Dépannage des réseaux multidiffusion avec les outils CLI

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Conventions
  - Stratégies de dépannage
  - Vérifier le flux de paquets source
  - Vérifier la signalisation réseau
  - Dépannage du mode intermédiaire PIM
  - Vérifier le flux de paquets réseau
  - Signalisation Du Récepteur De Contrôle
  - Contrôler le flux de paquets du récepteur
  - Outils Power CLI
  - Mstat
  - Mrinfo
  - Mtrace
  - Ping
  - 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 outils et les techniques de dépannage d'un réseau multidiffusion.

Conditions préalables

Exigences

Ce document nécessite une connaissance de la multidiffusion IP, du protocole IGMP (Internet Group Management Protocol), du protocole PIM (Protocol Independent Multicast) et du protocole RPF (Reverse Path Forwarding).

Composants utilisés

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



Remarque : La disponibilité, la syntaxe et le résultat des commandes de ce document varient selon la plate-forme et la version du logiciel Cisco. Les exemples utilisent les résultats des commandes Cisco IOS® et Cisco IOS XE®.

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

Lorsque vous dépannez des réseaux de multidiffusion, tenez compte du protocole de signalisation utilisé dans le réseau et le flux de paquets. Le protocole de signalisation est utilisé pour configurer et supprimer des sessions de multidiffusion (telles que le mode dense PIM, le mode intermédiaire PIM et le protocole DVMRP). Le flux de paquets envoie, réplique et reçoit les paquets de multidiffusion entre la source et le récepteur, en fonction de la table de transfert créée par le processus de signalisation.

Ce tableau organise les contrôles de signalisation et de flux de paquets pour la source, le réseau et les récepteurs :

	Source	Réseau	Récepteurs
Signalisation	S/O	Vérifier la signalisation réseau	Signalisation Du Récepteur De Contrôle
Flux de paquets	Vérifier le flux de paquets source	Vérifier le flux de paquets réseau	Contrôler le flux de paquets du récepteur

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

Vérifier 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. Vérifiez les compteurs d'interface sur l'hôte. Tout d'abord, vérifiez les compteurs d'interface (si vous êtes sur un système UNIX, exécutez la commande netstat) sur l'hôte source pour voir s'il envoie des paquets. Si ce n'est pas le cas, recherchez les erreurs de configuration ou les bogues dans la pile hôte et l'application.

2. Exécutez la commande show ip igmp groups <interface-name> pour vérifier que le routeur a reçu un rapport d'appartenance IGMP sur cette interface.

3. Vérifiez la valeur de durée de vie des paquets dans l'application de multidiffusion. Il doit être au moins égal à 2 pour traverser un saut routé. Si l'application envoie des paquets avec une valeur de durée de vie de 1, le premier routeur en amont abandonne les paquets lorsque la durée de vie expire. Pour vérifier, exécutez la commande show ip traffic et recherchez une augmentation de la

valeur du compteur « mauvais nombre de sauts ». Tout paquet avec une valeur TTL de 1, ou inférieure au seuil TTL défini par l'interface avec la commande ip multicast ttl-threshold est abandonné et le compteur « bad hop-count » est augmenté de un. Exécutez la commande show ip igmp interface <interface-name> pour afficher la valeur de seuil de durée de vie de l'interface.

4. Exécutez les commandes show ip mroute count et show ip mroute active pour vérifier le premier routeur ou commutateur en amont pour voir s'il voit des paquets de multidiffusion de la source. La sortie de la commande affiche les statistiques de flux de trafic pour chaque paire (S, G). Si vous n'observez aucun trafic, continuez à vérifier l'application source, la pile hôte, la capture de paquets et l'interface du routeur de premier saut.

5. Exécutez la commande debug ip mpacket sur le routeur en amont le plus proche, avec un filtre de groupe de multidiffusion ou de liste d'accès (ACL) prise en charge et le mot clé detail pour obtenir des informations supplémentaires sur les paquets et la granularité.



Remarque : Exécutez cette commande avec précaution en cas de trafic de multidiffusion important sur le réseau. Si nécessaire seulement, exécutez la commande debug ip mpacket sur le routeur. Exécutez l'argument detail pour afficher les en-têtes de paquet dans la sortie de débogage, et les listes d'accès pour vérifier le trafic provenant de sources spécifiques. N'oubliez pas que cette commande peut avoir de graves répercussions sur les performances d'autres trafics.

