Guía rápida de configuración para Multicast (Multidifusión)

Contenido

Introducción

La multidifusión IP es una tecnología de conservación de ancho de banda que reduce el tráfico porque entrega simultáneamente una sola secuencia de información a los millares de destinatarios corporativos y a los hogares. Entre las aplicaciones que utilizan multicast se incluyen aplicaciones de videoconferencia, comunicaciones corporativas, aprendizaje a distancia o distribución de software, cotizaciones y noticias. Este documento discute los aspectos fundamentales para configurar el multicast para los diversos escenarios de conexión entre redes.

prerrequisitos

Requisitos

Cisco recomienda que los lectores de este documento tengan conocimientos básicos sobre Multicast con Internet Protocol (IP).

Nota: Consulte la documentación sobre Multicast con Internet Protocol para obtener más información.

Componentes Utilizados

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

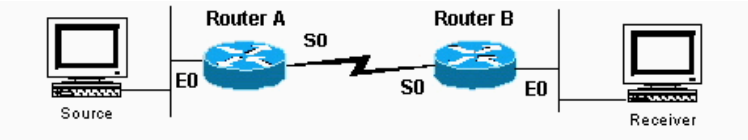
Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Modo denso

Cisco recomienda que utilice el modo disperso de Multicast con Protocolo Independiente (PIM), en particular RP Automático, en lo posible y especialmente para las nuevas implementaciones. **No obstante, si desea el modo denso, configure el comando global ip multicast-routing y el comando de interfaz ip pim sparse-dense-mode en cada interfaz que necesita procesar tráfico Multicast.** El requisito común para todas las configuraciones contempladas en este documento es configurar la multidifusión en forma global y configurar PIM en las interfaces. **En cuanto a la versión 11.1 del software del IOS® de Cisco, puede configurar los comandos de interfaz ip pim dense-mode e ip pim sparse-mode de manera simultánea mediante el comando ip pim sparse-dense-mode.** En este modo, la interfaz se trata como en modo denso si el grupo está en modo denso. Si el grupo se encuentra en modo disperso (por ejemplo, si un RP es conocido), la interfaz es tratada como modo disperso.

Nota: Origen" en los ejemplos a lo largo de este documento representa el origen del tráfico de multidifusión y "Receptor" representa el receptor del tráfico de multidifusión.

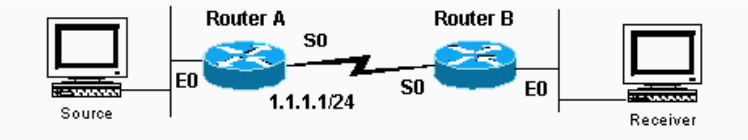


Configuración del router A
ip multicast-routing interface ethernet0 ip address <address> <mask> ip pim sparse-dense-mode interface serial0 ip address <address> <mask> ip pim sparse-dense-mode

Configuración del Router B
ip multicast-routing interface serial0 ip address <address> <mask> ip pim sparse-dense-mode interface ethernet0 ip address <address> <mask> ip pim sparse-dense-mode

Modo escaso con un RP

En este ejemplo, el router A es el RP que es típicamente el router más cercano al origen. La configuración estática del RP requiere que todos los routers en el dominio PIM tengan configurados los mismos **comandos ip pim rp-address**. Puede configurar varios RP, pero sólo puede existir un RP por grupo específico.

