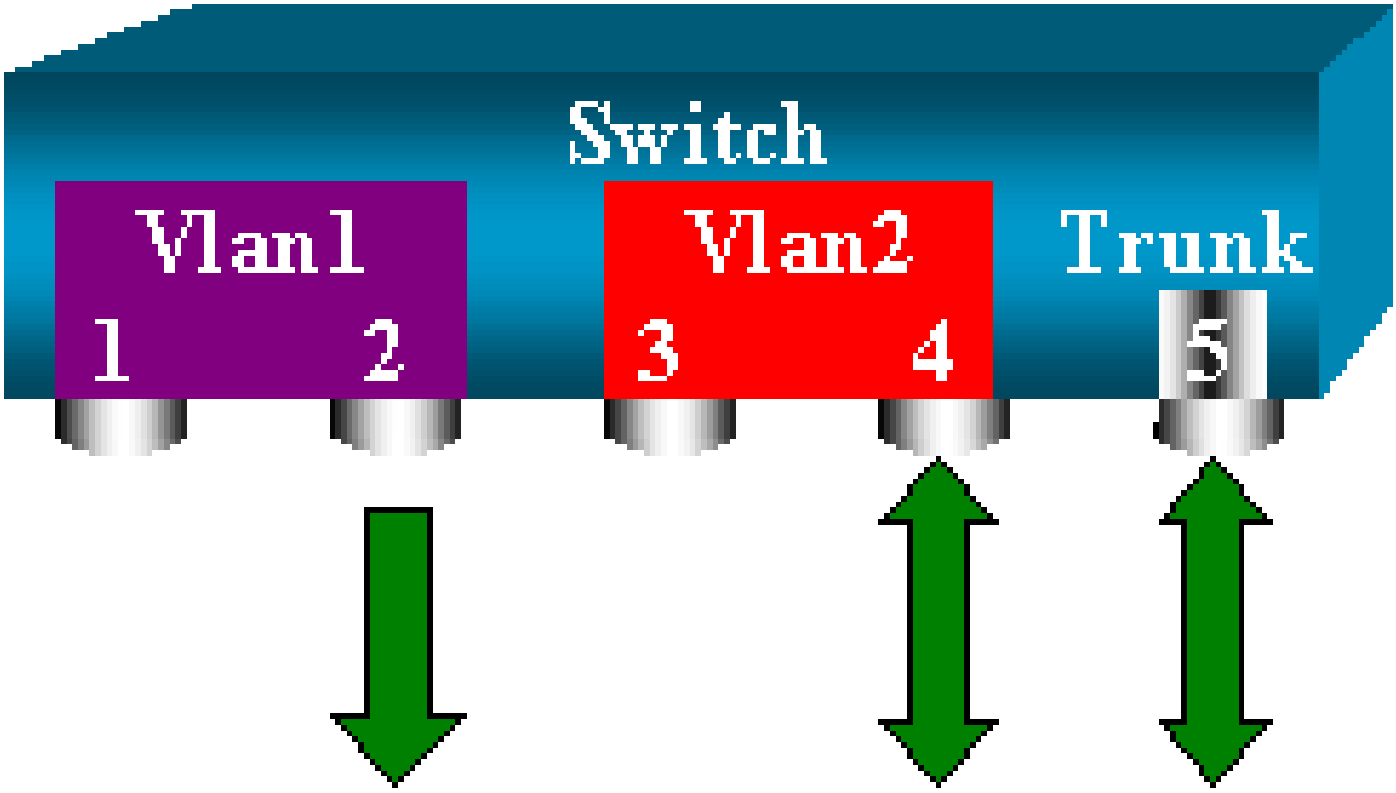
CatOS inclut un autre mot clé qui vous permet de sélectionner des VLAN à surveiller à partir d'une jonction :

<#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
```



Cette commande atteint l'objectif, car vous sélectionnez VLAN 2 sur toutes les jonctions qui sont surveillées. Vous pouvez spécifier plusieurs VLAN avec cette option de filtre.

Remarque : cette option de filtre est uniquement prise en charge sur les commutateurs Catalyst 4500/4000 et Catalyst 6500/6000. Catalyst 5500/5000 ne prend pas en charge l'option de filtre qui est disponible avec la commande set span.

Définition du mode Trunk sur le port de destination

Si vous avez des ports sources qui appartiennent à plusieurs VLAN différents, ou si vous utilisez la fonctionnalité SPAN sur plusieurs VLAN sur un port de jonction (trunk), vous pouvez identifier à quel VLAN un paquet que vous recevez sur le port SPAN de destination appartient.

Cette identification est possible si vous activez le mode Trunk sur le port de destination avant de configurer le port pour la fonctionnalité SPAN. Ainsi, tous les paquets qui sont transférés au renifleur sont également marqués avec leur ID de VLAN respectif.

Remarque : votre analyseur doit reconnaître l'encapsulation correspondante.

<#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

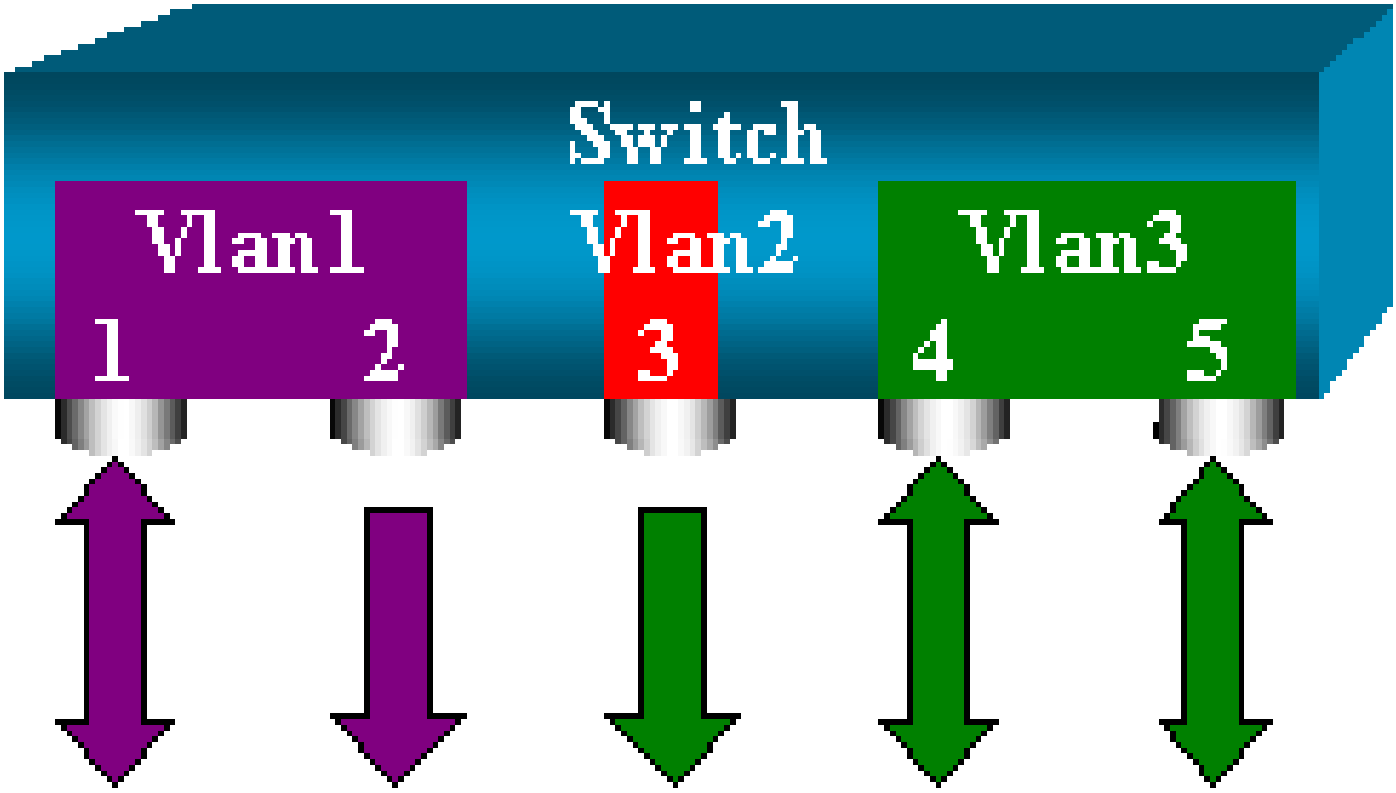
```
Port(s) 6/2 trunk mode set to nonegotiate.
Port(s) 6/2 trunk type set to isl.
switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become
  isl trunk
switch (enable)
```

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
```

Créer plusieurs sessions simultanées

Jusqu'ici, une seule session SPAN a été créée. Chaque fois que vous émettez une nouvelle commande set span, la configuration précédente est invalidée. CatOS a maintenant la possibilité d'exécuter plusieurs sessions simultanées. Il peut donc avoir différents ports de destination en même temps. Pour ajouter une session SPAN supplémentaire, émettez la commande set span source destination create. En cette session, le port 6/1 à 6/2 est surveillé, et en même temps, VLAN 3 vers le port 6/3 est surveillé :



<#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
```

Émettez maintenant la commande show span pour déterminer si vous avez deux sessions en même temps :

<#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
```

Des sessions supplémentaires sont créées. Il vous faut une façon de supprimer certaines sessions. La commande est la suivante :

<#root>

set span disable {all | destination_port}

Étant donné qu'il ne peut y avoir qu'un seul port de destination par session, le port de destination identifie une session. Supprimer la première session qui est créée, laquelle est celle qui utilise le port 6/2 comme destination :

<#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
```

Vous pouvez à présent vérifier qu'il ne reste qu'une seule session :

<#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
```

Pour désactiver toutes les sessions actuelles en une seule étape, émettez la commande suivante :

<#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
```

Autres options de la fonctionnalité SPAN

La syntaxe pour la commande set span est la suivante :

<#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]
```

Cette section présente brièvement les options décrites dans ce document :

