

Herramientas de resolución de problemas de la multidifusión básica

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Estrategias de solución de problemas](#)

[Verifique el Flujo de Paquetes de Origen](#)

[Verificación de la señalización de la red](#)

[Herramientas de energía](#)

[mstat](#)

[mrinfo](#)

[mtrace](#)

[ping](#)

[Comandos 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 route](#)

[show ip mroute count](#)

[show ip route](#)

[show ip pim rp mapping](#)

[comandos debug](#)

[debug ip igmp](#)

[debug ip mpacket](#)

[debug ip mrouting](#)

[debug ip pim](#)

[Información Relacionada](#)

[Introducción](#)

Este documento explica las diferentes herramientas y técnicas para resolver los problemas que se

presentan en las redes multicast. Si comprende las diversas herramientas de interfaz de línea de comando y los campos de información clave en su resultado, podrá resolver los problemas que se presentan en la redes multicast.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Estrategias de solución de problemas

Al resolver problemas de las redes multicast, es bueno considerar el protocolo de señalización utilizado en la red y el flujo de paquetes. El protocolo de señalización se utiliza para configurar y para cerrar sesiones de multicast (tales como modo denso de PIM, modo disperso de PIM, y DVMRP), y el flujo de paquetes es el envío, la duplicación y la recepción reales de los paquetes de multicast entre el y el origen y el receptor, en función de la tabla de reenvío creada por el proceso de señalización.

Esta tabla ayuda a verificar la información de troubleshooting al comprobar que cada sección de la tabla funciona correctamente:

| | Fuente | Red | Receptores |
|-------------------|--|---|---|
| Señalización | NA | Verificación de la señalización de la red | Verificar la señal del receptor |
| Flujo de paquetes | Verifique el Flujo de Paquetes de Origen | Verifique el flujo de paquetes de la red | Verifique el flujo de paquetes del receptor |

Las subdivisiones siguientes detallan las herramientas de troubleshooting que puede utilizar para verificar y solucionar problemas frecuentes.

Verifique el Flujo de Paquetes de Origen

Siga estos pasos para determinar si el origen realmente distribuye los paquetes e inserta los campos correctos del paquete:

1. Verifique los contadores de la interfaz en el host. Primero, verifique los contadores de la interfaz (si está en un sistema UNIX, utilice el **comando netstat**) en el host de origen para ver si está enviando los paquetes. Si no lo está haciendo, verifique si la configuración es correcta o si hay bugs en la stack de host y la aplicación.
2. Utilice el **comando show ip igmp groups interface-name para** verificar el router ascendente y comprobar si recibió un informe de afiliación cuando la interfaz se conectó directamente con el origen.
3. Verifique el valor TTL en los paquetes de distribución de la aplicación; debe ser superior a 1. Si la aplicación envía los paquetes con un valor TTL inferior a 1, debe detectar el tráfico caído en el primer router ascendente. Para verificar, use el **comando show ip traffic** y busque un aumento en el valor del contador "conteo de saltos incorrectos". Cualquier paquete con un valor TTL de 1 o menor que el umbral TTL establecido por la interfaz con el **comando ip multicast ttl-threshold** se descarta y el contador "conteo de saltos incorrectos" aumenta un punto. Utilice el **comando show ip igmp interface interface-name** para determinar el valor del umbral TTL de la interfaz.
4. Use los comandos **show ip mroute count** y **show ip mroute active** para verificar el primer router ascendente o switch y determinar si detecta paquetes multicast del origen. El resultado del comando muestra la estadística de flujo de tráfico para cada par (S, G). Si no observa ningún tráfico, verifique la señalización del receptor.
5. Utilice el **comando debug ip mpacket** en el router ascendente más cercano, con el **detalle** o el argumento de granularidad **acl**. Utilice este comando con cautela cuando hay tráfico multicast pesado en la red. Solamente en caso necesario, utilice el **comando debug ip mpacket** en la ruta. Utilice el argumento de **detalle** para mostrar los encabezados del paquete en el **resultado de los debugs** y las listas de acceso para verificar si hay tráfico de los orígenes específicos. Recuerde que este comando puede tener un impacto negativo en el rendimiento en el otro tráfico, así que utilícelo con cautela.

