

Consultez le guide de configuration rapide de la multidiffusion IP

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Mode dense](#)

[Mode clairsemé avec un RP](#)

[Mode clairsemé avec RP multiples](#)

[Auto-RP avec un RP](#)

[Auto-RP avec RP multiples](#)

[DVMRP](#)

[MBGP](#)

[MSDP](#)

[Routage multicast d'extrémité](#)

[IGMP UDLR pour liaisons satellites](#)

[PIMv2 BSR](#)

[CGMP](#)

[IGMP Snooping](#)

[PGM](#)

[MRM](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les bases de la configuration de la multidiffusion pour différents scénarios de mise en réseau.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- Multidiffusion IP (Internet Protocol).

Composants utilisés

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

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

La multidiffusion sur IP est une technologie de préservation de la bande passante qui réduit le trafic parce qu'elle livre simultanément un flux unique d'informations aux milliers de destinataires en entreprise et aux foyers.

Les applications qui profitent de la multidiffusion comprennent la vidéoconférence, les communications d'entreprise, l'enseignement à distance, la distribution de logiciels, les valeurs boursières et les informations.

Mode dense

Cisco recommande que vous utilisez le Protocol Independent Multicast Sparse Mode (PIM-SM), en particulier Auto-RP, si possible, notamment pour de nouveaux déploiements.

Cependant, si le mode dense est souhaité, configurez la commande globale `ip multicast-routing` et la commande d'interface `ip pim sparse-dense-mode` sur chaque interface qui doit traiter le trafic de multidiffusion.

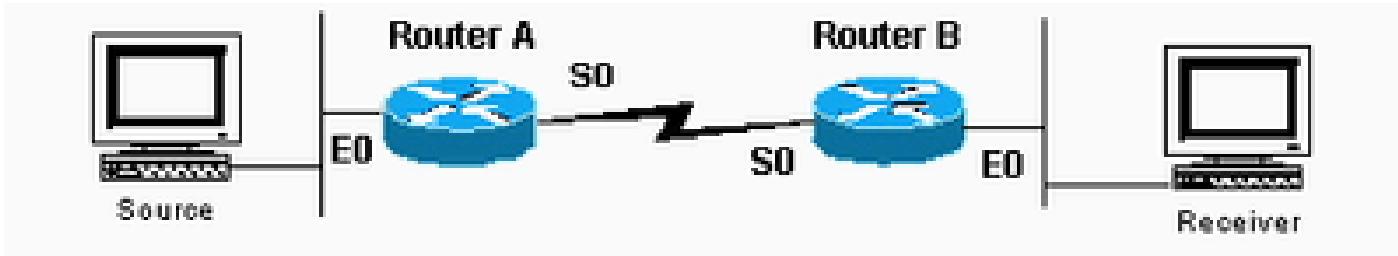
La condition commune, pour toutes les configurations abordées dans ce document, est de configurer la multidiffusion globalement et de configurer PIM sur les interfaces.

Depuis la version 11.1 de Cisco d'IOS®, vous pouvez configurer les commandes d'interface `ip pim dense-mode` et `ip pim sparse-mode` simultanément avec la commande `ip pim sparse-dense-mode`.

Dans ce mode, l'interface est traitée comme mode dense si le groupe est en mode dense. Si le groupe est en mode clairsemé (par exemple, si RP est connu), l'interface est traitée comme mode clairsemé.



Remarque : La « source » dans les exemples tout au long de ce document représente la source du trafic de multidiffusion et le « récepteur » représente le récepteur de trafic de multidiffusion.



L'interface est traitée en mode dense si le groupe est en mode dense

Configuration du routeur A

```

ip multicast-routing
interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode

interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode
  
```

Configuration du routeur B

```

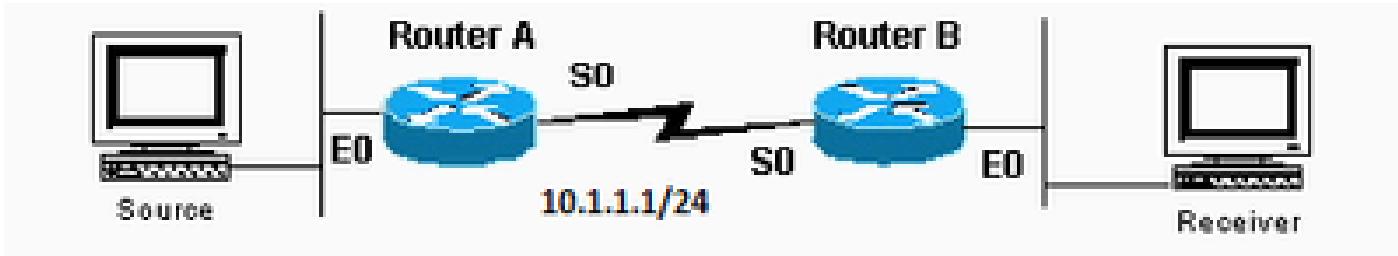
ip multicast-routing
interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode

interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
  
```

Mode clairsemé avec un RP

Dans cet exemple, le routeur A est le RP qui est généralement le routeur le plus proche de la source. La configuration RP statique nécessite que tous les routeurs dans le domaine PIM aient les mêmes commandes `p pim rp-address` configurées.

Vous pouvez configurer de multiples RP, mais il peut seulement y avoir un RP par groupe spécifique.



Il peut y avoir plusieurs RP, mais un seul RP par groupe spécifique

Configuration du routeur A

```
ip multicast-routing
ip pim rp-address 10.1.1.1

interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode

interface serial0
ip address 10.1.1.1 255.255.255.0
ip pim sparse-dense-mode
```

Configuration du routeur B

```
ip multicast-routing
ip pim rp-address 10.1.1.1

interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode

interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
```