- sc0 : vous spécifiez le mot clé sc0 dans une configuration SPAN lorsque vous devez surveiller le trafic vers l'interface de gestion sc0. Cette fonctionnalité est disponible sur les commutateurs Catalyst 5500/5000 et 6500/6000, version de code CatOS 5.1 ou ultérieures.
- inpkts enable/disable : Cette option est extrêmement importante. Comme l'indique ce document, un port que vous configurez en tant que destination de la fonctionnalité SPAN appartient encore à son VLAN d'origine. Les paquets qui sont reçus sur un port de destination entrent alors dans le VLAN, comme si ce port était un port d'accès normal. Ce comportement peut être souhaité. Si vous utilisez un PC comme renifleur, vous pouvoir vouloir que ce PC soit totalement connecté au VLAN. Néanmoins, la connexion peut être dangereuse si vous connectez le port de destination à un autre équipement réseau qui crée une boucle dans le réseau. Le port SPAN de destination n'exécute pas le protocole STP, et vous pouvez terminer dans une situation de boucle de pontage dangereuse. Consultez la section Pourquoi la session SPAN crée-t-elle une boucle de pontage ? de ce document afin de comprendre comment cette situation peut se produire. Le paramètre par défaut de cette option est disable, ce qui signifie que le port SPAN de destination ignore les paquets que le port reçoit. Cet abandon protège le port contre les boucles de pontage. Cette option apparaît dans CatOS 4.2.
- learning enable/disable : Cette option vous permet de désactiver l'apprentissage sur le port de destination. Par défaut, l'apprentissage est activé et le port de destination apprend les adresses MAC des paquets entrants que le port reçoit. Cette fonctionnalité apparaît dans CatOS 5.2 sur Catalyst 4500/4000 et 5500/5000, et dans CatOS 5.3 sur Catalyst 6500/6000.
- multicast enable/disable : Comme son nom l'indique, cette option vous permet d'activer ou de désactiver la surveillance des paquets de multidiffusion. La valeur par défaut est enable. Cette fonctionnalité est disponible sur Catalyst 5500/5000 et 6500/6000, CatOS 5.1 et versions ultérieures.
- spanning port 15/1 : sur le Catalyst 6500/6000, vous pouvez utiliser le port 15/1 (ou 16/1) comme source SPAN. Le port peut surveiller le trafic qui est transféré à la carte de commutation multicouche (MSFC). Le port capture le trafic qui est routé par logiciel ou acheminé vers la MSFC.

Fonctionnalité Remote SPAN

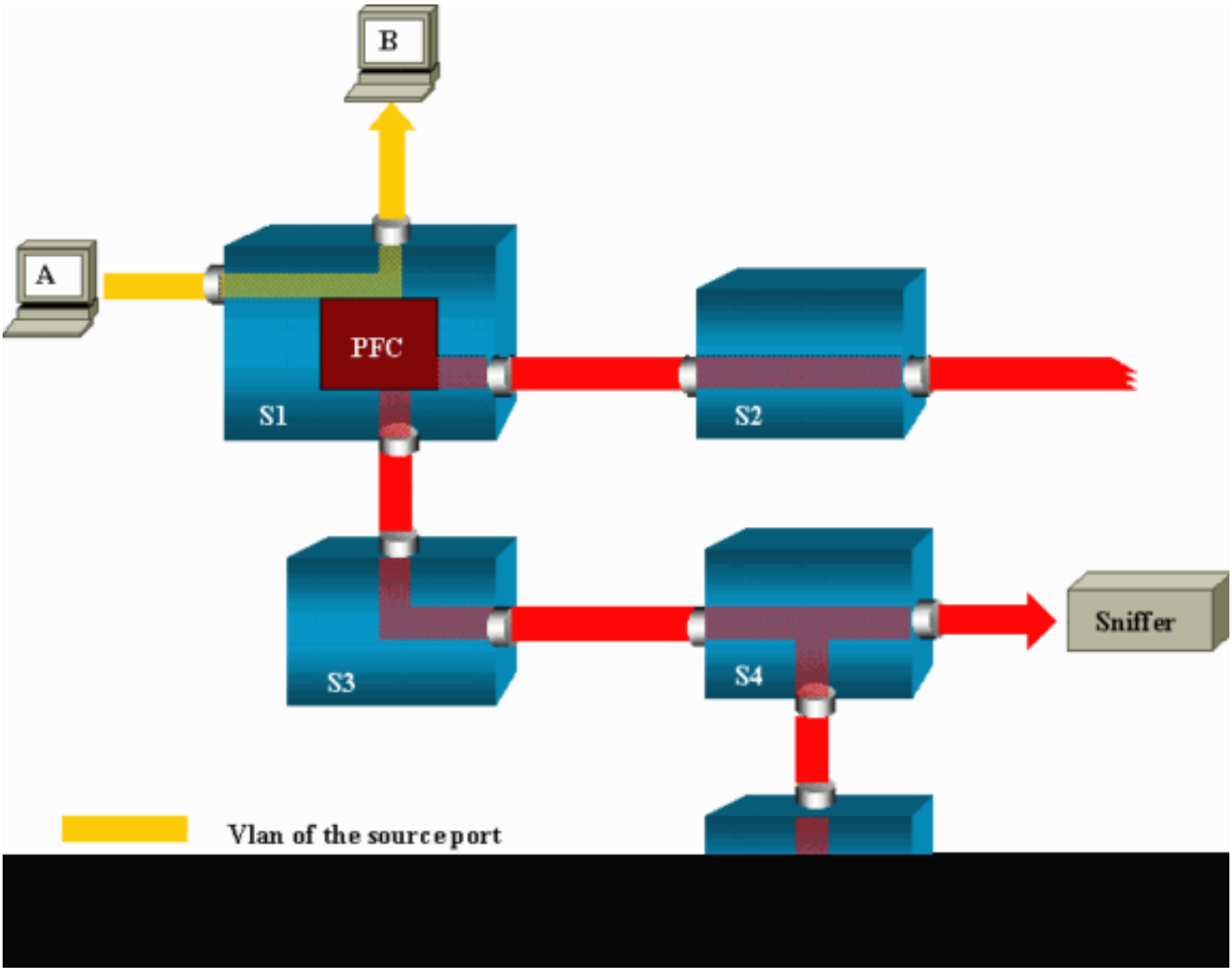
Présentation de la fonctionnalité RSPAN

La fonctionnalité RSPAN vous permet de surveiller les ports sources qui sont répartis sur l'ensemble d'un réseau commuté, et pas seulement localement sur un commutateur avec la

fonctionnalité SPAN. Cette fonctionnalité apparaît dans CatOS 5.3 dans les commutateurs de la gamme Catalyst 6500/6000 et est ajoutée dans les commutateurs de la gamme Catalyst 4500/4000 dans CatOS 6.3 et versions ultérieures.

La fonctionnalité fonctionne exactement comme une session SPAN normale. Le trafic qui est surveillé par la fonctionnalité SPAN n'est pas copié directement vers le port de destination, mais est propagé dans un VLAN RSPAN. Le port de destination peut donc se trouver n'importe où dans ce VLAN RSPAN. Il peut même y avoir plusieurs ports de destination.

Le diagramme suivant illustre la structure d'une session RSPAN :



Dans cet exemple, vous configurez la fonctionnalité RSPAN pour surveiller le trafic envoyé par l'hôte A. Lorsque A génère une trame qui est destinée à B, le paquet est copié par un circuit intégré à application spécifique (ASIC) de la carte Catalyst 6500/6000 Policy Feature Card (PFC) dans un VLAN RSPAN prédéfini. De là, le paquet est propagé vers tous autres ports qui appartiennent au VLAN RSPAN. Toutes les liaisons intercommutateurs dessinées ici sont des jonctions, ce qui est une spécification de la fonctionnalité RSPAN. Les seuls ports d'accès sont des ports de destination, où les renifleurs sont connectés (ici, sur S4 et S5).

Voici quelques remarques relatives à cette conception :

- S1 est appelé « commutateur source ». Les paquets entrent dans le VLAN RSPAN uniquement dans les commutateurs qui sont configurés en tant que source de la fonctionnalité RSPAN. Actuellement, un commutateur ne peut être la source que pour une session RSPAN, ce qui signifie qu'un commutateur source ne peut alimenter qu'un seul VLAN RSPAN à la fois.
- S2 et S3 sont des commutateurs intermédiaires. Ce ne sont pas des sources de la fonctionnalité RSPAN et ils n'ont pas de ports de destination. Un commutateur peut être intermédiaire pour un nombre indéfini de sessions RSPAN.
- S4 et S5 sont des commutateurs de destination. Certains de leurs ports sont configurés pour être la destination d'une session RSPAN. Actuellement, Catalyst 6500/6000 peut avoir jusqu'à 24 ports de destination RSPAN, pour une ou plusieurs sessions différentes. Vous pouvez également noter que S4 est à la fois un commutateur de destination et un commutateur intermédiaire.
- Vous pouvez voir que les paquets RSPAN sont propagés dans le VLAN RSPAN. Même les commutateurs qui ne sont pas sur le chemin conduisant à un port de destination, tels que S2, reçoivent le trafic pour le VLAN RSPAN. Vous pouvez trouver utile de nettoyer ce VLAN sur des liaisons telles que S1-S2.
- Pour que la propagation s'effectue, l'apprentissage est désactivé sur le VLAN RSPAN.
- Pour empêcher les boucles, le protocole STP a été maintenu sur le VLAN RSPAN. Par conséquent, la fonctionnalité RSPAN ne peut pas surveiller les unités de données de protocole de pont (BDPU).

Exemple de configuration RSPAN

Les informations de cette section illustrent la configuration de ces différents éléments avec une conception RSPAN très simple. S1 et les S2 sont deux commutateurs Catalyst 6500/6000. Pour surveiller certains ports S1 ou VLAN à partir de S2, vous devez configurer un VLAN RSPAN dédié. Le reste des commandes ont la même syntaxe que celles que vous utilisez dans une session SPAN standard.