Verificación de la señalización de la red

Ésta es la parte más compleja y más importante de troubleshooting en cualquier red. Depende del protocolo de señalización de la red utilizado, por ejemplo, el modo disperso de PIM, el modo denso de PIM y el DVMRP. Recomendamos el enfoque de varios pasos descrito en esta sección.

Solución de problemas de modo disperso de PIM

Complete estos pasos para resolver problemas del modo disperso de PIM:

1. Verifique si el ruteo IP multicast está habilitado en todos los routers de multicast.
2. Utilice el **comando show ip pim neighbor para** verificar el temporizador de vencimiento y el modo para asegurar el establecimiento correcto del vecino PIM, y busque cualquier problema de conectividad y de temporizador posibles que podrían inhibir el establecimiento de vecinos PIM. De ser necesario, use el subcomando del **nivel de interfaz ip pim [version] [dense-mode] [sparse-mode] [sparse-dense-mode]** para configurar la versión y el modo

correctos y establecer los vecinos PIM adecuados.

3. Utilice el [comando show ip pim rp mapping](#) para asegurar el mapeo RP-Group correcto y verificar el temporizador de vencimiento si auto-RP se configura. Utilice el **comando debug ip pim auto-rp** para determinar fallas auto-RP. Si no detecta ningún mapeo del grupo hacia RP del PIM, verifique la configuración auto-RP, o configure los mapeos estáticos Group-RP con el **comando ip pim rp-address ip address of RP [access-list] [named-accesslist] [override]**. La configuración auto-RP puede realizarse con los comandos **ip pim send-rp-announce interface-id scope TTL value** y **ip pim send-rp-discovery interface-id scope TTL value**. Estos comandos deben configurarse solamente si hay configuraciones auto-RP.
4. Use el [comando show ip rpf ip address of source para](#) verificar la falla de RPF para la dirección de origen. El modo denso de PIM y el modo disperso de PIM envían los mensajes de Eliminación al origen si el tráfico llega en una interfaz punto a punto que no es RPF. Las ayudas del [comando debug ip pim](#) identifican las razones posibles de un error en una red PIM — compara el resultado típico con lo que usted ve. Use este resultado para identificar las tres etapas discretas en el modo disperso de PIM: unión, registro y switchover de SPT. El [comando show ip mroute](#) permite que observe las entradas nulas en las listas de Interfaz Saliente y las entradas eliminadas en la tabla mroute.

[Verifique el flujo de paquetes de la red](#)

Utilice estos comandos para verificar el flujo de paquetes multicast a través de la red:

- multicast trace hop-by-hop con el [comando mtrace](#)
- [mstat](#)
- [ping](#)
- [show ip mroute count](#)
- [show ip mroute active](#)
- [debug ip mpacket](#)

[Verificar la señal del receptor](#)

Siga estos pasos para verificar la señalización del receptor:

1. Utilice el [comando show ip igmp groups](#) en el primer router ascendente conectado con el receptor para verificar que la interfaz se ha unido al grupo.
2. Utilice el [comando ping para](#) verificar el alcance del host y del primer router ascendente.
3. Utilice el [comando show ip igmp interface para](#) verificar la versión de IGMP de la interfaz. **Nota:** Recuerde que un router configurado con la versión de IGMP 1 considera los paquetes de la versión de IGMP 2 recibidos del host como inválidos. Estos paquetes IGMP no se unen al grupo hasta que el router recibe un paquete de la versión de IGMP 1 del host.
4. Utilice el [comando debug ip igmp](#) para resolver problemas con la señalización del receptor.

[Verifique el flujo de paquetes del receptor](#)

Siga estos pasos para verificar el flujo de paquetes del receptor:

1. Utilice el **comando netstat** en un sistema Unix para verificar las estadísticas de la interfaz del receptor.

2. Verifique que la pila IP/TCP se haya instalado y configurado correctamente.
3. Verifique que la aplicación del cliente receptor de multidifusión se haya instalado y configurado correctamente.
4. Observe si hay paquetes multicast duplicados en un segmento de multiacceso.