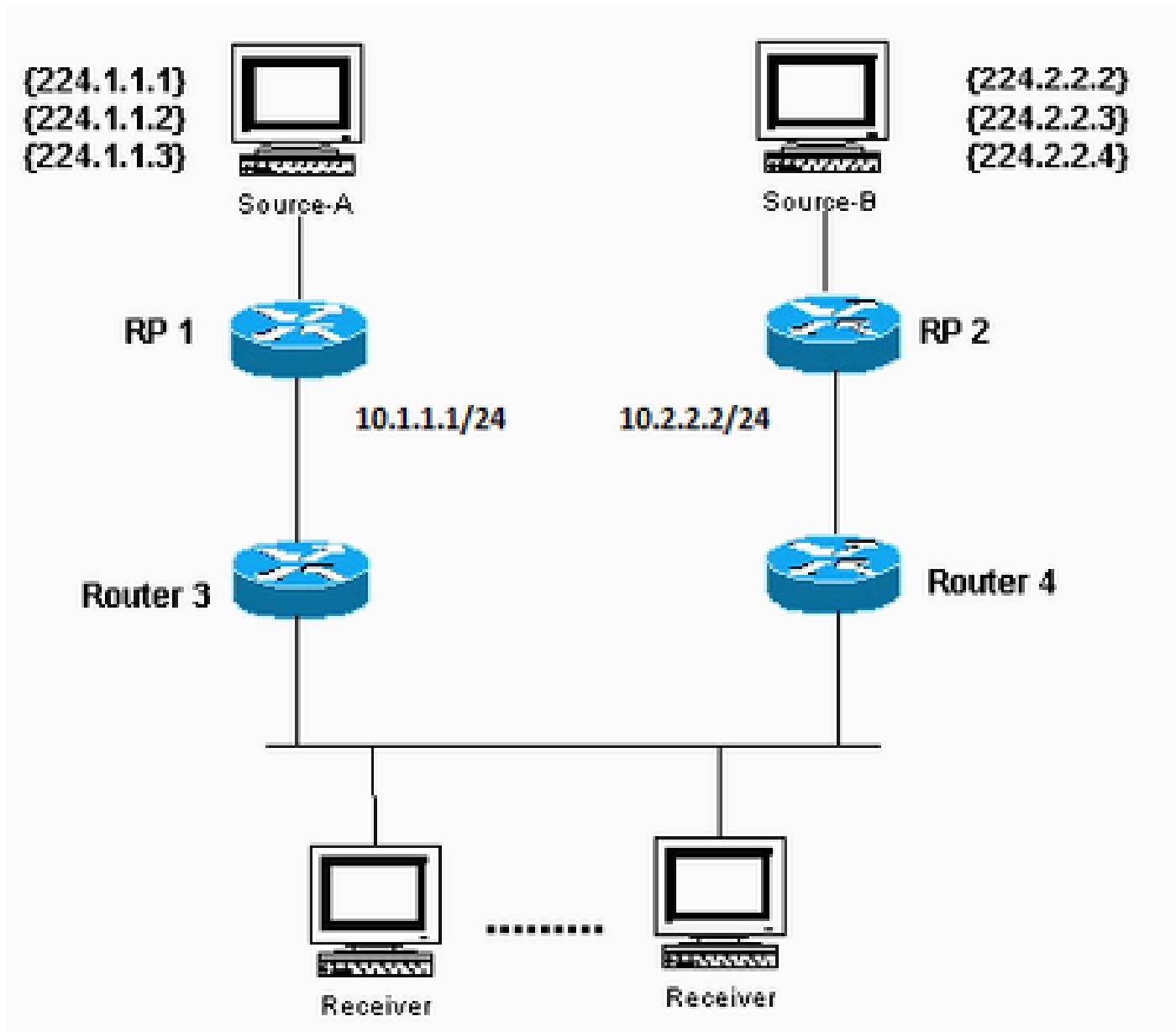
Mode clairsemé avec RP multiples

Dans cet exemple, Source-A envoie à 224.1.1.1, 224.1.1.2 et 224.1.1.3. Source-B envoie à 224.2.2.2, 224.2.2.3 et 224.2.2.4. Vous pouvez avoir un routeur, RP 1 ou RP 2, comme RP pour tous les groupes.

Cependant, si vous voulez que différents RP gèrent différents groupes, vous devez configurer tous les routeurs pour inclure quels groupes les RP peuvent servir.

Ce type de configuration RP statique nécessite que tous les routeurs du domaine PIM aient les mêmes commandes `ip pim rp-address address acl` configurées.

Vous pouvez également utiliser l'Auto-RP afin d'obtenir la même configuration, qui est plus facile.



Source-A envoie à 224.1.1.1, 224.1.1.2 et 224.1.1.3 ; La source B envoie à 224.2.2.2, à 224.2.2.3 et à 224.2.2.4.

Configuration du RP 1
ip multicast-routing
ip pim RP-address 10.1.1.1 2
ip pim RP-address 10.2.2.2 3
access-list 2 permit 224.1.1.1
access-list 2 permit 224.1.1.2
access-list 2 permit 224.1.1.3
access-list 3 permit 224.2.2.2
access-list 3 permit 224.2.2.3
access-list 3 permit 224.2.2.4

Configuration du RP 2

```
ip multicast-routing
ip pim RP-address 10.1.1.1 2
ip pim RP-address 10.2.2.2 3

access-list 2 permit 224.1.1.1
access-list 2 permit 224.1.1.2
access-list 2 permit 224.1.1.3
access-list 3 permit 224.2.2.2
access-list 3 permit 224.2.2.3
access-list 3 permit 224.2.2.4
```

Configuration pour les routeurs 3 et 4

```
ip multicast-routing
ip pim RP-address 10.1.1.1 2
ip pim RP-address 10.2.2.2 3

access-list 2 permit 224.1.1.1
access-list 2 permit 224.1.1.2
access-list 2 permit 224.1.1.3
access-list 3 permit 224.2.2.2
access-list 3 permit 224.2.2.3
access-list 3 permit 224.2.2.4
```

Auto-RP avec un RP

L'Auto-RP implique que vous configureriez les RP pour annoncer leur disponibilité en tant que RP et agents de mappage. Les RP utilisent 224.0.1.39 pour envoyer leurs annonces.

L'agent de mappage RP écoute les paquets annoncés par les RP, puis envoie les mappages RP-vers-groupe dans un message de détection qui est envoyé à 224.0.1.40.

Ces messages de détection sont utilisés par les routeurs résiduels pour leur mappage RP-vers-groupe.

Vous pouvez utiliser un RP qui sert également d'agent de mappage ou vous pouvez configurer plusieurs RP et plusieurs agents de mappage à des fins de redondance.