Configuration du tronc ISL entre les deux commutateurs S1 et S2

Pour commencer, placez le même domaine VTP (VLAN Trunking Protocol) sur chaque commutateur et configurez le mode Trunk desirable sur un côté. La négociation VTP fait le reste. Émettez la commande suivante sur S1 :

```
<#root>

S1> (enable)

set vtp domain cisco


      VTP domain cisco modified
```

Émettez les commandes suivantes sur 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
```

Création du VLAN RSPAN

Une session RSPAN a besoin d'un VLAN RSPAN. Vous devez créer ce VLAN. Vous ne pouvez pas convertir un VLAN existant en VLAN RSPAN. Cet exemple utilise le VLAN VLAN 100 :

```
<#root>

S2> (enable)

set vlan 100 rspan


      Vlan 100 configuration successful
```

Émettez cette commande sur un commutateur qui est configuré en tant que serveur VTP. La connaissance du VLAN VLAN 100 RSPAN est automatiquement propagée dans tout le domaine VTP.

Configuration du port 5/2 de S2 comme port de destination de la fonctionnalité RSPAN

<#root>

```
S2> (enable)

set rspan destination 5/2 100


      Rspan Type : Destination
      Destination : Port 5/2
      Rspan Vlan : 100
      Admin Source : -
      Oper Source : -
      Direction : -
      Incoming Packets: disabled
      Learning : enabled
      Multicast : -
      Filter : -
      Status : active
      2000 Sep 12 04:34:47 %SYS-5-SPAN_CFGSTATECHG:remote span destination session
      active for destination port 5/2
```

Configuration d'un port source RSPAN sur S1

Dans cet exemple, le trafic entrant qui entre dans S1 via le port 6/2 est surveillé. Émettez la commande suivante :

<#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
```

Tous les paquets entrants sur le port 6/2 sont maintenant propagés sur le VLAN 100 RSPAN et atteignent le port de destination qui est configuré sur S1 via la jonction.

Vérifier la configuration

La commande show rspan donne un résumé de la configuration RSPAN actuelle sur le commutateur. À nouveau, il ne peut y avoir qu'une seule session RSPAN source à la fois.

<#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
```

Autres configurations possibles avec la commande set rspan

Vous utilisez plusieurs lignes de commande pour configurer la source et la destination avec la fonctionnalité RSPAN. Hormis cette différence, les fonctionnalités SPAN et RSPAN se comportent vraiment de la même manière. Vous pouvez même utiliser RSPAN localement, sur un seul commutateur, si vous voulez avoir plusieurs ports SPAN de destination.

Résumé des fonctionnalités et limitations

Le tableau suivant résume les différentes fonctionnalités qui ont été introduites et fournit la version minimale de CatOS requise pour exécuter la fonctionnalité sur la plate-forme spécifiée :

Fonctionnalité	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
Option inpkts enable/disable	4.4	4.2	5.1
Plusieurs sessions, ports dans différents VLAN	5.1	5.1	5.1
Option sc0	—	5.1	5.1
Option multicast enable/disable	—	5.1	5.1
Option learning enable/disable	5.2	5.2	5.3

RSPAN	6.3	—	5.3

Le tableau suivant fournit un bref résumé des restrictions actuelles concernant le nombre de sessions SPAN possibles :

Fonctionnalité	Commutateurs de la gamme Catalyst 4500/4000	Commutateurs de la gamme Catalyst 5500/5000	Commutateurs de la gamme Catalyst 6500/6000
Sessions SPAN rx ou both	5	1	2
Sessions SPAN tx	5	4	4
Sessions de mini-analyseur de protocole	Non pris en charge	Non pris en charge	1
Sessions sources RSPAN rx, tx ou both	5	Non pris en charge	1 Le Supervisor Engine 720 prend en charge deux sessions source RSPAN.
Destination RSPAN	5	Non pris en charge	24
Nombre total de sessions	5	5	30

Pour obtenir des restrictions et des directives de configuration supplémentaires, reportez-vous aux documents suivants :

- Configuration de SPAN et RSPAN (Catalyst 4500/4000)
- Configuration de SPAN et RSPAN (Catalyst 6500/6000)

Fonctionnalité SPAN sur les commutateurs de la gamme Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 et 3750-E

Vous trouverez ci-après des directives pour la configuration de la fonctionnalité SPAN sur les commutateurs de la gamme Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 et 3750-E :

- Les commutateurs Catalyst 2950 ne peuvent avoir qu'une seule session SPAN active à la fois et peuvent surveiller uniquement les ports sources. Ces commutateurs ne peuvent pas surveiller les VLAN.
- Les commutateurs Catalyst 2950 et 3550 peuvent transférer le trafic sur un port SPAN de destination dans le logiciel Cisco IOS Version 12.1(13)EA1 et ultérieures.
- Les commutateurs Catalyst 3550, 3560 et 3750 peuvent prendre en charge jusqu'à deux sessions SPAN à la fois et peuvent surveiller les ports sources aussi bien que les VLAN.

- Les commutateurs Catalyst 2970, 3560 et 3750 ne requièrent pas la configuration d'un port de réflecteur lorsque vous configurez une session RSPAN.
- Les commutateurs Catalyst 3750 prennent en charge la configuration de session à l'aide de ports sources et de destination qui résident sur n'importe lequel des membres de la pile de commutateurs.
- Un seul port de destination est autorisé par session SPAN, et le même port ne peut pas être un port de destination pour plusieurs sessions SPAN. Par conséquent, vous ne pouvez pas avoir deux sessions SPAN qui utilisent le même port de destination.

Les commandes de configuration de la fonctionnalité SPAN sont semblables sur Catalyst 2950 et sur Catalyst 3550. Cependant, Catalyst 2950 ne peut pas surveiller les VLAN. Vous pouvez configurer la fonctionnalité SPAN, comme dans cet exemple :

```
<#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#
```

Vous pouvez également configurer un port comme destination pour la fonctionnalité SPAN locale et la fonctionnalité RSPAN pour le trafic du même VLAN. Pour surveiller le trafic d'un VLAN

particulier qui réside dans deux commutateurs directement connectés, configurez ces commandes sur le commutateur qui a le port de destination. Dans cet exemple, nous surveillons le trafic en provenance du VLAN 5 qui est réparti entre deux commutateurs :

```
<#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.
```

Sur le commutateur distant, utilisez la configuration suivante :

```
<#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
```

Dans l'exemple précédent, un port a été configuré comme port de destination pour la fonctionnalité SPAN locale et la fonctionnalité RSPAN afin de surveiller le trafic pour le même VLAN qui réside dans des deux commutateurs.

Remarque : contrairement aux commutateurs des gammes 2900XL et 3500XL, les commutateurs Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 et 3750-E prennent en charge la fonctionnalité SPAN sur le trafic du port source dans la direction Rx

---

uniquement (Rx SPAN ou SPAN d'entrée), dans la direction Tx uniquement (Tx SPAN ou SPAN de sortie), ou les deux.

Remarque : les commandes de la configuration ne sont pas prises en charge sur le Catalyst 2950 avec le logiciel Cisco IOS Version 12.0(5.2)WC(1) ou tout logiciel antérieur au logiciel Cisco IOS Version 12.1(6)EA2. Pour configurer la fonctionnalité SPAN sur Catalyst 2950 avec un logiciel antérieur au logiciel Cisco IOS Version 12.1(6)EA2, reportez-vous à la section Activation de l'analyseur de port de commutateur de Gestion des commutateurs.

Remarque : les commutateurs Catalyst 2950 qui utilisent le logiciel Cisco IOS version 12.1.(9)EA1d et les versions antérieures de la gamme de logiciels Cisco IOS version 12.1 prennent en charge la fonctionnalité SPAN. Cependant, tous les paquets qui sont vus sur le port de destination de la fonctionnalité SPAN (connecté au périphérique de reniflage ou au PC) ont une balise IEEE 802.1Q, même si le port source de la fonctionnalité SPAN (port surveillé) peut ne pas être un port de tronc (Trunk) 802.1 Si le périphérique de reniflage ou la carte d'interface réseau (NIC) du PC ne comprend pas les paquets à balises 802.1Q, le périphérique peut supprimer les paquets ou avoir des difficultés lorsqu'il tente de décoder les paquets. Il est important de pouvoir voir les trames à balises 802.1Q uniquement lorsque le port source de la fonctionnalité SPAN est un port de jonction. Avec le logiciel Cisco IOS Version 12.1(11)EA1 et ultérieures, vous pouvez activer et désactiver le balisage des paquets sur le port de destination de la fonctionnalité SPAN. Pour activer l'encapsulation des paquets sur le port de destination, émettez la commande monitor session session_number destination interface interface_id encapsulation dot1q. Si vous ne spécifiez pas le mot clé encapsulation, les paquets sont envoyés sans balise, ce qui est la valeur par défaut dans le logiciel Cisco IOS Version 12.1(11)EA1 et ultérieures.

Fonctionnalité	Catalyst 2950/3550
Option Ingress (inpkts) enable/disable	Logiciel Cisco IOS Version 12.1(12c)EA1
RSPAN	Logiciel Cisco IOS Version 12.1(12c)EA1

Fonctionnalité	Catalyst 2940[1], 2950, 2955, 2960, 2970, 3550, 3560, 3750
Sessions SPAN rx ou both	2
Sessions SPAN tx	2
Sessions sources RSPAN rx, tx ou both	2
Destination RSPAN	2
Nombre total de sessions	2

[1] Les commutateurs Catalyst 2940 prennent uniquement en charge la fonctionnalité SPAN locale. La fonctionnalité RSPAN n'est pas prise en charge dans cette plate-forme.

Pour plus d'informations sur la configuration des fonctionnalités SPAN et RSPAN, reportez-vous aux guides de configuration suivants :

- Configuration de la fonctionnalité SPAN (Catalyst 2940)
- Configuration des fonctionnalités SPAN et RSPAN (Catalyst 2950 et 2955)
- Configuration des fonctionnalités SPAN et RSPAN (Catalyst 2960)
- Configuration des fonctionnalités SPAN et RSPAN (Catalyst 3550)
- Configuration des fonctionnalités SPAN et RSPAN (Catalyst 3560)
- Configuration des fonctionnalités SPAN et RSPAN (Catalyst 3560-E et 3750-E)
- Configuration des fonctionnalités SPAN et RSPAN (Catalyst 3750)

Fonctionnalité SPAN sur les commutateurs de la gamme Catalyst 4500/4000 et Catalyst 6500/6000 qui exécutent la plate-forme logicielle Cisco IOS

La fonctionnalité SPAN est prise en charge sur les commutateurs de la gamme Catalyst 4500/4000 et Catalyst 6500/6000 qui exécutent la plate-forme logicielle Cisco IOS. Ces deux plates-formes de commutation utilisent la même interface de commande en ligne (CLI), et une configuration semblable à la configuration traitée dans la section Fonctionnalité SPAN sur les commutateurs de la gamme Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 et 3750-E. Pour connaître la configuration associée, reportez-vous aux documents suivants :

- Configuration de SPAN et RSPAN (Catalyst 6500/6000)
- Configuration de SPAN et RSPAN (Catalyst 4500/4000)

Exemple de configuration

Vous pouvez configurer la fonctionnalité SPAN, comme dans cet exemple :

