Configurer l'analyseur de ports commutés (SPAN) Catalyst : Exemple

Table des matières

- Introduction
- Conditions préalables
  - Commutateurs Catalyst prenant en charge les protocoles SPAN, RSPAN et ERSPAN
  - Exigences
  - Composants utilisés
- Informations générales
  - Brève description de SPAN
  - Terminologie SPAN
  - Caractéristiques du port source
  - Caractéristiques du VLAN source
  - Caractéristiques du port de destination
  - Caractéristiques du port du réflecteur
- SPAN sur Catalyst Express 500/520
- Fonction SPAN sur les commutateurs Catalyst 2900XL/3500XL
  - Fonctionnalités disponibles et restrictions
  - Exemple de configuration
    - Diagramme du réseau
    - Exemple de configuration sur Catalyst 2900XL/3500XL
    - Explication des étapes de configuration
- SPAN sur les commutateurs Catalyst 2948G-L3 et 4908G-L3
- SPAN sur le Catalyst 8500
- Fonctionnalité SPAN sur les commutateurs des gammes Catalyst 2900, 4500/4000, 5500/5000 et 6500/6000 qui exécutent CatOS
  - SPAN local
    - PSPAN, VSPAN : Surveiller certains ports ou un VLAN entier
    - Surveiller un seul port avec la fonctionnalité SPAN
    - Surveillance de plusieurs ports avec la fonctionnalité SPAN
    - Surveillance des VLAN avec SPAN
    - SPAN d'entrée/sortie
    - Implémenter la fonctionnalité SPAN sur une agrégation
    - Surveiller un sous-ensemble de VLAN qui appartiennent à une agrégation
    - Agrégation sur le port de destination
    - Création de plusieurs sessions simultanées
    - Autres options SPAN
  - SPAN distant
    - Présentation de RSPAN
    - Exemple de configuration RSPAN
    - Configuration de la liaison ISL entre les deux commutateurs S1 et S2
    - Création du VLAN RSPAN
    - Configuration du port 5/2 de S2 comme port de destination RSPAN

Configuration d'un port source RSPAN sur S1

Vérification de la configuration

Autres configurations possibles avec la commande set rspan

Résumé des fonctionnalités et limitations

Fonctionnalité SPAN sur les commutateurs des gammes Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 et 3750-E

Fonctionnalité SPAN sur les commutateurs des gammes Catalyst 4500/4000 et Catalyst 6500/6000 qui exécutent le logiciel système Cisco IOS

Exemple de configuration

Résumé des fonctionnalités et limitations

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

Gamme Catalyst 2900XL/3500XL

Présentation de l'architecture

Impact sur les performances

Gammes Catalyst 4500/4000

Présentation de l'architecture

Impact sur les performances

Gammes Catalyst 5500/5000 et 6500/6000

Présentation de l'architecture

Impact sur les performances

Foire aux questions et problèmes courants

Problèmes de connectivité dus à une mauvaise configuration SPAN

Port de destination SPAN actif/inactif

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

La fonctionnalité SPAN affecte-t-elle les performances ?

Pouvez-vous configurer la fonctionnalité SPAN sur un port EtherChannel ?

Pouvez-vous exécuter plusieurs sessions SPAN en même temps ?

Erreur "% La Limite De Session Locale A Été Dépassée"

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

Pourquoi ne parvenez-vous pas à capturer des paquets corrompus avec la fonctionnalité SPAN ?

Erreur : % session 2 utilisée par le module de service

Le port du réflecteur abandonne les paquets

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

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

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

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

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

L'analyseur de réseau/périphérique de sécurité connecté au port de destination SPAN n'est pas accessible

Informations connexes

Introduction

Le présent document décrit les fonctionnalités récentes de Switched Port Analyzer (SPAN) qui ont été mises en œuvre.

Conditions préalables

Commutateurs Catalyst prenant en charge les protocoles SPAN, RSPAN et ERSPAN

commutateurs Catalyst	Support SPAN	Prise en charge RSPAN	Support ERSPAN
Gammes Catalyst Express 500 / 520	Oui	Non	Non
Gammes 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 qui possède la version matérielle 3.2 ou ultérieure et qui exécute le logiciel Cisco IOS® version 12.2(18)SXE ou ultérieure.
Gammes Catalyst 5500/5000	Oui	Non	Non
Gamme Catalyst 4900	Oui	Oui	Non
Gammes 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 2960	Oui	Oui	Non
Gamme Catalyst	Oui	Oui	Non

commutateurs Catalyst	Support SPAN	Prise en charge RSPAN	Support ERSPAN
2955			
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
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 utilisé. Bien que ce document soit mis à jour pour refléter les modifications apportées à la fonctionnalité SPAN, reportez-vous aux notes de mise à jour de la documentation de votre plate-forme 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 de réseau peut être un périphérique Cisco Switch Probe ou un autre analyseur RMON (Remote Monitoring).

Auparavant, la fonctionnalité SPAN était une fonctionnalité relativement basique sur les commutateurs Cisco Catalyst. Cependant, les dernières versions de Catalyst OS (CatOS) ont

introduit de grandes améliorations et de nombreuses nouvelles possibilités qui sont maintenant disponibles pour l'utilisateur.

Ce document n'est pas destiné à être un guide de configuration alternatif pour la fonctionnalité SPAN. Ce document répond aux questions les plus courantes sur la fonctionnalité SPAN, telles que :

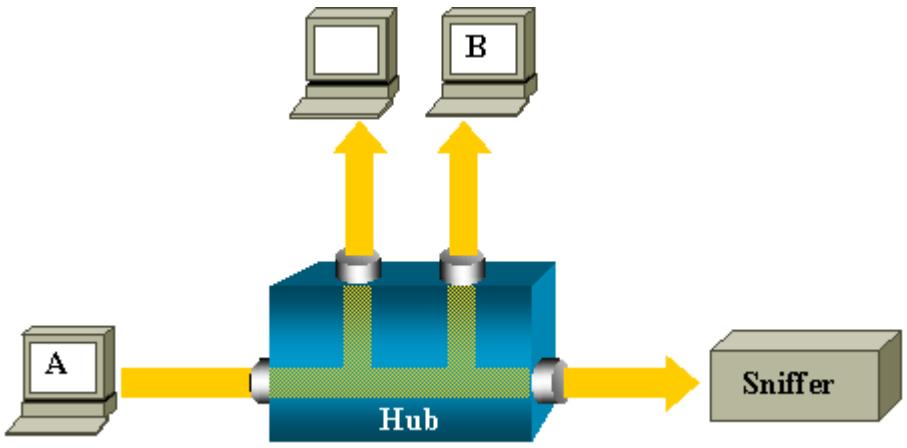
- Qu'est-ce que la fonctionnalité SPAN et comment la configurez-vous ?
- Quelles sont les différentes fonctionnalités disponibles (en particulier plusieurs sessions SPAN simultanées) et quel niveau de logiciel est nécessaire pour les exécuter ?
- La fonctionnalité SPAN affecte-t-elle les performances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

Brève description de SPAN

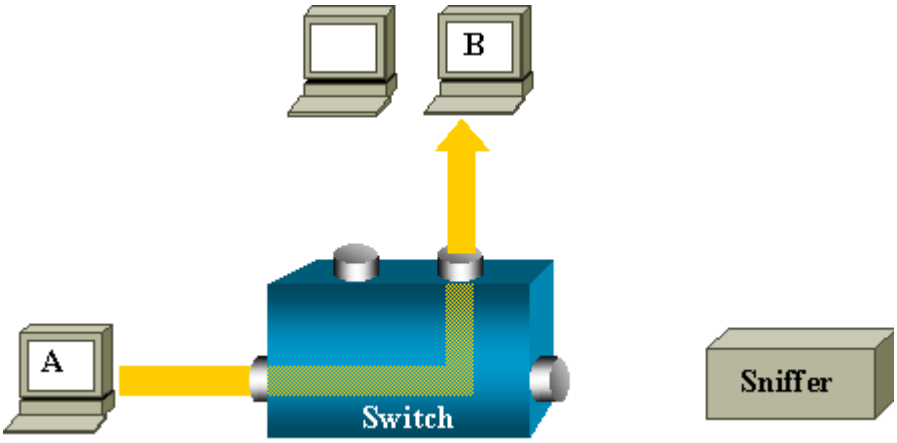
La fonctionnalité SPAN a été introduite sur les commutateurs en raison d'une différence fondamentale entre les commutateurs et les concentrateurs. Lorsqu'un concentrateur reçoit un paquet sur un port, il envoie une copie de ce paquet sur tous les ports, à l'exception de celui où le concentrateur a reçu le paquet.

Après le démarrage d'un commutateur, il commence à créer une table de transfert de couche 2 sur la base de l'adresse MAC source des différents paquets que le commutateur reçoit. Une fois cette table de transfert créée, le commutateur transfère le trafic 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 transmis au port B. Par conséquent, l'analyseur ne voit pas ce trafic :



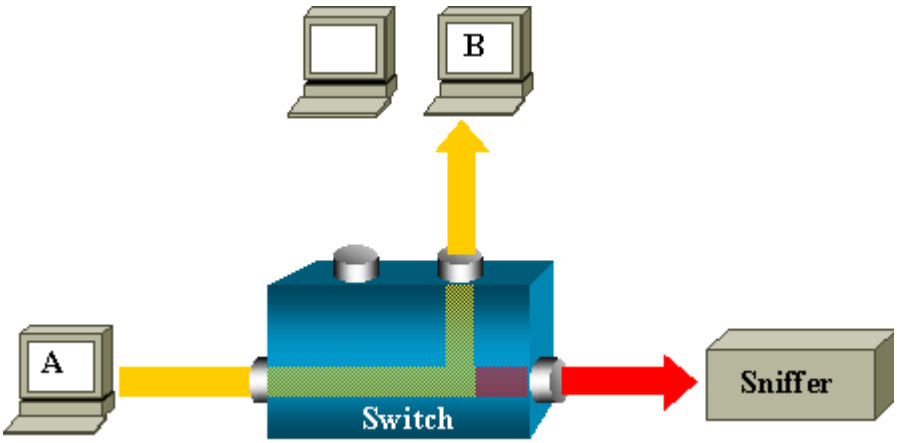
Dans cette configuration, l'analyseur capture uniquement le trafic qui est diffusé vers tous les ports, par exemple :

- Trafic de diffusion
- Trafic multidiffusion avec surveillance CGMP ou IGMP (Internet Group Management Protocol) désactivée
- Trafic de monodiffusion inconnu

L'inondation de monodiffusion se produit lorsque le commutateur ne dispose pas de l'adresse MAC de destination dans sa table CAM (Content-Addressable Memory).