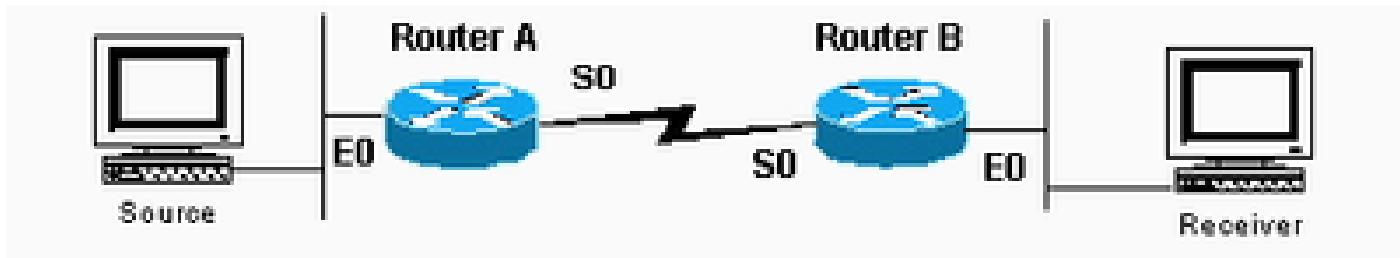
Remarquez que quand vous choisissez une interface d'où créer des annonces RP, Cisco recommande que vous utilisez une interface telle qu'un bouclage au lieu d'une interface physique.

En outre, il est possible d'utiliser les interfaces VLAN (SVI) commutées. Si une interface VLAN est utilisée pour annoncer l'adresse RP, puis l'option interface type dans {numéro d'interface / type d'interface ip pim [vrf vrf-name] send-rp-announce | ip-address} scope ttl-value doit contenir l'interface VLAN et le numéro VLAN. Par exemple, la commande ressemble à ip pim send-rp-announceVlan500 scope 100 .

Si vous choisissez une interface physique, vous vous attendez à ce que l'interface soit toujours en marche. Ce n'est pas toujours le cas. Le routeur cesse de s'annoncer en tant que RP une fois que l'interface physique tombe en panne.

Avec une interface de bouclage, elle est toujours en marche et ne tombe jamais en panne, ce qui assure que le RP continue à s'annoncer à travers toutes les interfaces disponibles en tant que RP.

C'est le cas même si une ou plusieurs de ses interfaces physiques tombent en panne. L'interface de bouclage doit être le PIM activé et annoncé par un Interior Gateway Protocol (IGP) ou doit être accessible avec un routage statique.



L'interface de bouclage doit être activée par PIM et annoncée par un protocole IGP (Interior Gateway Protocol) ou accessible avec routage statique

Configuration du routeur A

```
ip multicast-routing
ip pim send-rp-announce loopback0 scope 16
ip pim send-rp-discover
scope 16
interface loopback0
ip address <address> <mask>
ip pim sparse-dense-mode
interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode
```

Configuration du routeur B

```
ip multicast-routing
interface ethernet0
ip address <address> <mask>
ip pim sparse-dense-mode
```

```
interface serial0
ip address <address> <mask>
ip pim sparse-dense-mode
```

Auto-RP avec RP multiples

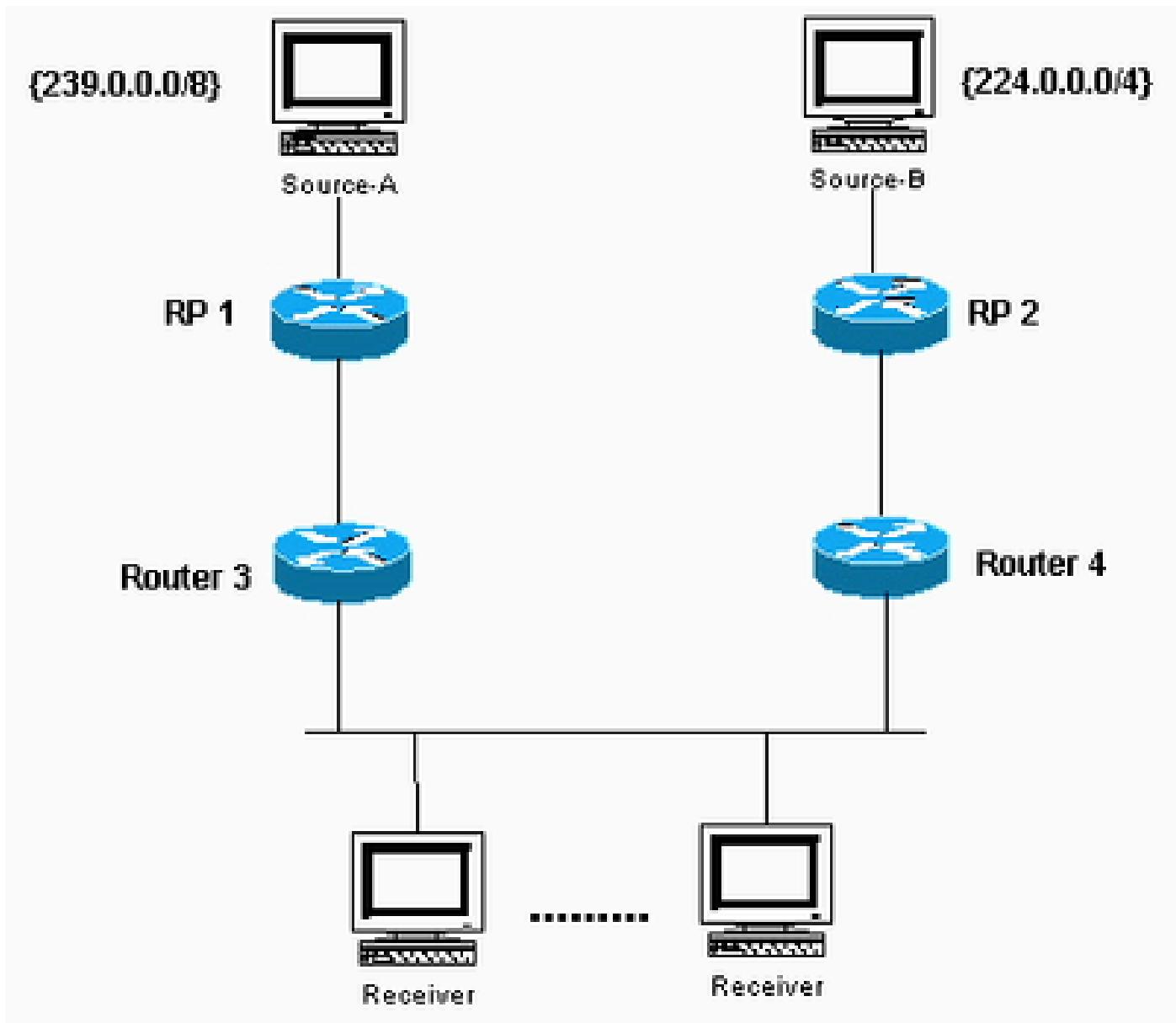
Les listes d'accès dans cet exemple permettent aux RP d'être RP seulement pour les groupes que vous voulez. Si aucune liste d'accès n'est configurée, les RPs sont disponibles en tant que RP pour tous les groupes.