Herramientas de energía

Los comandos en esta sección también pueden ser útiles para resolver problemas, especialmente cuando prueba el flujo de paquetes de la red y encuentra puntos de falla en la red multicast. Para obtener información más completa sobre los comandos de la herramienta multicast, consulte los [Comandos de las Herramientas IP Multicast](#).

mstat

Este comando muestra la trayectoria multicast en el formato de gráfico ASCII. Traza la trayectoria entre dos puntos cualesquiera en la red, muestra los descartes y los duplicados, los TTL y los retrasos en cada nodo de la red. Es muy útil cuando usted necesita localizar los puntos de congestión en la red, o centrarse en un router con recuentos altos de descartes/duplicados. Los duplicados se indican en el resultado como descartes “negativos”.

```
Router# mstat lwei-home-ss2 171.69.58.88 224.0.255.255
Type escape sequence to abort
Mtrace from 171.69.143.27 to 171.69.58.88 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
171.69.143.27   171.69.62.144   All Multicast Traffic     From 171.69.143.27
|              ___/  rtt 48  ms   Lost/Sent = Pct Rate      To 224.0.255.255
v              /    hop 48  ms   -----
171.69.143.25   lwei-cisco-isdn.cisco.com
|              ^    ttl  1
v              |    hop 31  ms   0/12 = 0%      1 pps   0/1 = --%  0 pps
171.69.121.84
171.69.121.45   eng-frmt12-pri.cisco.com
|              ^    ttl  2
v              |    hop -17 ms   -735/12 = --%   1 pps   0/1 = --%  0 pps
171.69.121.4
171.69.5.27     eng-cc-4.cisco.com
|              ^    ttl  3
v              |    hop -21 ms   -678/23 = --%   2 pps   0/1 = --%  0 pps
171.69.5.21
171.69.62.130   eng-ios-2.cisco.com
|              ^    ttl  4
v              |    hop  5  ms   605/639 = 95%   63 pps  1/1 = --%  0 pps
171.69.62.144
171.69.58.65    eng-ios-f-5.cisco.com
|              \___  ttl  5
v              \    hop  0  ms     4         0 pps     0         0 pps
171.69.58.88    171.69.62.144
Receiver        Query Source
```

mrinfo

Este comando muestra la información del router vecino multicast, las capacidades del router y la

versión del código, información de la interfaz multicast, los umbrales TTL, la métrica, el protocolo y el estado. Es útil cuando necesita verificar los vecinos multicast, confirmar que existe adyacencia de vecinos bidireccional y verificar que los túneles estén activos en ambas direcciones.

```
Router# mrinfo
 192.1.7.37 (b.cisco.com) [version cisco 11.1] [flags: PMSA]:
 192.1.7.37 -> 192.1.7.34 (s.cisco.com) [1/0/pim]
 192.1.7.37 -> 192.1.7.47 (d.cisco.com) [1/0/pim]
 192.1.7.37 -> 192.1.7.44 (d2.cisco.com) [1/0/pim]
131.9.26.10 -> 131.9.26.9 (su.bbnplanet.net) [1/32/pim]
```

Los indicadores en el resultado muestran lo siguiente:

- P = prune-capable
- M = compatible con mtrace
- S = apto para SNMP
- A = compatible con Auto-RP

[mtrace](#)

Este comando muestra la trayectoria multicast desde el origen hacia el receptor, y localiza la trayectoria entre los puntos en las redes, que muestra los umbrales TTL y el retraso en cada nodo. Al resolver problemas, utilice el **comando mtrace** para encontrar dónde se detiene el flujo de tráfico multicast, para verificar la trayectoria del tráfico multicast y para identificar las trayectorias subóptimas.

```
Router# mtrace 171.69.215.41 171.69.215.67 239.254.254.254
Type escape sequence to abort.
Mtrace from 171.69.215.41 to 171.69.215.67 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
0 171.69.215.67
-1 171.69.215.67 PIM thresh^ 0 0 ms
-2 171.69.215.74 PIM thresh^ 0 2 ms
-3 171.69.215.57 PIM thresh^ 0 894 ms
-4 171.69.215.41 PIM thresh^ 0 893 ms
-5 171.69.215.12 PIM thresh^ 0 894 ms
-6 171.69.215.98 PIM thresh^ 0 893 ms
```