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

Une fonctionnalité supplémentaire est nécessaire pour copier artificiellement les paquets de monodiffusion que l'hôte A envoie au port de l'analyseur :

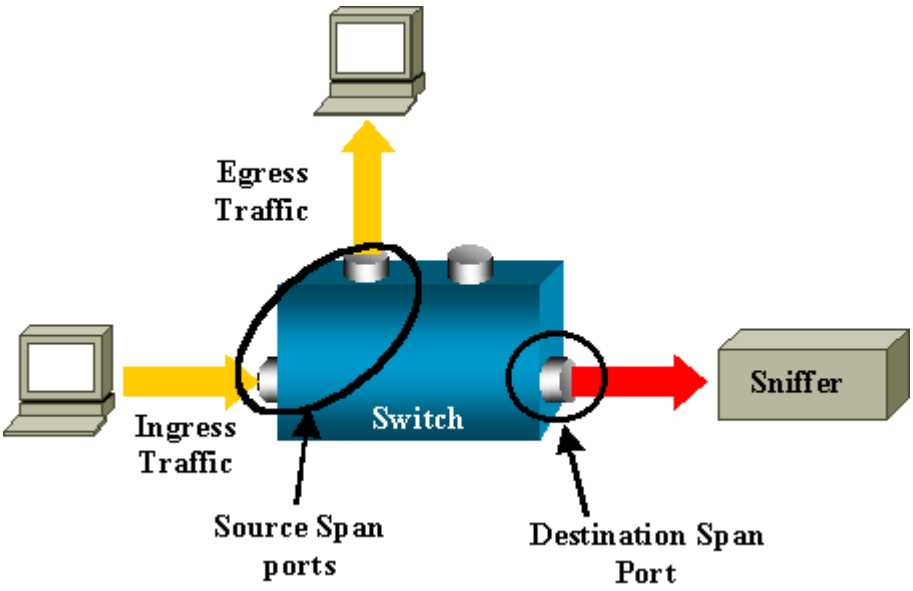


Dans ce schéma, l'analyseur est attaché à un port configuré pour recevoir une copie de chaque paquet envoyé par l'hôte A. Ce port est appelé port SPAN.

Les autres sections de ce document décrivent comment vous pouvez régler cette fonctionnalité très précisément pour faire plus que simplement surveiller un port.

Terminologie SPAN

- Trafic entrant : trafic entrant dans le commutateur.
- Trafic de sortie : trafic sortant du commutateur.
- Port source (SPAN) : port surveillé à l'aide de la fonctionnalité SPAN.
- VLAN source (SPAN) : VLAN dont le trafic est surveillé à l'aide de la fonctionnalité SPAN.
- Port de destination (SPAN) : port qui surveille les ports source, généralement là où un analyseur de réseau est connecté.
- Reflector Port : 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 Catalyst 2900XL/3500XL/2950.



- Local SPAN : la fonctionnalité SPAN est locale lorsque les ports surveillés sont tous situés sur le même commutateur que le port de destination. Cette fonctionnalité est différente de la fonctionnalité Remote SPAN (RSPAN), que cette liste définit également.
- Remote SPAN (RSPAN) : certains ports source ne sont pas situés sur le même commutateur que le port de destination.

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

RSPAN n'est pas pris en charge sur tous les commutateurs. Consultez les notes de version ou le guide de configuration respectifs pour voir si vous pouvez utiliser RSPAN sur le commutateur que vous déployez.

- SPAN basé sur les ports (PSPAN) : l'utilisateur spécifie un ou plusieurs ports source sur le commutateur et un port de destination.
- VLAN-based SPAN (VSPAN) : sur un commutateur particulier, l'utilisateur peut choisir de surveiller tous les ports qui appartiennent à un VLAN particulier dans une seule commande.
- ESPAN — Cela signifie version SPAN améliorée. Ce terme a été utilisé plusieurs fois au cours de l'évolution de la fonctionnalité SPAN pour désigner des fonctionnalités supplémentaires. Par conséquent, il n'est pas très clair et est évité dans ce document.
- Source administrative : liste des ports source ou des VLAN configurés pour être surveillés.
- Source opérationnelle : liste des ports effectivement surveillés. Cette liste de ports peut être différente de la source administrative.

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

Caractéristiques du port source

Un port source, également appelé port surveillé, est un port commuté ou routé que vous surveillez 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 (les deux). Le commutateur prend en charge un nombre illimité de ports source (jusqu'au nombre maximal de ports disponibles sur le commutateur) et un nombre illimité de VLAN source.

Un port source présente les caractéristiques suivantes :

- Il peut s'agir de n'importe quel type de port, tel qu'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 source peuvent se trouver dans le même VLAN ou dans des VLAN différents.
- Pour les sources SPAN VLAN, tous les ports actifs du VLAN source sont inclus en tant que ports source.

Filtrage VLAN

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

- Le filtrage VLAN s'applique uniquement aux ports trunk ou aux ports VLAN voix.
- Le filtrage VLAN s'applique uniquement aux sessions basées sur les ports et n'est pas autorisé dans les sessions avec des sources VLAN.
- Lorsqu'une liste de filtres VLAN est spécifiée, seuls les VLAN de la liste sont surveillés sur les ports d'agrégation ou sur les ports d'accès VLAN voix.
- Le trafic SPAN provenant d'autres types de ports n'est pas affecté par le filtrage VLAN, ce qui signifie que tous les VLAN sont autorisés sur d'autres ports.
- Le filtrage VLAN affecte uniquement le trafic transféré au port SPAN de destination et n'affecte pas la commutation du trafic normal.
- Vous ne pouvez pas mélanger des VLAN source et des VLAN de filtre au sein d'une session. Vous pouvez avoir des VLAN source ou des VLAN de filtre, mais pas les deux en même temps.

Caractéristiques du VLAN source

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

VSPAN présente les caractéristiques suivantes :

- Tous les ports actifs du VLAN source sont inclus en tant que ports source et peuvent être surveillés dans l'une ou l'autre direction 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 source et n'est pas surveillé.
- Si des ports sont ajoutés ou supprimés des VLAN sources, le trafic sur le VLAN source reçu par ces ports est ajouté ou supprimé des sources qui sont surveillées.
- Vous ne pouvez pas utiliser des VLAN de filtre dans la même session avec des sources VLAN.
- Vous ne pouvez surveiller que 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 des ports source et VLAN.

Un port de destination présente 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 : Référez-vous à Destinations SPAN, RSPAN et ERSPAN locales pour plus d'informations.

- Un port de destination peut être un port physique affecté à un groupe EtherChannel, même si le groupe EtherChannel a été spécifié comme source SPAN. Le port est supprimé du groupe lorsqu'il est configuré comme port de destination SPAN.
- Le port ne transmet aucun trafic, à l'exception du trafic requis pour la session SPAN, sauf si l'apprentissage est activé. Si l'apprentissage est activé, le port transmet également le trafic dirigé vers les hôtes qui ont été appris sur le port de destination.

  Remarque : Référez-vous à Destinations SPAN, RSPAN et ERSPAN locales pour plus d'informations.

- L'état du port de destination est up/down par conception. L'interface affiche le port dans cet état pour indiquer clairement que le port n'est actuellement pas utilisable en tant que port de production.
- Si le transfert du trafic entrant est activé pour un périphérique de sécurité réseau. Le port de destination transfère le trafic au niveau de la couche 2.
- Un port de destination ne participe pas au Spanning Tree tant que la session SPAN est active.
- Lorsqu'il s'agit d'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 source et n'est pas surveillé.
- Un port de destination reçoit des copies du trafic envoyé et reçu pour tous les ports source surveillés. Si un port de destination est surabonné, il peut devenir encombré. Cet encombrement peut affecter le transfert du trafic sur un ou plusieurs des ports sources.

Caractéristiques du port du réflecteur

Le port du réflecteur est le mécanisme qui copie les paquets sur un VLAN RSPAN. Le port du réflecteur transfère uniquement le trafic de la session source RSPAN à laquelle il est affilié. Tout périphérique connecté à un port défini comme port de réflecteur perd sa connectivité jusqu'à ce que la session source RSPAN soit désactivée.

Le port du réflecteur présente les caractéristiques suivantes :

- Il s’agit d’un port configuré pour le bouclage.
- Il ne peut pas s'agir d'un groupe EtherChannel, il n'effectue pas d'agrégation et il ne peut pas effectuer de filtrage de protocole.
- Il peut s'agir d'un port physique attribué à un groupe EtherChannel, même si le groupe EtherChannel est spécifié comme source SPAN. Le port est supprimé du groupe lorsqu'il est configuré en tant que port de réflecteur.
- Un port utilisé comme port de réflecteur ne peut pas être un port source ou de destination SPAN, ni un port de réflecteur pour plusieurs sessions à la fois.
- Il est invisible pour tous les VLAN.
- Le VLAN natif pour le trafic en boucle sur un port de réflecteur est le VLAN RSPAN.
- Le port du réflecteur renvoie en boucle le trafic non étiqueté au commutateur. Le trafic est ensuite placé sur le VLAN RSPAN et diffusé vers tous les ports agrégés qui transportent le VLAN RSPAN.
- Le Spanning Tree est automatiquement désactivé sur un port de réflecteur.
- Un port réflecteur reçoit des copies du trafic envoyé et reçu pour tous les ports source surveillés.