Si deux RP annoncent leur disponibilité comme RP pour le même groupe, le ou les agents de mappage résolvent ces conflits avec la règle « l'adresse IP la plus élevée gagne ».

Lorsque deux RP s'annoncent pour ce groupe, vous pouvez configurer chaque routeur avec une adresse de bouclage afin d'influer sur quel routeur sera le RP pour un groupe particulier.

Placez l'adresse IP la plus haute sur le RP préféré, puis utilisez l'interface de bouclage en tant que source des paquets de l'annonce ; par exemple, ip pim send-RP-announceloopback0 .

Quand plusieurs agents de mappage sont utilisés, chacun d'entre eux annoncent le même groupe RP aux mappages RP au groupe de détection 224.0.1.40.



Placez l'adresse IP supérieure sur le RP préféré

Configuration du RP 1

```
ip multicast-routing
interface loopback0
ip address <address> <mask>
ip pim sparse-dense-mode
ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery scope 16
access-list 1 permit 239.0.0.0 0.255.255.255
```

Configuration du RP 2

```
ip multicast-routing
```

```
interface loopback0
ip address <address> <mask>
ip pim sparse-dense-mode

access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 10.255.255.255
```

DVMRP

Votre prestataire de services Internet (ISP) pourrait proposer que vous créeiez un tunnel Distance Vector Multicast Routing Protocol (DVMRP) vers l'ISP afin d'accéder au circuit principal de multidiffusion dans Internet (mbone).

Les commandes minimums afin de configurer un tunnel DVMRP sont montrées ici :

```
interface tunnel0
ip unnumbered <any pim interface>
tunnel source <address of source>
tunnel destination <address of ISPs mrouted box>
tunnel mode dvmrp
ip pim sparse-dense-mode
```

En général, le FAI vous fait passer un tunnel vers une machine UNIX qui exécute « mrouted » (DVMRP). Si l'ISP vous dirige par tunnel plutôt vers un autre périphérique Cisco, utilisez le mode tunnel GRE par défaut.

Si vous voulez produire des paquets de multidiffusion pour d'autres sur le mbone pour voir plutôt qu'envoyer des paquets de multidiffusion, vous devez annoncer les sous-réseaux sources.

Si votre adresse hôte source de multidiffusion est 172.16.108.1, vous avez besoin d'annoncer l'existence de ce sous-réseau au mbone. Des réseaux directement connectés sont annoncés avec une métrique 1 par défaut.

Si votre source n'est pas directement connectée au routeur avec le tunnel DVMRP, configurez ceci sous l'interface tunnel0 :

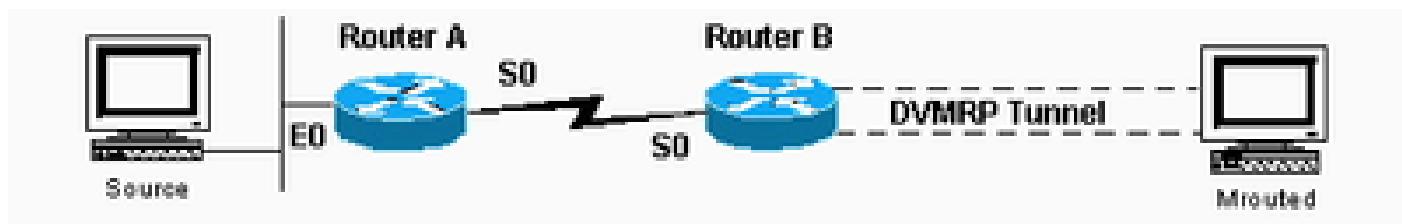
```
ip dvmrp metric 1 list 3
access-list 3 permit 172.16.108.0 0.0.0.255
```

 Remarque : Vous devez inclure une liste d'accès avec cette commande afin d'empêcher l'annonce de la table de routage entière de monodiffusion vers le mbone.

Si votre configuration est similaire à celle présentée ici et que vous souhaitez propager des routes DVMRP à travers le domaine, configurez la commande `ip dvmrp unicast-routing` sur les interfaces `serial0` des routeurs A et B.

Cette action assure la transmission des routes DVMRP vers des voisins PIM qui ont alors une table de routage DVMRP utilisée pour la retransmission par le chemin inverse (RPF).

Les routes DVMRP apprises ont la priorité RPF sur tous les autres protocoles, excepté pour les routes directement connectées.



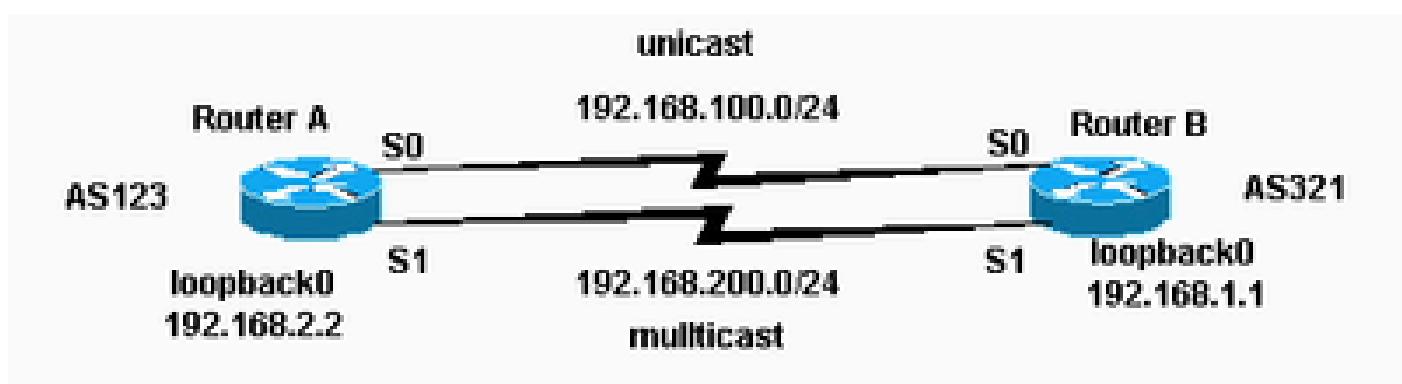
Propager des routes DVMRP à travers le domaine

MBGP

Multiprotocol Border Gateway Protocol (MBGP) est une méthode de base pour porter deux ensembles de routes : un ensemble pour le routage de monodiffusion et un ensemble pour le routage de multidiffusion.

