

Résolution des problèmes de trafic multidiffusion dans le même VLAN sur les commutateurs Catalyst

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Problème](#)

[Revoir les principaux concepts de multidiffusion](#)

[IGMP](#)

[IGMP Snooping](#)

[Port Mrouter](#)

[Multicast à L2](#)

[Comprendre le problème et ses solutions](#)

[Solutions](#)

[Solution 1 : activation de PIM sur l'interface VLAN/routeur de couche 3](#)

[Solution 2 : activer la fonctionnalité de demandeur IGMP sur un commutateur Catalyst de couche 2](#)

[Solution 3 : configurez le port du routeur statique sur le commutateur](#)

[Solution 4 : configurez les entrées MAC de multidiffusion statique sur tous les commutateurs](#)

[Solution 5 : désactivez la surveillance IGMP sur tous les commutateurs](#)

[Informations connexes](#)

Introduction

Ce document décrit comment corriger une défaillance d'application de multidiffusion quand elle est déployée dans le même VLAN entre les commutateurs Catalyst.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 6500 avec Supervisor Engine 720 qui exécute la version 12.2(18)SXD5 de Cisco IOS®
- Catalyst 3750 qui exécute une image de la version du logiciel Cisco IOS 12.2(25)SEB2
- Tout commutateur Catalyst qui exécute une version du logiciel Cisco IOS et prend également en charge la surveillance IGMP (Internet Group Management Protocol)

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

En outre, certains serveurs/applications qui utilisent des paquets de multidiffusion pour l'opération de cluster/haute disponibilité peuvent ne pas fonctionner si vous ne configurez pas les commutateurs de manière appropriée. Cette question est également traitée dans cet article.

Remarque : reportez-vous à la section [Matrice de prise en charge des commutateurs Catalyst pour la fonctionnalité de surveillance IGMP](#) du document [Matrice de prise en charge des commutateurs Catalyst multidiffusion](#) pour identifier ces commutateurs.

Problème

Le trafic de multidiffusion ne passe pas par les commutateurs Catalyst, même dans le même VLAN. La Figure 1 illustre ce scénario.