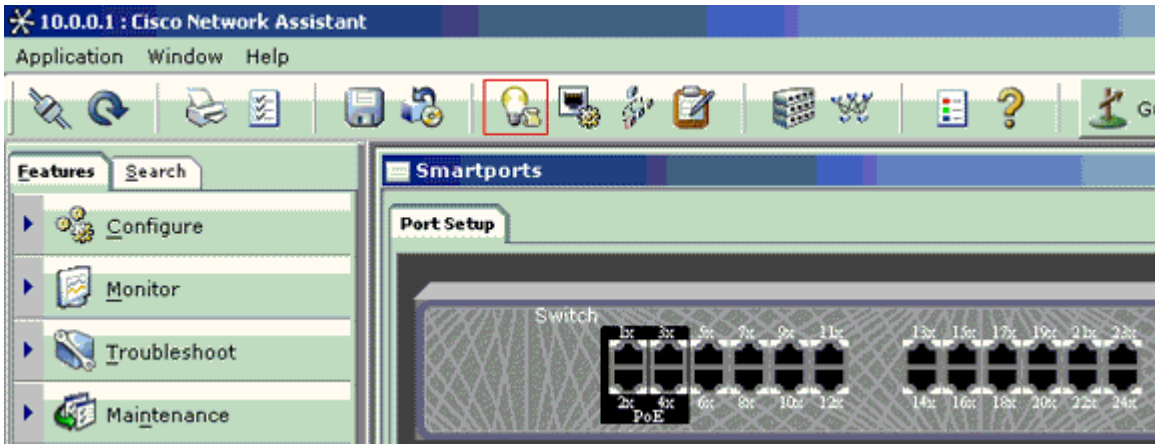
SPAN sur Catalyst Express 500/520

Catalyst Express 500 ou Catalyst Express 520 prend uniquement en charge 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). Complétez ces étapes pour configurer la fonctionnalité SPAN :

1. Téléchargez et installez CNA sur le PC.

   Téléchargez CNA depuis Software Download (clients enregistrés uniquement).

2. Suivez les étapes décrites dans le Guide de démarrage rapide des commutateurs Catalyst Express 500 12.2(25)FY pour personnaliser les paramètres des commutateurs Catalyst Express 500 et 520.
3. Utilisez CNA pour vous connecter au commutateur et cliquez sur Smartport.

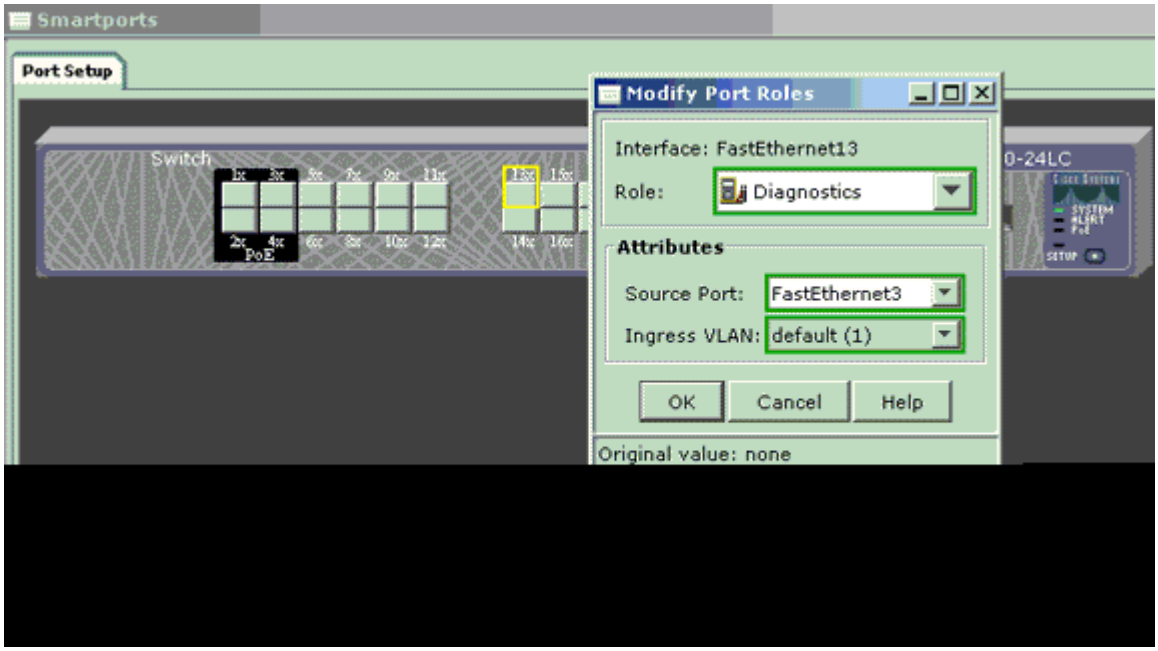


4. Cliquez sur l'interface à laquelle vous souhaitez connecter le PC pour capturer les traces de l'analyseur.
5. Cliquez sur Modifier.

   Une petite fenêtre contextuelle s'affiche.

6. Sélectionnez le rôle Diagnostics du port.
7. Choisissez le port source et sélectionnez le VLAN que vous souhaitez surveiller.

   Si vous sélectionnez Aucun, le port reçoit uniquement le trafic. Le VLAN d'entrée permet au PC connecté au port de diagnostic d'envoyer des paquets au réseau qui utilise ce VLAN.



8. Cliquez sur OK pour fermer la fenêtre contextuelle.
9. Cliquez sur OK, puis sur Apply.
10. Vous pouvez utiliser n'importe quel logiciel Sniffer pour suivre le trafic une fois que vous avez configuré le port de diagnostic.

Fonction SPAN sur les commutateurs Catalyst 2900XL/3500XL

Fonctionnalités disponibles et restrictions

La fonction de surveillance des ports n'est pas très étendue sur les commutateurs Catalyst 2900XL/3500XL. Par conséquent, cette caractéristique est relativement facile à comprendre.

Vous pouvez créer autant de sessions PSPAN locales que nécessaire. Par exemple, vous pouvez créer des sessions PSPAN sur le port de configuration que vous avez choisi comme port SPAN de destination. Dans ce cas, exécutez la commande d'interface port monitor pour répertorier les ports sources que vous souhaitez surveiller. Un port de surveillance est un port SPAN de destination dans la terminologie Catalyst 2900XL/3500XL.

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

Cette liste fournit quelques 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 dotés de la fonctionnalité port-monitor.

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

Veillez à ce qu'un port à l'état de surveillance n'exécute pas le protocole STP (Spanning Tree Protocol) tant qu'il appartient toujours au VLAN des ports qu'il met en miroir. Le moniteur de port peut faire partie d'une boucle si, par exemple, vous le connectez à un concentrateur ou à un pont et que vous effectuez une boucle sur une autre partie du réseau. Dans ce cas, vous pouvez vous retrouver dans une condition catastrophique de boucle de pontage parce que STP ne vous protège plus. Reportez-vous à 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.

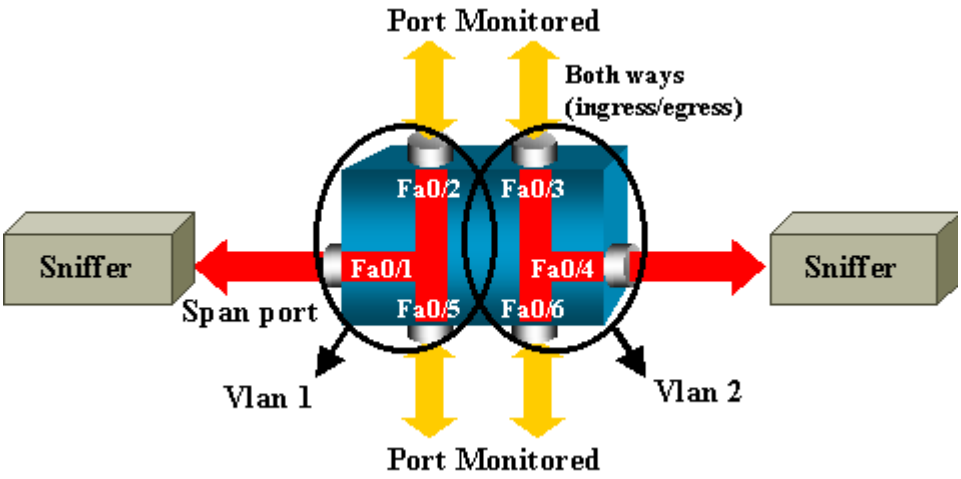
Exemple de configuration

Cet exemple crée deux sessions SPAN simultanées.

- Le port Fast Ethernet 0/1 (Fa0/1) surveille le trafic envoyé et reçu par les ports Fa0/2 et Fa0/5. Le port Fa0/1 surveille également le trafic en provenance et à destination 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 le VLAN 2. Les autres ports et l'interface de gestion sont configurés dans le VLAN 1 par défaut.