MBGP assure le contrôle nécessaire pour décider où les paquets de multidiffusion sont autorisés à circuler. PIM utilise les routes associées au routage de multidiffusion afin de construire des arbres de distribution de données.

MBGP fournit le chemin RPF, pas la création d'état de multidiffusion. PIM est toujours nécessaire afin de transmettre les paquets de multidiffusion.



PIM est toujours nécessaire afin de transmettre les paquets de multidiffusion

Configuration du routeur A

```
ip multicast-routing
interface loopback0
```

```
ip pim sparse-dense-mode
ip address 192.168.2.2 255.255.255.0

interface serial0
ip address 192.168.100.1 255.255.255.0

interface serial1
ip pim sparse-dense-mode
ip address 192.168.200.1 255.255.255.0

router bgp 123
network 192.168.100.0 nlri unicast
network 192.168.200.0 nlri multicast
neighbor 192.168.1.1 remote-as 321 nlri unicast multicast
neighbor 192.168.1.1 ebgp-multihop 255
neighbor 192.168.100.2 update-source loopback0
neighbor 192.168.1.1 route-map setNH out

route-map setNH permit 10
match nlri multicast
set ip next-hop 192.168.200.1

route-map setNH permit 20
```

Configuration du routeur B

```
ip multicast-routing

interface loopback0
ip pim sparse-dense-mode
ip address 192.168.1.1 255.255.255.0

interface serial0
ip address 192.168.100.2 255.255.255.0

interface serial1
ip pim sparse-dense-mode
ip address 192.168.200.2 255.255.255.0

router bgp 321
network 192.168.100.0 nlri unicast
network 192.168.200.0 nlri multicast
neighbor 192.168.2.2 remote-as 123 nlri unicast multicast
neighbor 192.168.2.2 ebgp-multihop 255
neighbor 192.168.100.1 update-source loopback0
neighbor 192.168.2.2 route-map setNH out

route-map setNH permit 10
match nlri multicast
```

```
set ip next-hop 192.168.200.2  
  
route-map set NH permit 20
```

Si vos topologies de monodiffusion et de multidiffusion sont congruentes (par exemple, elles passent par la même liaison), la principale différence de configuration réside dans la commande `nlri unicast multicast`.

Un exemple est montré ici :

```
network 192.168.100.0 nlri unicast multicast
```

Les topologies conformes avec MBGP ont un avantage - quoique le trafic traverse les mêmes chemins, différentes réglementations peuvent être appliquées au BGP de monodiffusion contre le BGP de multidiffusion.

MSDP

Le Multicast Source Discovery Protocol (MSDP) connecte des domaines multiples de PIM-SM.

Chaque domaine PIM-SM utilise ses propres RP indépendants et n'a pas besoin de dépendre des RP dans d'autres domaines.

Le MSDP permet à des domaines de détecter des sources de multidiffusion dans d'autres domaines. Si vous avez également établi un partenariat avec un pair MSDP, vous devez utiliser la même adresse IP pour MSDP que pour BGP.

Quand MSDP fait des contrôles de pair RPF, MSDP s'attend à ce que l'adresse du pair MSDP soit identique à l'adresse que BGP/MBGP lui donne quand il effectue une recherche dans la table de routes sur le RP dans le message SA.

Cependant, il n'est pas nécessaire que vous exécutiez BGP/MBGP avec le pair MSDP s'il y a un chemin BGP/MBGP entre les pairs MSDP.

S'il n'y a aucun chemin BGP/MBGP et plus d'un pair MSDP, vous devez utiliser la commande `ip msdp default-peer` .

L'exemple montre ici que le RP A est le RP pour son domaine et que le RP B est le RP pour son domaine.



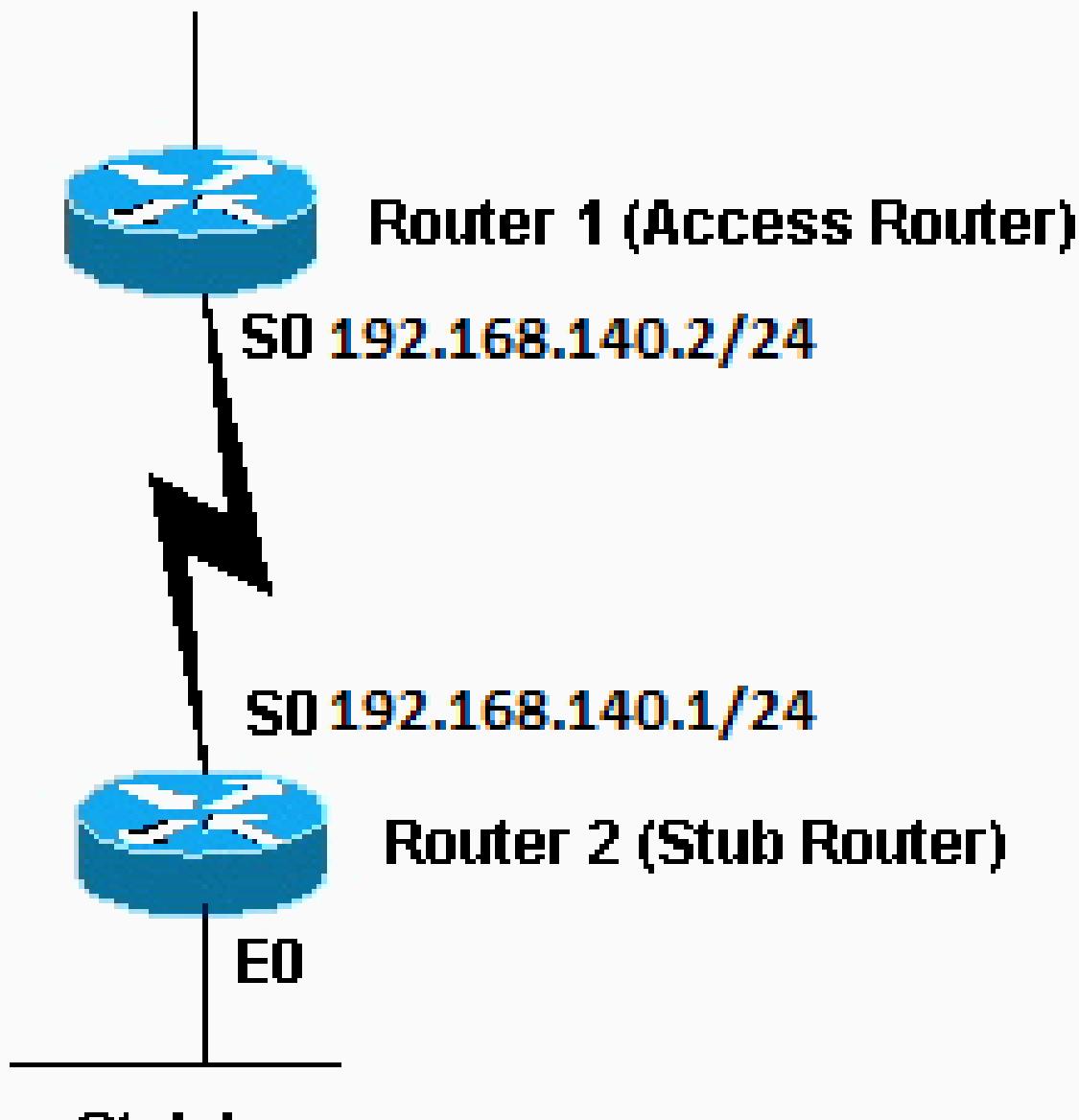
Le Multicast Source Discovery Protocol (MSDP) connecte des domaines multiples de PIM-SM

