Multicast dans un réseau campus : Snooping CGMP et IGMP

Contenu

Introduction

Le but de la surveillance de trafic du Cisco Group Management Protocol (CGMP) et de l'Internet Group Management Protocol (IGMP) est de limiter le trafic de multidiffusion dans un réseau

commuté. Par défaut, un commutateur LAN propage le trafic de multidiffusion dans le domaine de diffusion, et ceci peut consommer beaucoup de bande passante si beaucoup de serveurs de multidiffusion envoient des flux au segment.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Informations générales

Le trafic de multidiffusion devient saturé, parce qu'un commutateur apprend habituellement les adresses MAC en cherchant dans le champ adresse source de toutes les trames qu'il reçoit. Une adresse MAC de multidiffusion n'est jamais utilisée comme adresse source pour un paquet. De telles adresses n'apparaissent pas dans la table d'adresses MAC et le commutateur n'a aucune méthode pour les apprendre.

La première solution à ce problème est de configurer des adresses MAC statiques pour chaque groupe et chaque client. Cette solution fonctionne bien, cependant, elle n'est ni évolutive ni dynamique. Vous utilisez cette solution sur un commutateur Catalyst 4000, 5000 ou 6000 en émettant l'une des commandes suivantes :

- **set cam static**
- **set cam permanent**

Ces deux commandes ont le même effet, sauf que les entrées statiques disparaissent au redémarrage et que les entrées permanentes ne font pas.

La seconde solution est d'utiliser CGMP, qui est un protocole propriétaire de Cisco qui fonctionne entre le routeur de multidiffusion et le commutateur. CGMP permet au routeur Cisco de multidiffusion de comprendre les messages IGMP envoyés par des hôtes et informe le commutateur des informations contenues dans le paquet IGMP.

La dernière solution (et la plus efficace) est d'utiliser l'IGMP Snooping. Avec l'IGMP Snooping, le commutateur intercepte les messages IGMP venant de l'hôte lui-même et met à jour sa table MAC en conséquence. Pour prendre en charge l'IGMP Snooping il faut du matériel avancé.

Les configurations CGMP données dans ce document sont pour des commutateurs Catalyst 4000 et 5000 exécutant CatOS (CGMP n'est pas pris en charge sur les commutateurs Catalyst 6000) et les configurations d'IGMP Snooping sont pour des commutateurs Catalyst 5000 et 6000 exécutant CatOS.

La section suivante décrit brièvement une adresse de multidiffusion, explique la fonctionnalité de l'IGMP et fournit des détails supplémentaires sur le CGMP et l'IGMP Snooping.

Adresse de multidiffusion

1. Les adresses IP de multidiffusion sont des adresses de classe D. Par conséquent, toutes les adresses IP entre 224.0.0.0 et 239.255.255.255 sont des adresses IP de multidiffusion. Elles sont également désignées sous le nom de groupe d'adresses de destination (GDA).
2. Pour chaque GDA, il y a une adresse MAC associée. Cette adresse MAC est constituée par 01-00-5e, suivi des 23 derniers bits du GDA traduit en hexadécimal, comme montré ci-dessous.239.20.20.20 correspond à MAC 01-00-5e-14-14-14.239.10.10.10 correspond à MAC 01-00-5e-0a-0a-0a.En conséquence, ce n'est pas un mappage un-à-un, mais un mappage un-à-plusieurs. De ces deux adresses, vous pouvez voir que le premier octet (239) n'est pas utilisé dans l'adresse MAC. Ainsi les adresses de multidiffusion avec les trois mêmes derniers octets, mais un premier octet différent, ont des adresses MAC qui se superposent.
3. Certaines adresse IP de multidiffusion sont réservées pour un usage spécial, comme montré ci-dessous.224.0.0.1 - Tous les hôtes capables de multidiffusion.224.0.0.2 - Tous les routeurs capables de multidiffusion.224.0.0.5 et 224.0.0.6 sont utilisés par Open Shortest Path First (OSPF).

Généralement, les adresses entre 224.0.0.1 et 224.0.0.255 sont réservées et utilisées par divers protocoles (standard ou propriétaires, telle que le Hot Standby Router Protocol (HSRP)). Cisco recommande que vous ne les utilisiez pas pour un GDA dans un réseau de multidiffusion. CGMP et IGMP Snooping ne fonctionnent pas avec cette plage d'adresses réservée.

Protocole de gestion de groupe Internet

IGMP est une norme définie dans RFC1112 pour IGMPv1, dans RFC2236 pour IGMPv2 et dans RFC3376 pour IGMPv3. IGMP spécifie comment un hôte peut s'enregistrer avec un routeur afin de recevoir un trafic de multidiffusion spécifique. La section suivante donne un bref aperçu sur l'IGMP.

IGMPv1

Les messages de l'IGMP Version 1 (IGMPv1) sont transmis dans des datagrammes IP et contiennent les champs suivants :

- Version : 1
- type : Il y a deux types de messages IGMP : la requête d'adhésion et le rapport d'adhésion.
- Somme de contrôle
- GDA

Les rapports d'adhésion sont émis par des hôtes qui veulent recevoir un groupe de multidiffusion spécifique (GDA). Les requêtes d'adhésion sont émises par des routeurs à intervalles réguliers pour vérifier s'il reste un hôte intéressé par le GDA dans ce segment.

Les rapports d'adhésion de l'hôte sont émis s'ils ne sont pas sollicités (quand l'hôte veut recevoir le trafic GDA d'abord) ou en réponse à une requête d'adhésion. Ils sont envoyés avec les champs suivants :

Informations L2

- MAC source : Adresse MAC de l'hôte
- MAC de destination : adresse MAC de destination pour le GDA

Informations L3

- Source IP : adresse IP de l'hôte
- Destination IP : GDA

Paquet IGMP

- Les données IGMP contiennent, en outre, le GDA et quelques autres champs.

Les requêtes d'adhésion de l'hôte sont envoyées par le routeur à l'adresse toute multidiffusion : 224.0.0.1 . Ces requêtes utilisent 0.0.0.0 dans le champ GDA de l'IGMP. Un hôte de chaque groupe doit répondre à cette requête ou le routeur arrête la transmission du trafic pour ce GDA vers ce segment (après trois tentatives). Le routeur garde une entrée de routage de multidiffusion pour chaque source et la lie à une liste d'interfaces sortantes (interface depuis laquelle le rapport IGMP est venu). Après trois tentatives de requête IGMP sans réponse, cette interface est effacé de la liste d'interfaces sortantes pour toutes les entrées liées à ce GDA.

> **Note**: IGMPv1 n'a aucun mécanisme de sortie. Si un hôte ne veut plus recevoir le trafic, il quitte simplement. Si c'est le dernier hôte dans le sous-réseau, le routeur ne reçoit aucune réponse à sa requête et supprime le GDA pour ce sous-réseau.