[ping](#)

Al resolver problemas, el **comando ping** es la manera más fácil de generar el tráfico multicast en el laboratorio para evaluar el árbol multicast debido a que hace ping con todos los miembros del grupo y todos los miembros responden.

```
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
```

[Comandos show](#)

Los comandos de esta sección lo ayudan a recopilar información útil al resolver un problema multicast. Consulte la [Guía de Referencia del Comando IP Multicast](#) para obtener información más completa sobre **estos comandos show**.

Consejo: Si sus respuestas del **comando show** son lentas, el motivo más probable es que el router realiza actualmente una búsqueda de dominio IP para las direcciones IP en el **comando show**. Puede inhabilitar la búsqueda de dominio IP. Puede utilizar el **comando no ip domain-lookup**, en el modo de configuración global del router, para inhabilitar la búsqueda de dominio IP. Esto detiene la búsqueda de dominio IP y aumenta la velocidad del **resultado del comando show**.

[show ip igmp groups](#)

Este comando muestra qué grupos multicast se conectan directamente al router, y cuáles se reconocen a través del Internet Group Management Protocol (IGMP). Puede utilizar este comando para verificar que un origen o un receptor se ha unido realmente al grupo de destino en la interfaz del router. La columna "Último Relator" muestra solamente un host IGMP, que indica que ha enviado una Incorporación de IGMP no solicitada o un Informe IGMP en respuesta a una Consulta IGMP del router PIM para ese grupo determinado. Debe ver solamente un "Último Relator" por el Grupo de Dirección.

```
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](#)

Utilice este comando para visualizar la información relacionada con multicast sobre una interfaz, y para verificar que el IGMP esté habilitado, la versión correcta se esté ejecutando, y los temporizadores, el valor de umbral del Tiempo de Funcionamiento (TTL), y el router del Solicitante de IGMP se hayan configurado correctamente. No es necesario configurar el IGMP en una interfaz. Se habilita de forma predeterminada cuando configura **ip pim dense-mode|modo disperso|sparse-dense-mode** .

```
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](#)

Utilice este comando para enumerar los vecinos de multidifusión independiente con protocolo (PIM) detectados por el software Cisco IOS®.

```
R1# show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface          Uptime/Expires    Ver    DR
Address
10.10.10.1        Ethernet0/0        02:19:41/00:01:38 v2     1 / DR B S
```

Los detalles de cada campo se explican aquí:

- **Dirección del Vecino:** especifica la dirección IP de un vecino PIM
- **Interfaz:** una interfaz donde fue detectado un vecino PIM
- **Tiempo activo:** el tiempo activo total del vecino
- **Vencimiento:** el tiempo transcurrido antes de que finalice el tiempo de espera de un vecino y hasta que se reciba el hello de PIM siguiente
- **Ver:** la versión de PIM en la interfaz del vecino
- **DR Prio:** los posibles valores van del 0 al 4294967294 o "N" Es una nueva columna que sigue la prioridad de una interfaz de PIM para la elección DR. La función configurar un DR basado en la prioridad más alta en comparación con la dirección IP más alta se introdujo en Cisco IOS Software Releases 12.1(2)T y 12.2 y las imágenes de Cisco IOS con BiDir-PIM. Puede utilizar el comando `ip pim dr-priority <0-4294967294>` interface para configurar la prioridad de DR. La prioridad predeterminada de DR se establece en 1. Para la interoperabilidad, si un vecino PIM ejecuta una versión anterior de Cisco IOS que no soporta la función de prioridad DR, la columna "DR" se muestra como "N". Si el vecino es el único router que muestra "N" para la interfaz, se convierte en el DR independientemente de qué router tiene realmente la dirección IP más alta. Si hay varios vecinos PIM que incluyen "N" en la columna, tiene prioridad la dirección IP más alta entre ellos.
- **Modo:** información sobre el DR y otras capacidades PIM. Esta columna enumera el DR además de cualquier capacidad soportada por el vecino PIM: **DR** - El vecino del PIM es router designado **B:** compatible con PIM bidireccional (BiDir-PIM) **S:** compatible con el estado de actualización (se aplica solamente para el modo denso)

