

# Dépannage des réseaux multidiffusion avec les outils CLI

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Stratégies de dépannage](#)

[Contrôlez le flux de paquets source](#)

[Contrôlez la signalisation de réseau](#)

[Dépannage du mode intermédiaire PIM](#)

[Contrôlez le flux de paquets du réseau](#)

[Contrôlez la signalisation du récepteur](#)

[Contrôlez le flux de paquets du récepteur](#)

[Outils Power CLI](#)

[mstat](#)

[mrinfo](#)

[mtrace](#)

[tintement](#)

[Commandes show](#)

[show ip igmp groups](#)

[show ip igmp interface](#)

[show ip pim neighbor](#)

[show ip pim interface](#)

[show ip mroute summary](#)

[show ip mroute](#)

[show ip mroute active](#)

[show ip rpf](#)

[show ip mcache](#)

[show ip mroute count](#)

[show ip route](#)

[show ip pim rp mapping](#)

[Commandes de débogage](#)

[debug ip igmp](#)

[debug ip mpacket](#)

[debug ip mrouting](#)

[debug ip pim](#)

[Informations connexes](#)

---

# Introduction

Ce document décrit les différents outils et techniques utilisés pour dépanner les réseaux de multidiffusion.

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### 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.

## Stratégies de dépannage

Quand vous dépannez des réseaux de multidiffusion, il est bon de considérer le protocole de signalisation utilisé en réseau et flux de paquets. Le protocole de signalisation est utilisé pour configurer et désactiver les sessions de multidiffusion (comme le mode dense PIM, le mode clairsemé PIM et le DVMRP) et le flux de paquets envoie, reproduit et reçoit des paquets de multidiffusion entre la source et le récepteur, en fonction de la table de transfert créée par le processus de signalisation.

Ce tableau permet de vérifier chaque élément d'information à dépanner et vérifie que chaque section du tableau fonctionne correctement :

	Source	Réseau	Récepteurs
Signalisation	S. O.	<a href="#">Contrôlez la signalisation de réseau</a>	<a href="#">Contrôlez la signalisation du récepteur</a>
Flux des paquets	<a href="#">Contrôlez le flux de paquets source</a>	<a href="#">Contrôlez le flux de paquets du réseau</a>	<a href="#">Contrôlez le flux de paquets du récepteur</a>


Les sous-sections suivantes détaillent les outils de dépannage que vous pouvez utiliser pour vérifier et résoudre les problèmes courants.

## Contrôlez le flux de paquets source

Effectuez ces étapes pour déterminer si la source a envoyé les paquets et si les champs de paquet corrects sont insérés :

1. Contrôlez les compteurs de l'interface sur l'hôte. Tout d'abord, vérifiez les compteurs d'interface (si vous êtes sur un système UNIX, utilisez la commande `netstat`) sur l'hôte source pour voir s'il envoie des paquets. Si ce n'est pas le cas, vérifiez toute erreur de configuration ou bogues dans la pile hôte et l'application.
2. Utilisez la commande `show ip igmp groups <interface-name>` pour vérifier le routeur en amont afin de voir s'il a reçu un rapport d'appartenance à la jointure au niveau de l'interface directement connectée à la source.
3. Vérifiez la valeur de durée de vie des paquets dans l'application de multidiffusion ; elle doit être supérieure à 1. Si l'application envoie des paquets avec une valeur de durée de vie inférieure à 1, vous devez voir le trafic abandonné au niveau du premier routeur en amont. Pour vérifier, utilisez la commande `show ip traffic` et recherchez une augmentation de la valeur du compteur de « nombre de sauts incorrects ». N'importe quel paquet avec une valeur de TTL de 1 ou inférieure au seuil de TTL déterminé par l'interface avec la commande `ip multicast ttl-threshold`, est abandonné et le compteur du « nombre de sauts incorrects » est augmenté d'un. Utilisez la commande `show ip igmp interface <interface-name>` pour voir la valeur de seuil de durée de vie de l'interface.
4. Utilisez les commandes `show ip mroute count` et `show ip mroute active` pour contrôler le premier routeur en amont ou commutez pour voir s'il détecte des paquets multidiffusés depuis la source. La sortie de la commande montre les statistiques du flux de trafic pour chaque paire (S, G). Si vous n'observez pas de trafic, contrôlez la signalisation du récepteur.
5. Utilisez la commande `debug ip mpacket` sur le routeur en amont le plus proche, avec l'argument `detail` ou `acl` pour la granularité.

---

 Attention : utilisez cette commande avec précaution en cas de trafic de multidiffusion important sur le réseau. Seulement s'il y a lieu, utilisez la commande `debug ip mpacket` sur la route. Employez l'argument `detail` pour montrer des en-têtes de paquet dans la sortie de débogage et des listes d'accès pour vérifier le trafic des sources spécifiques. N'oubliez pas que cette commande peut avoir un impact important sur les performances d'autres trafics.

---

## Contrôlez la signalisation de réseau

Il s'agit de l'élément de dépannage le plus complexe et le plus important d'un réseau. Elle dépend du protocole de signalisation de réseau utilisé, tel que le mode intermédiaire PIM, le mode dense PIM et DVMRP. Nous recommandons l'approche multiétapes décrite dans cette section.