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 en tant que port de destination, les ports source Fa0/2 et Fa0/5 et l'interface de gestion (VLAN 1), sélectionnez l'interface Fa0/1 en mode de configuration :

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

Entrez la liste des ports à surveiller :

```
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 sur le port Fa0/1. Émettez une variante de la commande port monitor pour configurer la surveillance pour l'interface d'administration :

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

Remarque : Cette commande ne signifie pas que le port Fa0/1 surveille la totalité du VLAN 1. Le mot clé vlan 1 fait simplement référence à l'interface administrative du commutateur. Cet exemple de commande montre que la surveillance d'un port dans un autre VLAN est impossible :

```
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, utilisez Fa0/4 comme port SPAN de destination :

```
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
```

Émettez une commande show running, ou utilisez la commande show port monitor pour vérifier la configuration :

```
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 le trafic Rx et Tx.

SPAN sur les commutateurs Catalyst 2948G-L3 et 4908G-L3

Les commutateurs Catalyst 2948G-L3 et Catalyst 4908G-L3 sont des routeurs de commutation à configuration fixe ou des commutateurs de couche 3. La fonctionnalité SPAN d'un commutateur de couche 3 est appelée surveillance de port.

Cependant, la surveillance des ports n'est pas prise en charge sur ces commutateurs.

SPAN sur le Catalyst 8500

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

Émettez la commande snoop pour configurer la mise en miroir du trafic basée sur les ports, ou snooping. Émettez la forme no de cette commande pour désactiver la surveillance :

```
snoop interface source_port direction snoop_direction

no snoop interface source_port
```

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

```
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 le résultat de la commande show snoop :

```
8500CSR#show snoop
Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option:         (configured=enabled)(actual=enabled)
Snoop direction:      (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```

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. À la place, vous devez utiliser une image de routeur de commutation de campus (CSR), telle que 8540c-in-mz.

Fonctionnalité SPAN sur les commutateurs des gammes Catalyst 2900, 4500/4000, 5500/5000 et 6500/6000 qui exécutent CatOS

Cette section s'applique uniquement aux commutateurs 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, notamment :

- Commutateurs de châssis modulaires :
  - Commutateur Cisco Catalyst 4003
  - Commutateur Cisco Catalyst 4006
- Commutateur à châssis fixe :
  - Commutateur Cisco Catalyst 4912G

SPAN local

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

<#root>

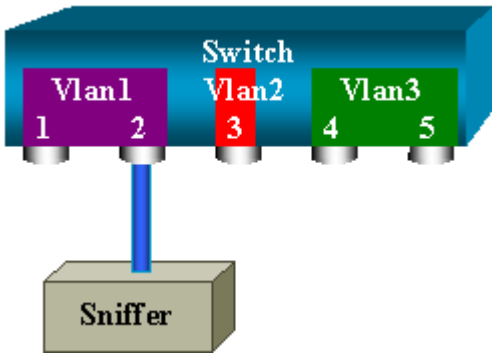
```
switch (enable)

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 schéma de réseau présente les différentes possibilités de la fonctionnalité SPAN avec l'utilisation de variantes :



Ce schéma représente une partie d'une carte de ligne unique située dans le logement 6 d'un commutateur Catalyst 6500/6000. Dans ce scénario :

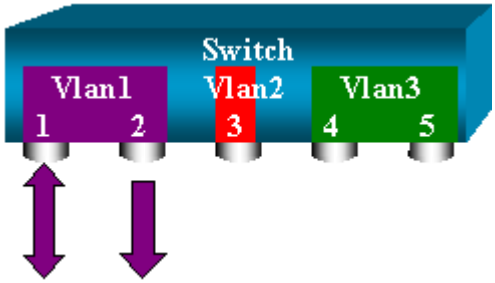
- Les ports 6/1 et 6/2 appartiennent au VLAN 1
- Le port 6/3 appartient au VLAN 2
- Les ports 6/4 et 6/5 appartiennent au VLAN 3

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

PSPAN, VSPAN : Surveiller certains ports ou un VLAN entier

Émettez la forme la plus simple de la commande set span pour surveiller un seul port. La syntaxe est set span source_port destination_port .

Surveiller un seul port avec la fonctionnalité SPAN



```
switch (enable)

set span 6/1 6/2



Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

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. Émettez la commande show span pour recevoir un résumé de la configuration SPAN actuelle :

<#root>

```
switch (enable)

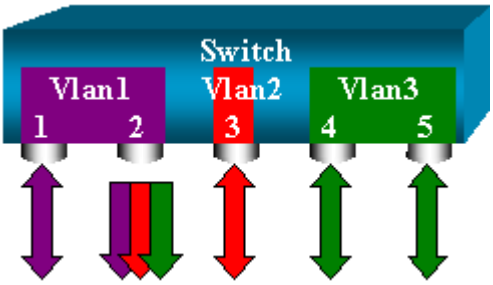
show span



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
```

Surveillance de plusieurs ports avec la fonctionnalité SPAN



La commande set span source_ports destination_port permet à l'utilisateur de spécifier plusieurs ports source. Répertoriez simplement tous les ports sur lesquels vous souhaitez implémenter la fonctionnalité SPAN et séparez-les par des virgules. L'interpréteur de ligne de commande vous permet également d'utiliser le trait d'union pour spécifier une plage de ports.

Cet exemple illustre cette capacité à spécifier plusieurs ports. L'exemple 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 SPAN.

<#root>

```
switch (enable)

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

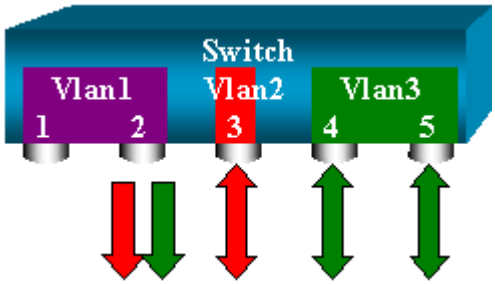


2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
       for destination port 6/2
       Destination : Port 6/2
       Admin Source : Port 6/1,6/3-5
       Oper Source : Port 6/1,6/3-5
       Direction : transmit/receive
       Incoming Packets: disabled
       Learning : enabled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

Surveillance des VLAN avec SPAN

Enfin, la commande set span vous permet de configurer un port pour surveiller le trafic local pour un VLAN entier. La commande est set span source_vlan(s) destination_port.



Utilisez une liste d'un ou 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 ou sort du VLAN 2 ou 3 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 `Source d'opération` et le champ `Source d'administration`. 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/sortie

Dans l'exemple de la section Surveiller les VLAN avec la fonctionnalité SPAN, le trafic entrant et sortant des ports spécifiés est surveillé.

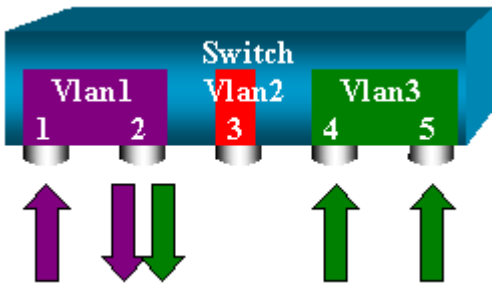
La `direction : le` champ `de transmission/réception` affiche ceci. Les commutateurs des gammes Catalyst 4500/4000, 5500/5000 et 6500/6000 vous permettent de collecter uniquement le trafic sortant (sortant) ou entrant (entrant) sur un port particulier.

Ajoutez le mot clé rx (receive) ou tx (transmit) à la fin de la commande. La valeur par défaut est les deux (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 agrégation

Les agrégations sont un cas particulier dans un commutateur, car ce sont des ports qui transportent plusieurs VLAN. Si une agrégation est sélectionnée en tant que port source, le trafic de tous les VLAN de cette agrégation est surveillé.

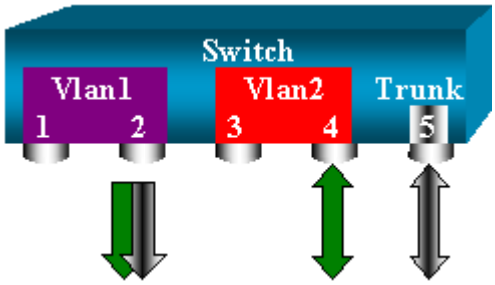
Surveiller un sous-ensemble de VLAN qui appartiennent à une agrégation

Dans ce schéma, le port 6/5 est maintenant une agrégation qui transporte tous les VLAN. Imaginez que vous souhaitez utiliser la fonctionnalité SPAN sur le trafic du VLAN 2 pour les ports 6/4 et 6/5. Il vous suffit d'exécuter cette commande :

<#root>

```
switch (enable)
```

set span 6/4-5 6/2



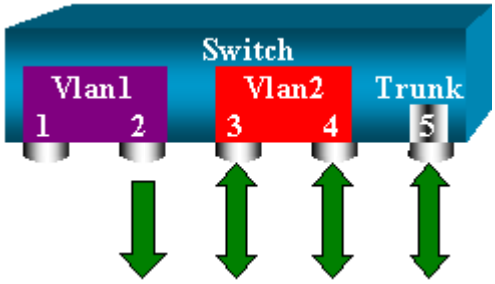
Dans ce cas, le trafic qui est reçu sur le port SPAN est une combinaison du trafic que vous voulez et de tous les VLAN que le trunk 6/5 transporte.

Par exemple, il n'y a aucun moyen de distinguer sur le port de destination si un paquet provient du port 6/4 dans le VLAN 2 ou du port 6/5 dans le VLAN 1. Une autre possibilité est d'utiliser la fonctionnalité SPAN sur l'ensemble du VLAN 2 :

<#root>

```
switch (enable)
```

set span 2 6/2



Avec cette configuration, au moins, vous ne surveillez que le trafic qui appartient au VLAN 2 à partir de l'agrégation. Le problème est que maintenant vous recevez également le trafic que vous ne vouliez pas du port 6/3.

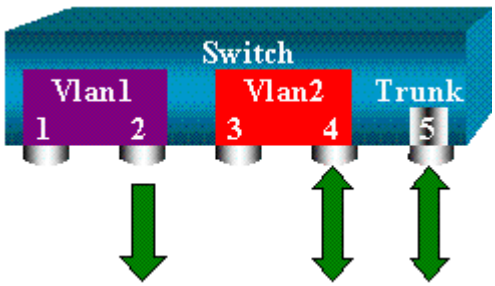
CatOS inclut un autre mot-clé qui vous permet de sélectionner certains VLAN à surveiller à partir d'une agrégation :

<#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 agrégations 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 disponible avec la commande set span.

Agrégation sur le port de destination

Si vous avez des ports source qui appartiennent à plusieurs VLAN différents, ou si vous utilisez la fonctionnalité SPAN sur plusieurs VLAN sur un port trunk, vous voulez identifier à quel VLAN appartient un paquet que vous recevez sur le port SPAN de destination. Cette identification est possible si vous activez l'agrégation sur le port de destination avant de configurer le port pour la fonctionnalité SPAN. De cette façon, tous les paquets qui sont transférés au sniffer sont également étiquetés avec leurs ID de VLAN respectifs.