Configuration du routeur A
<pre>ip multicast-routing ip pim send-RP-announce loopback0 scope 16 group-list 1 ip pim send-RP-discovery scope 16 ip msdp peer 192.168.100.2 ip msdp sa-request 192.168.100.2 interface loopback0 ip address <address> <mask> ip pim sparse-dense-mode interface serial0 ip address 192.168.100.1 255.255.255.0 ip pim sparse-dense-mode</pre>
Configuration du routeur B
<pre>ip multicast-routing ip pim send-RP-announce loopback0 scope 16 group-list 1 ip pim send-RP-discovery scope 16 ip msdp peer 192.168.100.1 ip msdp sa-request 192.168.100.1 interface loopback0 ip address <address> <mask> ip pim sparse-dense-mode interface serial0 ip address 192.168.100.2 255.255.255.0 ip pim sparse-dense-mode</pre>

Routage multicast d'extrémité

Le routage multicast d'extrémité vous permet de configurer les routeurs distants/d'extrémité en tant qu'agents proxy IGMP. Plutôt que de participer pleinement au protocole PIM, ces routeurs

d'extrémité transfèrent les messages IGMP des hôtes au routeur multicast en amont.



Les routeurs d'extrémité transfèrent les messages IGMP des hôtes au routeur multidiffusion en amont

Configuration du routeur 1

```
int s0
ip pim sparse-dense-mode
ip pim neighbor-filter 1

access-list 1 deny 192.168.140.1
```

La commande ip pim neighbor-filter est nécessaire pour que le Routeur 1 ne reconnaisse pas le Routeur 2 comme voisin PIM.

Si vous configurez le Routeur 1 en mode clairsemé, le filtre du voisin n'est pas nécessaire. Le Routeur 2 ne doit pas être exécuté en mode clairsemé.

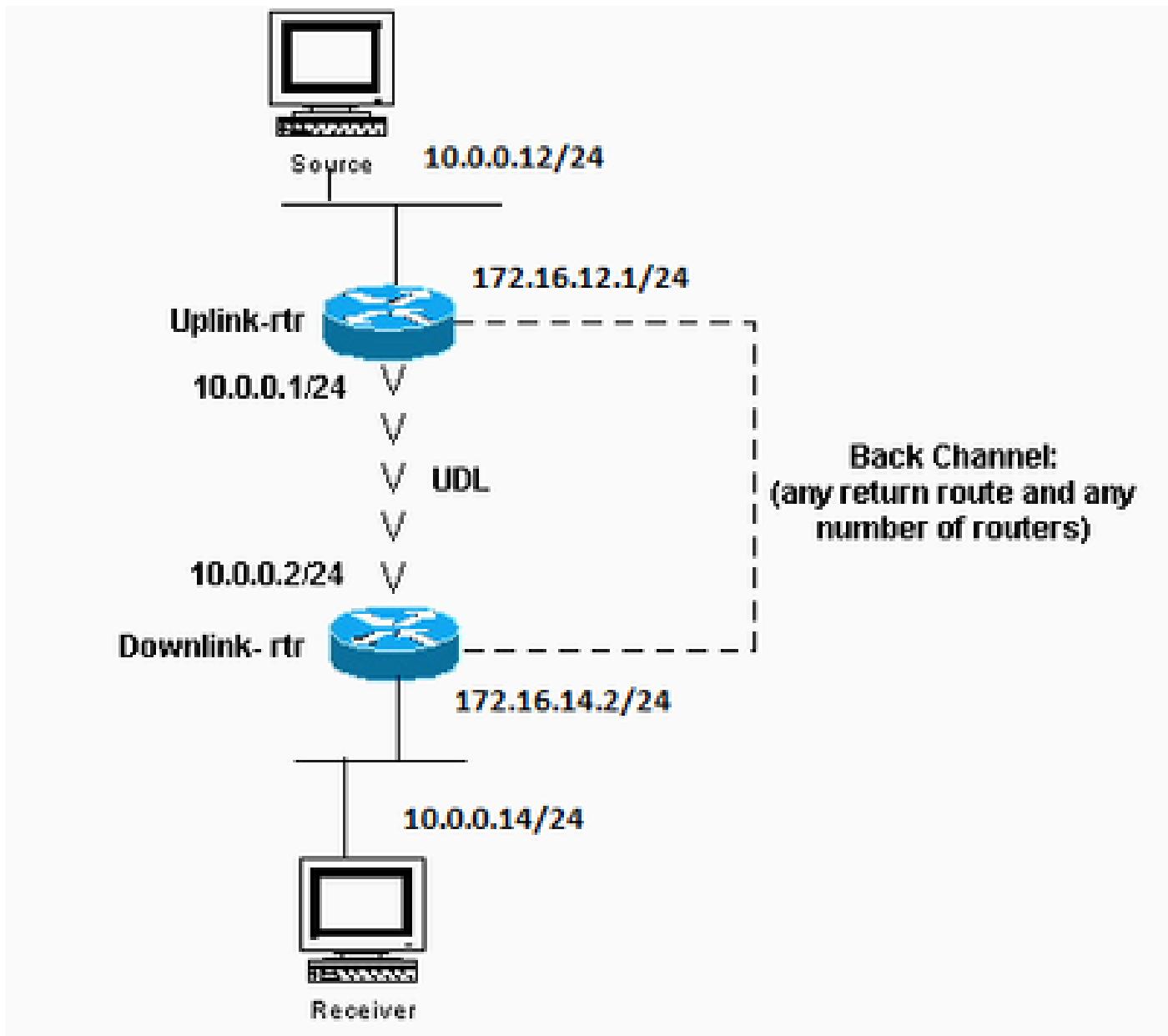
En mode dense, les sources de multidiffusion d'extrémité peuvent inonder les routeurs de réseau principal.