Dépannage du mode intermédiaire PIM

Complétez ces étapes pour dépanner le mode intermédiaire PIM :

1. Vérifiez que le routage multicast IP est activé sur tous les routeurs multidiffusés.
2. Utilisez la commande [show ip pim neighbor](#) pour vérifier le compteur et le mode d'expiration afin de garantir l'établissement réussi du voisin PIM, et recherchez tout problème de connectivité et de compteur qui peut empêcher l'établissement des voisins PIM. S'il y a lieu, utilisez la commande secondaire ip pim [version] [dense-mode] [sparse-mode] [sparse-dense-mode] interface level pour établir le mode correct et la version pour établir avec succès les voisins PIM.
3. Utilisez la commande show ip pim rp mapping pour assurer le tracé RP-Group correct et pour vérifier le temporisateur d'expiration si auto-RP est configuré. Utilisez la commande debug ip pim auto-rp pour aider à identifier toute panne d'auto-RP.! Si vous ne voyez aucun tracé PIM Group-to-RP, contrôlez la configuration de l'auto-RP ou configurez les tracés statiques Group-RP avec la commande ip pim rp-address ip address of RP [access-list] [named-accesslist] [override]. La configuration de l'auto-RP peut être exécutée avec les commandes ip pim send-rp-announce interface-id scope TTL value et ip pim send-rp-discovery interface-id scope TTL value. Ces commandes doivent être configurées seulement s'il y a des configurations d'Auto-RP.
4. Utilisez la commande [show ip rpf](#) <ip address of source> pour vérifier l'échec RPF de l'adresse source. Le mode dense PIM et le mode intermédiaire PIM renvoient des messages Prune à la source si le trafic arrive sur une interface point à point non-RPF. La commande [debug ip pim](#) permet d'identifier les causes possibles d'une panne dans un réseau PIM : elle compare le résultat typique avec ce que vous voyez. Utilisez cette sortie pour identifier les trois étapes discrètes en mode intermédiaire PIM : la jonction, l'enregistrement et la commutation SPT. La commande show ip mroute vous permet d'observer les entrées nulles dans les listes d'interfaces sortantes et les entrées élaguées dans la table mroute.

Contrôlez le flux de paquets du réseau

Utilisez ces commandes pour contrôler le flux des paquets multidiffusés à travers le réseau :

- Utilisez la commande [mtrace](#) pour vérifier la trace de multidiffusion saut par saut
- [mstat](#)
- [tintement](#)
- [show ip mroute count](#)
- [show ip mroute active](#)
- [debug ip mpacket](#)

Contrôlez la signalisation du récepteur

Complétez ces étapes pour vérifier la signalisation du récepteur :

1. Utilisez la commande `show ip igmp groups` sur le premier routeur en amont connecté au récepteur pour vérifier que l'interface a joint le groupe.
2. Utilisez la commande `ping` pour contrôler l'accessibilité de l'hôte et le premier routeur en amont.
3. Utilisez la commande `show ip igmp interface` pour contrôler la version d'IGMP de l'interface.



---

Remarque : n'oubliez pas qu'un routeur configuré avec IGMP version 1 considère les paquets IGMP version 2 reçus de l'hôte comme non valides. Ces paquets IGMP ne rejoignent pas le groupe jusqu'à ce que le routeur reçoive un paquet de la version 1 d'IGMP de l'hôte.

---

4. Utilisez la commande `debug ip igmp` pour poursuivre le dépannage de la signalisation du récepteur.

Contrôlez le flux de paquets du récepteur

Complétez ces étapes pour contrôler le flux de paquets du récepteur :

1. Utilisez la commande `netstat` sur un système UNIX pour vérifier les statistiques de l'interface du récepteur.
2. Vérifiez que la pile TCP/IP a été installée et configurée correctement.
3. Vérifiez que l'application cliente du récepteur de multidiffusion a été installée et configurée correctement.
4. Recherchez des paquets de multidiffusion en double sur un segment à plusieurs accès.

## Outils Power CLI

Les commandes de cette section peuvent également être utiles lors du dépannage, en particulier lorsque vous testez le flux de paquets réseau et que vous trouvez les points de défaillance dans le réseau de multidiffusion.

### mstat

Cette commande montre le chemin de multidiffusion dans le format graphique ASCII. Elle trace le chemin entre deux points quelconques dans le réseau, montre des abandons et des doubles, des TTL et des retards à chaque noeud dans le réseau. Il est très utile lorsque vous devez localiser des points de congestion sur le réseau ou vous concentrer sur un routeur avec un nombre élevé de pertes/doublons. Les doublons sont indiqués dans la sortie comme des abandons négatifs.

```
<#root>
```

```
Router#
```

```
mstat lwei-home-ss2 172.16.58.88 224.0.255.255
```

```
Type escape sequence to abort
```

```
Mtrace from 172.16.143.27 to 172.16.58.88 via group 224.0.255.255
```

```
>From source (lwei-home-ss2.cisco.com) to destination (lwei-ss20.cisco.com)
```

```
Waiting to accumulate statistics.....
```

```
Results after 10 seconds:
```

Source	Response Dest	Packet Statistics For	Only For Traffic
172.16.143.27	172.16.62.144	All Multicast Traffic	From 172.16.143.27
	___/	rtt 48 ms	To 224.0.255.255
v	/	hop 48 ms	-----
172.16.143.25	lwei-cisco-isdn.cisco.com		
	^	ttl 1	
v		hop 31 ms	0/12 = 0% 1 pps 0/1 = --% 0 pps
172.16.121.84			
172.16.121.45	eng-frmt12-pri.cisco.com		
	^	ttl 2	
v		hop -17 ms	-735/12 = --% 1 pps 0/1 = --% 0 pps
172.16.121.4			
172.16.5.27	eng-cc-4.cisco.com		
	^	ttl 3	
v		hop -21 ms	-678/23 = --% 2 pps 0/1 = --% 0 pps
172.16.5.21			
172.16.62.130	eng-ios-2.cisco.com		
	^	ttl 4	
v		hop 5 ms	605/639 = 95% 63 pps 1/1 = --% 0 pps
172.16.62.144			
172.16.58.65	eng-ios-f-5.cisco.com		
	___	ttl 5	
v	\	hop 0 ms	4 0 pps 0 0 pps
172.16.58.88	172.16.62.144		
Receiver	Query Source		