Remarque : Votre analyseur doit reconnaître l'encapsulation correspondante.

<#root>

```
switch (enable)

set span disable 6/2


      This command can 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)

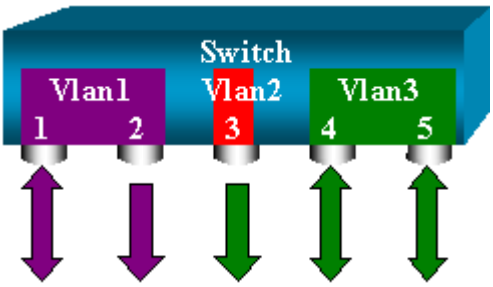
set trunk 6/2 nonegotiate isl



      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
```

Création de plusieurs sessions simultanées

Jusqu'à présent, une seule session SPAN a été créée. Chaque fois que vous émettez une nouvelle commande set span, la configuration précédente est invalidée. CatOS peut désormais exécuter plusieurs sessions simultanément, de sorte qu'il peut avoir différents ports de destination en même temps. Émettez la commande set span source destination create pour ajouter une session SPAN supplémentaire. Au cours de cette session, le port 6/1 à 6/2 est surveillé, et en même temps, le VLAN 3 au 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
```

Maintenant, émettez 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. Vous avez besoin d'un moyen de supprimer certaines sessions. La commande est la suivante :

<#root>

set span disable {all | destination_port}

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

<#root>

```
switch (enable)
```

set span disable 6/2

```
      This command can 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 maintenant 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
```

Émettez cette commande pour désactiver toutes les sessions en cours en une seule étape :

<#root>

```
switch (enable)

set span disable all


  This command can 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 SPAN

La syntaxe de 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 <enable|disable>]
                [learning <enable|disable>]
                [multicast <enable|disable>]


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

Cette section présente brièvement les options présentées 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 ultérieure.
- inpkts enable/disable — Cette option est extrêmement importante. Comme l'indique ce document, un port que vous configurez comme destination SPAN appartient toujours 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 voulez que ce PC soit entièrement 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 vous retrouver 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 pour 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 rejette les paquets que le port reçoit. Cette suppression protège le port des 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 à partir 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 multicast. La valeur par défaut est enable. Cette fonctionnalité est disponible sur les 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 MSFC (Multilayer Switch Feature Card). Le port capture le trafic qui est acheminé par logiciel ou dirigé vers la carte MSFC.

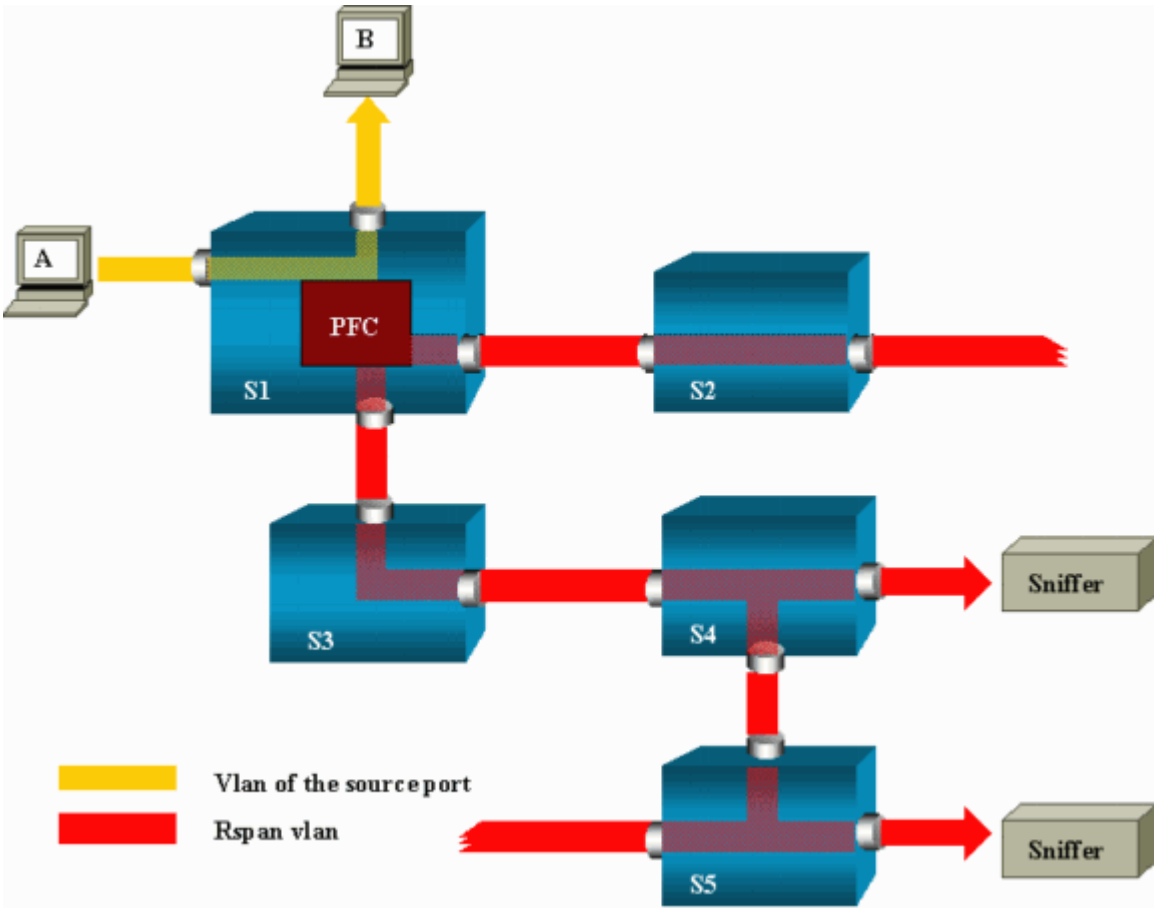
SPAN distant

Présentation de RSPAN

La fonctionnalité RSPAN vous permet de surveiller les ports source répartis sur un réseau commuté, et pas seulement localement sur un commutateur doté de 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 directement copié vers le port de destination, mais diffusé dans un VLAN RSPAN spécial. Le port de destination peut alors être situé n'importe où dans ce VLAN RSPAN. Il peut même y avoir plusieurs ports de destination.

Ce schéma illustre la structure d'une session RSPAN :



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

Voici quelques remarques sur cette conception :

- S1 est appelé commutateur source. Les paquets entrent uniquement dans le VLAN RSPAN dans les commutateurs configurés comme source RSPAN. Actuellement, un commutateur ne peut être la source que d'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. Ils ne sont pas des sources RSPAN et ne possèdent pas de ports de destination. Un commutateur peut être intermédiaire pour un nombre quelconque 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, un Catalyst 6500/6000 peut avoir jusqu'à 24 ports de destination RSPAN, pour une ou plusieurs sessions différentes. Vous pouvez également remarquer que S4 est à la fois un commutateur de destination et un commutateur intermédiaire.

- Vous pouvez voir que les paquets RSPAN sont diffusés dans le VLAN RSPAN. Même les commutateurs qui ne sont pas sur le chemin d'un port de destination, tel que S2, reçoivent le trafic pour le VLAN RSPAN. Vous pouvez trouver utile d'élaguer ce VLAN sur ces liaisons S1-S2.
- Pour atteindre l'inondation, l'apprentissage est désactivé sur le VLAN RSPAN.
- Pour empêcher les boucles, le protocole STP a été maintenu sur le VLAN RSPAN. Par conséquent, RSPAN ne peut pas surveiller les unités BPDU (Bridge Protocol Data Unit).

Exemple de configuration RSPAN

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



Configuration de la liaison ISL entre les deux commutateurs S1 et S2

Pour commencer, placez le même domaine VTP (VLAN Trunk Protocol) sur chaque commutateur et configurez un côté comme agrégation souhaitable. La négociation VTP fait le reste. Exécutez cette commande sur S1 :

<#root>

```
S1> (enable)

set vtp domain cisco


      VTP domain cisco modified
```

Exécutez ces commandes 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 nécessite un VLAN RSPAN spécifique. Vous devez créer ce VLAN. Vous ne pouvez pas convertir un VLAN existant en VLAN RSPAN. Cet exemple utilise le VLAN 100 :

<#root>

```
S2> (enable)

set vlan 100 rspan


      Vlan 100 configuration successful
```

Exécutez cette commande sur un commutateur configuré en tant que serveur VTP. La connaissance du VLAN 100 RSPAN est propagée automatiquement dans l'ensemble du domaine VTP.

Configuration du port 5/2 de S2 comme port de destination 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 dans S1 via le port 6/2 est surveillé. Émettez cette commande :

<#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 diffusés sur le VLAN 100 RSPAN et atteignent le port de destination qui est configuré sur S1 via l'agrégation.