IGMPv2

Dans l'IGMP Version 2 (IGMPv2), le champ de version a été retiré et le champ de type peut maintenant accepter des valeurs différentes. Les types sont montrés ci-dessous.

- Membership query
- IGMPv1 Membership Report
- Version 2 Membership Report
- Leave Group

Les descriptions des nouvelles caractéristiques les plus importantes ajoutées dans IGMPv2 sont énumérées ci-dessous.

- Message de sortie IGMP : quand un hôte veut sortir d'un groupe, il doit envoyer un message de sortie du groupe IGMP à l'adresse de destination 224.0.0.2 (au lieu de sortir silencieusement comme dans IGMPv1).
- Un routeur peut maintenant envoyer une requête spécifique au groupe en envoyant une requête d'adhésion au groupe GDA au lieu de l'envoyer à 0.0.0.0.

IGMPv3

Dans l'IGMP Version 3 (ICMPv3), il y a un champ de type qui peut avoir les valeurs suivantes :

- Membership query
- Version 3 Membership Report

Une mise en œuvre d'IGMPv3 *doit également prendre en charge les trois types de message suivants pour l'interopérabilité avec les versions précédentes d'IGMP :*

- Version 1 Membership Report [RFC1112]
- Version 2 Membership Report [RFC2236]
- Version 2 Leave Group [RFC2236]

IGMPv3 ajoute la prise en charge du filtrage de source, c'est-à-dire la capacité pour un système de rapporter l'intérêt dans la réception de paquets depuis des adresses sources spécifiques ou depuis **toutes, sauf des adresses sources spécifiques envoyées à une adresse de multidiffusion spécifique.** Cette fonctionnalité s'appelle également Source Specific Multicast (SSM).

Pour qu'un ordinateur prenne en charge le SSM, il doit prendre en charge l'IGMPv3. Relativement peu de systèmes d'exploitation, cependant, prennent en charge l'IGMPv3. Windows XP prend en charge l'IGMPv3, et il y a des corrections de prise en charge d'IGMPv3 disponibles pour FreeBSD et Linux.

Les administrateurs doivent distinguer la prise en charge d'IGMPv3 au niveau du routeur et l'IGMPv3 Snooping au niveau du commutateur. Ce sont deux fonctionnalités différentes.

Prise en charge d'IGMPv3 sur les commutateurs Catalyst (L2)

- Le Catalyst 6000 exécutant le logiciel en mode hybride (CatOS sur Superviseur et le logiciel Cisco IOS® sur MSFC) prend officiellement en charge l'IGMPv3 Snooping à partir de la version 7.5(1).
- Dans les versions antérieures à la 7.5(1), le commutateur Catalyst 6000 ne prenait pas officiellement en charge l'IGMPv3, mais il devait normalement pouvoir gérer des paquets IGMPv3.
- Le Catalyst 6000 exécutant le logiciel IOS intégré prend en charge l'IGMPv3 au niveau du routeur (interface L3) à partir de la version 12.1(8a)E.
- Le Catalyst 4000 prend en charge l'IGMPv3 seulement au niveau du routeur sur Supervisor III et IV. Il ne prend pas en charge l'IGMPv3 Snooping.

Prise en charge d'IGMPv3 sur les routeurs Cisco (L3)

IGMPv3 est pris en charge sur toutes les plates-formes exécutant le logiciel Cisco IOS® Version 12.1(5)T et ultérieures.

Cavates

Quand un commutateur exécute l'IGMP Snooping, il intercepte des paquets IGMP et remplit la table de transmission de la couche statique 2 (L2) en fonction du contenu des paquets interceptés. Quand il y a des hôtes IGMPv1 ou v2 sur le réseau, le commutateur lit les messages d'arrivée ou de sortie de l'IGMP pour déterminer quels hôtes veulent recevoir quel flux multidiffusion ou arrêter de recevoir le flux multidiffusion.

L'IGMPv3 est plus compliqué, parce qu'il utilise non seulement l'adresse de groupe (adresse de multidiffusion), mais également les sources depuis lesquelles le trafic est prévu. À part le

commutateur Catalyst 6000 exécutant CatOS 7.5 ou ultérieur et Native IOS Version 12.1(8a)E ou ultérieure, aucun autre commutateur ne peut actuellement surveiller efficacement ces paquets et élaborer une table de transmission basée sur ces informations. Par conséquent, l'IGMP Snooping devrait être arrêté quand il y a un hôte IGMPv3 sur le commutateur. Quand l'IGMP Snooping est arrêté, le commutateur ne peut pas élaborer dynamiquement une table de transmission L2 pour les flux multidiffusion. En d'autres termes, le commutateur sature les flux multidiffusion.

Quand l'IGMP Snooping est désactivé, une solution est de configurer manuellement les entrées dynamiques de multidiffusion de la Mémoire adressable par contenu (CAM) afin d'éviter de saturer le sous-réseau avec le trafic de multidiffusion. Toutefois, c'est une charge d'administration et ce n'est pas une solution dynamique. Quand un client ne veut plus recevoir le trafic, l'entrée CAM n'est pas supprimée du commutateur (sauf intervention manuelle), ainsi le trafic sur le réseau est toujours adressé à l'hôte.

En outre, lors de l'utilisation d'IGMPv3 dans le réseau, les commutateurs utilisant le CGMP fonctionnent normalement, si ce n'est que CGMP Fastleave ne fonctionne pas. Si CGMP Fastleave est nécessaire, il est préférable de retourner à l'IGMPv2.

Les mises en garde exceptionnelles spécifiques aux plate-formes se trouvent dans les notes de publication pour les commutateurs correspondants.

Interopérabilité entre IGMPv1 et IGMPv2

Avec IGMPv1 et IGMPv2, seul un routeur par sous-réseau IP envoie des requêtes. Ce routeur est appelé le routeur de requête. Dans IGMPv1, le routeur de requête est choisi avec l'aide du protocole de routage de multidiffusion. Dans IGMPv2, il est choisi par la plus basse adresse IP parmi les routeurs. Voici plusieurs possibilités :

Scénario 1 : Routeur IGMPv1 avec un mélange d'hôtes IGMPv1 et IGMPv2

Le routeur ne comprend pas le rapport IGMPv2, et ainsi, tous les serveurs doivent seulement utiliser le rapport IGMPv1.

Scénario 2 : Routeur IGMPv2 avec un mélange d'hôtes IGMPv2 et IGMPv3

Les hôtes IGMPv1 ne comprennent pas la requête IGMPv2 ou la requête d'adhésion au groupe IGMPv2. Le routeur doit seulement utiliser IGMPv1 et suspend l'opération de sortie.

Scénario 3 : Routeur IGMPv1 et routeur IGMPv2 situés sur le même segment

Le routeur IGMPv1 n'a aucun moyen de détecter le routeur IGMPv2. Par conséquent, le routeur IGMPv2 router doit être configuré par l'administrateur comme routeur IGMPv1. En tous cas, il est possible qu'ils ne soient pas d'accord sur le routeur de requête.