Figure 1 - Configuration réseau avec source multicast et récepteurs

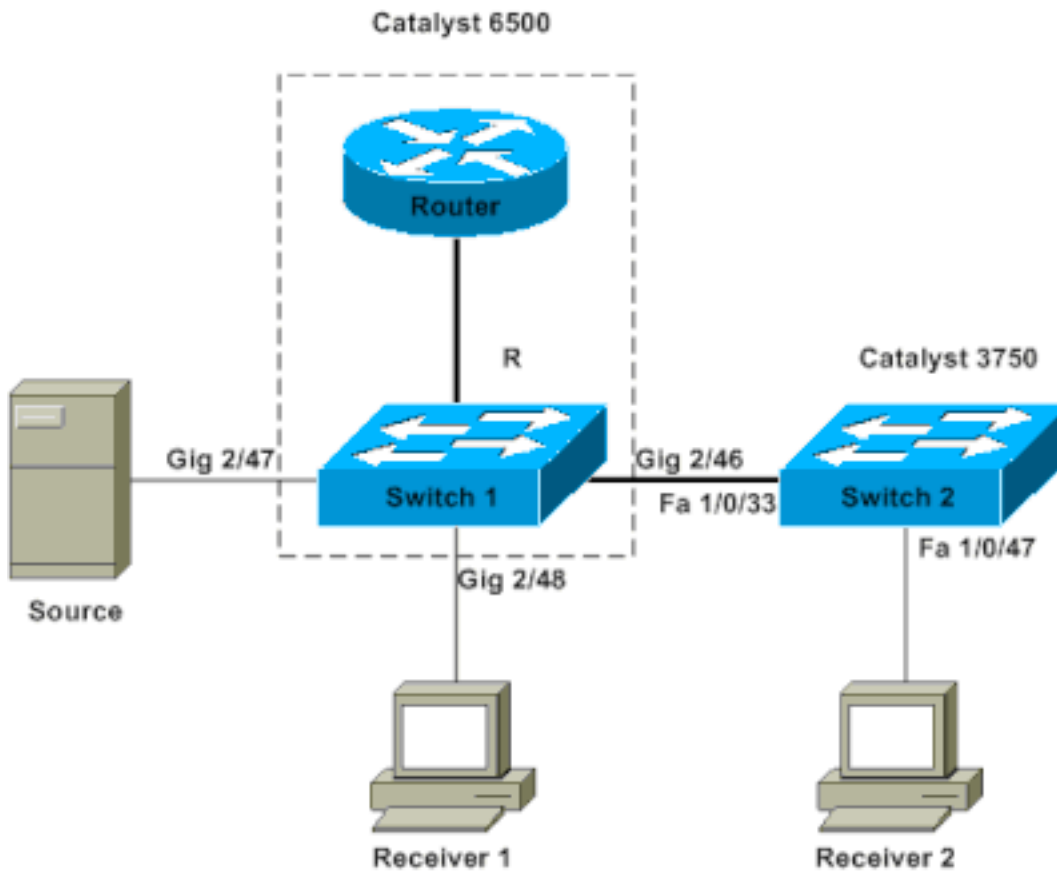


Diagramme du réseau

La source multicast est connectée au commutateur 1, qui est un commutateur Catalyst 6500 avec Supervisor Engine 720 qui exécute le logiciel Cisco IOS. Le récepteur 1 est connecté au commutateur 1 et le récepteur 2 est connecté au commutateur 2. Le commutateur 2 est un commutateur Catalyst 3750. Il y a une liaison de couche 2, accès ou agrégation, entre le commutateur 1 et le commutateur 2.

Dans cette configuration, vous voyez que le récepteur 1, qui est sur le même commutateur que la source, obtient le flux multicast sans problème. Cependant, le récepteur 2 *ne* reçoit aucun trafic de multidiffusion. Ce document vise à résoudre ce problème.

Revoir les principaux concepts de multidiffusion

Avant d'explorer la solution et les différentes options disponibles, vous devez comprendre clairement certains concepts clés du multicast de couche 2. Cette section définit ces concepts.

Remarque : cette section fournit une explication très simple et directe qui se concentre uniquement sur ce problème particulier. Consultez la section **Informations connexes** à la fin de ce document pour une explication détaillée de ces termes.

IGMP

IGMP est un protocole qui permet à des hôtes finaux (récepteurs) d'informer un routeur multicast (requérant IGMP) de l'intention d'hôte final de recevoir un trafic multicast particulier. C'est donc un protocole qui s'exécute entre un routeur et des hôtes finaux et qui permet :

- aux routeurs de demander aux hôtes finaux s'ils ont besoin d'un flux multicast particulier

(requête IGMP) ;

- aux hôtes finaux de dire ou de répondre au routeur qu'ils recherchent un flux multicast particulier (rapports IGMP).

IGMP Snooping

IGMP Snooping est un mécanisme permettant de contraindre le trafic multicast seulement aux ports qui ont des récepteurs attachés. Le mécanisme permet plus d'efficacité car grâce à lui, un commutateur de couche 2 peut envoyer sélectivement des paquets multicast seulement sur les ports qui en ont besoin. Sans IGMP Snooping, le commutateur sature les paquets sur chaque port. Le commutateur « écoute » l'échange de messages IGMP entre le routeur et les hôtes finaux. De cette façon, le commutateur construit une table de routage IGMP Snooping qui liste tous les ports qui ont demandé un groupe multicast particulier.

Port Mrouter

Le port mrouter est simplement le port du point de vue du commutateur qui se connecte à un routeur multicast. La présence d'au moins un port mrouter est absolument essentielle pour que l'opération IGMP Snooping fonctionne entre les commutateurs. Consultez la section [Comprendre le problème et ses solutions](#) de ce document pour plus de détails.

Multicast à L2

N'importe quel trafic IP version 4 (IPv4) avec un IP de destination entre 224.0.0.0 et 239.255.255.255 est un flux multicast. Tous les paquets de multidiffusion IPv4 sont mappés vers une adresse MAC IEEE prédéfinie au format 01.00.5e. xx . xx . xx .

Remarque : la surveillance IGMP ne fonctionne que si l'adresse MAC de multidiffusion correspond à cette plage MAC conforme à la norme IEEE. Certaines plages de multidiffusion réservées sont exclues de celles surveillées par la conception. Si un paquet multicast non conforme est originaire d'un réseau commuté, le paquet est saturé dans tout ce VLAN, ce qui signifie qu'il est traité comme un trafic de diffusion.

Comprendre le problème et ses solutions

Par défaut, les commutateurs Catalyst ont IGMP Snooping activé. Avec IGMP Snooping, le commutateur surveille (ou écoute) les messages IGMP sur tous les ports. Le commutateur construit une table IGMP Snooping qui mappe fondamentalement un groupe multicast à tous les ports de commutateur qui l'ont demandé.