Vérification de la configuration

La commande show rspan fournit un résumé de la configuration RSPAN actuelle sur le

commutateur. Là encore, 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 RSPAN. En dehors de cette différence, SPAN et RSPAN se comportent réellement 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

Ce tableau récapitule les différentes fonctionnalités qui ont été introduites et fournit la version minimale de CatOS qui est nécessaire pour exécuter la fonctionnalité sur la plate-forme spécifiée :

Fonctionnalité	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
inpkts, option 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 d'activation/désactivation de la multidiffusion	—	5.1	5.1
option learning enable/disable	5.2	5.2	5.3
RSPAN	6.3	—	5.3

Ce tableau fournit un bref résumé des restrictions actuelles sur le nombre de sessions SPAN

possibles :

Fonctionnalité	Gamme de commutateurs Catalyst 4500/4000	Gamme de commutateurs Catalyst 5500/5000	Gamme de commutateurs Catalyst 6500/6000
Rx ou les deux sessions SPAN	5	1	2
Sessions SPAN Tx	5	4	4
Sessions Mini Protocol Analyzer	Non pris en charge	Non pris en charge	1
Rx, Tx ou les deux sessions source RSPAN	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

Reportez-vous à ces documents pour connaître les restrictions supplémentaires et les consignes de configuration :

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

Fonctionnalité SPAN sur les commutateurs des gammes Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 et 3750-E

Voici des instructions pour la configuration de la fonctionnalité SPAN sur les commutateurs des gammes 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 ne peuvent surveiller que les ports source. 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 ultérieure.
- 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 ainsi que les VLAN.
- Les commutateurs Catalyst 2970, 3560 et 3750 ne nécessitent 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 avec l'utilisation de ports source et de destination qui résident sur l'un 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 similaires sur Catalyst 2950 et Catalyst 3550. Cependant, le 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 en tant que destination pour la fonctionnalité SPAN locale et la fonctionnalité RSPAN pour le même trafic VLAN. Pour surveiller le trafic pour 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 du VLAN 5 qui est réparti sur 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 cette configuration :