Interopérabilité entre IGMPv1/IGMPv2 et IGMPv3

Avec toutes les versions d'IGMP, seul un routeur par sous-réseau IP envoie des requêtes. Ce routeur est appelé le routeur de requête. Dans IGMPv1, le routeur de requête est choisi avec l'aide du protocole de routage de multidiffusion. Dans IGMPv2 et IGMPv3, il est choisi par la plus basse adresse IP parmi les routeurs. Voici plusieurs options d'interopérabilité.

Scénario 1 : Routeur IGMPv1/IGMPv2 avec un mélange d'hôtes IGMPv1/IGMPv2 et IGMPv3

Comme le routeur ne comprend pas les rapports IGMPv3, tous les hôtes utilisent les rapports d'IGMPv1/IGMPv2.

Scénario 2 : Routeur IGMPv3 avec un mélange d'hôtes IGMPv1/IGMPv2 et IGMPv3

Les hôtes IGMPv1/IGMPv2 ne comprennent pas la requête IGMPv3 ou la requête d'adhésion IGMPv3. Le routeur doit seulement utiliser la version d'IGMP qui correspond à la version du client IGMP présente la plus basse. S'il y a des clients IGMPv3 et d'IGMPv2, le routeur utilise IGMPv2. S'il y a des clients IGMPv1, IGMPv2 et IGMPv3, le routeur utilise l'IGMPv1.

Scénario 3 : Différentes versions de routeurs sur le même segment

Quand des routeurs de différentes versions sont présents sur le même segment, les routeurs ayant une version plus basse n'ont aucun moyen de détecter les routeurs ayant une version plus haute. Par conséquent, les différents routeurs doivent être configurés par l'administrateur pour la même version. Cette version doit correspondre à la version la plus basse de n'importe quel routeur présent envoyant des requêtes.

IGMP sur un routeur

Si, par défaut, il n'y a aucun utilisateur enregistré pour un groupe spécifique dans un sous-réseau, le routeur ne transmet pas le trafic de multidiffusion pour ce groupe dans ce sous-réseau. Cela signifie qu'un routeur a besoin de recevoir un rapport IGMP pour un GDA afin de l'ajouter à la table de routage de multidiffusion et de commencer à transmettre le trafic pour ce groupe.

Sur un routeur, vous devez exécuter les actions suivantes :

1. Activez le routage de multidiffusion dans le mode global, comme montré ci-dessous.

   ```
   ip multicast-routing
   ```

2. Configurez un protocole de routage de multidiffusion sur l'interface concernée, comme montré ci-dessous.

   ```
   ip pim dense-mode
   ```

3. Surveillez l'IGMP, comme montré ci-dessous.

   ```
   show ip igmp interface
   show ip igmp group
   show ip mroute
   ```

4. Configurez un routeur pour envoyer le rapport IGMP (sur l'interface), comme montré ci-dessous.

   ```
   ip igmp join-group [GDA_ip_address]
   ip igmp version [1 | 2 | 3]
   ```

Exemple pratique sur un routeur

Un routeur est configuré pour router entre deux sous-interfaces, Fast Ethernet 0.2 et Fast Ethernet 0.3. Les deux interfaces sont également configurées pour exécuter IGMP. Dans la sortie ci-dessous, vous pouvez voir la version d'IGMP, le groupe joint, etc.

Configuration

```
ip multicast-routing


interface FastEthernet0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
```

show ip igmp interface

```
 Fa0.2 is up, line protocol is up
 Internet address is 10.2.2.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
 IGMP activity: 3 joins, 2 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.2.2.1 (this system)
 IGMP querying router is 10.2.2.1 (this system)
 Multicast groups joined: 224.0.1.40

 Fa0.3 is up, line protocol is up
 Internet address is 10.3.3.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
```

```
IGMP activity: 1 joins, 1 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 10.3.3.1 (this system)
IGMP querying router is 10.3.3.1 (this system)
No multicast groups joined
```