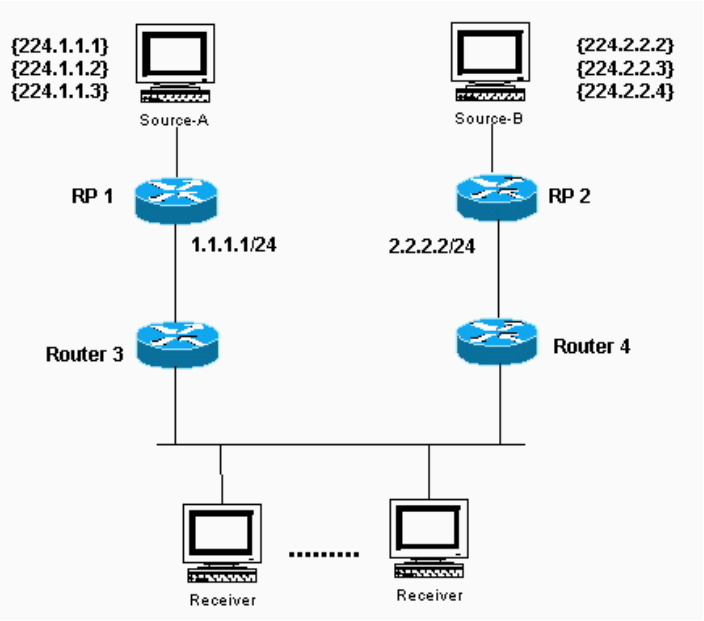


Configuración del router A
ip multicast-routing ip pim rp-address 1.1.1.1   interface ethernet0 ip address <address> <mask> ip pim sparse-dense-mode interface serial0 ip address 1.1.1.1 255.255.255.0 ip pim sparse-dense-mode

Configuración del Router B
ip multicast-routing ip pim rp-address 1.1.1.1   interface serial0 ip address <address> <mask> ip pim sparse-dense-mode interface ethernet0 ip address <address> <mask> ip pim sparse-dense-mode

Modo Disperso con Múltiples RP

En este ejemplo, el Origen A envía a 224.1.1.1, 224.1.1.2 y 224.1.1.3. El Origen B envía a 224.2.2.2, 224.2.2.3 y 224.2.2.4. Sólo un router, RP1 o RP2, puede ser el RP para todos los grupos. Sin embargo, si desea que diversos RP administren diversos grupos, necesita configurar todos los routers para incluir los grupos que reciben servicios de los RPs. Este tipo de configuración RP estática requiere que todos los routers en el dominio PIM tengan configurados los mismos **comandos ip pim rp-addressaddress acl.** También puede utilizar RP Automático para lograr la misma instalación, que es más fácil de configurar.



Configuración RP1

```
ip multicast-routing

ip pim RP-address 1.1.1.1 2
ip pim RP-address 2.2.2.2 3

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

Configuración RP 2

```
ip multicast-routing

ip pim RP-address 1.1.1.1 2
ip pim RP-address 2.2.2.2  3

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

Configuración para los routers 3 y 4

```
ip multicast-routing
ip pim RP-address 1.1.1.1  2
ip pim RP-address 2.2.2.2  3


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

RP automático en un RP

El RP Automático requiere que configure los RPs para que anuncien su disponibilidad como RPs y agentes de mapping. Los RPs utilizan

224.0.1.39 para enviar sus anuncios. El agente de correlación RP escucha los paquetes anunciados de los RP, luego envía correlaciones de RP a grupo en un mensaje de detección que se envía a 224.0.1.40. Estos mensajes de detección son utilizados por los routers restantes para su mapa RP a grupo. Puede utilizar un RP que también sirva como agente de mapping, o puede configurar los RPs múltiples y los agentes de mapping múltiples por cuestiones de redundancia.

Observe que cuando elige una interfaz de la cual originar avisos RP, Cisco recomienda que utilice una interfaz como loopback en vez de una interfaz física. También, es posible utilizar las Interfaces VLAN Conmutadas (SVI). Si se usa una interfaz VLAN para anunciar la dirección RP, la opción **interfaz-tipo** en el comando **ip pim [vrf vrf-name] send-rp-announce {interface-type interface-number | ip-address} scope ttl-value** debe contener la interfaz VLAN y el número de VLAN. **Por ejemplo, el comando es similar a ip pim send-rp-announce Vlan500 scope 100.** Si elige una interfaz física, confía que esa interfaz esté siempre activa. Éste no siempre es el caso, y el router deja de anunciarse como RP una vez que la interfaz física deja de funcionar. Con una interfaz loopback, siempre está activa y nunca deja de funcionar, lo que se asegura que el RP continúa anunciándose a través de cualquier interfaz disponible como RP. Éste es el caso incluso si una o más de sus interfaces físicas fallan. La interfaz loopback debe estar habilitada para PIM y ser anunciada por un Interior Gateway Protocol (IGP), o debe ser accesible con el ruteo estático.

Configuración del router A