```
<#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#
```

Résumé des fonctionnalités et limitations

Le tableau suivant résume les différentes fonctionnalités qui ont été introduites et fournit la version minimale du logiciel Cisco IOS requise pour exécuter la fonctionnalité sur la plate-forme spécifiée :

Fonctionnalité	Catalyst 4500/4000 (logiciel Cisco IOS)	Catalyst 6500/6000 (logiciel Cisco IOS)
Option Ingress (inpkts) enable/disable	Logiciel Cisco IOS Version 12.1(19)EW	Non pris en charge actuellement[1]
RSPAN	Logiciel Cisco IOS Version 12.1(20)EW	Logiciel Cisco IOS Version 12.1(13)E

[1] La fonctionnalité n'est actuellement pas disponible et la disponibilité de ces fonctionnalités n'est généralement pas publiée avant la version.

Remarque : la fonctionnalité SPAN des commutateurs Cisco Catalyst 6500/6000 présente des limites par rapport au protocole PIM. Quand un commutateur est configuré à la fois pour le protocole PIM et la fonctionnalité SPAN, l'analyseur de réseau/le renifleur attaché au port de destination de la fonctionnalité SPAN peut voir les paquets PIM qui ne font pas partie du trafic du port source SPAN/du VLAN. Ce problème se produit en raison d'une limitation dans l'architecture de transfert de paquets du commutateur. Le port de destination de la fonctionnalité SPAN n'effectue aucune vérification de la source des paquets. Ce problème est également décrit dans le bogue Cisco ayant l'ID CSCdy57506 (réservé aux clients inscrits).

Le tableau suivant fournit un bref résumé des restrictions actuelles concernant le nombre de sessions SPAN et RSPAN possibles :

Fonctionnalité	Catalyst 4500/4000 (logiciel Cisco IOS)

Sessions SPAN rx ou both	2
Sessions SPAN tx	4
Sessions sources RSPAN rx, tx ou both	2 (Rx, Tx ou both), et jusqu'à 4 pour Tx seulement
Destination RSPAN	2
Nombre total de sessions	6

Pour connaître les commutateurs Catalyst 6500/6000 exécutant le logiciel Cisco IOS, reportez-vous à Limites des sessions SPAN locales, RSPAN et ERSPAN.

Dans la gamme Catalyst 6500, il est important de noter que la fonctionnalité SPAN de sortie est effectuée sur le superviseur. Cela permet l'envoi, à travers la trame, de tout le trafic soumis à la fonctionnalité SPAN de sortie au superviseur, puis au port de destination de la fonctionnalité SPAN, ce qui peut utiliser une grande quantité de ressources système et affecter le trafic utilisateur. La fonctionnalité SPAN d'entrée sera effectuée sur des modules d'entrée. Ainsi, les performances de la fonctionnalité SPAN sont la somme de tous les moteurs de réplication participants. Les performances de la fonctionnalité SPAN dépendent de la taille des paquets et du type de circuit intégré à application spécifique (ASIC) disponible dans le moteur de réplication.

Avec des versions antérieures au logiciel Cisco IOS Version 12.2(33)SXH, une interface de canal de port, un port EtherChannel, ne peut pas être une destination de la fonctionnalité SPAN. Avec le logiciel Cisco IOS Version 12.2(33)SXH et ultérieures, un port EtherChannel peut être une destination de la fonctionnalité SPAN. Les EtherChannels de destination ne prennent pas en charge les protocoles EtherChannel PAgP (Port Aggregation Control Protocol) ou LACP (Link Aggregation Control Protocol) ; seul le mode on est pris en charge, avec la prise en charge de tous les protocoles EtherChannel désactivée.

Pour obtenir des restrictions et des directives de configuration supplémentaires, reportez-vous aux documents suivants :

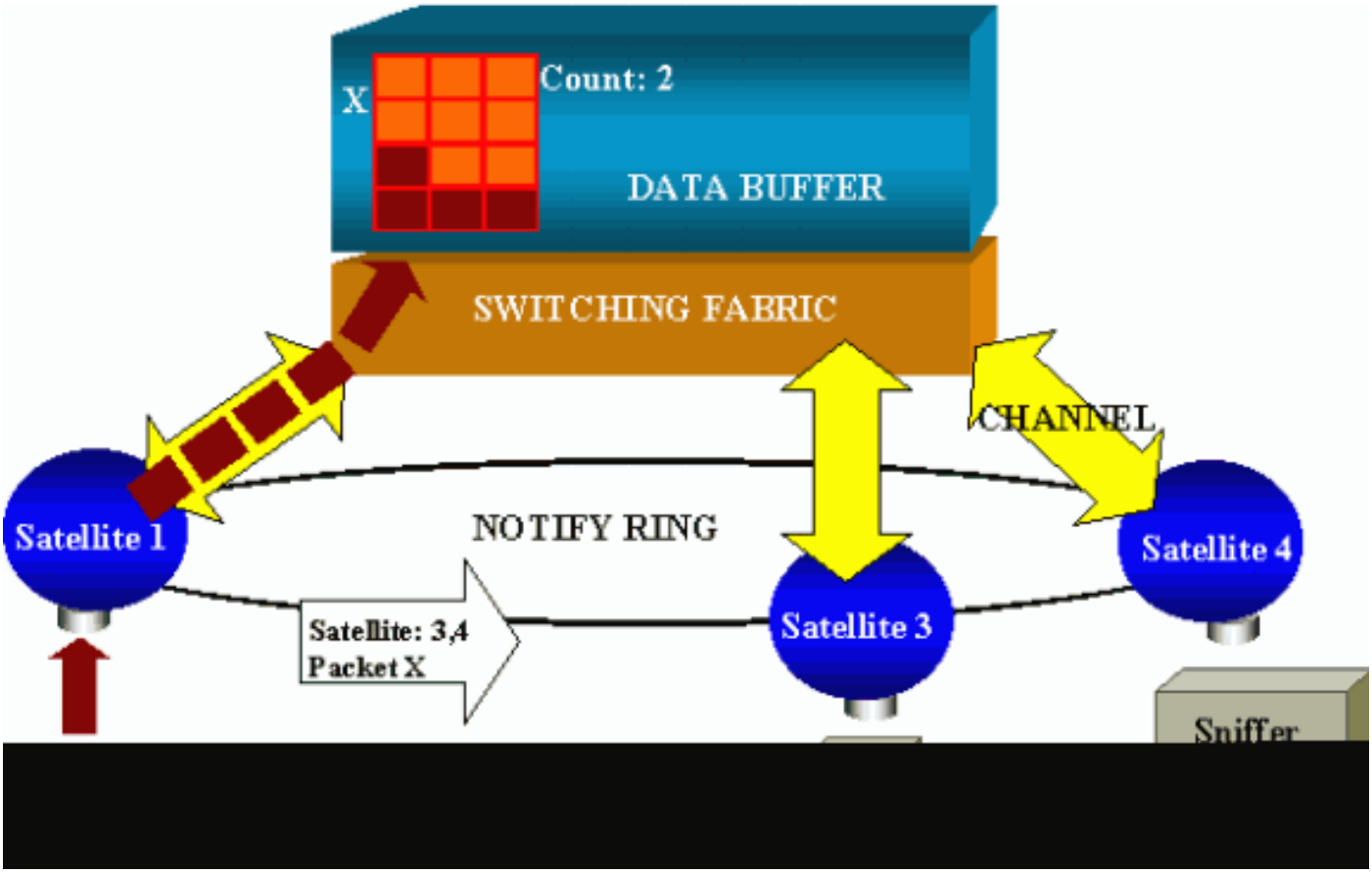
- Configuration des fonctionnalités SPAN et RSPAN (Catalyst 4500/4000)
- Configuration des fonctionnalités SPAN locale, Remote SPAN (RSPAN) et RSPAN encapsulée (Catalyst 6500/6000)

Impact sur les performances de la fonctionnalité SPAN sur les différentes plates-formes Catalyst

Gamme Catalyst 2900XL/3500XL

Présentation de l'architecture

Voici une vue très simpliste de l'architecture interne des commutateurs 2900XL/3500XL :