Al resolver problemas, utilice este comando para verificar que todos los vecinos sean ascendentes y que utilicen el modo, la versión y el temporizador de vencimiento adecuados. También puede verificar la configuración del router o utilizar el [comando show ip pim interface para](#) verificar el modo (modo disperso o modo denso PIM). Use el [comando debug ip pim](#) para observar el intercambio del mensaje pim-query.

[show ip pim interface](#)

Utilice este comando para mostrar información sobre las interfaces configuradas para PIM. Además, puede utilizar este comando para verificar si se configuró el modo PIM correcto (denso o disperso) en la interfaz y para verificar si el recuento de vecinos y el router designado (DR) son correctos (que es fundamental para el modo disperso de PIM). Los segmentos de acceso múltiple (tales como Ethernet, Token Ring, FDDI) eligen un DR basado en la dirección IP más alta. Los links punto a punto no muestran la información DR.


```
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](#)

Utilice este comando para visualizar el contenido resumido de la tabla ruteo IP multicast. También puede utilizarlo para verificar el grupo multicast activo y qué remitentes multicast están activos al observar los temporizadores y los indicadores.

```
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
(133.33.33.32, 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](#)

Utilice este comando para visualizar el contenido total de la tabla ruteo IP multicast. Para resolver problemas, utilice este comando para verificar lo siguiente:

- Las entradas de estado (S,G) y (*,G) desde los indicadores.
- Si la interfaz entrante es correcta. Si no lo es, verifique la tabla ruteo unicast.
- Si la interfaz saliente es correcta. Si se eliminó de forma incorrecta, verifique el estado en el router descendente.

```
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

(133.33.33.32, 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](#)

Utilice este comando para visualizar el origen y los grupos del tráfico activo por encima del umbral. Al resolver problemas, utilícelo para verificar los grupos de origen activos, la velocidad del tráfico para cada par de grupo de origen (S, G) (debe haber conmutado al Árbol de Trayectoria más Corta [SPT]), y para verificar si se está recibiendo el tráfico multicast del grupo de destino. Si el tráfico no se está recibiendo, busque el tráfico activo desde el origen hacia el receptor.

```
R1# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.255.0.1, (?)
  Source: 133.33.33.32 (?)
  Rate: 10 pps/115 kbps(1sec), 235 kbps(last 23 secs), 87 kbps(life avg)
```

[show ip rpf](#)

Utilice este comando para visualizar cómo el ruteo IP multicast realiza el Reenvío de Trayectoria Inversa (RPF). Al resolver problemas, utilícelo para verificar que la información RPF sea correcta. Si no lo es, verifique la tabla de ruteo unicast para la dirección de origen. También utilice los comandos **ping** y **trace** en la dirección de origen para verificar que el ruteo unicast funcione. Posiblemente necesite utilizar rutas del Distance Vector Multicast Routing Protocol (DVMRP) o mroutes estáticas para reparar cualquier inconsistencia unicast-multicast.

```
R1# show ip rpf 133.33.33.32
RPF information for ? (133.33.33.32)
  RPF interface: Ethernet0
  RPF neighbor: ? (192.168.10.2)
  RPF route/mask: 133.33.0.0/16
  RPF type: unicast (eigrp 1)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

[show ip route](#)

Este comando puede verificar la memoria caché de switching multicast rápido IP y ejecutar un debug de los bugs de switching rápido.

```
R1# show ip mcache
IP Multicast Fast-Switching Cache
(133.33.33.32/32, 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](#)

Utilice este comando para verificar que el tráfico multicast se haya recibido y para comprobar sus velocidades y pérdidas de flujo. Si no recibe tráfico, trabaje desde el origen hacia el receptor hasta que encuentre dónde se detiene el tráfico. También puede utilizar este comando para verificar que se está reenviando el tráfico. Si no está sucediendo lo anterior, utilice el [comando show ip mroute](#) para buscar fallas de “lista de interfaz de Salida Nula” y de RPF.