<#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  <Remote vlan id>
```

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 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.

Remarque : Les commutateurs Catalyst 2950 qui utilisent le logiciel Cisco IOS version 12.1.(9)EA1d et les versions antérieures de la catégorie du logiciel Cisco IOS version 12.1 prennent en charge la fonctionnalité SPAN. Cependant, tous les paquets visibles sur le port de destination SPAN (connecté au périphérique ou au PC de détection) ont une étiquette IEEE 802.1Q, même si le port source SPAN (port surveillé) ne peut pas être un port d'agrégation 802.1Q. Si le périphérique d'analyse ou la carte réseau du PC ne comprend pas les paquets étiquetés 802.1Q, le périphérique peut abandonner les paquets ou rencontrer des difficultés lorsqu'il tente de les décoder. La possibilité de voir les trames étiquetées 802.1Q n'est importante que lorsque le port source SPAN est un port agrégé. Avec le logiciel Cisco IOS version 12.1(11)EA1 et ultérieure, vous pouvez activer et désactiver l'étiquetage des paquets au niveau du port de destination SPAN. Émettez la commande monitor session number destination interface interface id encapsulation dot1q pour activer l'encapsulation des paquets au port de destination. 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 ultérieure.

Fonctionnalité	Catalyst 2950/3550
Option d'activation/désactivation d'entrée (entrées)	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
Rx ou les deux sessions SPAN	2
Sessions SPAN Tx	2
Rx, Tx ou les deux sessions source RSPAN	2
Destination RSPAN	2
Nombre total de sessions	2

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

Fonctionnalité SPAN sur les commutateurs des gammes Catalyst 4500/4000 et Catalyst 6500/6000 qui exécutent le logiciel système Cisco IOS

La fonctionnalité SPAN est prise en charge sur les commutateurs des gammes Catalyst 4500/4000 et Catalyst 6500/6000 qui exécutent la plate-forme logicielle Cisco IOS. Ces deux

plates-formes de commutation utilisent l'interface de ligne de commande (CLI) identique à la configuration décrite dans cette section, ainsi qu'une configuration similaire. Reportez-vous à ces documents pour la configuration associée :

- 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

Ce tableau récapitule les différentes fonctionnalités qui ont été introduites et fournit la version minimale du logiciel Cisco IOS nécessaire pour exécuter la fonctionnalité sur la plate-forme spécifiée :

Fonctionnalité	Catalyst 4500/4000 (logiciel Cisco IOS)	Catalyst 6500/6000 (logiciel Cisco IOS)
Option d'activation/désactivation d'entrée (entrées)	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 de la gamme Cisco Catalyst 6500/6000 présente une limitation par rapport au protocole PIM. Lorsqu'un commutateur est configuré à la fois pour PIM et SPAN, l'analyseur/analyseur de réseau connecté au port de destination SPAN peut voir les paquets PIM qui ne font pas partie du trafic du port source/VLAN SPAN. Ce problème se produit en raison d'une limitation dans l'architecture de transfert de paquets du commutateur. Le port de destination SPAN n'effectue aucun contrôle pour vérifier la source des paquets. Ce problème est également documenté dans l'ID de bogue Cisco CSCdy57506 (clients enregistrés seulement).

Ce tableau fournit un bref résumé des restrictions actuelles sur le nombre de sessions SPAN et RSPAN possibles :

Fonctionnalité	Catalyst 4500/4000 (logiciel Cisco IOS)
Rx ou les deux sessions SPAN	2
Sessions SPAN Tx	4
Rx, Tx ou les deux sessions source RSPAN	2 (Rx, Tx ou les deux) et jusqu'à 4 pour Tx uniquement
Destination RSPAN	2
Nombre total de sessions	6

Référez-vous à Limites de session SPAN, RSPAN et ERSPAN locales pour les commutateurs Catalyst 6500/6000 exécutant le logiciel Cisco IOS.

Dans la gamme Catalyst 6500, il est important de noter que la fonctionnalité SPAN de sortie est exécutée sur le superviseur. Cela permet d'envoyer tout le trafic soumis à la fonctionnalité SPAN de sortie sur le fabric vers le superviseur, puis vers le port de destination de la fonctionnalité SPAN, ce qui peut utiliser des ressources système importantes et affecter le trafic utilisateur. La

fonctionnalité SPAN en entrée peut être effectuée sur les modules en entrée, de sorte que les performances de la fonctionnalité SPAN correspondent à la somme de tous les moteurs de réplication participants. Les performances de la fonctionnalité SPAN dépendent de la taille du paquet et du type d'ASIC disponible dans le moteur de réplication.

Dans les versions antérieures au logiciel Cisco IOS Version 12.2(33)SXH, une interface port-channel, un EtherChannel, ne peut pas être une destination SPAN. Avec le logiciel Cisco IOS Version 12.2(33)SXH et ultérieure, un EtherChannel peut être une destination 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.

Reportez-vous à ces documents pour connaître les restrictions supplémentaires et les consignes de configuration :

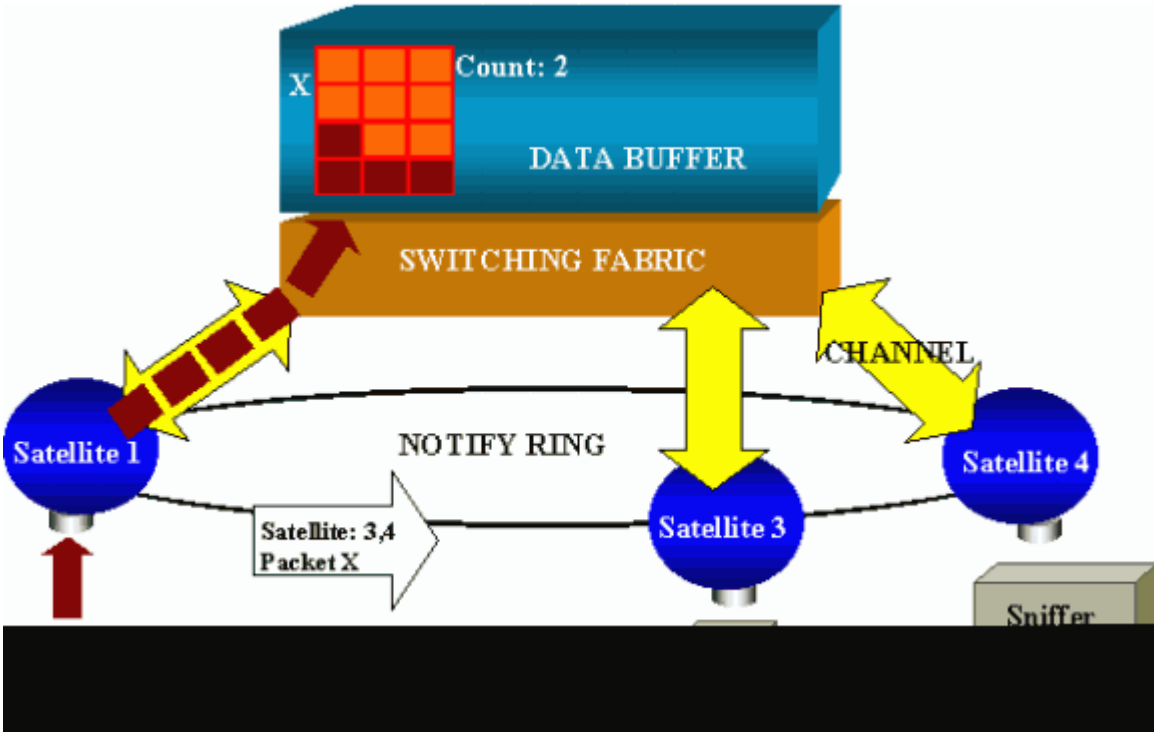
- Configuration des fonctions SPAN et RSPAN (Catalyst 4500/4000)
- Configuration de la fonctionnalité SPAN locale, RSPAN distante (RSPAN) et RSPAN encapsulée (Catalyst 6500/6000)

Impact de la fonctionnalité SPAN sur les performances des 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 reliés à des satellites qui communiquent avec une matrice de commutation via des canaux radiaux. En haut, tous les satellites sont interconnectés via un anneau de notification à haut débit dédié au trafic de signalisation.

Lorsqu'un satellite reçoit un paquet d'un port, le paquet est divisé 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 schéma de 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 de la mémoire partagée via leurs canaux radiaux et éventuellement transférer le paquet. Le satellite source connaissant la destination, ce satellite transmet également un index 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 index est décrémenté. Lorsque l'index 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 nouveau du tampon de données vers un satellite. L'impact sur le fabric de commutation haut débit est négligeable.

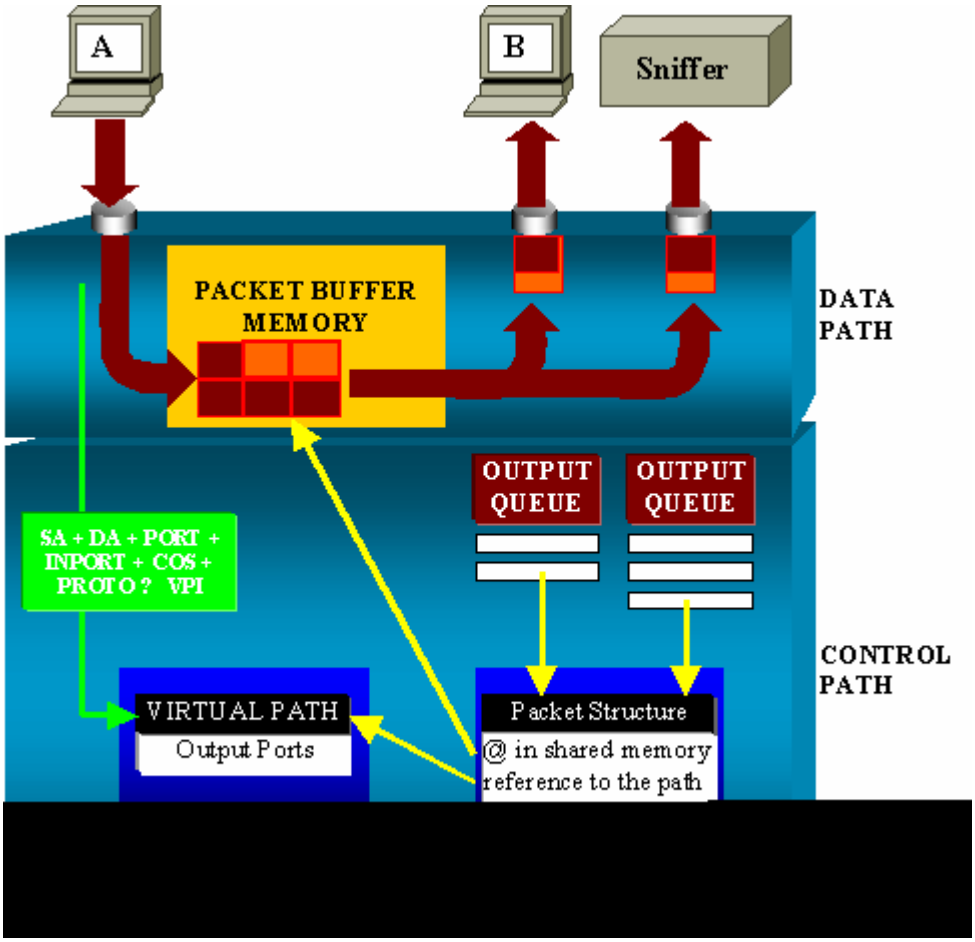
Le port de surveillance reçoit des copies du trafic transmis et reçu pour tous les ports surveillés. Dans cette architecture, un paquet destiné à plusieurs destinations est stocké en mémoire jusqu'à ce que toutes les copies soient transférées. Si le port de surveillance est surabonné à 50 pour cent pendant une période prolongée, le port risque d'être encombré et de conserver une partie de

la mémoire partagée. Il est possible qu'un ou plusieurs des ports qui sont surveillés subissent également un ralentissement.

Gammes Catalyst 4500/4000

Présentation de l'architecture

Le Catalyst 4500/4000 est basé sur une matrice de commutation à mémoire partagée. Ce schéma est une présentation générale du chemin d'un paquet à travers le commutateur. La mise en oeuvre effective est en fait beaucoup plus complexe :



Sur un commutateur Catalyst 4500/4000, vous pouvez distinguer le chemin des données. Le chemin de données correspond au transfert réel de données au sein du commutateur, à partir du chemin de contrôle, où toutes les décisions sont prises.

Lorsqu'un paquet entre dans le commutateur, une mémoire tampon est allouée dans la mémoire tampon de paquet (une mémoire partagée).

Une structure de paquets qui pointe vers cette mémoire tampon est initialisée dans la table des

descripteurs de paquets (PDT).

Pendant que les données sont copiées dans la mémoire partagée, le chemin de contrôle détermine où commuter le paquet. Pour effectuer cette détermination, une valeur de hachage est calculée à partir de ces informations :

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

Cette valeur est utilisée pour rechercher l'index de chemin virtuel (VPI) d'une structure de chemin dans la table de chemin virtuel (VPT). Cette entrée de chemin virtuel dans le VPT contient plusieurs champs qui se rapportent à ce flux particulier. Les champs incluent les ports de destination. La structure des paquets dans le PDT est maintenant mise à jour avec une référence au chemin virtuel et au compteur.

Dans l’exemple de cette section, le paquet doit être transmis à deux ports différents, de sorte que le compteur s’initialise à 2. Enfin, la structure du paquet 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 dans la mémoire tampon de sortie du port, et le compteur de structure de paquet décrémente. Lorsqu'elle atteint 0, la mémoire tampon partagée est libérée.

Impact sur les performances

Avec la fonctionnalité SPAN, un paquet doit être envoyé à deux ports différents, comme dans l'exemple de la section Présentation 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 encombré, les paquets sont abandonnés dans la file d'attente de sortie et sont correctement libérés de la mémoire partagée. Par conséquent, il n'y a aucun impact sur le fonctionnement du commutateur.

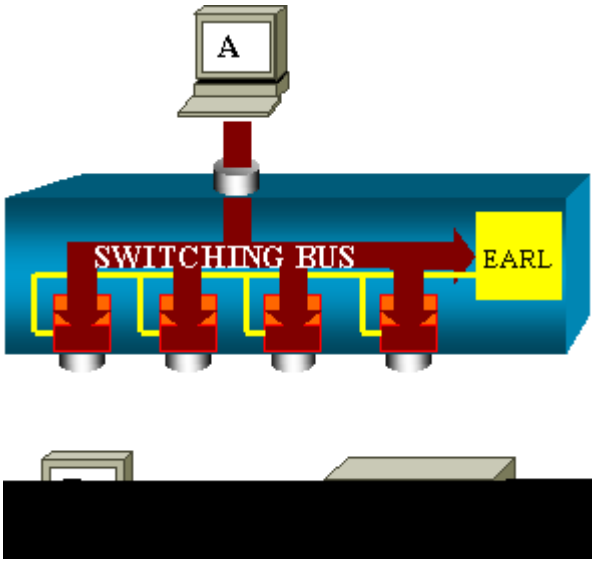
Gammes Catalyst 5500/5000 et 6500/6000

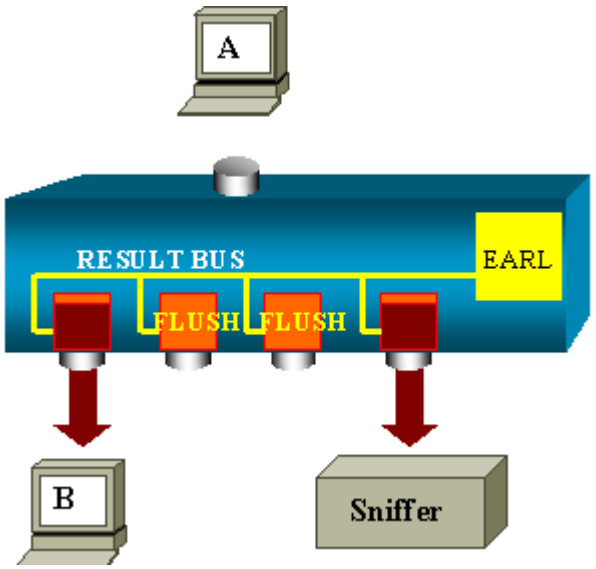
Présentation de l'architecture

Sur les commutateurs des gammes Catalyst 5500/5000 et 6500/6000, un paquet reçu sur un port

est transmis sur le bus de commutation interne. Chaque carte de ligne du commutateur commence à stocker ce paquet dans des mémoires tampons internes.

Simultanément, la logique de reconnaissance d'adresse codée (EARL) reçoit l'en-tête du paquet et calcule un indice de résultat. EARL envoie l'index de résultat à toutes les cartes de ligne via le bus de résultat. La connaissance de cet index permet à la carte de ligne de décider individuellement si elle peut vider ou transmettre le paquet lorsque la carte de ligne reçoit le paquet dans ses tampons.





Impact sur les performances

Le fait qu'un ou plusieurs ports transmettent finalement le paquet n'a absolument aucune influence sur le fonctionnement du commutateur. Par conséquent, si vous considérez cette architecture, la fonctionnalité SPAN n'a aucun impact sur les performances.

Foire aux questions et problèmes courants

Problèmes de connectivité dus à une mauvaise configuration SPAN

Les problèmes de connectivité dus à une mauvaise configuration de la fonctionnalité SPAN se produisent fréquemment dans les versions de CatOS antérieures à la version 5.1. Avec ces versions, une seule session SPAN est possible.

La session reste dans la configuration, même lorsque vous désactivez la fonctionnalité SPAN. En exécutant 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. De graves problèmes de connectivité peuvent survenir si le port de destination est utilisé pour transférer le trafic utilisateur.

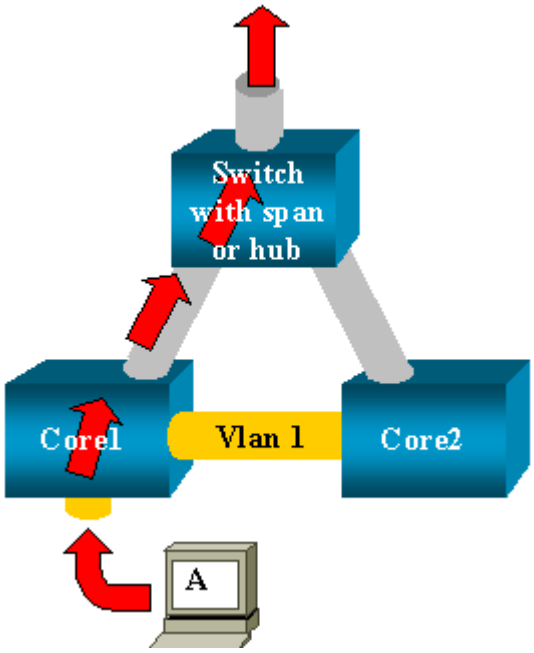
⚠ Mise en garde : Ce problème est toujours dans l'implémentation actuelle de CatOS. Faites très attention au port que vous choisissez comme destination SPAN.

Port de destination SPAN actif/inactif

Lorsque les ports sont étendus pour la surveillance, l'état du port est UP/DOWN. Lorsque vous configurez une session SPAN pour surveiller le port, l'interface de destination affiche l'état down (surveillance), par conception. L'interface affiche le port dans cet état pour indiquer clairement que le port n'est actuellement pas utilisable en tant que port de production. La surveillance du port comme up/down est normale.

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

La création d'une boucle de pontage se produit généralement lorsque l'administrateur tente de simuler la fonctionnalité RSPAN. En outre, une erreur de configuration peut provoquer le problème. Exemple de scénario :

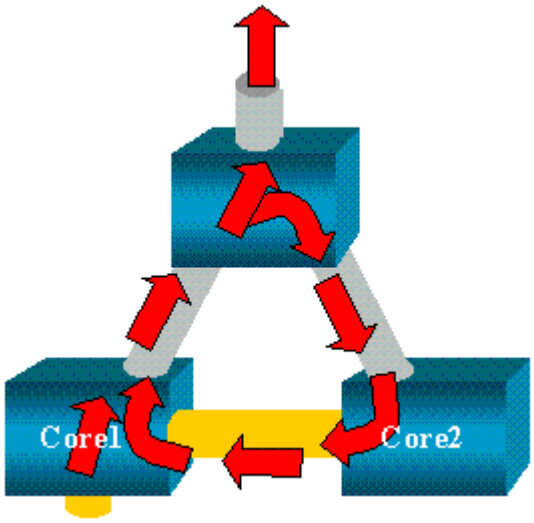


Deux commutateurs principaux sont reliés par une agrégation. Dans ce cas, plusieurs serveurs, clients ou autres ponts sont connectés à chaque commutateur. L'administrateur souhaite surveiller le VLAN 1, qui apparaît sur plusieurs ponts avec la fonctionnalité SPAN.

L'administrateur crée une session SPAN qui surveille l'ensemble 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, avec l'utilisation d'une autre session SPAN).

L'administrateur atteint l'objectif. Chaque paquet qu'un commutateur principal reçoit sur VLAN 1 est dupliqué sur le port SPAN et transféré vers le concentrateur. Un analyseur 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 coeur 2 crée une boucle de pontage dans le VLAN 1. N'oubliez pas qu'un port SPAN de destination n'exécute pas le protocole STP et ne peut pas empêcher une telle boucle.



Remarque : En raison de l'introduction de l'option inpkts (input packets) sur CatOS, un port de destination SPAN abandonne par défaut tout paquet entrant, 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 entraîner certains problèmes sur le réseau. Des problèmes réseau peuvent se produire en raison de problèmes d’apprentissage d’adresses MAC associés à l’apprentissage activé sur le port de destination.

La fonctionnalité SPAN affecte-t-elle les performances ?

Reportez-vous aux sections suivantes de ce document pour obtenir des informations sur l'impact sur les performances des plates-formes Catalyst spécifiées :

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

Pouvez-vous configurer la fonctionnalité SPAN sur un port EtherChannel ?

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

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

Vous pouvez utiliser un port d'un bundle EtherChannel comme port source SPAN.

Pouvez-vous exécuter plusieurs sessions SPAN 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 la fois. 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.

Reportez-vous aux sections Créer plusieurs sessions simultanées et Résumé des fonctionnalités et limitations de ce document.

Erreur "% La Limite De Session Locale A Été Dépassée"

Ce message apparaît lorsque la session SPAN autorisée dépasse la limite pour le Supervisor Engine :

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

Les Supervisor Engines ont une limitation des sessions SPAN. Référez-vous à la section Limites de session SPAN, RSPAN et ERSPAN locales de Configuration de SPAN, RSPAN et ERSPAN locales pour plus d'informations.

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

Avec ce problème, le module VPN (Virtual Private Network) est inséré dans le châssis, où un module de matrice de commutation a déjà été inséré.

Le logiciel Cisco IOS crée automatiquement une session SPAN pour que le module de service VPN gère le trafic de multidiffusion.

Émettez cette commande pour supprimer la session SPAN que le logiciel crée pour le module de service VPN :

<#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 ne parvenez-vous pas à 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. Lorsqu'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 un tampon.
3. Le paquet est finalement retransmis sur le port de sortie.



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

Un commutateur n'est pas complètement transparent en ce qui concerne la capture du trafic. De même, lorsque vous voyez un paquet corrompu sur votre analyseur dans le scénario de 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 renifleur sur un concentrateur. Le concentrateur n'effectue aucun contrôle d'erreur.

Par conséquent, contrairement au commutateur, le concentrateur ne supprime pas les paquets. De cette manière, vous pouvez afficher les paquets.

Erreur : % session 2 utilisée par le module de service

Si un module de service de pare-feu (FWSM) a été installé, par exemple, et retiré ultérieurement, dans le CAT6500, il a automatiquement activé la fonctionnalité SPAN Reflector. La fonction SPAN Reflector utilise une session SPAN dans le commutateur.

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

Le port du réflecteur abandonne les paquets

Un port réflecteur reçoit des copies du trafic envoyé et reçu pour tous les ports source surveillés. Si un port de réflecteur est surabonné, il peut devenir encombré. Cela peut affecter le transfert du trafic sur un ou plusieurs des ports sources.

Si la bande passante du port du réflecteur n'est pas suffisante pour le volume de trafic provenant des ports source correspondants, les paquets excédentaires sont abandonnés.

Un port 10/100 reflète à 100 Mbits/s. Un port Gigabit se reflète à 1 Gbit/s.

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

Lorsque vous utilisez Supervisor Engine 720 avec un FWSM dans le châssis qui exécute Cisco Native IOS, une session SPAN est utilisée par défaut. Si vous recherchez des sessions inutilisées avec la commande show monitor, la session 1 est utilisée :

<#root>