Configuration du Routeur 2
ip multicast-routing int e0 ip pim sparse-dense-mode ip igmp helper-address 192.168.140.2 int s0 ip pim sparse-dense-mode

IGMP UDLR pour liaisons satellites

Le Protocole de routage unidirectionnel (UDLR) fournit une méthode pour la transmission de paquets de multidiffusion sur une liaison satellite unidirectionnelle vers les réseaux d'extrémité qui ont un canal de retour.

Ceci est semblable au routage multicast d'extrémité. Sans cette fonctionnalité, le routeur de liaison ascendante n'est pas en mesure d'apprendre dynamiquement quelles adresses de groupe multicast IP transmettre sur la liaison unidirectionnelle, parce que le routeur de liaison descendante ne peut rien envoyer en retour.



Le routage de liaison unidirectionnel (UDLR) fournit une méthode pour transférer des paquets multidiffusion

Configuration de routeur de liaison ascendante

```
ip multicast-routing

interface Ethernet0
description Typical IP multicast enabled interface
ip address 172.16.12.1 255.0.0.0
ip pim sparse-dense-mode

interface Ethernet1
description Back channel which has connectivity to downlink-rtr
ip address 172.16.11.1 255.0.0.0
ip pim sparse-dense-mode

interface Serial0
```

```
description Unidirectional to downlink-rtr
ip address 10.0.0.1 255.0.0.0
ip pim sparse-dense-mode
ip igmp unidirectional-link
no keepalive
```

Configuration de routeur de liaison descendante

```
ip multicast-routing

interface Ethernet0
description Typical IP multicast enabled interface
ip address 172.16.14.2 255.0.0.0
ip pim sparse-dense-mode
ip igmp helper-address udl serial0

interface Ethernet1
description Back channel which has connectivity to downlink-rtr
ip address 172.16.13.2 255.0.0.0
ip pim sparse-dense-mode

interface Serial0
description Unidirectional to uplink-rtr
ip address 10.0.0.2 255.0.0.0
ip pim sparse-dense-mode
ip igmp unidirectional-link
no keepalive
```

PIMv2 BSR

Si tous les routeurs du réseau exécutent PIMv2, vous pouvez configurer un BSR au lieu d'Auto-RP. BSR et Auto-RP sont très semblables.

Une configuration du BSR implique que vous configureriez des candidats BSR (semblables à l'annonce RP dans l'Auto-RP) et BSR (semblable aux agents de mappage d'Auto-RP). Afin de configurer un BSR, utilisez ces étapes :

1. Sur le candidat BSR, configuez :

```
ip pim bsr-candidate interface hash-mask-len pref
```

Où l'interface contient le candidat BSR de l'adresse IP. Il est recommandé (mais pas nécessaire) que hash-mask-Len soit identique parmi tous les candidats BSR. Un candidat BSR avec la plus grande valeur de préférence est élu comme BSR pour ce domaine.

Un exemple de l'utilisation de la commande est montré :

```
ip pim bsr-candidate ethernet0 30 4
```

Le PIMv2 BSR rassemble les informations sur le RP candidat et diffuse les informations du RP établi associées à chaque préfixe de groupe. Afin d'éviter le point de panne unique, vous pouvez configurer plus d'un routeur dans un domaine comme candidat BSR.

Un BSR est élu parmi les candidats BSR automatiquement, sur la base des valeurs de préférence configurées. Afin de servir en tant que candidats BSR, les routeurs doivent être connectés et être dans le circuit principal du réseau, plutôt que dans la zone d'accès commuté du réseau.

2. Configurez les routeurs RP candidats. Cet exemple montre un candidat RP, sur l'interface ethernet0, pour la plage entière des adresses de portée ADMIN :

```
access-list 11 permit 239.0.0.0 0.255.255.255
ip pim rp-candidate ethernet0 group-list 11
```

CGMP

Afin de configurer le protocole CGMP (Group Management Protocol), configurez ceci sur l'interface du routeur qui fait face au commutateur :

```
ip pim sparse-dense-mode
ip cgmp
```

Puis, configurez ceci sur le commutateur :

```
set cgmp enable
```

IGMP Snooping

La surveillance de trafic Internet Group Management Protocol (IGMP) est disponible avec la version 4.1 de Catalyst 5000. IGMP snooping requiert une carte Supervisor III.

Aucune configuration autre que PIM n'est nécessaire pour configurer IGMP Snooping sur le

routeur. Un routeur est toutefois nécessaire avec IGMP Snooping pour fournir les requêtes d'IGMP.

L'exemple fourni ici montre comment activer IGMP Snooping sur le commutateur :

```
<#root>
Console> (enable)
set igmp enable

IGMP Snooping is enabled.
CGMP is disabled.
```

Si vous essayez d'activer IGMP, mais que CGMP est déjà activé, vous voyez ceci :

```
<#root>
Console> (enable)
set igmp enable

Disable CGMP to enable IGMP Snooping feature.
```

PGM

Le Pragmatic General Multicast (PGM) est un protocole de transport de multidiffusion fiable pour les applications qui une remise de données de multidiffusion ordonnées, sans répétition de plusieurs sources vers plusieurs récepteurs.

PGM garantit qu'un récepteur dans le groupe soit reçoit tous les paquets de données des transmissions et des retransmissions soit peut détecter la perte irrémédiable de paquets de données.