Vérifier la signalisation réseau

Il s'agit de l'élément le plus complexe et le plus important à dépanner dans un réseau. Elle dépend du protocole de signalisation réseau utilisé, tel que le mode intermédiaire PIM, le mode dense PIM et le protocole DVMRP. Cisco recommande l'approche en plusieurs étapes décrite dans cette section.

Dépannage du mode intermédiaire PIM

Complétez ces étapes pour dépanner le mode intermédiaire PIM :

1. Vérifiez que le routage multidiffusion IP est activé sur tous les routeurs multidiffusion.

2. Exécutez 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 possible de connectivité et de compteur qui peut empêcher l'établissement des voisins PIM. Si nécessaire,

exécutez les commandes d'interface ip pim version {1 | 2} et ip pim {dense-mode | mode intermédiaire | sparse-dense-mode} pour configurer la version et le mode PIM requis.

3. Exécutez la commande show ip pim rp mapping pour assurer le mappage correct du groupe RP et pour vérifier le minuteur d'expiration si auto-RP est configuré. Exécutez la commande debug ip pim auto-rp pour identifier les échecs Auto-RP. Si vous ne voyez pas de mappages PIM Group-to-RP, vérifiez la configuration auto-RP, ou configurez des mappages statiques group-to-RP avec la commande ip pim rp-address <rp-address> [<access-list>] [override]. Configurez un RP candidat avec ip pim send-rp-announce <interface> scope <ttl> group-list <access-list> et configurez l'agent de mappage avec ip pim send-rp-discovery <interface> scope <ttl>. Ces commandes s'appliquent uniquement à Auto-RP : configurez send-rp-announce sur un RP candidat et send-rp-discovery sur un agent de mappage.

4. Exécutez la commande show ip rpf <isource-address> pour vérifier l'interface, le voisin et la route RPF pour l'adresse source. PIM abandonne les paquets de multidiffusion qui arrivent sur une interface non-RPF. Le traitement supplémentaire d'assertion ou d'élagage dépend du mode PIM et du type d'interface. La commande debug ip pim permet d'identifier les raisons possibles d'une panne dans un réseau PIM. Comparez le résultat observé avec le résultat type de ce document. Exécutez cette sortie pour identifier les trois étapes discrètes en mode intermédiaire PIM : connexion, enregistrement et basculement SPT. La commande show ip mroute vous permet de surveiller les entrées null dans les listes d'interfaces sortantes et les entrées élaguées dans la table mroute.

Vérifier le flux de paquets réseau

Utilisez ces commandes pour contrôler le flux des paquets de multidiffusion sur le réseau :

- Exécutez 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

Signalisation Du Récepteur De Contrôle

Suivez ces étapes pour vérifier la signalisation du récepteur :

1. Exécutez la commande show ip igmp groups au premier routeur en amont connecté au récepteur pour vérifier l'appartenance du groupe appris par le routeur sur l'interface orientée récepteur.

2. Exécutez la commande ping pour vérifier l'accessibilité de l'hôte et du premier routeur en amont.

3. Exécutez la commande show ip igmp interface pour vérifier la version IGMP de l'interface.

Remarque : Assurez-vous que le routeur et les récepteurs utilisent des versions IGMP compatibles. Un routeur IGMPv1 ne traite pas les rapports d'appartenance à IGMPv2. Lorsqu'un récepteur IGMPv2 détecte un demandeur IGMPv1, il utilise le mode de compatibilité IGMPv1 et envoie des rapports d'appartenance IGMPv1.

---

4. Exécutez la commande debug ip igmp pour dépanner davantage la signalisation du récepteur.

Contrôler le flux de paquets du récepteur

Effectuez ces étapes pour vérifier le flux de paquets du récepteur :

1. Exécutez 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. Utilisez une capture de paquets sur l'interface du destinataire afin d'identifier les paquets de multidiffusion en double sur un segment à accès multiple.

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 affiche le chemin de multidiffusion au format graphique ASCII. Il suit le chemin entre deux points du réseau, indique les abandons et les doublons, les durées de vie et les délais à chaque noeud du réseau.

Cela est 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. Une valeur d'abandon calculée négative indique que l'interface en aval signale plus de paquets que l'interface en amont, ce qui peut indiquer des paquets en double ou des différences de contre-échantillonnage.