Supposez que, sans configuration préalable, le récepteur 1 et le récepteur 2 ont signalé leur intention de recevoir un flux multicast pour 239.239.239.239 qui mappe à l'adresse MAC multicast L2 de 01.00.5e.6f.ef.ef. Le commutateur 1 et le commutateur 2 créent une entrée dans leurs tables de snooping pour ces récepteurs en réponse aux rapports IGMP générés par les récepteurs. Le commutateur 1 entre le port Gigabit Ethernet 2/48 dans sa table, et le commutateur 2 entre le port Fast Ethernet 1/0/47 dans sa table.

Remarque : à ce stade, la source de multidiffusion n'a pas démarré son trafic et aucun des commutateurs ne connaît le port mrouter du commutateur.

Lorsque la source sur le commutateur 1 commence à diffuser du trafic multidiffusion, le commutateur 1 a « vu » le rapport IGMP du récepteur 1. Par conséquent, le commutateur 1 fournit le port de multidiffusion Gigabit Ethernet 2/48. Mais, puisque le commutateur 2 « a absorbé » le rapport IGMP du récepteur 2 en tant qu'élément du procédé IGMP Snooping, le commutateur 1 ne voit pas de rapport IGMP (requête multicast) sur le port Gigabit Ethernet 2/46. En conséquence, le commutateur 1 n'envoie aucun trafic multicast au commutateur 2. Par conséquent, le récepteur 2 n'obtient aucun trafic multicast, même si le récepteur 2 est dans le même VLAN, mais simplement sur un commutateur différent que la source multicast.

La raison de ce problème est que IGMP Snooping n'est vraiment pris en charge sur aucune plateforme Catalyst sans un mrouter. Le mécanisme ne fonctionne pas sans un port mrouter. Si vous voulez un correctif, vous devez faire en sorte que les commutateurs apprennent ou connaissent un port mrouter. Reportez-vous à la section [Solutions](#) de ce document pour plus d'explications sur la procédure. Vous devez encore découvrir comment la présence d'un port mrouter sur les commutateurs résout le problème.

Fondamentalement, quand les commutateurs apprennent ou connaissent statiquement un port mrouter, deux choses se produisent :

- Le commutateur « relaye » les rapports IGMP des récepteurs au port mrouter, ce qui signifie que les rapports IGMP vont vers le routeur multicast. Le commutateur ne relaye pas tous les rapports IGMP. Au lieu de cela, le commutateur envoie seulement quelques uns des rapports au port mrouter. Pour les besoins de cette discussion, le nombre de rapports n'est pas important. Le routeur multicast doit juste savoir s'il y a au moins un récepteur qui est toujours intéressé par un flux en aval multicast. Pour déterminer cela, le routeur multicast reçoit les rapports périodiques IGMP en réponse à ses requêtes IGMP.
- Dans un scénario multicast avec source unique, dans lequel aucun récepteur ne s'est encore « joint », le commutateur envoie seulement le flux multicast à son port mrouter.

Quand les commutateurs connaissent leur port mrouter, le commutateur 2 relaie le rapport IGMP reçu du récepteur 2 à son port mrouter. Ce port est Fast Ethernet 1/0/33. Le commutateur 1 obtient ce rapport IGMP sur son port Gigabit Ethernet 2/46. Du point de vue du commutateur 1, le commutateur a reçu simplement autre rapport IGMP. Le commutateur ajoute ce port dans sa table IGMP Snooping et commence à envoyer le trafic multicast aussi sur ce port. À ce stade, les deux récepteurs reçoivent le trafic multicast demandé et l'application fonctionne comme prévu.

Pour savoir comment les commutateurs identifient leur port mrouter afin que la surveillance IGMP fonctionne comme prévu dans un environnement simple, consultez la section [Solutions](#) pour obtenir des réponses.

Solutions

Utilisez ces solutions pour résoudre le problème.

Solution 1 : activation de PIM sur l'interface VLAN/routeur de couche 3

Toutes les plates-formes Catalyst ont la capacité de se renseigner dynamiquement sur le port mrouter. Les commutateurs écoutent passivement les Hellos PIM (Protocol Independent Multicast) ou les messages de requête IGMP qu'un routeur multicast envoie périodiquement.

Cet exemple configure l'interface virtuelle commutée (SVI) VLAN 1 sur le Catalyst 6500 avec `ip pim`

sparse-dense-mode .

```
Switch1#show run interface vlan 1
!
interface Vlan1
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-dense-mode
end
```

Switch 1 now reflects itself (Actually the internal router port) as an Mrouter port.

```
Switch1#show ip igmp snooping mrouter
vlan          ports
-----+-----
 1 Router
```

Switch 2 receives the same PIM hellos on its Fa 1/0/33 interface. So it assigns that port as its Mrouter port.

```
Switch2#show ip igmp snooping mrouter
Vlan      ports
----      -
 1 Fa1/0/33(dynamic)
```