show ip mroute and show ip igmp group

```
Router_A#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode


(*, 239.10.10.10), 00:01:15/00:02:59, RP 0.0.0.0, flags: DJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:01:16/00:00:00

(10.2.2.2, 239.10.10.10), 00:00:39/00:02:20, flags: CT
  Incoming interface: FastEthernet0.2, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:00:39/00:00:00

Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

Cisco Group Management Protocol

Pour la prise en charge de CGMP sur des commutateurs Catalyst, référez-vous au Tableau de prise en charge des commutateurs de multidiffusion Catalyst.

Trames CGMP et types de message

Le CGMP a été mis en œuvre la première fois par Cisco pour retenir le trafic de multidiffusion dans un réseau L2. Puisqu'un commutateur, par nature, n'est pas capable de regarder des paquets L3, il ne peut pas distinguer un paquet IGMP. Avec le CGMP, le routeur fournit l'interface entre les hôtes. Les routeurs « parlent » IGMP et les commutateurs « parlent » CGMP.

Les trames CGMP sont des trames Ethernet avec l'adresse de destination MAC 01-00-0c-dd-dd-dd et avec un en-tête de protocole d'accès au sous-réseau (SNAP) ayant la valeur 0x2001. Les trames CGMP contiennent les champs suivants :

- Version : 1 ou 2.
- Message Type : Joindre ou quitter.
- Nombre : Le nombre de paires d'adresses de multidiffusion/monodiffusion dans le message.
- GDA : l'adresse MAC 48 bits du groupe de multidiffusion.
- Unicast Source Address (USA) : L'adresse MAC 48 bits de monodiffusion des périphériques

qui veulent joindre le GDA.

Note: La valeur du champ Count détermine combien de fois les deux derniers champs s'affichent.

Par défaut, les processeurs d'un commutateur (appelé NMP dans Catalyst) écoutent uniquement les adresses de multidiffusion lorsque **show cam system** est exécutée. Lorsque vous activez CGMP sur un commutateur, l'adresse 01-00-0c-dd-dd-dd est ajoutée au **show cam system** sortie de commande.

Le tableau ci-dessous donne la liste de tous les messages CGMP possibles.

GDA	ÉTATS-UNIS	Join/Leave	Signification
Mcast MAC	Client MAC	Rejoindre	Ajouter un port au groupe.
Mcast MAC	Client MAC	Congé	Supprimer un port du groupe.
00-00-00-00-00-00	Router MAC	Rejoindre	Affecter un port du routeur.
00-00-00-00-00-00	Router MAC	Congé	Retirer l'affectation d'un port du routeur.
Mcast MAC	00-00-00-00-00-00	Congé	Supprimer un groupe.
00-00-00-00-00-00	00-00-00-00-00-00	Congé	Supprimer tous les groupes.

Apprendre des ports de routeur

Le commutateur doit être au courant de tous les ports du routeur de sorte qu'ils soient automatiquement ajoutés à toute entrée de multidiffusion de création récente. Le commutateur apprend les ports du routeur quand il reçoit un message CGMP Join to GDA 00-00-00-00-00-00 avec l'adresse MAC USA (troisième type de message dans le tableau). Ces messages sont produits par le routeur sur toutes les interfaces configurées pour exécuter CGMP. Il y a également une méthode statique, cependant, pour configurer des ports du routeur sur le commutateur.

Joindre un groupe avec CGMP

- Un nouveau client demande à recevoir du trafic pour un GDA, ainsi un client envoie un rapport d'adhésion IGMP.
- Le routeur reçoit le rapport IGMP, le traite, et envoie un message CGMP au commutateur. Le

routeur copie l'adresse de destination MAC dans le champ GDA du message CGMP Join, et copie l'adresse MAC source dans l'USA du CGMP Join. Il le renvoie alors au commutateur.
- Un commutateur avec CGMP activé a besoin d'écouter les adresses CGMP 01-00-0c-dd-dd-dd. Le processeur du commutateur regarde dans la table CAM pour l'USA. Une fois que l'USA est vu dans la table CAM, le commutateur sait sur quel port l'USA est localisé, et fait l'une des choses suivantes :Crée une nouvelle entrée statique pour le GDA et lie le port USA à celle-ci avec tous les ports du routeur.Ajoute le port USA à la liste des ports pour ce GDA (si l'entrée statique existe déjà).

Sortir d'un groupe avec CGMP

Les entrées statiques apprises avec CGMP sont permanentes, à moins qu'une modification de la topologie de spanning tree se produise dans le VLAN ou que le routeur envoie l'un des derniers messages CGMP Leave dans la table précédente.

Quand l'IGMPv1 est l'hôte, n'envoyez pas de messages IGMP Leave. Le routeur envoie seulement des messages Leave s'il ne reçoit pas de réponse à trois requêtes IGMP consécutives. Ceci signifie qu'aucun port n'est supprimé d'un groupe si des utilisateurs sont toujours intéressés dans ce groupe.

Avec l'introduction d'IGMPv2 et la présence d'IGMP Leave, Cisco a enrichi la spécification CGMP d'origine (CGMPv2). Cet ajout s'appelle CGMP Fast-Leave.

Le traitement CGMP Fast-Leave permet au commutateur de détecter des messages IGMPv2 Leave envoyés à l'adresse de multidiffusion tout routeur (224.0.0.2) par des hôtes sur l'un des ports de module du supervisor engine. Quand le module du supervisor engine reçoit un message Leave, il déclenche un temporisateur de requête-réponse et envoie un message sur le port sur lequel ce message de sortie a été reçu pour déterminer s'il reste un hôte disposé à recevoir ce groupe de multidiffusion sur ce port. Si ce temporisateur expire avant qu'un message CGMP Join soit reçu, le port est élagué depuis l'arbre de multidiffusion pour le groupe de multidiffusion spécifié dans le message de sortie. Si c'est le dernier port dans le groupe de multidiffusion, il transmet le message IGMP Leave à tous les ports du routeur. Le routeur commence ensuite le processus de suppression normal en envoyant une requête spécifique au groupe. Comme aucune réponse n'est reçue, le routeur supprime ce groupe de la table de routage de multidiffusion pour cette interface. Il envoie également un message CGMP Leave au commutateur qui efface le groupe de la table statique. Le traitement Fast-Leave assure la gestion optimale de la bande passante pour tous les hôtes sur un réseau commuté, même lorsque des groupes de multidiffusion multiples sont en service simultanément.

Lorsque CGMP Leave est activé, deux entrées sont ajoutées à **show cam system** , comme indiqué ci-dessous.