<#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   Lost/Sent = Pct  Rate     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 affiche les informations du routeur voisin de multidiffusion, les capacités du routeur et la version du code, les informations de l'interface de multidiffusion, les seuils de durée de vie, les mesures, le protocole et l'état. Cela est utile lorsque vous devez vérifier les voisins de multidiffusion, confirmer la contiguïté de voisinage bidirectionnelle et vérifier que les tunnels sont actifs 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 de la sortie indiquent :

- P = Prune-capable
- M = Compatible Mtrace
- S = compatible SNMP
- A = Compatible avec le protocole Auto-RP

Mtrace

Cette commande affiche le chemin de multidiffusion de la source au récepteur, et elle trace le chemin entre les points dans les réseaux, qui montre les seuils TTL et le délai à chaque noeud.

Lors du dépannage, exécutez 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
```

Ping

Lorsque vous dépannez, la commande ping est un moyen simple de générer du trafic de multidiffusion dans les travaux pratiques pour tester l'arborescence de multidiffusion parce que les membres de groupe accessibles qui traitent des requêtes d'écho ICMP de multidiffusion peuvent répondre.

<#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 lorsque vous dépannez un problème de multidiffusion. Référez-vous au Guide de configuration de multidiffusion IP, Cisco IOS XE 17.x pour plus d'informations.



Conseil : Si les réponses de la commande show sont lentes, le routeur peut effectuer des recherches de domaine IP pour les adresses dans le résultat de la commande. Vous pouvez désactiver la recherche de domaine IP en exécutant la commande no ip domain lookup en mode de configuration globale. Cela arrête la recherche de domaine IP et augmente la vitesse de sortie de la commande show.

---

show ip igmp groups

Cette commande indique quels groupes de multidiffusion sont directement connectés au routeur et lesquels sont appris via le protocole IGMP (Internet Group Management Protocol). Vous pouvez utiliser cette commande pour vérifier qu'un récepteur ou une interface de routeur jointe localement a rejoint le groupe cible sur l'interface de 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 pouvez voir un dernier rapporteur pour chaque entrée de groupe et d'interface.

<#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

Exécutez 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

Exécutez 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          Interface               Uptime/Expires    Ver   DR
Address                                                           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 sur laquelle un voisin PIM a été détecté.
- Uptime : temps de disponibilité total d'un voisin.
- Expire : délai avant l'expiration d'un voisin et jusqu'à la réception du prochain Hello PIM.
- Ver : version de PIM sur l'interface voisine.
- DR Prio : les valeurs possibles sont comprises entre 0 et 4294967294 ou N.
    - Il s'agit d'une nouvelle colonne qui suit la priorité d'une interface PIM pour la sélection du DR. La fonctionnalité permettant de configurer un routeur désigné en fonction de la priorité la plus élevée par rapport à l'adresse IP la plus élevée a été introduite dans les versions 12.1(2)T et 12.2 du logiciel Cisco IOS® et dans les images Cisco IOS® avec Bidir-PIM. Vous pouvez exécuter la commande d'interface ip pim dr-priority <0-4294967294> pour définir la priorité du routeur désigné. La priorité DR par défaut est définie sur 1.
    - Pour l'interopérabilité, si un voisin PIM exécute une version antérieure de Cisco IOS® qui ne prend pas en charge la fonctionnalité de priorité DR, la colonne « DR Prior » indique N. Si un routeur du réseau à accès multiple n'annonce pas l'option de priorité DR, la sélection DR utilise l'adresse IP principale la plus élevée parmi tous les routeurs PIM de ce réseau.
- Mode : informations sur le DR et d'autres fonctionnalités PIM.

  Cette colonne répertorie le DR en plus de toutes les fonctionnalités prises en charge par le voisin PIM :

DR - Le voisin PIM est le routeur désigné

B - Compatible PIM bidirectionnel (Bidir-PIM)

S - Fonction d'actualisation d'état (s'applique uniquement au mode dense)

Lorsque vous dépannez, utilisez cette commande pour vérifier que tous les voisins sont actifs et qu'ils utilisent le mode, la version et le minuteur d'expiration appropriés. Vous pouvez également vérifier la configuration du routeur, ou utiliser la commande show ip pim interface pour vérifier le mode (PIM sparse ou dense mode). Utilisez la commande debug ip pim pour observer l'échange de messages pim-query.

---

show ip pim interface

Exécutez cette commande pour afficher des informations sur les interfaces configurées pour PIM. En outre, vous pouvez exécuter cette commande pour vérifier que le mode PIM correct (dense ou clairsemé) est configuré sur l'interface, que le nombre de voisins est correct et que le routeur désigné (DR) est correct (ce qui est essentiel pour le mode clairsemé PIM). Les segments à accès multiple (tels qu'Ethernet, Token Ring et FDDI) sélectionnent un routeur désigné en fonction de la priorité de routeur désigné annoncée la plus élevée, l'adresse IP principale la plus élevée étant utilisée comme point de rupture. Si un routeur n'annonce pas la priorité du routeur désigné, la sélection utilise l'adresse IP principale la plus élevée. Les liaisons point à point n'affichent pas les informations de DR.

<#root>