```
Cat6K#

show monitor


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

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

Si les flux de multidiffusion provenant du FWSM doivent être répliqués au niveau de la couche 3 sur plusieurs cartes de ligne, la session automatique copie le trafic vers le superviseur via un canal de fabric.

Si vous avez une source de multidiffusion qui génère un flux de multidiffusion depuis l'arrière du FWSM, vous avez besoin du réflecteur SPAN. Si vous placez la source de multidiffusion sur le VLAN externe, le réflecteur SPAN n'est pas nécessaire. Le réflecteur SPAN est incompatible avec le pontage des BPDU via le 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 normale et une session de destination RSPAN. 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. Assurez-vous également qu'aucun périphérique de couche 3 n'est présent dans le chemin de la source de la session vers la destination de la session.

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

Non. La session RSPAN ne peut traverser aucun périphérique de couche 3, car RSPAN est une fonctionnalité LAN (couche 2). Pour surveiller le trafic sur un WAN ou sur différents réseaux, utilisez l'analyseur ERSPAN (Encapsulated Remote SwitchPort Analyzer). La fonctionnalité ERSPAN prend en charge les ports source, les VLAN source et les ports de destination sur différents commutateurs, ce qui permet de surveiller à distance plusieurs commutateurs sur votre réseau.

ERSPAN se compose d'une session source ERSPAN, d'un trafic routable ERSPAN encapsulé GRE et d'une session de destination ERSPAN.

Vous configurez séparément les sessions source et 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 ultérieure
- Supervisor 720 avec PFC3A qui possède la version matérielle 3.2 ou ultérieure et qui exécute le logiciel Cisco IOS Version 12.2(18)SXE ou ultérieure

Référez-vous à Configuration de SPAN local, RSPAN distant (RSPAN) et RSPAN encapsulé - Guide de configuration du logiciel Cisco IOS de la gamme Catalyst 6500, 12.2SX pour plus d'informations sur ERSPAN.

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 peut pas transmettre les paquets capturés à partir de la session source RSPAN en raison de limitations matérielles. Ceci n'est pas pris en charge sur les commutateurs des gammes 4500 et 3750.

Ce problème est documenté dans l'ID de bogue Cisco CSCeg08870 (clients enregistrés seulement). 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 régulière.

L'analyseur de réseau/périphérique de sécurité connecté au port de destination SPAN n'est pas accessible

La caractéristique de base d'un port de destination SPAN est qu'il ne transmet aucun trafic, à l'exception du trafic requis pour la session SPAN. Si vous devez atteindre (l'accessibilité IP) l'analyseur de réseau / le périphérique de sécurité via 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, qui sont potentiellement étiquetés en fonction du mode d'encapsulation spécifié, et les commute normalement. Lorsque vous configurez un port de destination SPAN, vous pouvez spécifier si la fonctionnalité d'entrée est activée ou non et quel VLAN utiliser pour commuter les paquets d'entrée non balisés.

La spécification d'un VLAN d'entrée n'est pas requise lorsque l'encapsulation ISL est configurée, car tous les paquets encapsulés ISL ont des balises VLAN. Bien que le port soit un transfert STP, il ne participe pas au STP. Par conséquent, soyez prudent lorsque vous configurez cette fonctionnalité, de peur qu'une boucle Spanning Tree ne soit introduite dans le réseau. Lorsque l’encapsulation d’entrée et d’agrégation est spécifiée sur un port de destination SPAN, le port est transféré dans tous les VLAN actifs. La configuration d'un VLAN inexistant en tant que VLAN d'entrée n'est pas autorisée.

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

Cet exemple montre comment configurer un port de destination avec une encapsulation 802.1q et des paquets d'entrée avec l'utilisation du VLAN 7 natif.

<#root>

```
Switch(config)#

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

Avec cette configuration, le trafic provenant des sources SPAN associées à la session 1 est copié à partir de l’interface Fast Ethernet 5/48, avec une encapsulation 802.1q.

Le trafic entrant est accepté et commuté, avec des paquets non étiquetés 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
- Assistance produit pour les commutateurs
- Prise en charge de la technologie de commutation LAN
- Documentation et assistance techniques

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.