```
ip multicast-routing

ip pim send-rp-announce loopback0 scope 16


ip pim send-rp-discovery

scope 16

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

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

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

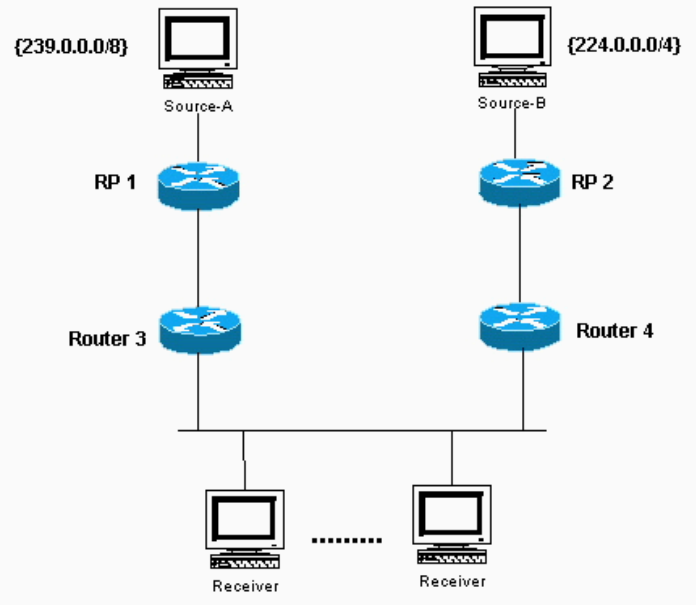
Configuración del Router B

```
ip multicast-routing


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

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

Auto-RP con múltiples RP

Las listas de acceso en este ejemplo permiten que los RP sean RP sólo para los grupos que usted quiera. Si no se configura ninguna lista de acceso, los RP estarán disponibles como un RP para todos los grupos. Si dos RPs anuncian su disponibilidad como RPs para los mismos grupos, el agente de mapping resuelve estos conflictos con la regla "la dirección IP más alta gana".

Cuando dos RPs se anuncian para ese grupo, puede configurar cada router con una dirección loopback para determinar qué router es el RP para un grupo determinado. Coloque la dirección IP más alta en el RP preferido, después utilice la interfaz loopback como el origen de los paquetes de anuncio; **por ejemplo, ip pim send-RP-announce loopback0.** Cuando se utilizan agentes múltiples de mapeo, cada uno de ellos anuncia al mismo grupo los mapeos RP del grupo de detección 224.0.1.40.



Configuración RP1

```
ip multicast-routing

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

ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery scope 16


access-list 1 permit 239.0.0.0 0.255.255.255
```

Configuración RP 2

```
ip multicast-routing

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

ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery scope 16


access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 15.255.255.255
```

Consulte Guía para Configurar un RP Automático y Diagnósticos para obtener más información sobre el RP Automático.

DVMRP

Su Proveedor de servicios de Internet (ISP) podría sugerir que cree un túnel de Distance Vector Multicast Routing Protocol (DVMRP) al ISP para acceder al backbone de multicast en Internet (mbone). Los comandos mínimos para configurar un túnel DVMRP se muestran aquí:

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

Típicamente, el ISP que usted tiene incluye un túnel a la máquina UNIX que ejecuta “mrouted” (DVMRP UNIX). Si el ISP que tiene incluye un túnel a otro dispositivo de Cisco, utilice el modo predeterminado del túnel GRE.

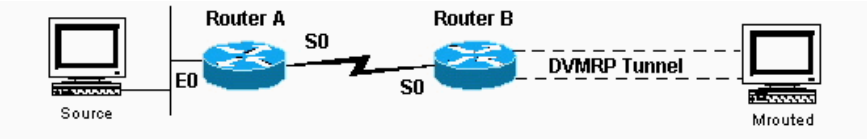
Si desea generar paquetes multicast para otros en el mbone para ver en lugar de recibir los paquetes multicast, debe anunciar las subredes de origen Si su dirección de host de origen multicast es 131.108.1.1, debe anunciar la existencia de esa subred al mbone. Las redes conectadas directamente están anunciadas con la métrica 1 de manera predeterminada. Si su origen no está conectado directamente con el router con el túnel DVMRP, configúrelo con la interfaz tunnel0:

```
ip dvmrp metric 1 list 3
```

```
access-list 3 permit 131.108.1.0 0.0.0.255
```

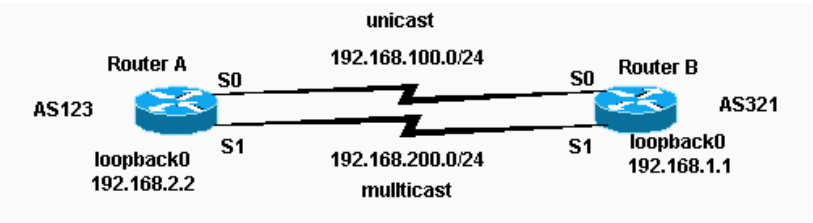
Nota: Debe incluir una lista de acceso con este comando para evitar el anuncio de la tabla de ruteo Unicast completa al mbone.

Si su configuración es similar a la que se muestra aquí, y desea propagar las rutas DVMRP con el dominio, configure el **comando ip dvmrp unicast-routing** en las interfaces serial0 de los routers A y B. Esta acción permite el reenvío de las rutas DVMRP a los vecinos de PIM que tienen una tabla de ruteo DVMRP utilizada para el reenvío de trayectoria inversa (RPF). Las rutas aprendidas DVMRP tienen precedencia RPF sobre todos los otros protocolos, a excepción de las rutas conectadas directamente.



MBGP

El Multiprotocol Border Gateway Protocol (MBGP) es un método básico para transportar dos conjuntos de rutas: un conjunto para el ruteo unicast y un conjunto para el ruteo multicast. MBGP proporciona el control necesario para decidir cuándo se permite que fluyan los paquetes de multidifusión. El PIM utiliza las rutas asociadas al ruteo multicast para construir los árboles de distribución de datos. MBGP proporciona el trayecto RPF, no la creación del estado de multidifusión. El PIM todavía se necesita para remitir los paquetes de multicast.



Configuración del router A

```
ip multicast-routing


interface loopback0
ip pim sparse-dense-mode
ip address 192.168.2.2 255.255.255.0


interface serial0
ip address 192.168.100.1 255.255.255.0


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


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


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


route-map setNH permit 20
```

Configuración del Router B

```
ip multicast-routing


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


interface serial0
ip address 192.168.100.2 255.255.255.0
```

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


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


route-map setNH permit 10
match nlri multicast
set ip next-hop 192.168.200.2


route-map set NH permit 20
```

Si sus topologías unicast y multicast son coherentes (por ejemplo, están pasando por el mismo link), la diferencia principal en la configuración reside en el **comando nlri unicast multicast**. Un ejemplo se muestra aquí:

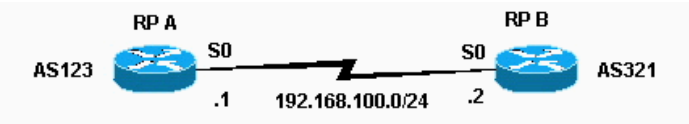
```
network 192.168.100.0 nlri unicast multicast
```

Las topologías coherentes con el MBGP tienen una ventaja, aunque el tráfico atraviesa las mismas trayectorias, se pueden aplicar diversas políticas al unicast BGP versus el multicast BGP.

Consulte ¿Qué es MBGP? para obtener más información sobre el MBGP.

MSDP

Protocolo de detección del origen de multidifusión (MSDP) conecta los dominios PIM-SM múltiples. Cada dominio PIM-SM utiliza su RP independiente y no depende de los RPs en otros dominios. El MSDP hace posible que los dominios detecten fuentes de multidifusión desde otros dominios. Si también forma par BGP con el par MSDP, debe utilizar la misma dirección IP para el MSDP que para el BGP. Cuando MSDP efectúa controles de pares RPF, MSDP espera que la dirección del par MSDP sea la misma que la que proporciona BGP/MBGP cuando realiza una búsqueda de tabla de ruteo en el RP, en el mensaje SA. Sin embargo, no es necesario que ejecute BGP/MBGP con el par MSDP si existe un trayecto BGP/MBGP entre los pares MSDP. Si no existe ruta BGP/MBGP y más de una entidad par MSDP, debe utilizar el **comando ip msdp default-peer**. El siguiente ejemplo muestra que el RP A es el RP para su dominio y el RP B es el RP para su dominio.