## mrinfo

Cette commande montre le voisin de multidiffusion sur l'information du routeur, les capacités du routeur et la version du code, l'information de multidiffusion de l'interface, des seuils de TTL, métrique, protocole et état. Elle est utile quand vous devez vérifier des voisins de multidiffusion, confirmer que la contiguïté de voisins bidirectionnels existe et vérifier que les tunnels sont en place dans les deux directions.

```
<#root>
```

```
Router#
```

```
mrinfo
```

```
192.168.7.37 (b.cisco.com) [version cisco 11.1] [flags: PMSA]:  
192.168.7.37 -> 192.168.7.34 (s.cisco.com) [1/0/pim]  
192.168.7.37 -> 192.168.7.47 (d.cisco.com) [1/0/pim]  
192.168.7.37 -> 192.168.7.44 (d2.cisco.com) [1/0/pim]  
192.168.9.26 -> 192.168.9.29 (su.bbnplanet.net) [1/32/pim]
```

Les indicateurs dans la sortie indiquent :

- P = prune-capable
- M = mtrace-capable
- S = SNMP-capable
- A = Auto-RP-capable

## mtrace

Cette commande montre le chemin de multidiffusion de la source au récepteur et elle trace le chemin entre les points dans les réseaux, qui montre des seuils TTL et le retard à chaque noeud. Lors du dépannage, utilisez la commande mtrace pour trouver où le flux de trafic de multidiffusion s'arrête, pour vérifier le chemin du trafic de multidiffusion et pour identifier les chemins sous-optimaux.

```
<#root>
```

```
Router#
```

```
mtrace 192.168.215.41 192.168.215.67 239.254.254.254
```

```
Type escape sequence to abort.
```

```
Mtrace from 192.168.215.41 to 192.168.215.67 via group 239.254.254.254
```

```
From source (?) to destination (?)
```

```
Querying full reverse path...
```

```
0 192.168.215.67
-1 192.168.215.67 PIM thresh^ 0 0 ms
-2 192.168.215.74 PIM thresh^ 0 2 ms
-3 192.168.215.57 PIM thresh^ 0 894 ms
-4 192.168.215.41 PIM thresh^ 0 893 ms
-5 192.168.215.12 PIM thresh^ 0 894 ms
-6 192.168.215.98 PIM thresh^ 0 893 ms
```

## tintement

Lors du dépannage, la commande ping est la façon la plus simple de générer du trafic de multidiffusion dans les travaux pratiques pour tester l'arborescence de multidiffusion parce qu'elle envoie une requête ping à tous les membres du groupe et que tous les membres répondent.

```
<#root>
```

```
R3#
```

```
ping 239.255.0.1
```


```
Type escape sequence to abort.
```

```
Sending 1, 100-byte ICMP Echos to 239.255.0.1, timeout is 2 seconds:
```

Reply to request 0 from 172.16.12.2, 16 ms  
Reply to request 0 from 172.16.7.2, 20 ms

## Commandes show

Les commandes de cette section vous aident à recueillir des informations utiles lors du dépannage d'un problème de multidiffusion. Référez-vous au [Guide de référence des commandes de multidiffusion IP Cisco IOS](#) pour plus d'informations sur ces commandes show.

 Conseil : si vos réponses à la commande show sont lentes, la raison la plus probable est que le routeur effectue actuellement une recherche de domaine IP pour les adresses IP dans la commande show. Vous pouvez désactiver la recherche de domaine IP, utiliser la commande `no ip domain-lookup`, sous le mode de configuration globale du routeur pour désactiver la recherche de domaine IP. Ceci arrête la recherche de domaine ip et augmente la vitesse de la commande show command output.

### show ip igmp groups

Cette commande montre quels groupes de multidiffusion sont directement connectés au routeur et qui sont appris par l'intermédiaire de l'Internet Group Management Protocol (IGMP). Vous pouvez utiliser cette commande pour vérifier qu'une source ou un récepteur a réellement joint le groupe cible sur l'interface du routeur. La colonne Last Reporter affiche seulement un hôte IGMP, ce qui indique qu'il a envoyé soit une jointure IGMP non sollicitée, soit un rapport IGMP en réponse à une requête IGMP du routeur PIM pour ce groupe particulier. Vous ne devez voir qu'un seul dernier rapporteur par adresse de groupe.

```
<#root>
```

```
R1#
```

```
show ip igmp groups
```

```
IGMP Connected Group Membership
```

Group Address	Interface	Uptime	Expires	Last Reporter
239.255.0.1	Ethernet1	00:10:54	00:01:10	192.168.9.1
224.0.1.40	Ethernet0	01:36:27	00:02:45	192.168.10.2
224.0.1.40	Ethernet1	01:48:15	never	192.168.9.3

### show ip igmp interface

Utilisez cette commande pour afficher des informations relatives à la multidiffusion sur une interface et pour vérifier que le protocole IGMP est activé, que la version correcte est exécutée, que les compteurs, la valeur de seuil de durée de vie (TTL) et le routeur demandeur IGMP sont correctement définis. IGMP n'a pas besoin d'être configuré sur une interface. Il est activé par défaut lorsque vous configurez `ip pim {dense-mode|sparse-mode|sparse-dense-mode}`.



<#root>

R1#

show ip igmp interface

Ethernet1 is up, line protocol is up  
Internet address is 192.168.9.3/24

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  
Last member query response interval is 1000 ms  
Inbound IGMP access group is not set  
IGMP activity: 22 joins, 18 leaves  
Multicast routing is enabled on interface  
Multicast TTL threshold is 0  
Multicast designated router (DR) is 192.168.9.5  
IGMP querying router is 192.168.9.3 (this system)  
Multicast groups joined (number of users):  
224.0.1.40(1)

show ip pim neighbor

Utilisez cette commande pour répertorier les voisins PIM (Protocol Independent Multicast) détectés par le logiciel Cisco IOS.