```
01-00-5e-00-00-01
01-00-5e-00-00-02
```

IGMP Leave utilise 224.0.0.2 et la requête IGMP utilise 224.0.0.1.

Suivez les étapes suivantes pour dépanner CGMP :

1. En raison d'un conflit avec le HSRP, le traitement CGMP Leave est désactivé par défaut. HSRP utilise l'adresse MAC 01-00-5e-00-00-02, qui la même qu'IGMP Leave avec l'IGMP

Version 2. Avec CGMP Fast-Leave, tous les paquets HSRP vont vers le CPU du commutateur. Puisqu'un message HSRP n'est pas un paquet IGMP, le commutateur régénère tous les messages de ce type et les envoie à tous les ports du routeur. Les routeurs recevant `hsrp hello ou hsrp peers perdent la connectivité.` Par conséquent, dans le débogage de HSRP, essayez de désactiver CGMP Fast-Leave.Pour activer le traitement CGMP Leave, émettez la commande **set cgmp leave enable** erasecat4000_flash:.

2. Quand le traitement CGMP Leave est activé, le commutateur de la gamme Catalyst 5000 apprend les ports du routeur via PIM-v1, HSRP et des messages CGMP Self-Join. Quand le traitement CGMP Leave est désactivé, le commutateur de la gamme Catalyst 5000 apprend les ports du routeur via des messages CGMP Self-Join.
3. Le CGMP n'élague pas le trafic de multidiffusion pour toute adresse de multidiffusion IP qui mappe dans cette plage d'adresses MAC comprise entre 01-00-5E-00-00-00 et 01-00-5E-00-00-FF. Les adresses de multidiffusion IP réservées, dans la plage 224.0.0.0 à 224.0.0.255, sont utilisées pour transmettre le trafic de multidiffusion IP local en un seul saut L3.

CGMP et réseau uniquement source

Un réseau uniquement source est un segment avec seulement une source multidiffusion et aucun client réel. Par conséquent, il y a une chance qu'aucun rapport IGMP ne soit produit dans ce segment. Cependant, le CGMP a toujours besoin de restreindre la saturation de cette source (pour l'usage d'un routeur seulement). Si un routeur détecte le trafic de multidiffusion sur une interface sans rapport IGMP, il est identifié comme réseau uniquement source de multidiffusion. Le routeur produit un message CGMP Join pour lui-même et le commutateur ajoute simplement ce groupe (avec seulement le port du routeur).

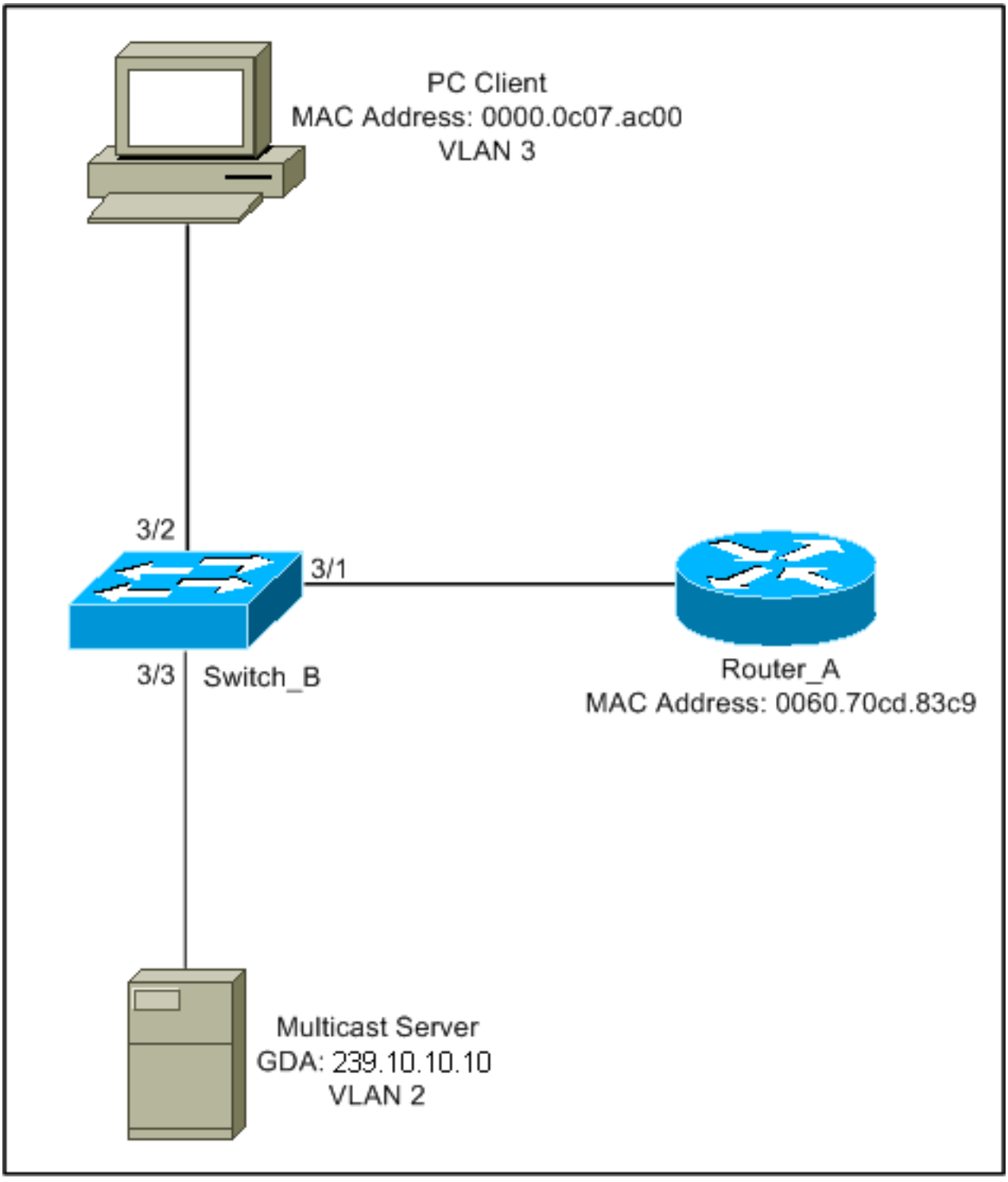
Configurer des routeurs Cisco et des commutateurs pour activer CGMP

Les commandes ci-dessous ne sont valides que pour les gammes Catalyst 4000 et 5000 (plus 2901, 2902, 2926, 2948G et 4912).

- Routeur de multidiffusionActivez la multidiffusion IP (commande globale) :**ip multicast-routing**Activez chaque interface exécutant CGMP (mode interface) avec les commandes suivantes :**ip pimip igmpip cgmp**Déboguez le problème de multidiffusion L2 avec les commandes suivantes :**debug ip igmpdebug ip cgmp**
- Gamme Catalyst 4000 ou 5000Activez/Désactivez le CGMP avec les commandes suivantes :**set cgmp**Activez/Désactivez CGMP Fast-Leave avec les commandes suivantes :**set cgmp leave**Configurez le routeur de multidiffusion (statique) avec les commandes suivantes :**set multicast router**Effacez le routeur de multidiffusion avec les commandes suivantes :**clear multicast router**Diverses commandes permettant de vérifier le fonctionnement de CGMP figurent ci-dessous.**show cam staticshow cgmp statisticshow cgmp leaveshow multicast routershow multicast groupshow multicast group cgmpshow multicast group count**

Exemple pratique d'utilisation de CGMP et commande et sortie de débogage

Voici un exemple pratique de configuration pour un routeur Cisco et des commutateurs Catalyst.



Cette configuration montre les opérations impliquées quand un hôte joint un groupe. Cette configuration montre également les opérations quand un hôte sort d'un groupe avec Fast-Leave activé. Un suivi de renifleur et la configuration du commutateur et du routeur sont également fournis.

Joindre un groupe avec CGMP

Référez-vous à ces étapes lorsque vois joignez un groupe avec CGMP.

1. Activez CGMP sur le commutateur, comme montré ci-dessous.

```
Switch_B (enable) set cgmp en
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
```

```
MCAST-CGMP: Set CGMP Sys Entrie
CGMP support for IP multicast enabled.
Switch_B (enable)
```

Comme vous pouvez le voir ci-dessous, l'entrée 01-00-0c-dd-dd-dd est incluse pour tous les VLAN dans le **show cam system** sortie de commande. En outre, le réseau exécutant CGMP Fast-Leave, vous pouvez voir les entrées pour 01-00-5e-00-00-01 et 01-00-5e-00-00-02.

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam system
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  ------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-80-c2-00-00-00  #          1/9
3     01-80-c2-00-00-01  #          1/9
Total Matching CAM Entries Displayed = 19
```

2. Le routeur envoie un message CGMP Join à GDA 00-00-00-00-00-00 avec l'adresse MAC USA du routeur. Par conséquent, le port du routeur est ajouté à la liste des ports du routeur (voir le premier exemple ci-dessous).**Sur le routeur**

```
6d01h: CGMP: Sending self Join on Fa0.3
6d01h:       GDA 0000.0000.0000, USA 0060.70cd.83c9
```

Sur le commutateur

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 00-00-00-00-00-00 MCAST-CGMP-JOIN:USA
                 00-60-70-cd-83-c9
MCAST-ROUTER: Adding QUERIER port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2

Switch_B (enable) show multi router
CGMP enabled
IGMP disabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
```

3. Le PC sur 3/1 envoie à l'IGMP un rapport contenant le GDA : 239.10.10.10 (voir trame 2 ci-dessous). La figure ci-dessous représente le **show ip igmp group** sortie de la commande sur le routeur Router_A.Ceci montre que le routeur transmet maintenant le trafic pour 224.10.10.10 à fa0.3. C'est une conséquence de la réception du rapport IGMP depuis 10.3.3.2, qui est le PC client.