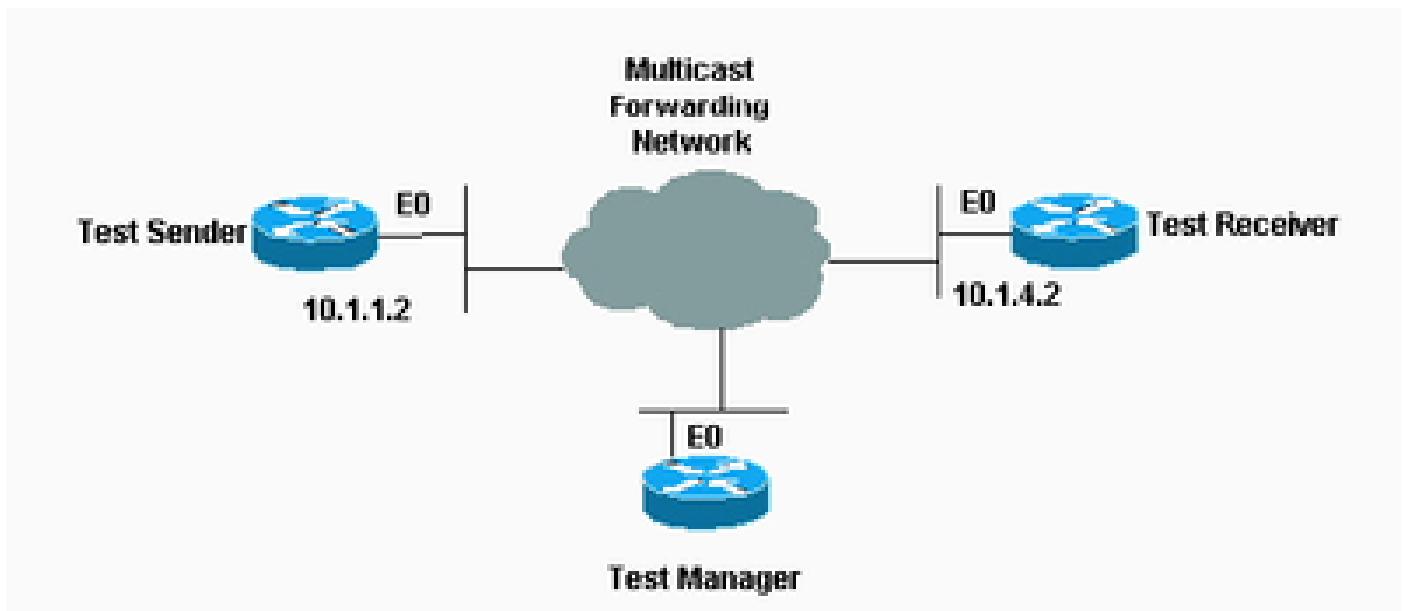
Il n'y a aucune commande PGM globale. PGM est configuré par interface avec la commande ip pgm. Vous devez activer le routage multicast sur le routeur avec PIM sur l'interface.

MRM

Le Multicast Routing Monitor (MRM) facilite la détection de faute automatisée dans une grande infrastructure de routage multicast. Le MRM est conçu pour alerter un administrateur réseau des problèmes de routage multicast en temps quasi-réel.

Le MRM a deux composants : Appareil de contrôle MRM et gestionnaire MRM. L'appareil de contrôle MRM est un expéditeur ou un récepteur.

MRM est disponible dans les versions 12.0(5)T du logiciel Cisco IOS et postérieures. Seuls les testeurs et les gestionnaires MRM doivent exécuter la version de Cisco IOS prise en charge par MRM.



Le Multicast Routing Monitor (MRM) facilite la détection de faute automatisée dans une grande infrastructure de routage multicast

Configuration de l'expéditeur de test

```
interface Ethernet0
  ip mrm test-sender
```

Configuration du récepteur de test

```
interface Ethernet0
  ip mrm test-receiver
```

Configuration du gestionnaire de test

```
ip mrm manager test1
  manager e0 group 239.1.1.1
  senders 1
  receivers 2 sender-list 1
```

```
access-list 1 permit 10.1.1.2
access-list 2 permit 10.1.4.2
```

La sortie de la commande `show ip mrm manager` sur le gestionnaire de test est montrée ici :

```
<#root>
```

```
Test_Manager#  
show ip mrm manager
```

Manager:test1/10.1.2.2 is not running Beacon interval/holdtime/ttl:60/86400/32 Group:239.1.1.1, UDP p

Lancez le test avec la commande montrée ici. Le gestionnaire de test envoie des messages de contrôle à l'expéditeur de test et au récepteur de test tel que configuré dans les paramètres de test.

Le récepteur de test joint le groupe et surveille les paquets de test envoyés par l'expéditeur de test.

```
<#root>  
Test_Manager#  
mrm start test1  
  
*Feb 4 10:29:51.798: IP MRM test test1 starts .....  
Test_Manager#
```

Afin d'afficher un rapport d'état pour le gestionnaire de test, entrez cette commande :

```
<#root>  
Test_Manager#  
show ip mrm status  
  
IP MRM status report cache:  
Timestamp Manager Test Receiver Pkt Loss/Dup (%) Ehsr  
*Feb 4 14:12:46 10.1.2.2 10.1.4.2 1 (4%) 29  
*Feb 4 18:29:54 10.1.2.2 10.1.4.2 1 (4%) 15  
Test_Manager#
```

La sortie montre que le récepteur a envoyé deux rapports d'état (une ligne chacun) sur un marqueur intemporel déterminé. Chaque rapport présente une perte de paquets pendant la fenêtre de l'intervalle (défaut d'une seconde).

La valeur de « Ehsr » montre la valeur du numéro de la prochaine séquence de l'expéditeur de test. Si le récepteur de test voit des paquets en double, il montre un numéro négatif dans la colonne « perte paq./doublon ».

Pour interrompre le test, entrez cette commande :

```
<#root>

Test_Manager#
mrm stop test1

*Feb  4 10:30:12.018: IP MRM test test1 stops
Test_Manager#
```

Pendant l'exécution du test, l'expéditeur MRM envoie des paquets RTP à l'adresse de groupe configurée à l'intervalle par défaut de 200 ms.

Le récepteur surveille (prévoit) les mêmes paquets au même intervalle par défaut.

Si le récepteur détecte une perte de paquets dans l'intervalle de fenêtre par défaut de cinq secondes, il envoie un rapport au gestionnaire MRM.

Vous pouvez afficher le rapport d'état du récepteur si vous émettez la commande `show ip mrm status` sur le gestionnaire.

Dépannage

Certains des problèmes les plus communs émergent quand vous mettez en application Multicast IP dans un réseau quand le routeur n'expédie pas le trafic multicast en raison d'une panne RPF ou de la configuration TTL.

Reportez-vous au Guide de dépannage de Multicast IP pour une analyse détaillée au sujet de ces derniers et d'autres problèmes communs, symptômes, et résolutions.

Informations connexes

- [Guide de dépannage de multidiffusion IP](#)
- [Dépannage des réseaux multidiffusion avec les outils CLI](#)
- [Prise en charge de multidiffusion IP](#)
- [Assistance technique de Cisco et téléchargements](#)

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.