Les ports du commutateur sont attachés à des satellites qui communiquent vers une matrice de commutation via des canaux radiaux. En haut, tous les satellites sont interconnectés via un anneau de notification haut débit qui est dédié à la signalisation du trafic.

Lorsqu'un satellite reçoit un paquet en provenance d'un port, le paquet est fractionné en cellules et envoyé à la matrice de commutation via un ou plusieurs canaux. Le paquet est ensuite stocké dans la mémoire partagée. Chaque satellite a connaissance des ports de destination. Dans le diagramme présenté dans cette section, le satellite 1 sait que le paquet X doit être reçu par les satellites 3 et 4. Le satellite 1 envoie un message aux autres satellites via l'anneau de notification. Ensuite, les satellites 3 et 4 peuvent commencer à récupérer les cellules dans la mémoire partagée via leurs canaux radiaux et peuvent finalement transférer le paquet. Étant donné que le satellite source connaît la destination, ce satellite transmet également un indice qui spécifie le nombre de fois que ce paquet est téléchargé par les autres satellites. Chaque fois qu'un satellite récupère le paquet dans la mémoire partagée, cet indice est décrémenté. Lorsque l'indice atteint 0, la mémoire partagée peut être libérée.

Impact sur les performances

Pour surveiller certains ports avec la fonctionnalité SPAN, un paquet doit être copié à partir du tampon de données vers un satellite une fois de plus. L'impact sur la matrice de commutation haut débit est négligeable.

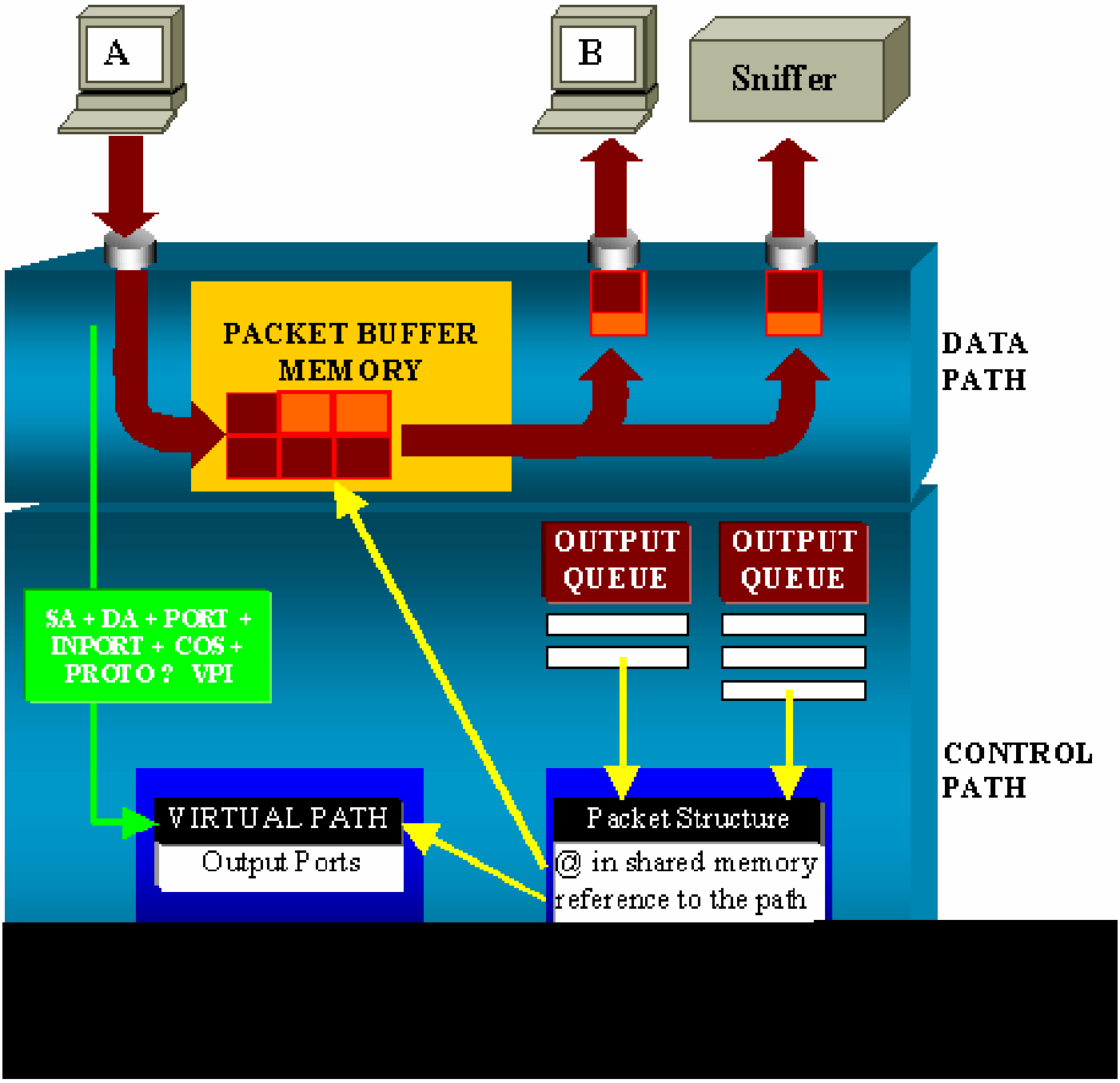
Le port de surveillance reçoit des copies du trafic transmis et reçu pour tous les ports surveillés. Dans cette architecture, un paquet qui est destiné à plusieurs destinations est stocké en mémoire jusqu'à ce que toutes les copies soient transférées. Si le port de surveillance est surabonné à 50

% pendant un certain temps, il est probable que le port va être saturé et qu'il va bloquer une partie de la mémoire partagée. Il est possible qu'un ou plusieurs des ports qui sont surveillés subissent également un ralentissement.

Gamme Catalyst 4500/4000

Présentation de l'architecture

Catalyst 4500/4000 est basé sur une matrice de commutation avec mémoire partagée. Le diagramme suivant est un aperçu général du chemin d'un paquet à travers le commutateur. L'implémentation réelle est, en fait, beaucoup plus complexe :



Sur Catalyst 4500/4000, vous pouvez distinguer le chemin des données. Le chemin des données correspond au transfert réel des données dans le commutateur, à partir du chemin de contrôle, où

toutes les décisions sont prises.

Lorsqu'un paquet entre dans le commutateur, une mémoire tampon est affectée dans la mémoire tampon des paquets (une mémoire partagée).

Une structure de paquets qui pointe vers cette mémoire tampon est initialisée dans la table de description des paquets (PDT).

Pendant que les données sont copiées dans la mémoire partagée, le chemin de contrôle détermine l'emplacement où commuter le paquet. Pour ce faire, une valeur de hachage est calculée à partir des informations suivantes :

- L'adresse source du paquet
- Adresse de destination
- VLAN
- Type de protocole
- Port d'entrée
- Classe de service (Cos) (balise IEEE 802.1p ou port par défaut)

Cette valeur est utilisée pour rechercher l'indice de chemin virtuel (VPI) d'une structure de chemin dans la table des chemins virtuels (VPT). Cette entrée de chemin virtuel dans la table VPT contient plusieurs champs qui sont associés à ce flux particulier.

Les champs incluent les ports de destination. La structure de paquets dans la table PDT est maintenant mise à jour avec une référence au chemin virtuel et au compteur.

Dans l'exemple présenté dans cette section, le paquet doit être transmis à deux ports différents ; le compteur est donc initialisé à 2. Enfin, la structure de paquets est ajoutée à la file d'attente de sortie des deux ports de destination.