<#root>

R1#

show ip pim neighbor

PIM Neighbor Table				
Neighbor Address	Interface	Uptime/Expires	Ver	DR Prio/Mode
10.10.10.1	Ethernet0/0	02:19:41/00:01:38	v2	1 / DR B S

Les détails de chaque champ sont expliqués ici :

- Neighbor Address : spécifie une adresse IP de voisinage PIM
- Interface - Interface où un voisin PIM a été découvert
- Disponibilité - Tout le temps de disponibilité du voisin

- Expire - Temps avant qu'un voisin dépasse le délai et jusqu'à ce que le PIM Hello suivant soit reçu
- Ver : version de PIM sur l'interface voisine
- DR Prio : les valeurs possibles sont comprises entre 0 et 4294967294 ou N

C'est une nouvelle colonne qui suit la priorité d'une interface PIM pour la sélection DR. La fonctionnalité permettant de configurer un DR basé sur l'adresse IP prioritaire vis-à-vis de l'adresse IP la plus haute a été introduite dans des versions du logiciel Cisco IOS 12.1(2)T et 12.2 et des images Cisco IOS avec Bidir-PIM. Vous pouvez utiliser la commande d'interface `ip pim dr-priority <0-4294967294>` pour définir la priorité du routeur désigné. La priorité DR par défaut est fixée à 1. Pour l'interopérabilité, si un voisin PIM exécute une ancienne version de Cisco IOS qui ne prend pas en charge la fonctionnalité de priorité DR, la colonne « DR Prior » affiche N. Si le voisin est le seul routeur qui affiche N pour l'interface, il devient le DR, quel que soit le routeur qui possède réellement l'adresse IP la plus élevée. Si plusieurs voisins PIM avec N sont répertoriés dans cette colonne, le séparateur de connexion est l'adresse IP la plus élevée parmi eux.

- Mode - Informations sur le DR et toutes autres capacités PIM.

Cette colonne répertorie le DR en plus de toute capacité prise en charge par le voisin PIM :

DR - Le voisin PIM est le routeur désigné

B - PIM bidirectionnel (Bidir-PIM) capable

S - État d'actualisation valide (s'applique seulement au mode dense)

Quand vous dépannez, utilisez cette commande pour vérifier que tous les voisins sont en marche et qu'ils utilisent le mode, la version et le temporisateur d'expiration appropriés. Vous pouvez également contrôler la configuration du routeur ou utiliser la commande `show ip pim interface` pour vérifier le mode (mode PIM intermédiaire ou dense). Utilisez la commande `debug ip pim` pour observer l'échange de message pim-requête.

## show ip pim interface

Utilisez cette commande pour afficher des informations sur des interfaces configurées pour PIM. En outre, vous pouvez utiliser cette commande pour vérifier que le mode PIM correct (dense ou intermédiaire) est configuré sur l'interface, le nombre du voisin est correct et le routeur désigné (DR) est correct (ce qui est important pour le mode intermédiaire). Les segments à plusieurs accès (tels que les Ethernets, le Token Ring, FDDI) élisent un DR basé sur une adresse IP plus haute. Les liens point par point n'affichent pas l'information DR.

```
<#root>
```

```
R1#
```

```
show ip pim interface
```

Address	Interface	Version/Mode	Nbr Count	Query Intvl	DR
192.168.10.1	Ethernet0	v2/Sparse-Dense	1	30	192.168.10.2
192.168.9.3	Ethernet1	v2/Sparse-Dense	1	30	192.168.9.5

## show ip mroute summary

Utilisez cette commande pour afficher le contenu récapitulé de la table de routage multicast IP. Vous pouvez également l'utiliser pour vérifier le(s) groupe(s) de multidiffusion actif(s) et les expéditeurs de multidiffusion actifs lorsque vous consultez les compteurs et les indicateurs.

<#root>

R1#

show ip mroute summary

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

M - MSDP created entry, X - Proxy Join Timer Running

A - Advertised via MSDP

Outgoing interface flags: H - Hardware switched

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

(\* , 239.255.0.1), 01:57:07/00:02:59, RP 192.168.7.2, flags: SJCF

(192.168.33.32, 239.255.0.1), 01:56:23/00:02:59, flags: CJT

(192.168.9.1, 239.255.0.1), 01:57:07/00:03:27, flags: CFT

(\* , 224.0.1.40), 1d00h/00:00:00, RP 192.168.7.2, flags: SJPCL

## show ip mroute

Utilisez cette commande pour afficher le contenu intégral de la table de routage Multicast IP. Quand vous dépannez, utilisez cette commande pour vérifier :

- Les entrées d'état (S, G) et (\*, G) des indicateurs.
- L'interface entrante est correcte. Si elle ne l'est pas, contrôlez la table de routage de monodiffusion.
- La ou les interfaces sortantes sont correctes. Si elle est inexactement élaguée, contrôlez l'état sur le routeur en aval.