Solution 2 : activer la fonctionnalité de demandeur IGMP sur un commutateur Catalyst de couche 2

Le requérant IGMP est une fonctionnalité relativement nouvelle sur les commutateurs de couche 2. Quand un réseau/VLAN n'a pas de routeur qui peut prendre le rôle de routeur multicast et fournir la détection du mrouter sur les commutateurs, vous pouvez activer la fonctionnalité de requérant IGMP. La fonctionnalité permet au commutateur de couche 2 de trouver un routeur multicast et d'envoyer des requêtes périodiques IGMP dans ce réseau. Cette action pousse le commutateur à se considérer lui-même comme un port mrouter. Les autres commutateurs du réseau définissent simplement leurs ports mrouter respectifs comme l'interface sur laquelle ils ont reçu cette requête IGMP.

```
Switch2(config)#ip igmp snooping querier
```

```
Switch2#show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----+-----
 1        10.1.1.2        v2                 Switch
```

Le commutateur 1 voit maintenant que le port Gig 2/46 est relié au commutateur 2 en tant que port mrouter.

```
Switch1#show ip igmp snooping mrouter
vlan          ports
-----+-----
 1 Gi2/46
```

Lorsque la source sur le commutateur 1 commence à diffuser du trafic de multidiffusion, le commutateur 1 transfère le trafic de multidiffusion au récepteur 1 trouvé via la surveillance IGMP (c'est-à-dire, le port de sortie Gig 2/48) et au port mrouter (c'est-à-dire, le port de sortie Gig 2/46).

Solution 3 : configurez le port du routeur statique sur le commutateur

Le trafic de multidiffusion échoue au sein du même VLAN de couche 2 en raison de l'absence d'un port mrouter sur les commutateurs. La section [Comprendre le problème et ses solutions](#) couvre cette rubrique. Si vous configurez statiquement un port mrouter sur tous les commutateurs, des rapports IGMP peuvent être relayés dans ce VLAN à tous les commutateurs. En conséquence, le multicast est possible. Ainsi, dans l'exemple, vous devez statiquement configurer le commutateur Catalyst 3750 pour avoir Fast Ethernet 1/0/33 comme port mrouter.

Dans cet exemple, vous avez besoin d'un port statique mrouter seulement sur le commutateur 2 :

```
Switch2(config)#ip igmp snooping vlan 1 mrouter interface fastethernet 1/0/33
```

```
Switch2#show ip igmp snooping mrouter
Vlan    ports
----    -
 1     Fa1/0/33(static)
```

Solution 4 : configurez les entrées MAC de multidiffusion statique sur tous les commutateurs

Vous pouvez créer une entrée de mémoire associative (CAM) statique pour l'adresse MAC de multidiffusion sur tous les commutateurs pour tous les ports de réception et les ports de commutation en aval. N'importe quel commutateur se conforme aux règles d'entrée CAM statique et envoie le paquet à toutes les interfaces qui sont spécifiées dans la table CAM. C'est la solution la moins extensible pour un environnement qui a beaucoup d'applications multicast.

```
Switch1(config)#mac-address-table static 0100.5e6f.efef vlan 1 interface
gigabitethernet 2/46 gigabitethernet 2/48
```

!--- Note: This command should be on one line. Switch1#show mac-address-table multicast vlan 1

vlan	mac address	type	learn	qos	ports
1	0100.5e6f.efef	static	Yes	-	Gi2/46,Gi2/48

```
Switch2(config)#mac-address-table static 0100.5e6f.efef vlan 1 interface
fastethernet 1/0/47
```

!--- Note: This command should be on one line. Switch2#show mac-address-table multicast vlan 1

Vlan	Mac Address	Type	Ports
1	0100.5e6f.efef	USER	Fa1/0/47

Solution 5 : désactivez la surveillance IGMP sur tous les commutateurs

Si vous désactivez IGMP Snooping, tous les commutateurs traitent le trafic multicast comme trafic de diffusion. Cela sature le trafic sur *tous les ports dans ce VLAN, indépendamment du fait que les ports ont des récepteurs intéressés à ce flux multicast.*

```
Switch1(config)#no ip igmp snooping
```

```
Switch2(config)#no ip igmp snooping
```

Informations connexes

- [Multidiffusion dans un réseau de campus : surveillance CGMP et IGMP](#)
- [Matrice de prise en charge des commutateurs Catalyst de multidiffusion](#)
- [Prise en charge de multidiffusion IP](#)
- [Notes techniques de dépannage des problèmes liés à la multidiffusion IP](#)
- [Guide de dépannage de la multidiffusion IP](#)
- [Assistance technique et téléchargements Cisco](#)

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.