À partir de là, les données sont copiées de la mémoire partagée vers la mémoire tampon de sortie du port, et le compteur de la structure de paquets décrémente. Lorsqu'il atteint 0, la mémoire tampon partagée est libérée.

Impact sur les performances

Lorsque la fonctionnalité SPAN est utilisée, un paquet doit être envoyé à deux ports différents, comme dans l'exemple présenté dans la section Description générale de l'architecture.

L'envoi du paquet à deux ports n'est pas un problème, car la matrice de commutation n'est pas bloquante.

Si le port SPAN de destination est saturé, les paquets sont déposés dans la file d'attente de sortie et sont correctement libérés de la mémoire partagée. T

Par conséquent, il n'y a aucun impact sur le fonctionnement du commutateur.

Gamme Catalyst 5500/5000 et 6500/6000

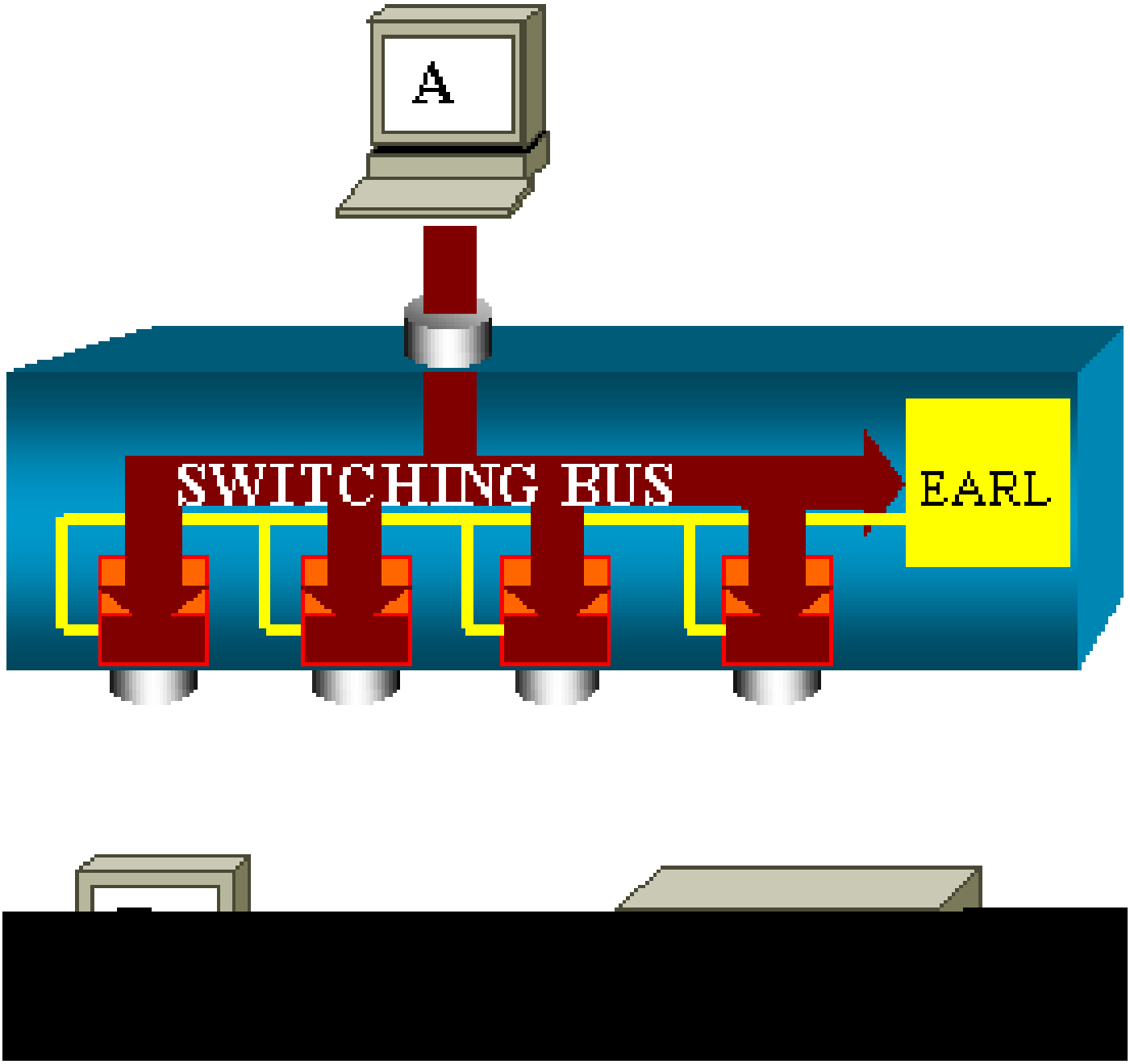
Présentation de l'architecture

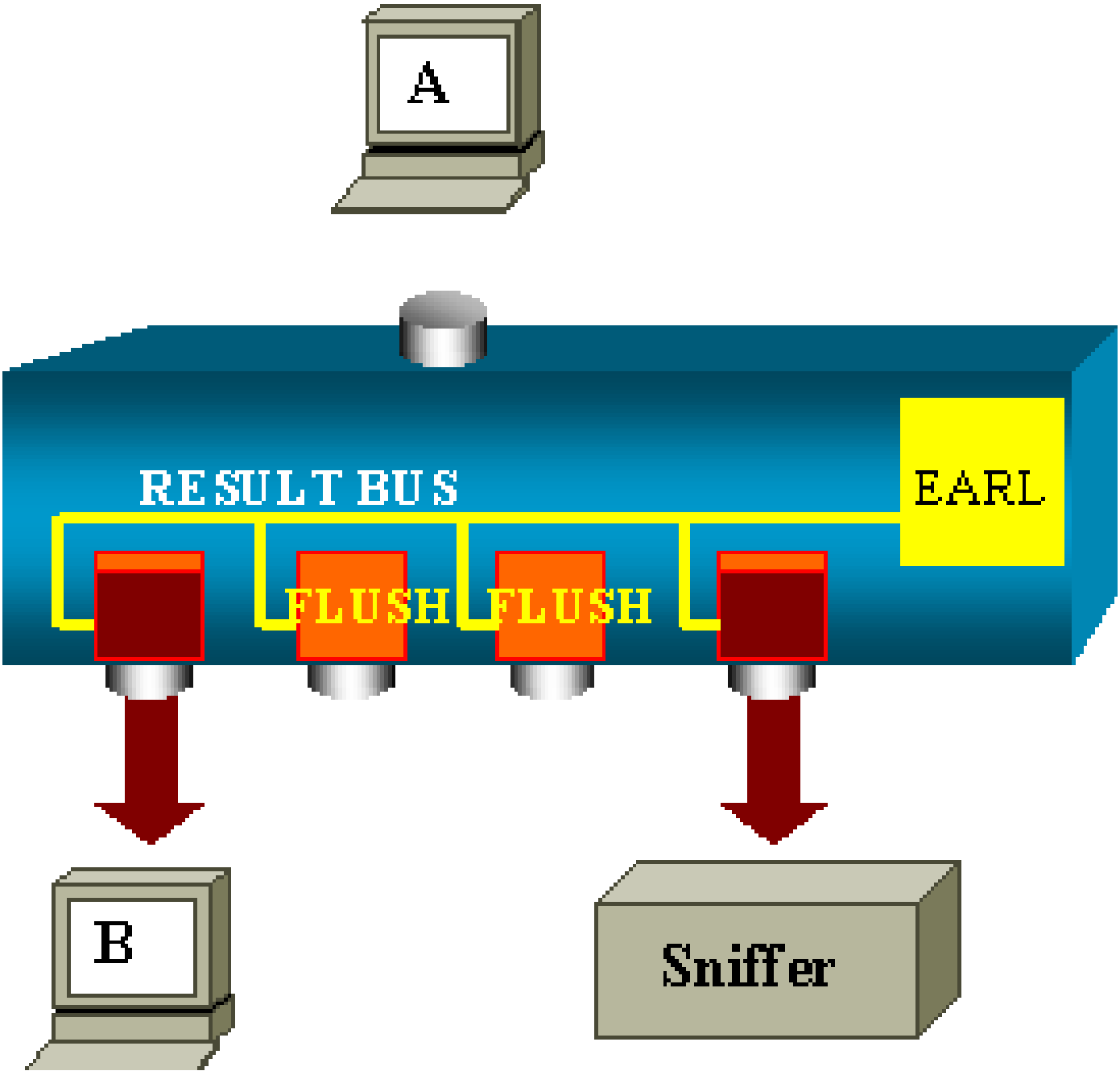
Sur les commutateurs de la gamme Catalyst 5500/5000 et 6500/6000, un paquet qui est reçu sur un port est transmis sur le bus de commutation interne.

Chaque carte de ligne dans le commutateur commence à stocker ce paquet dans des mémoires tampons internes.

En même temps, la logique de reconnaissance des adresses encodées (EARL) reçoit l'en-tête du paquet et calcule un indice de résultat. EARL envoie l'indice de résultat à toutes les cartes de ligne via le bus de résultat.

La connaissance de cet indice permet à la carte de ligne de décider individuellement si elle doit vider ou transmettre le paquet lorsqu'elle reçoit le paquet dans ses mémoires tampons.


A
SWITCHING BUS
EARL



Impact sur les performances

Que le paquet soit finalement transmis par un ou plusieurs ports n'a absolument aucune influence sur l'opération de commutation. Par conséquent, quand vous considérez cette architecture, la fonctionnalité SPAN n'a aucun impact sur les performances.

Forum aux questions et problèmes courants

Problèmes de connectivité en raison d'une configuration incorrecte de la fonctionnalité SPAN

Les problèmes de connectivité dus à la configuration incorrecte de la fonctionnalité SPAN se produisent souvent dans les versions de CatOS antérieures à 5.1. Avec ces versions, une seule

session SPAN est possible.

La session reste dans la configuration, même lorsque vous désactivez la fonctionnalité SPAN. Avec l'émission de la commande set span enable, un utilisateur réactive la session SPAN stockée.

L'action se produit souvent en raison d'une erreur typographique, par exemple si l'utilisateur veut activer le protocole STP. Cela peut entraîner des problèmes de connectivité graves si le port de destination est utilisé pour transférer le trafic utilisateur.

⚠ Attention : ce problème est toujours dans l'implémentation actuelle de CatOS. Soyez très attentif au port que vous choisissez comme destination de la fonctionnalité SPAN.

Port de destination de la fonctionnalité SPAN actif/inactif

Quand des ports sont étendus pour la surveillance, l'état des ports s'affiche comme étant UP/DOWN.

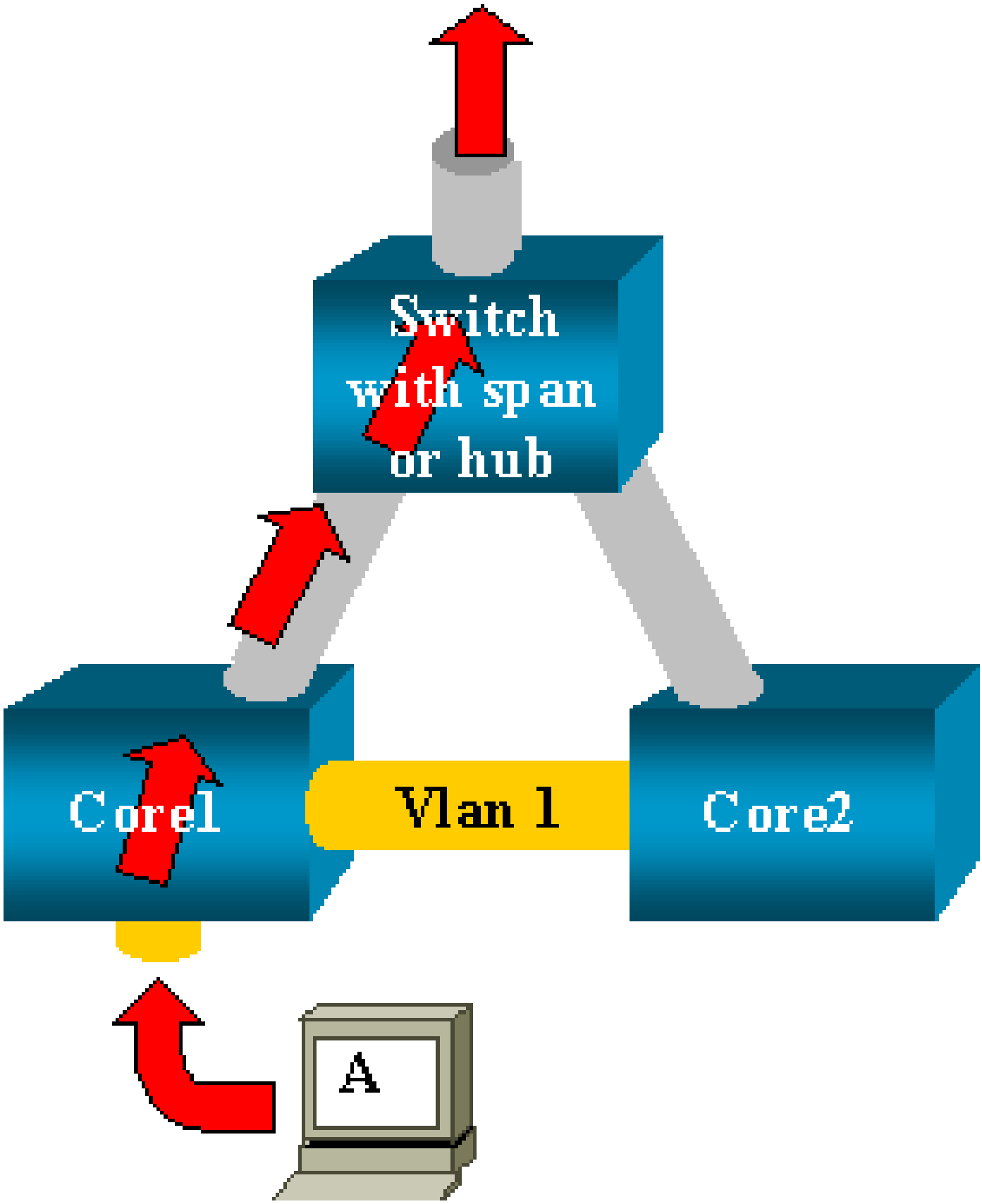
Lorsque vous configurez une session SPAN pour surveiller le port, l'interface de destination affiche l'état down (en surveillance), par conception.

L'interface montre le port dans cet état pour indiquer clairement qu'il n'est actuellement pas utilisable comme port de production. Le port en tant que surveillance active/inactive est normal.

Pourquoi la session SPAN crée-t-elle une boucle de pontage ?

La création d'une boucle de pontage se produit généralement quand l'administrateur tente de falsifier la fonctionnalité RSPAN. De plus, une erreur de configuration peut provoquer ce problème.

Voici un exemple du scénario :



Il y a deux commutateurs principaux qui sont liés par une jonction. Dans cet exemple, plusieurs serveurs, clients ou autres ponts sont connectés à chaque commutateur.

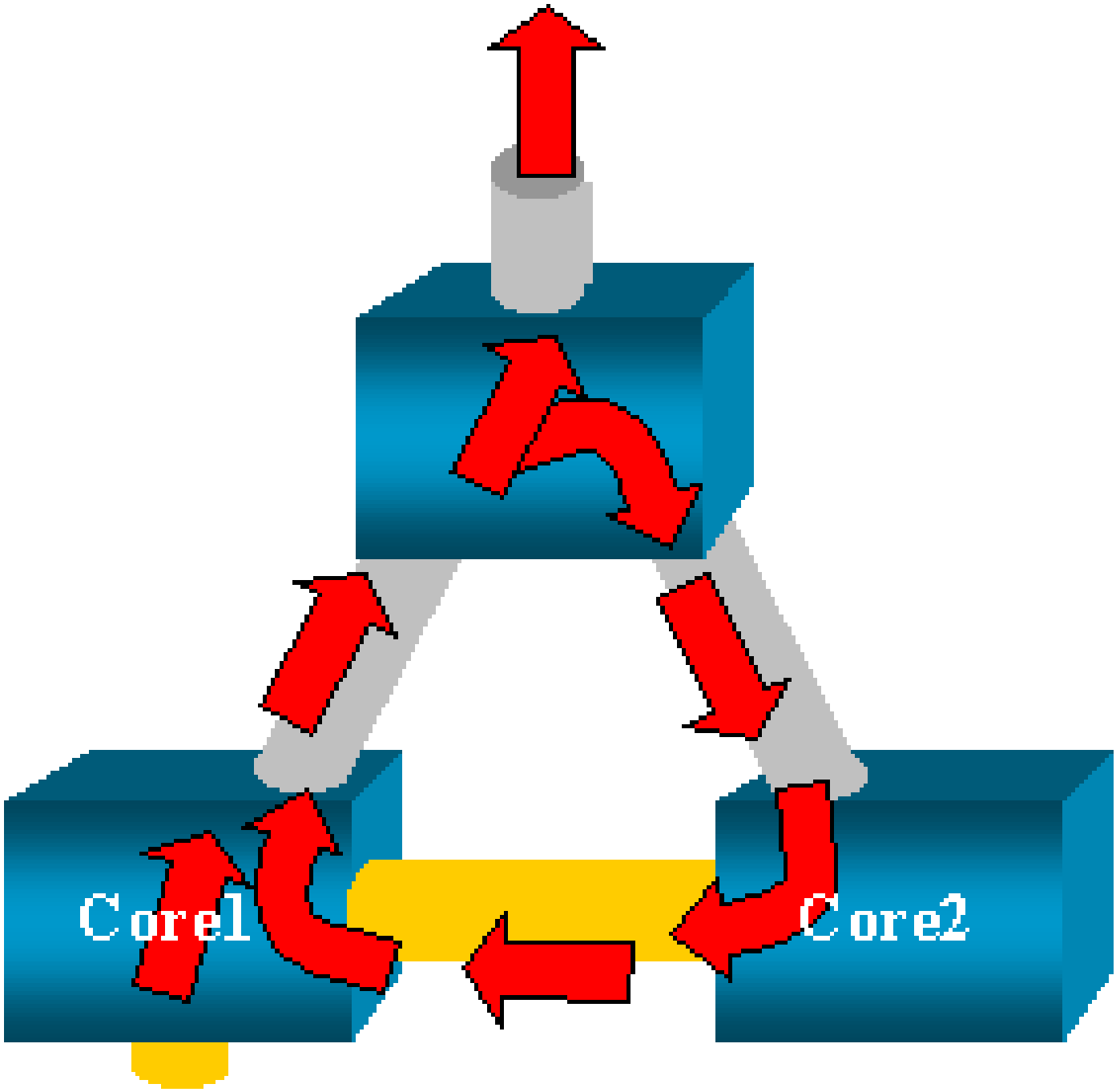
L'administrateur veut surveiller VLAN 1, qui apparaît sur plusieurs ponts avec la fonctionnalité SPAN.