<#root>

R1#

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  
M - MSDP created entry, X - Proxy Join Timer Running  
A - Advertised via MSDP  
Outgoing interface flags: H - Hardware switched  
Timers: Uptime/Expires  
Interface state: Interface, Next-Hop or VCD, State/Mode

(\* , 239.255.0.1), 01:55:27/00:02:59, RP 192.168.7.2, flags: SJCF

Incoming interface: Ethernet0, RPF nbr 192.168.10.2  
Outgoing interface list:  
Ethernet1, Forward/Sparse, 01:55:27/00:02:52

(192.168.33.32 , 239.255.0.1), 01:54:43/00:02:59, flags: CJT

Incoming interface: Ethernet0, RPF nbr 192.168.10.2

### Outgoing interface list:

Ethernet1, Forward/Sparse, 01:54:43/00:02:52

(192.168.9.1, 239.255.0.1), 01:55:30/00:03:26, flags: CFT

Incoming interface: Ethernet1, RPF nbr 0.0.0.0  
Outgoing interface list:  
Ethernet0, Forward/Sparse, 01:55:30/00:03:12

(\* , 224.0.1.40), 1d00h/00:00:00, RP 192.168.7.2, flags: SJPC

Incoming interface: Ethernet0, RPF nbr 192.168.10.2  
Outgoing interface list: Null

## show ip mroute active

Utilisez cette commande pour afficher les sources et les groupes de trafic actifs au-delà du seuil. Lors du dépannage, utilisez-le pour vérifier les groupes sources actifs, le débit de chaque paire de groupes sources (S, G) (vous devez avoir basculé vers l'arborescence du plus court chemin (SPT)) et pour vérifier si le trafic de multidiffusion du groupe cible est reçu. Si le trafic n'est pas reçu, recherchez le trafic actif qui commence à la source vers le récepteur.

<#root>

R1#

show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 239.255.0.1, (?)

Source: 192.168.33.32 (?)

Rate: 10 pps/115 kbps(1sec), 235 kbps(last 23 secs), 87 kbps(life avg)

## show ip rpf

Utilisez cette commande pour afficher comment le routage de multicast IP fait la retransmission par le chemin inverse (RPF). Quand vous dépannez, utilisez-la pour vérifier que l'information RPF est correcte. Si elle ne l'est pas, examinez la table de routage de monodiffusion pour l'adresse source. Utilisez également les commandes ping et trace sur l'adresse source pour vérifier que le routage de monodiffusion fonctionne. Vous pouvez utiliser les routes DVMRP (Distance Vector Multicast Routing Protocol) ou les mroutes statiques pour corriger les incohérences de monodiffusion-multidiffusion.

```
<#root>
```

```
R1#
```

```
show ip rpf 192.168.33.32
```

```
RPF information for ? (192.168.33.32)
```

```
RPF interface: Ethernet0
```

```
RPF neighbor: ? (192.168.10.2)
```

```
RPF route/mask: 192.168.33.0/16
```

```
RPF type: unicast (eigrp 1)
```

```
RPF recursion count: 0
```

```
Doing distance-preferred lookups across tables
```

## show ip mcache

Cette commande peut vérifier le cache de commutation rapide de Multicast IP et déboguer les bogues de commutation rapide.

```
<#root>
```

```
R1#
```

```
show ip mcache
```

```
IP Multicast Fast-Switching Cache
```

```
(192.168.33.32/32, 239.255.0.1), Ethernet0, Last used: 00:00:00
```

```
Ethernet1      MAC Header: 01005E7F000100000C13DBA90800
```

```
(192.168.9.1/32, 239.255.0.1), Ethernet1, Last used: 00:00:00
```

```
Ethernet0      MAC Header: 01005E7F000100000C13DBA80800
```

## show ip mroute count

Utilisez cette commande pour vérifier que le trafic de multidiffusion est reçu pour vérifier ses débits et baisses. Si aucun trafic n'est reçu, travaillez à partir de la source du récepteur jusqu'à ce que vous trouviez où le trafic s'arrête. Vous pouvez également utiliser cette commande pour vérifier

que le trafic est transféré. S'il ne l'est pas, utilisez la commande show ip mroute pour rechercher « la liste d'interfaces en sortie nulle » et les pannes RPF.

```
<#root>
```

```
R1#
```

```
show ip mroute count
```

```
IP Multicast Statistics
  routes using 2406 bytes of memory
  2 groups, 1.00 average sources per group
  Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
  Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
  Group: 239.255.0.1, Source count: 2, Group pkt count: 11709
  RP-tree: Forwarding: 3/0/431/0, Other: 3/0/0
```

```
Source: 192.168.33.32/32, Forwarding: 11225/6/1401/62, Other: 11225/0/0
```

```
Source: 192.168.9.1/32, Forwarding: 481/0/85/0, Other: 490/0/9
```

```
Group: 224.0.1.40, Source count: 0, Group pkt count:
```

```
show ip route
```

Utilisez cette commande pour contrôler la table de routage de monodiffusion et résoudre les pannes RPF dans la table mroute.

```
<#root>
```

```
R2#
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
D   192.168.9.0/24 [90/307200] via 192.168.10.1, 00:59:45,    Ethernet0
C   192.168.10.0/24 is directly connected, Ethernet0
D   192.168.4.0/24 [90/11040000] via 192.168.7.1, 23:21:00,    Serial0
D   192.168.5.0/24 [90/11023872] via 192.168.7.1, 23:21:02,    Serial0
C   192.168.7.0/24 is directly connected, Serial0
D   192.168.33.0/16 [90/2195456] via 192.168.7.1, 1d23h, Serial0
D   192.168.1.0/24 [90/11552000] via 192.168.7.1, 22:41:27,    Serial0
```

```
show ip pim rp mapping
```

Utilisez cette commande pour contrôler l'affectation du RP par plage de groupe de multidiffusion et pour vérifier que la source d'apprentissage RP (statique ou de l'Auto-RP) et le mappage sont corrects. Si vous trouvez une erreur, contrôlez la configuration du routeur local ou la configuration de l'auto-RP.

```
<#root>
```

```
R1#
```

```
show ip pim rp mapping
```

```
    PIM Group-to-RP Mappings
```

```
Group(s) 224.0.1.40/32
```

```
  RP 192.168.7.2 (?), v1
```

```
    Info source: local, via Auto-RP
```

```
      Uptime: 2d00h, expires: never
```

```
Group(s): 224.0.0.0/4, Static
```

```
  RP: 192.168.7.2 (?)
```

## Commandes de débogage

Cette section est conçue pour vous montrer à quoi certaines sorties de commande debug doivent ressembler dans un réseau qui fonctionne. Lorsque vous dépannez, vous pouvez faire la distinction entre la sortie de débogage correcte et celle qui pointe vers un problème dans votre réseau. Pour de plus amples informations sur ces commandes debug, reportez-vous à [la référence de débogage des commandes de Cisco IOS](#).

```
debug ip igmp
```

Utilisez la commande debug ip igmp pour afficher des paquets IGMP reçus et transmis aussi bien que les événements relatifs à l'hôte IGMP. La forme non de cette commande désactive la sortie de débogage.