```
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: 133.33.33.32/32, 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](#)

Utilice este comando para verificar la tabla de ruteo unicast y para reparar las fallas RPF en la tabla mroute.

```
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    133.33.0.0/16 [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](#)

Utilice este comando para verificar la asignación RP en función del rango de grupos de multicast y para verificar que el origen del aprendizaje RP (o auto-RP) y el mapeo sean correctos. Si encuentra un error, verifique la configuración del router local o la configuración de RP automática.

```
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 (?)
```

[comandos debug](#)

Esta sección fue creada para mostrarle cómo ciertos **resultados del comando debug** deberían verse en una red en funcionamiento. Al resolver problemas, puede distinguir entre el **resultado de debug** "correcto" y el que indica un problema en su red. Para obtener información más completa sobre estos **comandos debug**, consulte [Referencia del Comando Debug de Cisco IOS](#).

[debug ip igmp](#)

Utilice el **comando debug ip igmp** para visualizar los paquetes IGMP recibidos y transmitidos, y los eventos relacionados del host IGMP. **La opción no de este comando inhabilita el resultado de debug.**

Este resultado lo ayuda a detectar si el IGMP procesa la función. Generalmente, si el IGMP no funciona, el proceso del router nunca detecta otro host en la red que se configure para recibir los paquetes multicast. En el modo denso de PIM, esto significa que los paquetes se entregan de forma intermitente (algunos cada tres minutos). En el modo disperso de PIM, nunca se entregan.

```
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
```

El resultado anterior muestra que el router envía una consulta de la versión de IGMP 2 fuera de la interfaz Ethernet 1 en la dirección multicast 224.0.0.1 (todos los sistemas de multicast en esta subred). La interfaz Ethernet 1 en sí misma es un miembro del grupo 224.0.1.40 (puede utilizar el [comando show ip igmp interface](#) para determinar esto), que establece un tiempo de retraso del informe de 9,4 segundos (determinados aleatoriamente). Como no recibe ningún informe de otro sistema para el grupo de multicast 224.0.1.40 en los 9,4 segundos siguientes, envía un informe de versión 2 de su membresía, que es recibida por el router mismo en Ethernet1. También recibe la versión de informe IGMP 1 del host 192.168.9.1, que está conectado directamente con las interfaces Ethernet 1 para el grupo 239.255.0.1.

Este **resultado de debug** es útil cuando verifica si la interfaz del router envía las consultas y para determinar el intervalo de consultas (en el caso anterior, 60 segundos). También puede utilizar el comando para determinar la versión del IGMP utilizada por los clientes.

[debug ip mpacket](#)

Utilice el **comando debug ip mpacket** para visualizar todos los paquetes de multicast recibidos y transmitidos del IP. **La opción no de este comando inhabilita el resultado de debug.**