```
R1#

show ip pim interface


Address          Interface          Version/Mode    Nbr   Query     DR
                                                    Count Intvl
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

Exécutez cette commande pour afficher le contenu résumé de la table de routage de multidiffusion IP. Vous pouvez également l'utiliser pour vérifier le ou les groupes de multidiffusion actifs 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

Exécutez cette commande pour afficher le contenu complet de la table de routage de multidiffusion IP. Lors du dépannage, exécutez cette commande pour vérifier :

- Les entrées d'état (S, G) et (*, G) des indicateurs.
- L’interface entrante est correcte. Si ce n'est pas le cas, vérifiez la table de routage de monodiffusion.
- La ou les interfaces sortantes sont correctes. Si l’élagage est incorrect, vérifiez l’état du 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: SJPCL
  Incoming interface: Ethernet0, RPF nbr 192.168.10.2
  Outgoing interface list: Null
```

---

show ip mroute active

Exécutez cette commande pour afficher les sources et les groupes de trafic actifs au-delà du seuil. Lorsque vous effectuez un dépannage, utilisez-le pour vérifier les paires source-groupe actives, le débit de trafic pour chaque entrée (S, G) qui dépasse le seuil configuré et 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

Exécutez cette commande pour afficher comment le routage de multidiffusion IP exécute le protocole RPF (Reverse Path Forwarding). Lors du dépannage, utilisez-le pour vérifier que les informations RPF sont correctes. Si ce n’est pas le cas, vérifiez l’adresse source dans la table de routage de monodiffusion. Exécutez également les commandes ping et trace sur l'adresse source pour vérifier le fonctionnement du routage de monodiffusion. 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

Sur les versions de Cisco IOS® qui prennent en charge le cache de commutation rapide multidiffusion, cette commande affiche les entrées du cache et permet d'isoler les problèmes de commutation rapide. Sur les plates-formes Cisco IOS XE® plus récentes, exécutez la commande show ip mfib pour afficher les informations de transfert multidiffusion.

<#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

Exécutez cette commande pour vérifier que le trafic de multidiffusion est reçu et pour vérifier ses débits et abandons. Si aucun trafic n'est reçu, travaillez de la source au récepteur jusqu'à ce que vous trouviez où le trafic s'arrête. Vous pouvez également exécuter cette commande pour vérifier que le trafic est transféré. Si ce n'est pas le cas, exécutez la commande show ip mroute pour rechercher « Null Outgoing interface list » et les échecs 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

Exécutez cette commande pour vérifier la table de routage de monodiffusion et corriger les échecs 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

Exécutez cette commande pour vérifier l'attribution RP par plage de groupes de multidiffusion et pour vérifier la source de l'apprentissage RP (statique ou auto-RP) et le mappage est correct. Si vous trouvez une erreur, vérifiez la configuration du routeur local ou la configuration 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 ce qui pointe vers un problème dans votre réseau. Pour plus d'informations sur ces commandes de débogage, référez-vous à Référence des commandes de débogage de Cisco IOS.

---

debug ip igmp

Exécutez la commande debug ip igmp pour afficher les paquets IGMP reçus et transmis, ainsi que les événements liés à l'hôte IGMP. La forme no de cette commande désactive la sortie de débogage.

Cette sortie vous aide à découvrir si les processus IGMP fonctionnent. En général, si IGMP ne fonctionne pas, le routeur n'apprend pas l'appartenance au groupe de récepteurs sur l'interface connectée. En mode dense PIM, l'inondation initiale peut envoyer du trafic sur le segment jusqu'à ce que l'élagage le supprime. En mode intermédiaire PIM, le routeur n'ajoute pas l'interface orientée récepteur à la liste des interfaces sortantes sans appartenir au destinataire ou sans autre exigence de transfert local.

<#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 exécuter la commande show ip igmp interface pour le déterminer), qui définit un délai de rapport de 9,4 secondes (déterminé aléatoirement). Étant donné qu'il ne reçoit aucun rapport d'un autre système pour le groupe de multidiffusion 224.0.1.40 pendant les 9,4 secondes suivantes, il envoie un rapport de version 2 de son appartenance, qui est reçu par le routeur lui-même sur Ethernet 1. Il reçoit également le rapport IGMP version 1 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 d'IGMP utilisée par les clients.

---

debug ip mpacket

Exécutez la commande debug ip mpacket pour afficher tous les paquets de multidiffusion IP reçus et transmis. La forme no 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 indique si le paquet est transféré (mforward) ou abandonné. Cela est utile lorsque vous déboguez des problèmes de flux de paquets dans le réseau pour examiner la valeur de durée de vie et la raison pour laquelle un paquet a été abandonné.

⚠ Mise en garde : Soyez prudent lorsque vous activez la sortie de débogage au niveau paquet, en particulier lorsque le routeur traite des chargements de paquets multidiffusion élevés.

---

debug ip mrouting

Cette commande est utile pour la maintenance de la table de routage. Utilisez-le pour vérifier que le mroute (S, G) est installé dans la table de routage de multidiffusion IP ou, si ce n'est pas le cas, pourquoi. Les informations clés dans ce résultat sont l'interface RPF. En cas d'échec du contrôle RPF, le mroute (S, G) ne s'installe pas dans la table de mrouting.

<#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

Exécutez la commande debug ip pim pour afficher les paquets PIM reçus et transmis, ainsi que les événements liés à PIM. La forme no 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 pour montrer une sortie de débogage typique.

Voici le résultat de la commande 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 Reçu accessible à R1 pour le groupe 239.255.0.1. Ceci met à jour à son tour le minuteur d'expiration du RP sur 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. Exécutez la commande show ip pim rp pour observer le délai d'expiration du RP.

Maintenant, regardez la sortie de débogage entre R1 et R2 quand un récepteur de multidiffusion pour le groupe 239.255.0.1 rejoint R1. Tout 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 (192.168.7.2/32, 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
```