Cette sortie vous aide à découvrir si les processus IGMP fonctionnent. Généralement, si l'IGMP ne fonctionne pas, le processus du routeur ne découvre jamais un autre hôte sur le réseau qui est configuré pour recevoir des paquets de multidiffusion. En mode dense PIM, ceci signifie que les paquets sont livrés par intermittence (quelques-uns toutes les trois minutes). En mode intermédiaire PIM, ils ne sont jamais livrés.

```
<#root>
```

```
R1#
```

```
debug ip igmp
```

```
12:32:51.065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1
12:32:51.069: IGMP: Set report delay time to 9.4 seconds for 224.0.1.40 on Ethernet1
12:32:56.909: IGMP: Received v1 Report from 192.168.9.1 (Ethernet1) for 239.255.0.1
12:32:56.917: IGMP: Starting old host present timer for 239.255.0.1 on Ethernet1
12:33:01.065: IGMP: Send v2 Report for 224.0.1.40 on Ethernet1
12:33:01.069: IGMP: Received v2 Report from 192.168.9.4 (Ethernet1) for 224.0.1.40
12:33:51.065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1
```

Le résultat précédent montre que le routeur envoie une requête IGMP version 2 à l'interface Ethernet 1 à l'adresse de multidiffusion 224.0.0.1 (Tous les systèmes de multidiffusion sur ce sous-réseau). L'interface Ethernet 1 elle-même est membre du groupe 224.0.1.40 (vous pouvez utiliser la commande [show ip igmp interface](#) pour le déterminer), qui définit un délai de rapport de 9,4 secondes (déterminé aléatoirement). Puisqu'elle ne reçoit aucun rapport d'un autre système pour un groupe de multidiffusion 224.0.1.40 dans les 9,4 secondes suivantes, elle envoie un rapport version 2 de son adhésion, qui est reçu par le routeur qui se trouve lui-même sur Ethernet 1. Elle reçoit également la version 1 du rapport IGMP de l'hôte 192.168.9.1, qui est directement connecté à l'interface Ethernet 1 pour le groupe 239.255.0.1.

Cette sortie de débogage est utile lorsque vous vérifiez que l'interface du routeur envoie des requêtes et pour déterminer l'intervalle de requête (dans le cas précédent, 60 secondes). Vous pouvez également utiliser la commande pour déterminer la version de l'IGMP utilisée par les clients.

## debug ip mpacket

Utilisez la commande `debug ip mpacket` pour afficher tous les paquets de multidiffusion reçus et transmis . La forme non de cette commande désactive la sortie de débogage.

```
<#root>
```


```
R1#
```

```
debug ip mpacket 239.255.0.1 detail
```

```
13:09:55.973: IP: MAC sa=0000.0c70.d41e (Ethernet0), IP last-hop=192.168.10.2
13:09:55.977: IP: IP tos=0x0, len=892, id=0xD3C1, ttl=12, prot=17
13:09:55.981: IP: s=192.168.33.32 (Ethernet0) d=239.255.0.1 (Ethernet1) len 906, mforward
```

Cette commande décode le paquet de multidiffusion et montre si le paquet est expédié (mforward) ou abandonné. Il est utile quand vous déboguez des problèmes de flux de paquet dans le réseau pour rechercher la valeur TTL et la raison pour laquelle un paquet a été abandonné.

---

 Attention : soyez prudent lorsque vous activez la sortie de débogage au niveau du paquet, en particulier lorsque le routeur traite des chargements de paquets multicast élevés.

---



## debug ip mrouting

Cette commande est utile à des fins d'entretien de la table de routage. Utilisez-la pour vérifier que la mroute (S, G) est installée dans la table de mrouage, ou savoir pourquoi au cas contraire. L'information clé dans cette sortie est l'interface RPF. S'il y a une panne de contrôle RPF, la mroute (S, G) échoue à s'installer dans la table de mrouage.

```
<#root>
```

```
R1#
```

```
debug ip mrouting 239.255.0.1
```

```
13:17:27.821: MRT: Create (*, 239.255.0.1), RPF Null, PC 0x34F16CE  
13:17:27.825: MRT: Create (192.168.33.32/32, 239.255.0.1), RPF Ethernet0/192.168.10.2,  
PC 0x34F181A  
13:17:30.481: MRT: Create (192.168.9.1/32, 239.255.0.1), RPF Ethernet1/0.0.0.0,  
PC 0x34F18
```

## debug ip pim

Utilisez la commande debug ip pim pour afficher des paquets PIM reçus et transmis aussi bien que les événements relatifs au PIM. La forme non de cette commande désactive la sortie de débogage.

Cette section utilise un exemple pour vous aider à comprendre la sortie de débogage du mode intermédiaire PIM et montrer une sortie de débogage habituelle.

Voici la sortie du debug ip pim sur R1 :

```
<#root>
```

```
R1#
```

```
debug ip pim
```

```
PIM: Send v2 Hello on Ethernet0  
PIM: Send v2 Hello on Ethernet1  
PIM: Received v2 Hello on Ethernet0 from 192.168.10.2  
PIM: Send v2 Hello on Ethernet0  
PIM: Send v2 Hello on Ethernet1  
PIM: Building Join/Prune message for 239.255.0.1  
PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit  
PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)  
PIM: Received RP-Reachable on Ethernet0 from 192.168.7.2 for group 239.255.0.1  
PIM: Update RP expiration timer (270 sec) for 239.255.0.1
```

Voici ce que chaque ligne de sortie indique : R1 et R2 établissent des voisins PIM lorsque des messages Hello sont échangés. Ces messages Hello périodiques, échangés à Intervalle-Requête

secondes entre R1 (E0) et R2 (E0), gardent une trace des voisins PIM.