```
Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

4. Le routeur reçoit le rapport et envoie un message CGMP Join avec les informations suivantes :MAC source : adresse MAC du routeurDest MAC : 01-00-cc-dd-dd-ddContenu: adresse MAC du PC client (USA) : adresse MAC 00-00-0c-07-ac-00 du groupe de multidiffusion : 01-00-5e-0a-0a-0a (voir trame 3 ci-dessous)**Sur le routeur**

```
6d01h: IGMP: Received v2 Report from 10.3.3.2 (Fa0.3) for 239.10.10.10
6d01h: CGMP: Received IGMP Report on Fa0.3
6d01h:       from 10.3.3.2 for 239.10.10.10
6d01h: CGMP: Sending Join on Fa0.3
```

5. Commutateur avec 01-00-cc-dd-dd-dd dans la **show cam system** CGMP est activé dans la sortie de commande. Le commutateur peut traiter le paquet.Le commutateur fait une recherche dans la table CAM dynamique pour déterminer sur quel port l'adresse MAC du PC client est localisée. L'adresse est localisée sur le port 3/2 et le commutateur fait une entrée statique dans la table CAM pour 01-00-5e-0a-0a-0a liée au port 3/2. Le commutateur ajoute également le port du routeur 3/1 à l'entrée statique pour ce GDA.**Sur le commutateur**

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 3
MCAST-CGMP-JOIN: join GDA 01-00-5e-0a-0a-0a MCAST-CGMP-JOIN:USA 00-60-5c-f4-bd-e2
MCAST-CGMP-JOIN: 3/2/3: index 81
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 01-00-5e-00-01-28 MCAST-CGMP-JOIN:USA 00-60-70-cd-83-c9
MCAST-CGMP-JOIN: 3/1/2: index 80
```

6. Tout trafic ultérieur pour le groupe de multidiffusion 239.10.10.10 est expédié seulement à ce port dans ce VLAN. Voici ci-dessous l'entrée statique dans le commutateur Catalyst dans lequel 3/1 est le port du routeur et 3/2 est port du client.

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
3     01-00-5e-0a-0a-0a             3/1-2
Total Matching CAM Entries Displayed = 3
Switch_B (enable)
```

Sortir d'un groupe avec CGMP Fast-Leave activé

L'exemple ci-dessous requiert que le client soit un client d'IGMP Version 2 et que Fast-Leave soit activé sur le commutateur.

1. La procédure suivante active CGMP Fast-Leave. Regardez la **show cgmp leave** pour déterminer si elle est activée. Regardez également la **show cam system** sortie de commande pour déterminer si le commutateur écoute 01-00-5e-00-00-01 et 01-00-5e-00-00-02 (adresses utilisées pour la sortie).

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-02  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-00-5e-00-00-01  #          1/9
3     01-00-5e-00-00-02  #          1/9
3     01-80-c2-00-00-00  #          1/9
Do you wish to continue y/n [n]?  y
Total Matching CAM Entries Displayed = 22
```

2. Le client envoie un message IMPG Leave à 224.0.0.2. Le commutateur l'intercepte et envoie une requête IGMP sur le port sur lequel il reçoit le message de sortie. Voici ce qui suit : **debug** sortie sur le commutateur :

```
MCAST-IGMP-LEAVE:Recvd leave on port 3/2 vlanNo 3
MCAST-IGMP-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-IGMP-LEAVE:deletion_timer = 1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
```

3. Puisqu'aucune réponse n'était reçue, le Catalyst transmet le message IGMP Leave au routeur, comme montré ci-dessous.

```
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1 vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1 vlanNo 3
```

4. Le routeur reçoit un message IGMP Leave, ainsi il envoie un message CGMP Leave au

commutateur et supprime également le groupe de sa liste de groupe IGMP. Ci-dessous se trouve le **debug** du routeur.**Sur le routeur**

```
IGMP: Received Leave from 10.200.8.108 (Fa0.3) for 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
CGMP: Sending Leave on Fa0.3
      GDA 0100.5e0a.0a0a, USA 0000.0000.0000
IGMP: Deleting 239.10.10.10 on Fa0.3
```

Suivi CGMP et configuration

Trame 1

La trame 1 est une trame CGMP Join au GDA 00-00-00-00-00-00. Elle est utilisée pour ajouter le port du routeur à la liste des ports de routeur.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
!--- Send to the CGMP !--- macaddress present in show cam sys !--- command output.

     ETHER: Source      = Station Cisco11411E1
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
```

```
     CGMP:
     CGMP:    GDA    =0000.0000.0000
     CGMP:    USA    =0000.0C14.11E1
!--- MAC address of the router. CGMP:
```

Le résultat de la trame 1 est sur le commutateur, avec 3/1 étant le port qui est connecté au routeur :

Trame 2

La trame 2 est un rapport d'adhésion IGMP envoyé par l'hôte pour demander (ou confirmer) que les utilisateurs veulent recevoir le trafic pour le groupe 239.10.10.10.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 195
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01005E0A0A0A
!--- Destination is the GDA MAC. ETHER: Source = Station Cisco176DCCA !--- Sourced by the PC
connected in 3/1. ETHER: Ethertype = 0800 (IP) ETHER: IP: ----- IP Header ----- IP: IP: Version
= 4, header length = 20 bytes IP: Type of service = C0 IP: 110. .... = internetwork control IP:
...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal reliability
IP: Total length = 28 bytes IP: Identification = 0 IP: Flags = 0X IP: .0.. .... = may fragment
IP: ..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to live = 1 seconds/hops
IP: Protocol = 2 (IGMP) IP: Header checksum = CC09 (correct) IP: Source address = [10.1.1.2] IP:
Destination address = [224.10.10.10] IP: No options IP: IGMP: ----- IGMP header ----- IGMP:
IGMP: Version = 1 IGMP: Type = 6 (Ver2 Membership Report) IGMP: Unused = 0x00 IGMP: Checksum =
FFEA (correct) IGMP: Group Address = [224.10.10.10] IGMP:
```

Trame 3

La trame 3 est la trame CGMP envoyée par le routeur au commutateur pour dire au commutateur d'ajouter une entrée statique pour 01-00-5e-0a-0a-0a.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 193
     ISL: Reserved
     ISL:
```

```
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
     ETHER: Source      = Station Cisco11411E1
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0100.5E0A.0A0A
!--- GDA MAC added in show cam static !--- command output.

     CGMP:    USA    =0000.0C76.DCCA
!--- MAC of the PC in 3/1. CGMP:
```

Voici ci-dessous la configuration du routeur et du commutateur.

```
 Router_A (router) Configuration:

 Router_A#write terminal
 Building configuration...

 Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router_A
 !
 !
 ip subnet-zero
 ip multicast-routing
 ip dvmrp route-limit 20000


 interface FastEthernet0
  no ip address
  no ip directed-broadcast
 !
 interface FastEthernet0.1
  encapsulation isl 1
  ip address 10.1.1.1 255.255.255.0
  no ip redirects
  no ip directed-broadcast
```

```
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
```