```
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=133.33.33.32 (Ethernet0) d=239.255.0.1 (Ethernet1) len 906, mforward
```

Este comando decodifica el paquete multicast y muestra si el paquete fue reenviado (mforward) o descartado. Es útil cuando ejecuta un debug de los problemas con el flujo de paquetes en la red para observar el valor TTL y la razón del descarte de un paquete.

Precaución: Tenga precaución al activar el resultado de debug a nivel del paquete, especialmente

cuando el router atiende una gran carga de paquetes multicast.

[debug ip mrouting](#)

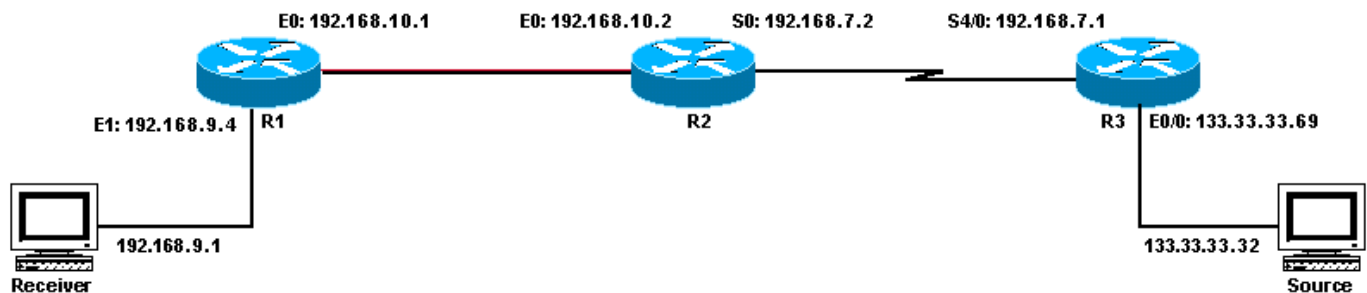
Este comando es útil para el mantenimiento de la tabla de ruteo. Utilícelo para verificar si la mroute (S, G) está instalada en la tabla mrouting, o si no lo está, cuál es el motivo. La información fundamental en este resultado es la interfaz RPF. Si hay una falla en la revisión de RPF, la mroute (S, G) no puede instalarse en la tabla mrouting.

```
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 (133.33.33.32/32, 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](#)

Utilice el **comando debug ip pim** para visualizar los paquetes PIM recibidos y transmitidos, y los eventos relacionados del PIM. La **opción no** de este comando inhabilita el resultado de debug.

Esta sección utiliza un ejemplo para ayudarlo a comprender el resultado de debug del modo disperso de PIM y para mostrarle un resultado de debug típico.



El siguientes es el resultado del **debug ip pim** en R1:

```
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
```

Cada línea del resultado significa lo siguiente: R1 y R2 establecen vecinos de PIM al intercambiar los mensajes Hello. Estos mensajes periódicos Hello, intercambiados en los segundos del “Intervalo de Consultas-Intervalo” entre R1 (E0) y R2 (E0), realizan un seguimiento de los vecinos de PIM.

El R1 envía un mensaje de Unión/Separación a la dirección RP 192.168.7.2. El RP (R2) contesta con un mensaje Accesible RP Recibido nuevamente al R1 para el grupo 239.255.0.1. Esto, a su

vez, actualiza el temporizador de vencimiento RP en R1. El temporizador de vencimiento establece un punto de control para asegurarse de que el RP todavía existe; de lo contrario, debe detectarse un nuevo RP. Utilice el **comando show ip pim rp** para observar el tiempo de vencimiento RP.

Ahora, observe el **resultado de debug** entre R1 y R2 cuando un receptor multicast para el grupo 239.255.0.1 se une a R1.

Primero, observe el resultado en R1:

```
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)
```

Ahora, observe el resultado en R2:

```
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
```

En la línea 1 anterior, el receptor multicast para el grupo 239.255.0.1 se une al R1. Esto instala una entrada (*, 239.255.0.1) en la tabla mroute. Entonces, en la línea 2, el receptor multicast envía una Unión IGMP a R2 (RP) para unirse al árbol compartido.

Cuando la unión IGMP ingresa en R2, el R2 instala una mroute (*, 239.255.0.1), tal y como se muestra en las líneas 12 a 15 del resultado R2.

Una vez que R2 se instala (*, 239.255.0.1) en su tabla mrouting, agrega la interfaz de la cual recibió el mensaje de Unión/Separación a su lista de interfaces de salida en el estado de reenvío. Luego envía un mensaje de alcance de RP nuevamente a la interfaz en la cual recibió el mensaje de Unión/Separación. Esta transacción se muestra en las líneas 15 a 21 del resultado R2.

R1 recibe el mensaje alcanzable a RP para el grupo 239.255.0.1 y actualiza su temporizador de vencimiento para el RP. Este intercambio se repite cada un minuto de forma predeterminada y actualiza su estado de reenvío multicast tal y como se muestra en las líneas 7 y 8 del resultado

R1.