25

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

Dans la ligne 1 précédente, le récepteur de multidiffusion pour le groupe 239.255.0.1 rejoint R1. Une entrée (*, 239.255.0.1) est ainsi installée 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.

Lorsque la jonction/élagage PIM arrive sur R2, R2 installe une mroute (*, 239.255.0.1), comme indiqué aux lignes 12 à 15 de la sortie de 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 ensuite un message d'accessibilité RP sur l'interface à laquelle il a reçu le message Join/Prune. Cette transaction est indiquée aux lignes 15 à 21 de la sortie de R2. R1 reçoit le message RP-reachable pour le groupe 239.255.0.1 et met à jour son compteur d'expiration pour RP. Cet échange se répète une fois par minute par défaut et actualise son état de transmission multidiffusion comme indiqué aux lignes 7 et 8 de la sortie de 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 au groupe 239.255.0.1.

Commencez par examiner le résultat 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, le 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

20

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 montre que R3, qui est directement connecté via Ethernet0/0 à la source, associe le RP 192.168.7.2 à l'entrée (*, 239.255.0.1), et les lignes 2 à 4 montrent que R3 envoie une jointure vers le RP. Les lignes 7 et 8 montrent que R3 reçoit le trafic source et envoie des messages de registre PIM au RP.

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

- Sur les lignes 5 et 6, R3 met à jour son compteur d'expiration RP après avoir reçu les informations d'accessibilité RP. Les lignes 7 et 8 montrent que R3, le DR source, encapsule les paquets de la source 192.168.33.32 dans les messages du registre PIM et les envoie au RP pour le groupe 239.255.0.1.

- Les lignes 18 à 20 indiquent que R2 a reçu le paquet Register, l'a désencapsulé et l'a transmis à l'arborescence avec une entrée préexistante (*, 239.255.0.1) dans la table de routage.

- Les lignes 21 et 29 indiquent que R2 envoie un message Join 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 Join de R2, installe une entrée (S, G) (192.168.33.32,239.255.0.1) dans la table mroute et définit l'interface connectée à RP en mode de transfert, qui construit l'arborescence SPT de multidiffusion (S, G) vers la source.

- Sur la ligne 23, R2 commence à recevoir (S, G) le trafic en aval de SPT et envoie un message Register-Stop (et un message Join) vers la source.

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

- Des messages Joindre/Élaguer périodiques sont échangés entre le RP et R3 pour maintenir l'arborescence de multidiffusion.

Informations connexes

- Guide de dépannage de la multidiffusion IP
- Guide de configuration de démarrage rapide de la multidiffusion
- Page d'assistance IP Multicast
- Page IP Routing Support
- 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.