Switch_B configuration for CGMP:

```
#cgmp
set cgmp enable
set cgmp leave enable
!
```

CGMP statistics for VLAN 3:

```
Switch_B (enable) show cgmp sta 3
CGMP enabled

CGMP statistics for vlan 3:
valid rx pkts received           109
invalid rx pkts received         0
valid cgmp joins received        108
valid cgmp leaves received       1
valid igmp leaves received       1
valid igmp queries received      63
igmp gs queries transmitted      1
igmp leaves transmitted          1
failures to add GDA to EARL      0
topology notifications received  0
Switch_B (enable)
```

IGMP Snooping

L'IGMP Snooping est une autre fonctionnalité qui vous permet de saisir directement des trames IGMP. Pour la prise en charge de l'IGMP Snooping sur des commutateurs Catalyst, référez-vous au Tableau de prise en charge des commutateurs de multidiffusion Catalyst.

Aperçu d'IGMP Snooping

L'IGMP Snooping, comme l'indique son nom, est une fonctionnalité qui permet au commutateur « d'écouter » la conversation sur l'IGMP entre les hôtes et les routeurs. Quand un commutateur entend un rapport IGMP venant d'un hôte pour un groupe de multidiffusion donné, le commutateur ajoute le numéro de port de l'hôte à la liste GDA pour ce groupe. Et quand le commutateur entend un message IGMP Leave, il retire le port de l'hôte de l'entrée de la table CAM.

Apprendre le port du routeur

Le commutateur écoute les messages suivants afin de détecter des ports du routeur avec l'IGMP Snooping :

- IGMP Membership query send to 01-00-5e-00-00-01
- PIMv1 hello send to 01-00-5e-00-00-02
- PIMv2 hello send to 01-00-5e-00-00-0d
- DVMRP probes send to 01-00-5e-00-04
- MOSPF message send to 01-00-5e-00-05 or 06

En activant la surveillance IGMP sur un commutateur, toutes les entrées MAC ci-dessus sont ajoutées au **show cam system** sortie de commande du commutateur de surveillance. Une fois qu'un port du routeur est détecté, il est ajouté à la liste des ports de tout les GDA dans ce VLAN.

Joindre un groupe avec l'IGMP Snooping

Ci-dessous, deux scénarios de jonction :

Scénario A : L'hôte A est le premier hôte à rejoindre un groupe dans le segment.

1. L'hôte A envoie un rapport d'adhésion IGMP non sollicité.
2. Le commutateur intercepte le rapport d'adhésion IGMP qui a été envoyé par l'hôte qui a voulu rejoindre le groupe.
3. Le commutateur crée une entrée de multidiffusion pour ce groupe et la lie au port sur lequel il a reçu le rapport et à tous les ports du routeur.
4. Le commutateur transmet le rapport IGMP à tous les ports du routeur. C'est ainsi que le routeur reçoit le rapport IGMP et met à jour sa table de routage de multidiffusion en conséquence.

Scénario B : L'hôte B est maintenant le second à rejoindre le même groupe.

1. L'hôte B envoie un rapport d'adhésion IGMP non sollicité.
2. Le commutateur intercepte le rapport d'adhésion IGMP qui a été envoyé par l'hôte qui veut rejoindre le groupe.
3. Le commutateur ne transmet pas nécessairement le rapport IGMP à tous les ports du routeur. En fait, le commutateur transmet les rapports IGMP aux ports du routeur utilisant la création de rapports de proxy, et transmet seulement un rapport par groupe dans un laps de temps de 10 s.

   Note: afin de maintenir l'adhésion à un groupe, le routeur de multidiffusion envoie une requête IGMP toutes les 60 secondes. Cette requête est interceptée par le commutateur et transmise à tous les ports sur le commutateur. Tous les hôtes qui sont des membres du groupe répondent à cette requête. Mais, compte tenu du fait que le commutateur intercepte aussi la réponse, l'autre hôte ne voit aucun des autres rapports, et ainsi, tous les hôtes envoient un rapport (au lieu d'un par groupe). Le commutateur utilise ensuite aussi la création de rapport de proxy pour transmettre un seul rapport par groupe parmi toutes les réponses reçues.

Supposez que l'hôte veule sortir d'un groupe, mais que l'hôte B veule toujours recevoir le groupe.

- Le commutateur saisit le message IGMP Leave venant de l'hôte A.
- Le commutateur émet un requête IGMP spécifique au groupe sur ce port (et seulement sur ce port).
- Si le commutateur ne reçoit pas un rapport, il rejette ce port de l'entrée. S'il reçoit une réponse de ce port, il ne fait rien et rejette le message de sortie.
- L'hôte B est toujours intéressé par ce groupe sur ce commutateur. Ce ne serait pas le dernier port non routeur dans l'entrée. Par conséquent, le commutateur ne transmet pas le message de sortie.

Maintenant, supposez que l'hôte B veule sortir du groupe et qu'il est le dernier utilisateur intéressé par ce groupe dans ce segment.

- Le commutateur saisit le message IGMP Leave venant de l'hôte A.
- Le commutateur émet un requête IGMP spécifique à ce groupe sur ce port.
- Si le commutateur ne reçoit pas un rapport, il rejette ce port de l'entrée.
- C'est le dernier port non routeur pour ce GDA. Le commutateur transmet le message IGMP Leave à tous les ports du routeur et retire l'entrée de sa table.

Interaction IGMP/CGMP

Dans certains réseaux, en raison de limitations matérielles, il se peut que vous ne pouviez pas exécuter l'IGMP Snooping sur tous les commutateurs. Dans ce cas, vous pourriez avoir besoin d'exécuter CGMP sur certains commutateurs dans le même réseau.

Notez que c'est un cas particulier. Le commutateur exécutant l'IGMP Snooping détecte des messages CGMP et détecte que certains commutateurs dans le réseau exécutent CGMP. Par conséquent, il passe dans un mode IGMP-CGMP spécial et désactive la création de rapport de proxy. C'est absolument nécessaire pour le bon fonctionnement de CGMP, parce que les routeurs utilisent l'adresse MAC source du rapport IGMP afin de créer un CGMP Join. Les routeurs exécutant CGMP ont besoin de voir tous les rapports IGMP, la création de rapport de proxy doit donc être désactivée. Tous les rapports envoyés au routeur devraient seulement être ceux qui sont strictement requis pour l'IGMP Snooping.