En las líneas siguientes, se observa el **resultado de debug** entre R2 (RP) y R3. El origen (conectado directamente con R3) comenzó a enviar los paquetes para el grupo 239.255.0.1.

Primero, observe el resultado en R3:

```
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 133.33.33.32, group 239.255.0.1
8 PIM: Send Register to 192.168.7.2 for 133.33.33.32, group 239.255.0.1
9 PIM: Received Join/Prune on Serial4/0 from 192.168.7.2
10 PIM: Join-list: (133.33.33.32/32, 239.255.0.1), S-bit set
11 PIM: Add Serial4/0/192.168.7.2 to (133.33.33.32/32, 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 (133.33.33.32/32, 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 (133.33.33.32/32, 239.255.0.1)
```

El siguiente es el resultado de R2, el RP:

```
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 133.33.33.32, 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 (133.33.33.32/32, 239.255.0.1), S-bit
22 PIM: Send Join on Serial0 to 192.168.7.1 for (133.33.33.32/32, 239.255.0.1), S-bit
23 PIM: Send Register-Stop to 192.168.7.1 for 133.33.33.32, group 239.255.0.1
24 PIM: Received Join/Prune on Serial0 from 192.168.7.1, to us
25 PIM: Prune-list: (133.33.33.32/32, 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 (133.33.33.32/32, 239.255.0.1)
30 PIM: Join-list: (133.33.33.32/32, 239.255.0.1), S-bit set
31 PIM: Add Ethernet0/192.168.10.1 to (133.33.33.32/32, 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: 133.33.33.32/32
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 (133.33.33.32/32, 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 línea 1 anterior muestra que R3, que está conectado directamente a través de Ethernet0/0 con el origen, recibe el tráfico multicast para el grupo 239.255.0.1. Crea una entrada (*, 239.255.0.1) y envía un mensaje de Unión al RP.

Las líneas 16 y 17 muestran que el R2, que es el RP, también recibe el mensaje de Unión/Separación y envía la información de alcance RP nuevamente al R3.

En las líneas 5 y 6, el R3 actualiza su temporizador de vencimiento RP después de recibir la información alcanzable a RP. Las líneas 7 y 8 anteriores muestran que R3 utiliza su entrada (*, G) para enviar los datos a RP encapsulados en un Paquete de registro con el origen que inicia la transmisión al grupo 239.255.0.1.

Las líneas 18 a 20 muestran que R2 recibió el Paquete de registro, desencapsulado y lo reenvió al árbol con una entrada preexistente (*, 239.255.0.1) en la tabla de ruta.

Las líneas 21 y 29 muestran que R2 envía un mensaje de unión hacia R3 e instala una entrada (S,G) (133.33.33.32, 239.255.0.1) en la tabla mroute.

Las líneas 9 a 11 muestran que R3 recibe el mensaje de Unión de R2, instala una entrada (S, G) (133.33.33.32,239.255.0.1) en la tabla mroute y actualiza la interfaz conectada con el RP en el modo de reenvío, que crea un árbol multicast SPT (S, G) hacia el origen.

En la línea 23, R2 comienza a recibir el tráfico (S,G) SPT y envía un mensaje de Detención de Registro (y un mensaje de Unión) hacia el origen.

Las líneas 12 a 15 muestran que el R3 recibe el mensaje de Detención de Registro, borra el indicador del registro y detiene el tráfico de encapsulación (S, G).

Los mensajes de unión/separación periódica son intercambiados entre RP y R3 para mantener el árbol de multifunción.

[Información Relacionada](#)

- [Guía de resolución de problemas de multidifusión IP](#)
- [Guía rápida de configuración para Multicast \(Multidifusión\)](#)
- [Página de soporte de multidifusión IP](#)
- [Página de Soporte de IP Routed Protocols](#)
- [Página de Soporte de IP Routing](#)
- [IP3R: Referencia del Comando ip de Cisco IOS, Volumen 3 de 3: Multicast, Versión 12.2](#)
- [Soporte Técnico - Cisco Systems](#)