R1 envoie un message Joindre/Élaguer à l'adresse RP 192.168.7.2. Le RP (R2) répond avec un message RP accessible reçu à R1 pour le groupe 239.255.0.1. Ceci met à jour consécutivement le temporisateur d'expiration RP à R1. Le minuteur d'expiration définit un point de contrôle pour s'assurer que le RP existe toujours ; sinon, un nouveau RP doit être découvert. Utilisez la commande `show ip pim rp` pour observer le temps d'expiration du RP.

Maintenant, regardez la sortie de débogage entre R1 et R2 quand un récepteur de multidiffusion pour groupe 239.255.0.1 joint R1.

D'abord, regardez la sortie sur R1 :

```
<#root>
```

```
1
```

```
PIM: Check RP 192.168.7.2 into the  
(*, 239.255.0.1) entry
```

```
2
```

```
PIM:
```

```
send v2 Join
```

```
on Ethernet0 to 192.168.10.2 for (192.168.8.7.2/32, 239.255.0.1), WC-bit, RPT-bit, S-bit
```

```
3
```

```
PIM: Building batch join message for 239.255.0.1
```

```
4
```

```
PIM: Building Join/Prune message for 239.255.0.1
```

```
5
```

```
PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit
```

```
6
```

```
PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)
```

```
7
```

```
PIM: Received RP-Reachable on Ethernet0 from 192.168.7.2 : for group 239.255.0.1
```

```
8
```

```
PIM: Update RP expiration timer (270 sec) for 239.255.0.1
```

```
9
```

```
PIM: Building Join/Prune message for 239.255.0.1
```

```
10
```

```
PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit
```

```
11
```

PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)

Maintenant, regardez la sortie sur R2 :

<#root>

12

PIM:

Received v2 Join/Prune on Ethernet0 from 192.168.10.1

, to us

13

PIM: Join-list: (\*, 239.255.0.1) RP 192.168.7.2

14

PIM: Check RP 192.168.7.2 into the (\*, 239.255.0.1) entry, RPT-bit set, WC-bit set, S-bit set

15

PIM:

Add Ethernet0/192.168.10.1 to (\*, 239.255.0.1), Forward state

16

PIM: Building Join/Prune message for 239.255.0.1

17

PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us

18

PIM: Join-list: (\*, 239.255.0.1) RP 192.168.7.2, RPT-bit set, WC-bit set, S-bit set

19

PIM: Add Ethernet0/192.168.10.1 to (\*, 239.255.0.1), Forward state

20

PIM: Building Join/Prune message for 239.255.0.1

21

PIM:

Send RP-reachability for 239.255.0.1 on Ethernet0

22

PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us

23

PIM: Join-list: (\*, 239.255.0.1) RP 192.168.7.2, RPT-bit set, WC-bit set, S-bit set

24

PIM: Add Ethernet0/192.168.10.1 to (\*, 239.255.0.1), Forward state

PIM: Building Join/Prune message for 239.255.0.1

Dans la ligne 1 précédente, le récepteur de multidiffusion du groupe 239.255.0.1 rejoint R1. Ceci installe une entrée (\*, 239.255.0.1) dans la table mroute. Ensuite, dans la ligne 2, le récepteur de multidiffusion envoie une jointure IGMP à R2 (RP) pour joindre l'arborescence partagée.

Quand la jointure IGMP arrive sur R2, R2 installe le mroute (\*, 239.255.0.1), selon les indications des lignes 12 à 15 de la sortie R2.

Une fois que R2 a installé (\*, 239.255.0.1) dans sa table de mrouting, il ajoute l'interface à partir de laquelle il a reçu le message Join/Prune à sa liste d'interfaces sortantes (OIL) à l'état de transmission. Il renvoie alors un message d'accessibilité RP sur l'interface sur laquelle il a reçu le message Joindre/Élaguer. Cette transaction est montrée dans les lignes 15 à 21 de la sortie R2.

R1 reçoit le message RP-accessible pour le groupe 239.255.0.1 et met à jour son temporisateur d'expiration pour RP. Cet échange se répète une fois par minute par défaut et régénère son état de transmission de multidiffusion comme indiqué dans les lignes 7 et 8 de la sortie R1.

Dans les lignes suivantes, la sortie de débogage entre R2 (RP) et R3 est vue. La source (directement connectée à R3) a commencé à envoyer des paquets pour le groupe 239.255.0.1.

D'abord, regardez la sortie sur R3 :

```
<#root>
```

```
1
```

```
PIM:
```

```
Check RP 192.168.7.2 into the (*, 239.255.0.1) entry
```

```
2
```

```
PIM: Building Join/Prune message for 239.255.0.1
```

```
3
```

```
PIM: For RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit
```

```
4
```

```
PIM: Send periodic Join/Prune to RP via 192.168.7.2 (Serial4/0)
```

```
5
```

```
PIM: Received RP-Reachable on Serial4/0 from 192.168.7.2
```

```
6
```

```
PIM: Update RP expiration timer (270 sec) for 239.255.0.1
```

```
7
```

```
PIM: Send Register to 192.168.7.2 for 192.168.33.32, group 239.255.0.1
```

8

PIM: Send Register to 192.168.7.2 for 192.168.33.32, group 239.255.0.1

9

PIM: Received Join/Prune on Serial4/0 from 192.168.7.2

10

PIM: Join-list: (192.168.33.32/32, 239.255.0.1), S-bit set

11

PIM: Add Serial4/0/192.168.7.2 to (192.168.33.32/32, 239.255.0.1), Forward state

12

PIM:

Received Register-Stop on Serial4/0 from 192.168.7.2

13

PIM: Clear register flag to 192.168.7.2 for (192.168.33.32/32, 239.255.0.1)

14

PIM: Received Register-Stop on Serial4/0 from 192.168.7.2

15

PIM: Clear register flag to 192.168.7.2 for (192.168.33.32/32, 239.255.0.1)

Voici la sortie de R2, RP :

<#root>

16

PIM:

Received Join/Prune on Serial0 from 192.168.7.1

, to us

17

PIM:

Send RP-reachability for 239.255.0.1 on Serial0

18

PIM: Received Register on Serial0 from 192.168.7.1 for 192.168.33.32, group 239.255.0.1

19

PIM: Forward decapsulated data packet for 239.255.0.1 on Ethernet0

10

PIM: Forward decapsulated data packet for 239.255.0.1 on Serial0  
21  
PIM: Send Join on Serial0 to 192.168.7.1 for (192.168.33.32/32, 239.255.0.1), S-bit  
22  
PIM: Send Join on Serial0 to 192.168.7.1 for (192.168.33.32/32, 239.255.0.1), S-bit  
23  
PIM:  
Send Register-Stop to 192.168.7.1 for 192.168.33.32, group 239.255.0.1  
24  
PIM: Received Join/Prune on Serial0 from 192.168.7.1, to us  
25  
PIM: Prune-list: (192.168.33.32/32, 239.255.0.1)  
26  
PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us  
27  
PIM: Join-list: (\*, 239.255.0.1) RP 192.168.7.2, RPT-bit set, WC-bit set, S-bit set  
28  
PIM: Add Ethernet0/192.168.10.1 to (\*, 239.255.0.1), Forward state  
29  
PIM: Add Ethernet0/192.168.10.1 to (192.168.33.32/32, 239.255.0.1)  
30  
PIM: Join-list: (192.168.33.32/32, 239.255.0.1), S-bit set  
31  
PIM: Add Ethernet0/192.168.10.1 to (192.168.33.32/32, 239.255.0.1), Forward state  
32  
PIM: Building Join/Prune message for 239.255.0.1  
33  
PIM: For 192.168.7.1, Join-list: 192.168.33.32/32  
34  
PIM: For 192.168.10.1, Join-list: 192.168.9.1/32  
35  
PIM: Send v2 periodic Join/Prune to 192.168.10.1 (Ethernet0)  
36  
PIM: Send periodic Join/Prune to 192.168.7.1 (Serial0)  
37  
PIM: Received Join/Prune on Serial0 from 192.168.7.1, to us

38

PIM: Join-list: (\*, 239.255.0.1) RP 192.168.7.2, RP-bit set, WC-bit set, S-bit set

39

PIM: Add Serial0/192.168.7.1 to (\*, 239.255.0.1), Forward state

40

PIM: Add Serial0/192.168.7.1 to (192.168.33.32/32, 239.255.0.1)

41

PIM: Add Serial0/192.168.7.1 to (192.168.9.1/32, 239.255.0.1)

42

PIM: Join-list: (192.168.9.1/32, 239.255.0.1), S-bit set

43

PIM: Add Serial0/192.168.7.1 to (192.168.9.1/32, 239.255.0.1), Forward state

44

PIM: Join-list: (\*, 239.255.0.1) RP 192.168.7.2, RP-bit set, WC-bit set, S-bit set

45

PIM: Add Serial0/192.168.7.1 to (\*, 239.255.0.1), Forward state

La ligne 1 indique que R3, qui est directement connecté via Ethernet0/0 à la source, reçoit le trafic de multidiffusion pour le groupe 239.255.0.1. Elle crée l'entrée (\*, 239.255.0.1) et envoie un message Joindre au RP.

Les lignes 16 et 17 montrent ce R2, qui est RP, reçoit également le message Joindre/Élaguer et renvoie les informations d'accessibilité RP à R3.

Dans les lignes 5 et 6, R3 met à jour son temporisateur d'expiration RP après avoir reçu l'information RP accessible. Les lignes 7 et 8 précédentes montrent que R3 utilise son entrée (\*, G) pour envoyer les données au RP encapsulé dans un paquet Register avec la source qui initie la transmission au groupe 239.255.0.1.

Les lignes 18 20 montrent que R2 a reçu le paquet de registre, l'a décapsulé et expédié dans l'arbre avec une entrée de préexistence (\*, 239.255.0.1) dans la table de routage.

Les lignes 21 et 29 montrent que R2 envoie un message Joindre vers R3 et installe une entrée (S, G) (192.168.33.32, 239.255.0.1) dans la table mroute.

Les lignes 9 à 11 montrent que R3 reçoit le message Joindre de R2, installe une entrée (S, G) (192.168.33.32,239.255.0.1) dans la table mroute et place l'interface connectée à RP en mode transmission, qui construit l'arbre de multidiffusion SPT (S, G) vers la source.

Dans la ligne 23, R2 commence à recevoir du trafic (S, G) sur le SPT et envoie un message d'Arrêt-Registre (et un message Joindre) vers la source.

Les lignes 12 à 15 montrent que R3 reçoit le message d'arrêt-registre, efface l'indicateur de registre et arrête le trafic (S, G) d'encapsulation.

Les messages périodiques Joindre/Élaguer sont échangés entre RP et R3 pour entretenir l'arbre de multidiffusion.

## Informations connexes

- [Guide de dépannage de multidiffusion IP](#)
- [Guide de configuration pour le démarrage rapide de la multidiffusion](#)
- [Page de support de multidiffusion IP](#)
- [Page de support pour le routage 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.