Configuración del router A

```
ip multicast-routing


ip pim send-RP-announce loopback0 scope 16
ip pim send-RP-discovery scope 16


ip msdp peer 192.168.100.2
ip msdp sa-request 192.168.100.2

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

interface serial0
ip address 192.168.100.1 255.255.255.0
ip pim sparse-dense-mode
```

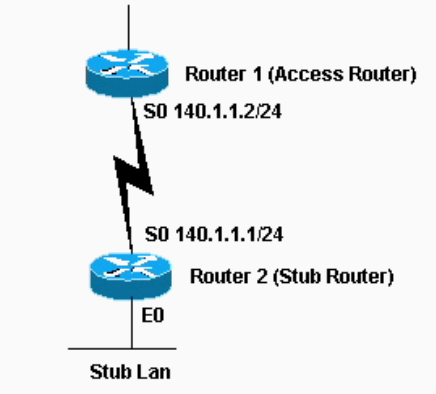
Configuración del Router B

```
ip multicast-routing

ip pim send-RP-announce loopback0 scope 16
ip pim send-RP-discovery scope 16
```

```
ip msdp peer 192.168.100.1
ip msdp sa-request 192.168.100.1

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

interface serial0
ip address 192.168.100.2 255.255.255.0
ip pim sparse-dense-mode
```

Stub Multicast Routing

El ruteo de multidifusión Stub le permite configurar routers Stub o remotos como agentes por poder IGMP. Bastante que participan completamente en el PIM, estos mensajes IGMP delanteros de los routeres Stub de los host al router de multidifusión en sentido ascendente.



Configuración del Router 1

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


access-list 1 deny 140.1.1.1
```

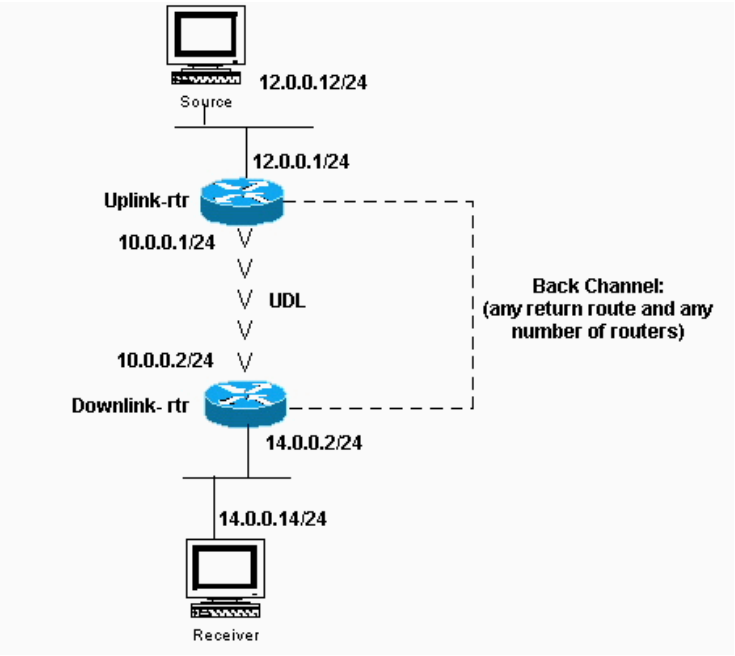
El comando ip pim neighbor-filter es necesario para que el Router 1 no reconozca al Router 2 como un PIM vecino. Si configura el Router 1 en modo disperso, el filtro vecino no es necesario. El Router 2 no debe ejecutarse en modo disperso. En el modo denso, los orígenes de multicast de stub pueden inundar los routers de backbone.

Configuración del router 2

```
ip multicast-routing
int e0
ip pim sparse-dense-mode
ip igmp helper-address 140.1.1.2


int s0
ip pim sparse-dense-mode
```

IGMP UDLR para links satelitales

El Ruteo de Link Unidireccional (UDLR) proporciona un método para los reenvíos de paquetes de multicast sobre un link satelital unidireccional a las redes stub que tienen un canal posterior. Es similar al ruteo de multidifusión stub. Sin esta función, el router de link ascendente no puede aprender dinámicamente qué grupo de direcciones IP multidifusión debe reenviar por encima del link unidireccional, debido a que el router de link descendente no puede enviar nada hacia atrás.



Configuración de Uplink-rtr