L'administrateur crée une session SPAN qui surveille la totalité du VLAN 1 sur chaque commutateur principal, et, pour fusionner ces deux sessions, connecte le port de destination au même concentrateur (ou au même commutateur, à l'aide d'une autre session SPAN).

L'administrateur atteint l'objectif. Chaque paquet individuel reçu par un commutateur principal sur VLAN 1 est dupliqué sur le port SPAN et transféré au concentrateur. Un renifleur capture finalement le trafic.

Le seul problème est que le trafic est également réinjecté dans le coeur 2 via le port SPAN de destination.

La réinjection du trafic dans le deuxième commutateur principal crée une boucle de pontage dans le VLAN VLAN 1. N'oubliez pas qu'un port SPAN de destination n'exécute pas STP et n'est pas en mesure d'empêcher une telle boucle.



Remarque : en raison de l'introduction de l'option inpkts (input packets) sur CatOS, un port de destination SPAN abandonne tout paquet entrant par défaut, ce qui empêche ce scénario d'échec. Cependant, le problème potentiel est toujours présent sur les commutateurs de la gamme Catalyst 2900XL/3500XL.

Remarque : même lorsque l'option inpkts empêche la boucle, la configuration présentée dans cette section peut provoquer des problèmes sur le réseau. Les problèmes réseau peuvent se produire en raison de problèmes d'apprentissage des adresses MAC qui sont associés à l'apprentissage activé sur le port de destination.

La fonctionnalité SPAN a-t-elle une incidence sur les performances ?

Pour plus d'informations sur l'impact sur les performances pour les plates-formes Catalyst spécifiées, consultez les sections suivantes de ce document :

- Gamme Catalyst 2900XL/3500XL
- Gamme Catalyst 4500/4000
- Gamme Catalyst 5500/5000 et 6500/6000

Est-il possible de configurer la fonctionnalité SPAN sur un port EtherChannel ?

Un port EtherChannel ne fonctionne pas si l'un des ports dans le lot est un port de destination de la fonctionnalité SPAN. Si vous essayez de configurer la fonctionnalité SPAN dans cette situation, le commutateur vous indique ceci :

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

Vous pouvez utiliser un lot de ports EtherChannel comme port source de la fonctionnalité SPAN.

Est-il possible d'avoir plusieurs sessions SPAN en cours d'exécution en même temps ?

Sur les commutateurs de la gamme Catalyst 2900XL/3500XL, le nombre de ports de destination disponibles sur le commutateur est la seule limite au nombre de sessions SPAN.

Sur les commutateurs de la gamme Catalyst 2950, un seul port de surveillance peut être affecté à tout moment.

Si vous sélectionnez un autre port comme port de surveillance, le port de surveillance précédent est désactivé, et le port nouvellement sélectionné devient le port de surveillance.

Sur les commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000 avec CatOS 5.1 et versions ultérieures, vous pouvez avoir plusieurs sessions SPAN simultanées.

Consultez les sections Créer plusieurs sessions simultanées et Résumé des fonctionnalités et limitations de ce document.

Erreur « % Local Session Limit Has Been Exceeded »

Ce message s'affiche lorsque la session SPAN autorisée dépasse la limite du moteur de superviseur :

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

Les moteurs de superviseur ont une limitation de sessions SPAN. Pour plus d'informations, reportez-vous à la section Limites des sessions SPAN locales, RSPAN et ERSPAN de Configuration des fonctionnalités SPAN locale, RSPAN et ERSPAN.

Impossible de supprimer une session SPAN sur le module de services VPN, avec l'erreur « % Session [Session No:] Used by Service Module »

Ce problème indique que le module VPN (réseau privé virtuel) est inséré dans le châssis, où un module de matrice de commutation a été déjà inséré.

Le logiciel Cisco IOS crée automatiquement une session SPAN pour le module de services VPN afin de traiter le trafic de multidiffusion.

Pour supprimer la session SPAN que le logiciel crée pour le module de services VPN, émettez la commande suivante :