Réseau Multicast uniquement source

Si le segment contient seulement un serveur de multidiffusion (source de multidiffusion) et aucun client, vous pourriez finir avec une situation dans laquelle vous n'auriez aucun paquet IGMP dans ce segment, mais beaucoup de trafic de multidiffusion. Dans ce cas, le commutateur transmet simplement le trafic venant de ce groupe à tout le monde dans le segment. Heureusement, un commutateur exécutant l'IGMP Snooping peut détecter ces flux multidiffusion et ajoute une entrée de multidiffusion pour ce groupe avec seulement le port du routeur. Ces entrées sont signalées en interne en tant que mcast_source_only et deviennent obsolètes toutes les 5 minutes ou quand le port du routeur part. Notez que même après ce vieillissement, l'adresse est réapprise au bout de quelques secondes si le trafic continue. Au cours de la période de réapprentissage, une saturation momentanée peut se produire dans le VLAN. Pour éviter cela et conserver les entrées, utilisez la **set igmp flooding enable | disable** erasecat4000_flash:. Une fois la saturation désactivée, le commutateur ne vieillit pas les entrées uniquement sources.

Limites

Comme avec CGMP, des GDA qui mappent une adresse MAC qui tombe dans la plage 01-00-5e-

00-00-xx n'est jamais élaguée par l'IGMP Snooping.

Configuration de l'IGMP Snooping sur des commutateurs Cisco

Pour activer/désactiver l'IGMP Snooping, émettez la commande suivante :

- **set igmp**

Pour configurer le routeur de multidiffusion (statique), émettez la commande suivante :

- **set multicast router**
- **clear multicast router *port* | *all*>**

Pour surveiller et contrôler les statistiques IGMP, émettez les commandes suivantes :

- **show igmp statistics**
- **show multicast router**

Exemple pratique d'IGMP Snooping

La configuration pour cet exemple est semblable à celle du test de CGMP, utilisée plus tôt dans ce document. La seule différence est que les ports 3/2 et 3/3 sont tous deux connectés au même VLAN et configurés au niveau du client pour joindre le groupe 224.10.10.10.

L'exemple qui explique plusieurs manipulations, regarde ce que le commutateur fait et examine la sortie en résultant. Dans l'exemple suivant, *Switch_B est un Catalyst 5500 exécutant l'IGMP Snooping et Router_A est le routeur de multidiffusion connecté au port 3/1.*

1. Activez la surveillance IGMP sur le commutateur et consultez le résultat en émettant la commande **debug** erasecat4000_flash:. Notez que chaque jeu d'entrées a été ajouté au **show cam sys** , permettant de détecter le port du routeur via PIM, MOSPF, etc.

```
Switch_B (enable)  set igmp en

MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 1
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 2
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 3

IGMP feature for IP multicast enabled

Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-00-5e-00-00-01  #          1/9
1     01-00-5e-00-00-04  #          1/9
1     01-00-5e-00-00-05  #          1/9
1     01-00-5e-00-00-06  #          1/9
1     01-00-5e-00-00-0d  #          1/9
```

```
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-04  #          1/9
2     01-00-5e-00-00-05  #          1/9
2     01-00-5e-00-00-06  #          1/9
2     01-00-5e-00-00-0d  #          1/9
```

2. Le commutateur reçoit un paquet PIMv2 du routeur Router_A et ajoute le port du routeur.

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 2
MCAST-ROUTER: Adding port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 3
MCAST-ROUTER: Adding port 3/1, vlanNo 3
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 3

Switch_B (enable) show multi router
CGMP disabled
IGMP enabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
Switch_B (enable)
```

3. Connectez un nouvel hôte dans le groupe 224.10.10.10 (sur le port 3/2). Cet hôte envoie un rapport d'adhésion IGMP. Le rapport est reçu, espionné par le commutateur, l'entrée est ajoutée, et le rapport IGMP est transmis au routeur.**Sur Switch_B**

```
MCAST-IGMPQ:recvd an IGMP V2 Report on the port 3/2 vlanNo 3
      GDA 224.10.10.10
MCAST-RELAY:Relaying packet on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 3/1
      vlanNo 3

Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
----  ------------------ ----- -------------------------------------------
3     01-00-5e-0a-0a-0a         3/1-2
```

4. Ajoutez un utilisateur de plus dans le VLAN 3 sur le port 3/3, comme montré ci-dessous.

```
Switch_B (enable) show cam static

  * = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.

  X = Port Security Entry

  VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
  ---- ------------------ ----- -------------------------------------------
```

```
3    01-00-5e-0a-0a-0a         3/1-3
```

5. Retirez le port 3/2. Le port 3/2 envoie un message IGMP Leave ; le commutateur renvoie une requête IGMP spécifique au groupe sur le port 3/2 et démarre un temporisateur. Quand le temporisateur expire sans recevoir une réponse, il supprime le port du groupe.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/2 vlanNo 3 GDA 224.10.10.10
MCAST-IGMPQ-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-DEL-TIMER: Deletion Timer Value set to Random Value  1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer:delete leave timer


Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
---- ------------------ ----- -------------------------------------------
3    01-00-5e-0a-0a-0a         3/1,3/3
```

6. L'hôte sur le port 3/3 sort du groupe et envoie un message IGMP Leave. La seule différence avec le point précédent est que le message IGMP Leave est finalement transmis au port du routeur.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/3 vlanNo 3 GDA 224.10.10.10
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/3 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on
             port 3/3 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/3 vlanNo 3 GDA
             01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1
             vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1
             vlanNo 3
MCAST-TIMER:IGMPLeaveTimer:delete leave timer
```

La configuration du sous-réseau est maintenant de nouveau au début, son état dans l'étape 1. L'entrée de multidiffusion a disparu de **show cam static** sortie de commande.

Pour terminer, consultez un exemple de **show igmp static** , comme indiqué ci-dessous.

```
Switch_B (enable) show igmp stat 2
IGMP enabled

IGMP statistics for vlan 2:
Total valid pkts rcvd:           329
Total invalid pkts recvd         0
General Queries recvd            82
Group Specific Queries recvd     0
MAC-Based General Queries recvd  0
Leaves recvd                     0
Reports recvd                    82
Queries  Xmitted                 0
```

```
GS Queries Xmitted              0
Reports Xmitted                 0
Leaves Xmitted                  0
Failures to add GDA to EARL     0
Topology Notifications rcvd     0

Switch_B (enable) show igmp stat 3
IGMP enabled

IGMP statistics for vlan 3:
Total valid pkts rcvd:          360
Total invalid pkts recvd        0
General Queries recvd           93
Group Specific Queries recvd    6
MAC-Based General Queries recvd 0
Leaves recvd                    11
Reports recvd                   64
Queries  Xmitted                0
GS Queries Xmitted              14
Reports Xmitted                 0
Leaves Xmitted                  10
Failures to add GDA to EARL     0
Topology Notifications rcvd     1
Switch_B (enable)
```

Informations connexes

- Matrice de prise en charge des commutateurs Catalyst de multidiffusion
- Page de support de multidiffusion IP
- Support technologique Cisco
- Assistance produit Cisco
- Support et documentation techniques - Cisco Systems