```
ip multicast-routing


interface Ethernet0
description Typical IP multicast enabled interface
ip address 12.0.0.1 255.0.0.0
ip pim sparse-dense-mode


interface Ethernet1
description Back channel which has connectivity to downlink-rtr
ip address 11.0.0.1 255.0.0.0
ip pim sparse-dense-mode


interface Serial0
description Unidirectional to downlink-rtr
ip address 10.0.0.1 255.0.0.0
ip pim sparse-dense-mode
ip igmp unidirectional-link
no keepalive
```

Configuración de Router de Link Descendente

```
ip multicast-routing


interface Ethernet0
description Typical IP multicast enabled interface
ip address 14.0.0.2 255.0.0.0
ip pim sparse-dense-mode
ip igmp helper-address udl serial0


interface Ethernet1
description Back channel which has connectivity to downlink-rtr
ip address 13.0.0.2 255.0.0.0
ip pim sparse-dense-mode


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

PIMv2 BSR

Si todos los routers de la red ejecutan PIMv2, puede configurar un BSR en lugar de Auto-RP. El BSR y RP Automático son muy similares. Una configuración BSR requiere que configure los candidatos BSR (similares al Anuncio RP en RP Automático) y los BSRs (similares al RP

Automático a los Agentes de Mapping). Para configurar un BSR, siga los siguientes pasos:

1. En los BSR candidatos configure:

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

   Donde la ***interfaz*** contiene la dirección IP del candidato BSR. Se recomienda (aunque no es obligatorio) que la duración de la máscara a utilizar en función del troceo sea idéntica en todos los BSR candidatos. Un BSR candidato con el valor ***pref*** más grande se elige como el BSR para este dominio.

   Se muestra un ejemplo del comando usage:

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

   El PIMv2 BSR recoge la información del RP candidato y difunde la información del conjunto de RP asociada a cada prefijo del grupo. Para evitar un único punto de falla, puede configurar más de un router en un dominio como candidato BSR.

   Un BSR se elige entre los BSRs candidatos automáticamente, sobre la base de los valores de preferencia configurados. Para servir como BSRs candidatos, los routers deben estar conectados y estar en el backbone de la red, y no en el área de marcación de la red.

2. Configure los routers RP candidatos. Este ejemplo muestra un candidato RP, en la interfaz ethernet0, para el rango completo de direcciones de alcance administrativo:

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

CGMP

Para configurar el Group Management Protocol (CGMP), hágalo en la interfaz de router orientada hacia el switch:

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

Luego, configure esto en el switch:

```
set cgmp enable
```

IGMP Snooping

La indagación de Internet Group Management Protocol (IGMP) está disponible con la versión 4.1 de Catalyst 5000. La indagación IGMP requiere una tarjeta Supervisor III. No se necesita otra configuración además de PIM para configurar la indagación IGMP en el router. Todavía es necesario tener un router con indagación IGMP para proporcionar la interrogación IGMP.

El ejemplo proporcionado aquí muestra cómo habilitar la indagación IGMP en el switch:

```
Console> (enable) set igmp enable
IGMP Snooping is enabled.
CGMP is disabled.
```

Si trata de habilitar IGMP, pero CGMP ya está habilitado, verá lo siguiente:

```
Console> (enable) set igmp enable
Disable CGMP to enable IGMP Snooping feature.
```

PGM

PGM (Multidifusión general pragmática) es un protocolo de transporte multidifusión confiable para aplicaciones que requieran una entrega de datos multidifusión ordenada y libre duplicación desde varias fuentes a varios receptores. PGM garantiza que el receptor del grupo reciba todos los paquetes de las transmisiones y retransmisiones o pueda detectar la pérdida irrecuperable de paquetes de datos.