```
<#root>

Switch(config)#

no monitor session session_number service-module
```

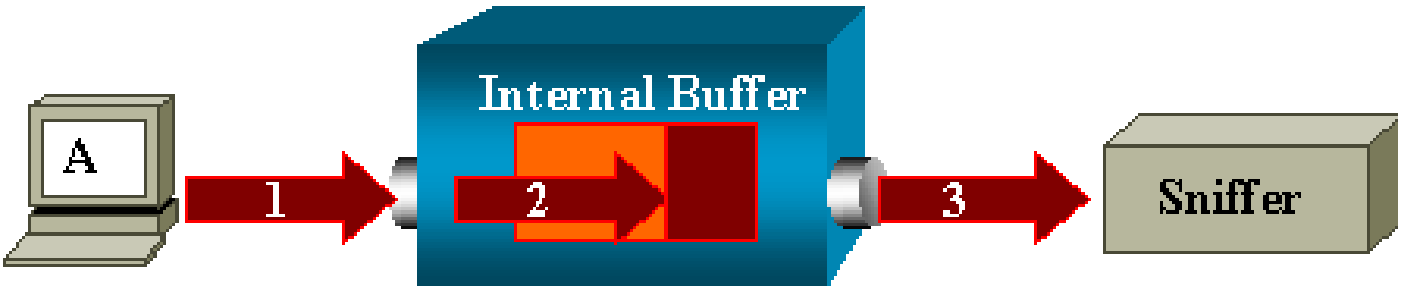
Remarque : si vous supprimez la session, le module de service VPN abandonne le trafic de multidiffusion.

Pourquoi est-il impossible de capturer des paquets corrompus avec la fonctionnalité SPAN ?

Vous ne pouvez pas capturer des paquets corrompus avec la fonctionnalité SPAN en raison du mode de fonctionnement général des commutateurs. Quand un paquet passe par un

commutateur, les événements suivants se produisent :

1. Le paquet atteint le port d'entrée.
2. Le paquet est stocké dans au moins une mémoire tampon.
3. Le paquet est finalement retransmis sur le port de sortie.



Si le commutateur reçoit un paquet corrompu, le port d'entrée supprime généralement le paquet. Par conséquent, vous ne voyez pas ce dernier sur le port de sortie.

Un commutateur n'est pas complètement transparent en ce qui concerne la capture du trafic.

De même, quand vous voyez un paquet corrompu sur votre renifleur dans le scénario présenté dans cette section, vous savez que les erreurs ont été générées à l'étape 3, sur le segment de sortie.

Si vous pensez qu'un périphérique envoie des paquets corrompus, vous pouvez choisir de placer l'hôte émetteur et le périphérique de reniflage sur un concentrateur. Le concentrateur n'effectue aucun contrôle des erreurs.

Par conséquent, contrairement au commutateur, le concentrateur ne supprime pas les paquets. Ainsi, vous pouvez voir les paquets.

Erreur : % session 2 utilisée par le module de service

Si un module de services de pare-feu (FWSM) a été, par exemple, installé puis ensuite supprimé, dans CAT6500, la fonctionnalité de réflecteur SPAN est alors automatiquement activée.

La fonctionnalité de réflecteur SPAN utilise une session SPAN dans le commutateur.

Si vous n'en avez plus besoin, vous devez pouvoir entrer la commande no monitor session service module en mode de configuration de CAT6500, puis entrer immédiatement la nouvelle configuration SPAN souhaitée.

Le port de réflecteur supprime des paquets

Un port de réflecteur reçoit des copies du trafic envoyé et reçu pour tous les ports sources surveillés. Si un port de réflecteur est surabonné, il peut devenir saturé.

Cela pourrait affecter le transfert du trafic sur un ou plusieurs des ports sources.

Si la bande passante du port de réflecteur n'est pas suffisante pour le volume de trafic en provenance des ports sources correspondants, les paquets excédentaires sont supprimés.

Un port 10/100 effectue la réflexion à 100 Mbits/s. Un port Gigabit effectue la réflexion à 1 Gbits/s.

La session SPAN est toujours utilisée avec un module FWSM dans le châssis Catalyst 6500

Quand vous utilisez Supervisor Engine 720 avec un module FWSM dans le châssis qui exécute la version native de Cisco IOS, une session SPAN est utilisée par défaut. Si vous recherchez les sessions non utilisées avec la commande show monitor, la session 1 est utilisée :

```
<#root>

Cat6K#

show monitor


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

Quand une lame de pare-feu est dans le châssis Catalyst 6500, cette session est automatiquement installée pour la prise en charge de la réplication en multidiffusion matérielle car un module FWSM ne peut pas répliquer des flux multidiffusion.

Si des flux multidiffusion qui proviennent de derrière le module FWSM doivent être répliqués au niveau de la couche 3 à plusieurs cartes de ligne, la session automatique copie le trafic vers le superviseur via un canal de matrice.

Si vous avez une source de multidiffusion qui génère un flux multidiffusion provenant de derrière le module FWSM, vous avez besoin du réflecteur SPAN.

Si vous placez la source de multidiffusion sur le VLAN extérieur, le réflecteur SPAN n'est pas nécessaire. Le réflecteur SPAN est incompatible avec le pontage des unités de données de protocole de pont (BDPU) à travers le module FWSM.

Vous pouvez utiliser la commande no monitor session service module pour désactiver le réflecteur SPAN.

Une session SPAN et une session RSPAN peuvent-elles avoir le même ID dans le même commutateur ?

Non, il n'est pas possible d'utiliser le même ID de session pour une session SPAN et une session de destination RSPAN normales. Chaque session SPAN et RSPAN doit avoir un ID de session différent.

Une session RSPAN peut-elle fonctionner sur différents domaines VTP ?

Oui. Une session RSPAN peut traverser différents domaines VTP. Mais assurez-vous que le VLAN RSPAN est présent dans les bases de données de ces domaines VTP.

De plus, vérifiez qu'aucun périphérique de couche 3 n'est présent dans le chemin de la source de la session à la destination de la session.

Une session RSPAN peut-elle fonctionner sur des WAN ou sur différents réseaux ?

Non. La session RSPAN ne peut traverser aucun périphérique de couche 3, car RSPAN est une fonctionnalité LAN (couche 2).

Pour surveiller le trafic à travers unWAN ou différents réseaux, utilisez la fonctionnalité ERSPAN (Encapsulated Remote SwitchPort Analyser).

La fonctionnalité ERSPAN prend en charge les ports sources, les VLAN sources et les ports de destination sur différents commutateurs, ce qui fournit une surveillance à distance de plusieurs commutateurs à travers votre réseau.

La fonctionnalité ERSPAN se compose d'une session source ERSPAN, d'un trafic ERSPAN routable encapsulé par encapsulation de routage générique (GRE) et d'une session de destination ERSPAN.

Vous configurez séparément les sessions sources et les sessions de destination ERSPAN sur différents commutateurs.

Actuellement, la fonctionnalité ERSPAN est prise en charge dans :

- Supervisor 720 avec PFC3B ou PFC3BXL exécutant le logiciel Cisco IOS Version 12.2(18)SXE ou ultérieures
- Supervisor 720 avec PFC3A disposant de la version de matériel 3.2 ou ultérieures et exécutant le logiciel Cisco IOS Version 12.2(18)SXE ou ultérieures

Pour plus d'informations sur la fonctionnalité ERSPAN, reportez-vous à Configuration des fonctionnalités SPAN locale, Remote SPAN (RSPAN) et RSPAN encapsulée - Guide de configuration des commutateurs Cisco IOS de la gamme Catalyst 6500 Version 12.2SX.

Une session source RSPAN et la session de destination peuvent-elles exister sur le même commutateur Catalyst ?

Non. RSPAN ne fonctionne pas lorsque la session source RSPAN et la session de destination RSPAN se trouvent sur le même commutateur.

Si une session source RSPAN est configurée avec un VLAN RSPAN particulier et qu'une session de destination RSPAN pour ce VLAN RSPAN est configurée sur le même commutateur, le port de destination de la session de destination RSPAN ne transmettra pas les paquets capturés en

provenance de la session source RSPAN en raison de limitations matérielles. Cela n'est pas pris en charge sur les commutateurs de la gamme 4500 et 3750.

Ce problème est décrit dans le bogue Cisco ayant l'ID CSCeg08870 (réservé aux clients inscrits).

Voici un exemple :

```
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
```

La solution de contournement pour ce problème consiste à utiliser la fonctionnalité SPAN normale.

Impossible d'accéder à l'analyseur réseau/au dispositif de sécurité connecté au port de destination de la fonctionnalité SPAN

La caractéristique de base d'un port de destination SPAN est qu'il n'en transmet aucun trafic excepté le trafic requis pour la session SPAN.

Si vous devez atteindre (accessibilité par adresse IP) l'analyseur réseau/le dispositif de sécurité par le port de destination SPAN, vous devez activer le transfert du trafic entrant.

Lorsque l'entrée est activée, le port de destination SPAN accepte les paquets entrants, lesquels comportent potentiellement des balises en fonction du mode d'encapsulation spécifié, et les commute normalement.

Lorsque vous configurez un port de destination SPAN, vous pouvez indiquer si la fonctionnalité d'entrée est activée et quel VLAN utiliser pour commuter les paquets entrants sans balises.

La spécification d'un VLAN d'entrée n'est pas requise lorsque l'encapsulation ISL est configurée, car tous les paquets encapsulés par ISL ont les balises de VLAN.

Bien que le port utilise le transfert via STP, il ne participe pas au protocole STP ; par conséquent, soyez prudent lorsque vous configurez cette fonctionnalité afin de ne pas introduire une boucle d'arborescence fractionnée (spanning-tree) dans le réseau.

Lorsque l'entrée et une encapsulation de jonction sont tous les deux spécifiées sur un port de destination SPAN, le port effectue le transfert dans tous les VLAN actifs.

La configuration d'un VLAN inexistant comme VLAN d'entrée n'est pas autorisée.

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

L'exemple suivant montre comment configurer un port de destination avec l'encapsulation 802.1Q et l'entrée des paquets avec l'utilisation du VLAN natif VLAN 7 .

<#root>

```
Switch(config)#
```

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

Avec cette configuration, le trafic en provenance des sources SPAN associées à la session 1 est copié hors de l'interface Fast Ethernet 5/48, avec l'encapsulation 802.1Q.

Le trafic entrant est accepté et commuté, avec les paquets sans balises classés dans le VLAN 7.

Informations connexes

- Comment configurer SPAN et RSPAN sur les commutateurs Cisco Catalyst 4500 qui exécutent le logiciel Cisco IOS
- Un port de destination SPAN est indiqué comme « non connecté » et ne communique pas avec le reste du réseau
- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.