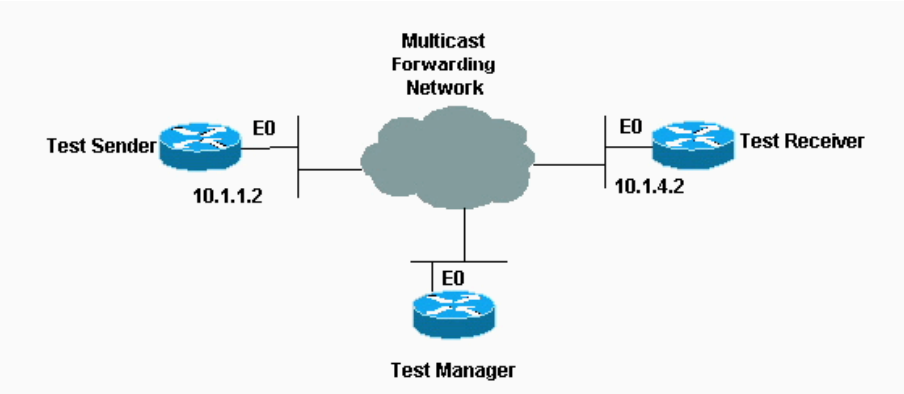
No existen comandos globales de PGM. El PGM se configura por interfaz con el **comando ip pgm**. Debe habilitar el ruteo Multicast en el router con la PIM en la interfaz.

MRM

El Monitor de Ruteo Multicast (MRM) facilita la detección automatizada de fallas en una infraestructura de ruteo multicast amplia. MRM está diseñado para dar avisos de alerta a un administrador de red sobre problemas de ruteo de multidifusión prácticamente en tiempo real.

MRM tiene dos componentes: Controlador MRM y administrador MRM. El Controlador MRM es un emisor o un receptor.

El MRM está disponible en el Cisco IOS Software Release 12.0(5)T y posterior. Sólo los controladores y administradores MRM necesitan estar ejecutando la versión IOS de Cisco compatible con MRM.



Configuración de un emisor de prueba

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

Configuración de Receptor de Prueba

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

Configuración del administrador de pruebas

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


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

El resultado del **comando show ip mrm manager** en el Administrador de Pruebas se muestra aquí:

```
Test_Manager# show ip mrm manager
  Manager:test1/10.1.2.2 is not running
    Beacon interval/holdtime/ttl:60/86400/32
    Group:239.1.1.1, UDP port test-packet/status-report:16384/65535
    Test sender:
      10.1.1.2
    Test receiver:
      10.1.4.2
```

Comience la prueba con el comando que se muestra. El administrador de pruebas envía mensajes de control al remitente y al receptor de pruebas como está configurado en los parámetros de pruebas. El receptor de la prueba se une a al grupo y monitorea los paquetes de prueba enviados por el emisor de pruebas.

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

Para visualizar un informe de estado para el administrador de pruebas, ingrese este comando:

```
Test_Manager# show ip mrm status

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

El resultado muestra que el receptor envió dos informes de estado (una línea cada uno) en una fecha y hora determinadas. Cada informe contiene una pérdida del paquete durante la ventana de intervalo (valor predeterminado de un segundo). El valor "Ehsr" muestra el valor de número de secuencia siguiente estimado del emisor de la prueba. Si el receptor de la prueba ve los paquetes duplicados, muestra un número negativo en la columna "Paquetes perdidos/duplicados".

Para detener la prueba, ingrese este comando:

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

Mientras ejecuta la prueba, el emisor MRM comienza a enviar los paquetes RTP a la dirección de grupo configurada en el intervalo predeterminado de 200 ms. El receptor monitorea (espera) los mismos paquetes en el mismo intervalo predeterminado. Si el receptor detecta una pérdida de paquetes en el intervalo de ventana predeterminado de cinco segundos, envía un informe al administrador de MRM. Puede visualizar el informe de estado del receptor si ejecuta el **comando show ip mrm status** en el administrador.

Resolución de problemas

Algunos de los problemas más comunes que surgen al implementar el multicast de IP en una red se presentan cuando el router no envía el tráfico multicast debido a una falla de RPF o configuraciones TTL. Consulte Guía de Troubleshooting de Multicast IP para obtener explicación detallada sobre éstos y otros problemas comunes, síntomas, y resoluciones.

Información Relacionada

- **Notas Técnicas de Troubleshooting**

Fecha de Generación del PDF: 7 Septiembre 2014

http://www.cisco.com/cisco/web/support/LA/102/1024/1024234_48.html